IMPLEMENTASI MANAJEMEN RISIKO BERBASIS ISO 31000 PADA *WEBSITE* MENGGUNAKAN *FRAMEWORK* OWASP (*OPEN WEB APPLICATION SECURITY PROJECT*)

SKRIPSI

Disusun Oleh:

MOCHAMAD ADAM ALIANSYAH

H96218064

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN AMPEL

SURABAYA

2022

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini,

Nama : Mochamad Adam Aliansyah

NIM : H96218064

Program Studi : Sistem Informasi

Angkatan : 2018

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul **"IMPLEMENTASI MANAJEMEN RISIKO BERBASIS ISO 31000 PADA *WEBSITE* MENGGUNAKAN *FRAMEWORK* OWASP (*OPEN WEB APPLICATION SECURITY PROJECT*)"**, apabila suatu saat nanti terbukti saya melakukan tindakan plagiat maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 11 Agustus 2022

Yang menyatakan,

(Mochamad Adam Aliansyah)

NIM. H96218064

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh

NAMA	:	MOCHAMAD ADAM ALIANSYAH
NIM	:	H96218064
JUDUL	:	IMPLEMENTASI MANAJEMEN RISIKO BERBASIS ISO 31000 PADA WEBSITE MENGGUNAKAN FRAMEWORK OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 13 Juli 2022

Dosen Pembimbing 1	Dosen Pembimbing 2
(Indri Sudanawati Rozas, M.Kom)	(Noor Wahyudi, M.Kom)
NIP 198207212014032001	NIP 198403232014031002

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi Mochamad Adam Aliansyah ini telah dipertahankan di depan tim penguji skripsi di Surabaya, 15 Juli 2022

Mengesahkan

Dewan Penguji

Dosen Penguji 1

(Muhammad Andik Izzuddin, M.T)

NIP. 198403072014031001

Dosen Penguji 2

(Achmad Teguh Wibowo, M.T)

NIP. 198810262014031003

Dosen Penguji 3

(Indri Sudanawati Rozas, M.Kom)

NIP. 198207212014032001

Dosen Penguji 4

(Noor Wahyudi, M.Kom)

NIP. 198403232014031002

Mengetahui,

Dekan Fakultas Sains dan Teknologi

UIN Sunan Ampel Surabaya

(Dr. Hepul Hamdani, M. Pd)

NIP. 196507312000031002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama	:	MOCHAMAD ADAM ALIANSYAH
NIM	:	H96218064
Fakultas/Jurusan	:	SAINS DAN TEKNOLOGI / SISTEM INFORMASI
E-mail address	:	adamaliansyah2@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :

■ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (……)

yang berjudul :

IMPLEMENTASI MANAJEMEN RISIKO BERBASIS ISO 31000 PADA *WEBSITE* MENGGUNAKAN *FRAMEWORK* OWASP (*OPEN WEB APPLICATION SECURITY PROJECT*)

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 11 Agustus 2022
Penulis

(Mochamad Adam Aliansyah)

ABSTRAK

IMPLEMENTASI MANAJEMEN RISIKO BERBASIS ISO 31000 PADA *WEBSITE* MENGGUNAKAN *FRAMEWORK* OWASP (*OPEN WEB APPLICATION SECURITY PROJECT*)

Oleh:

Mochamad Adam Aliansyah

ISO 31000 merupakan salah satu framework pada manajemen risiko yang bertujuan untuk mengatasi risiko-risiko yang muncul pada suatu objek. Penelitian ini memiliki beberapa langkah berdasarkan pada ISO 31000 dan dengan penyesuaian dari studi kasus yaitu Lingkup Konteks Kriteria, Pengukuran Risiko (terdiri dari Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko) dan Perlakuan Risiko (terdiri dari Menyusun Strategi mitigasi, Uji Coba Desain Mitigasi dan Rekomendasi Mitigasi Risiko). Langkah tersebut diimplementasikan pada suatu objek yaitu Website OJS Rumah Jurnal Saintek Universitas Islam Negeri Sunan Ampel guna untuk mencari risiko-risiko kerentanan keamanan website lalu kemudian dilakukan mitigasi atau perbaikan agar risiko-risiko tersebut dapat teratasi. Dalam usaha mencari kerentanan risiko, digunakannya beberapa tools dari perusahaan OWASP (Open Web Application Security Project) yaitu OWASP ASVS (Application Security Verification Standard) versi 4.0.3 dan OWASP ZAP (Zed Attack Proxy). Hasil yang didapatkan yaitu terdapat 10 risiko kerentanan keamanan dari website tersebut dan setelah melewati langkah-langkah yang ada tersisa 5 risiko yang dilakukan mitigasi atau perbaikan, dari mitigasi yang telah dilakukan didapatkan bahwa 5 risiko tersebut telah terselesaikan dan berhasil diatasi.

Kata Kunci: ISO 31000, OWASP, Manajemen Risiko

ABSTRACT

IMPLEMENTATION OF RISK MANAGEMENT BASED ON ISO 31000 ON THE WEBSITE USING OWASP (OPEN WEB APPLICATION SECURITY PROJECT) FRAMEWORK

By:

Mochamad Adam Aliansyah

ISO 31000 is one of the frameworks on risk management that aims to overcome the risks that arise in an object. This study has several steps based on ISO 31000 and with adjustments from case studies, namely Scope Context Criteria, Risk Assessment (Risk Identification, Risk Analysis and Risk Evaluation) and Risk Treatment (Developing Mitigation Strategies, Mitigation Design Trials and Recommendations Risk Mitigation). This step is implemented on an object, namely the OJS Website of the Scientific Journal House of Sunan Ampel State Islamic University in order to find the risks of website security vulnerabilities and then mitigation or repair is carried out so that these risks can be overcome. In an effort to find risk vulnerabilities, several tools from OWASP (Open Web Application Security Project) companies are used, namely OWASP ASVS (Application Security Verification Standard) version 4.0.3 and OWASP ZAP (Zed Attack Proxy). The results obtained are that there are 10 security vulnerabilities risks from the website and after going through the existing steps, the remaining 5 risks are mitigated or repaired, from the mitigation that has been carried out it is found that these 5 risks have been resolved and successfully overcome.

Keywords: ISO 31000, OWASP, Risk Management

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Pada bab satu membahas tentang inti dari pembahasan penelitian ini, hal-hal yang menjadi latar belakang studi kasus pada penelitian ini, dan pembahasan-pembahasan lainnya yang menjadi dasar dilakukannya penelitian ini. Bab ini terdiri dari: latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian dan sistematika penulisan skripsi.

1.1 Latar Belakang

Manusia memiliki kehidupan dan harus menjalaninya dengan baik, terkadang terdapat banyak hal yang terjadi seiring berjalannya kehidupan, banyak ancaman dan risiko yang muncul. Menurut Harimurti, risiko seringkali menimbulkan suatu kerugian ataupun kerusakan, namun hal tersebut masih terbilang wajar, seringkali risiko muncul pada semua aspek kehidupan manusia, risiko bisa muncul saat kita melakukan banyak kegiatan; seperti kegiatan ekonomi, sosial, hukum, kegiatan pendidikan dan kegiatan lainnya (Harimurti, 2006). Risiko dapat dipelajari dan dapat dilakukan penanganan, dengan itulah ilmu manajemen risiko diperlukan di kehidupan manusia. ISO 31000 menjadi salah satu ilmu manajemen risiko yang dapat dipelajari, di dalamnya terdapat beberapa tahapan seperti: penentuan lingkup, konteks dan kriteria risiko, pengukuran risiko yang terdiri dari identifikasi risiko, analisis risiko dan evaluasi risiko, serta melakukan perlakuan risiko.

Media digital menjadi kebutuhan yang penting untuk masyarakat pada zaman sekarang, semua kegiatan dapat dilakukan di media digital. Menurut Supratman, data terbaru dari *Google consumer behaviour* yang ditulis oleh Kemp (2018,h. 1) menyatakan bahwa Indonesia memiliki total populasi 265,4 juta dan 50% dari total penduduk tersebut merupakan pengguna internet. Setengah total pengguna internet tersebut disebut dengan para *digital native* (Supratman, 2018). Menurut Fikri Kurniawan, pada data Exabytes Indonesia sebuah perusahaan yang bergerak di bidang pendaftaran *domain* dan *web hosting* di Indonesia menyatakan bahwa terdapat 1057 *website* pada tahun 2020 yang artinya angka tersebut naik 61,6% dari laporan tahun lalu (Fikri Kurniawan, 2021). Dari data tersebut dapat kita

ketahui bahwa banyak masyarakat yang menggunakan media digital khususnya *website* untuk kepentingan pribadi maupun kepentingan pekerjaan khususnya dalam hal penyebaran informasi.

Website sudah digunakan oleh banyak orang dan juga dapat diakses oleh semua orang melalui internet. Dari banyaknya pengguna yang mengakses *website* tersebut tidak diketahui apakah pengguna tersebut merupakan pengguna yang baik atau pengguna yang iseng atau sedikit nakal atau bahkan justru membahayakan. Kasus kejahatan siber banyak terjadi diseluruh belahan dunia, dimulai dari yang terkecil hingga yang terbesar. Contohnya, salah satu situs resmi Kementerian Pertahanan Republik Indonesia atau yang biasa disebut Kemham RI dibobol oleh *hacker,* yaitu *website* Direktorat Jenderal Potensi Pertahanan (Ditjen Pothan) mengalami perubahan laman pada *website* tersebut atau yang biasa disebut *defacing*. Hal tersebut pastinya akan sangat merugikan banyak pihak khususnya pihak pemerintah (Rahmawati, 2017). Diperlukannya manajemen risiko dari ancaman keamanan *website* khususnya *website* universitas supaya tidak terjadi kasus serupa dan menimbulkan banyak kerugian.

Dalam melakukan aktivitas manajemen risiko diperlukannya dasar atau suatu hal yang menjadi aturan utama dalam melakukan suatu kegiatan. Aturan-aturan atau *framework* tersebut harus memiliki alur yang jelas dan sesuai dengan suatu permasalahan yang ada. *Framework* yang digunakan haruslah khusus pada keamanan *website*, karena itu yang menjadi faktor utama permasalahan yang terjadi. *Open Web Application Security Project* dapat digunakan menjadi *framework* karena OWASP khusus membahas tentang keamanan aplikasi berbasis *web* atau *website*. OWASP adalah komunitas yang bersifat terbuka di seluruh dunia yang berfokus pada peningkatan keamanan aplikasi, misi dari OWASP adalah membuat keamanan aplikasi lebih terlihat atau *visible*, sehingga orang-orang atau organisasi dapat membuat keputusan yang tepat tentang risiko dari keamanan aplikasi (OWASP, 2021).

OWASP memiliki beberapa proyek dalam rangka untuk meningkatkan keamanan aplikasi, namun penelitian ini hanya menggunakan diantaranya: OWASP ZAP (*Zed Attack Proxy*) dan OWASP ASVS (*Application Security Verification Standard*) dengan versi terbaru yaitu versi 4.0.3. Penelitian ini

menggunakan dua proyek OWASP tersebut dalam melakukan analisis risiko terhadap *website* yang bersangkutan. Namun analisis risiko selalu bersifat subjektif sampai batas tertentu, yang menciptakan tantangan ketika mencoba untuk melakukan generalisasi dalam standar yang sama. Diharapkan pembaruan terbaru yang dibuat dalam versi terbaru ini menjadi langkah ke arah yang lebih baik dan benar, serta meningkatkan konsep yang diperkenalkan dalam standar industri penting ini (OWASP, 2021). Dengan demikian diharapkan saat melakukan implementasi manajemen risiko yang dilakukan memiliki alur yang jelas dan sesuai dengan inti permasalahan yakni ancaman keamanan *website*.

1.2 Rumusan Masalah

Pada penelitian ini, terdapat beberapa rumusan masalah yang menjadi inti pembahasan pada penelitian ini, berikut adalah rumusan masalah yang digunakan pada penelitian ini:

1. Bagaimana tahapan manajemen risiko berbasis ISO 31000 pada studi kasus *website* OJS?
2. Bagaimana desain mitigasi risiko yang sesuai dengan rekomendasi OWASP (*Open Web Application Security Project*)?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengatasi permasalahan terkait kerentanan keamanan *website* universitas dengan mengimplementasikan manajemen risiko berbasis ISO 31000 dan *framework* OWASP dengan tujuan akhir sebagai berikut:

1. Melakukan implementasi manajemen risiko yang berbasis pada manajemen risiko ISO 31000.
2. Memperoleh hasil desain mitigasi risiko sesuai dengan rekomendasi OWASP (*Open Web Application Security Project*).

1.4 Batasan Penelitian

Ilmu manajemen risiko menjadi ilmu yang sangat luas, sehingga terdapat batasan penelitian yang digunakan pada penelitian ini untuk fokus pada studi kasus yang dilakukan. Batasan penelitiannya yaitu:

1. *Website* yang menjadi objek pada penelitian ini adalah *website* OJS Rumah Jurnal Saintek Universitas Islam Negeri Sunan Ampel.
2. Standar Verifikasi Keamanan Aplikasi yang digunakan adalah OWASP (*Open Web Application Security Project*) ASVS (*Application Security Verification Standard*) 4.0.3
3. Manajemen risiko yang digunakan penelitian ini berbasis pada ISO 31000.
4. Penelitian ini menggunakan *tools* OWASP ZAP (*Zed Attack Proxy*) 2.11.0.
5. Penelitian ini membahas tentang kerentanan keamanan *website* universitas berdasarkan keilmuan manajemen risiko.

1.5 Manfaat Penelitian

1. Manfaat Teoritis

Harapannya, penelitian ini dapat menambah pengetahuan dan wawasan tentang implementasi manajemen risiko berbasis ISO 31000, pentingnya menjaga keamanan *website*, *framework* OWASP *(Open Web Application Security Project*) yang terdiri dari OWASP ASVS (*Application Security Verification Standard*) 4.0.3 dan *tools* OWASP ZAP (*Zed Attack Proxy*) 2.11.0.

2. Manfaat Praktis

Penelitian ini diharapkan dapat menambah pengetahuan tentang cara penulisan penelitian. Hasil dari penelitian ini juga dapat dimanfaatkan untuk para pengembang *website* yang bersangkutan untuk dilakukannya perbaikan supaya masalah keamanan *website* tersebut dapat teratasi. Penelitian ini juga dapat digunakan oleh peneliti selanjutnya dengan menggunakan metode lain dan cara lain agar mendapatkan hasil yang maksimal dan kompleks.

1.6 Sistematika Penulisan Skripsi

Penulisan penelitian ini menggunakan sistematika dan berbagai macam aturan penulisan yang terbagi menjadi beberapa bagian sebagai berikut:

1. BAB 1 Pendahuluan, terdiri dari latar belakang, rumusan masalah dari penelitian yang dilakukan, batasan penelitian, tujuan penelitian dan manfaat yang dihasilkan dari penelitian ini.
2. BAB 2 Tinjauan Pustaka, terdiri dari penelitian yang sudah ada terdahulu dan teori-teori yang berkaitan dengan manajemen risiko, *Risk Assessment* ISO 31000, *framework* OWASP dan integrasi keilmuan sesuai dengan ajaran agama Islam.
3. BAB 3 Metodologi Penelitian, terdiri dari alur penelitian, tempat dan waktu penelitian ini dilaksanakan.
4. BAB 4 Hasil dan Pembahasan, berisikan pembahasan terhadap penelitian yang dilakukan dalam hal penyelesaian rumusan masalah serta mengungkapkan hasil yang diperoleh dari penelitian ini.
5. BAB 5 Penutup, terdiri dari kesimpulan dan saran terhadap studi kasus yang dilakukan.

BAB II
TINJAUAN PUSTAKA

Pada bab dua ini membahas terkait ilmu-ilmu yang digunakan, studi literatur yang digunakan dan dasar-dasar keilmuan lainnya yang menjadi referensi pada penelitian ini. Bab ini terdiri dari: tinjauan penelitian terdahulu, teori yang digunakan dan integrasi keilmuan.

2.1 Tinjauan Penelitian Terdahulu

Tabel 1 Penelitian Terdahulu

No	Judul Penelitian	Hasil	Perbandingan
1	"IT Risk Management Based on ISO 31000 and OWASP *Framework* using OSINT at the Information Gathering Stage (Case Study: X Company)" (Wiradarma & Sasmita, 2019)	Penetration testing digunakan untuk mencari kerentanan *website*. Membuat skenario penyerangan palsu supaya terlihat kerentanannya. Pelaksanaan penetration testing dilakukan dengan menggunakan panduan dari OWASP versi 4. Akhirnya dari terlihatnya kerentanan pada *website* yang bersangkutan, risiko yang dapat membahayakan dapat terlihat. Manajemen risiko sangat diperlukan untuk penanganan dan mitigasi dari risiko tersebut. Penilaian manajemen risiko dilakukan berdasarkan standar ISO 31000: 2018 dengan tahapan identifikasi, analisis dan evaluasi. Hasil dari manajemen risiko menunjukkan bahwa 4 dari 6 risiko memiliki tingkat sedang dan 2 lainnya memiliki tingkat rendah. Hasil yang diperoleh diharapkan dapat membantu pengembang *website* dapat melakukan perbaikan dan penanganan dari risiko yang telah ditemukan.	Penelitian terdahulu ini membahas tentang keamanan *website* menggunakan *framework* Manajemen Risiko ISO 31000 tanpa melakukan mitigasi risiko dan menggunakan tools OWASP ASVS versi 4. Namun yang membedakan dari penelitian ini yaitu Penelitian ini menggunakan OWASP ASVS versi terbaru yaitu versi 4.0.3 dan OWASP ZAP versi 2.11.0 serta melakukan mitigasi risiko dari masing-masing risiko.
2	"Analisis Keamanan *Web* Server *Open Journal System* (OJS) menggunakan Metode ISSAF dan	Penelitian ini melakukan pengujian penetrasi menggunakan metode ISSAF dan OWASP versi 4 dengan tujuan untuk menguji tingkat keamanan sistem OJS dari Universitas Lancang Kuning. Berdasarkan pengujian yang telah	Penelitian terdahulu ini membahas tentang Analisis keamanan *website* OJS dengan menggunakan metode ISSAF dan

	OWASP (Studi Kasus OJS Universitas Lancang Kuning)" (Guntoro, Loneli Costaner & Musfawati, 2020)	dilakukan, dapat diambil kesimpulan: (1) *Website* OJS dari Universitas Lancang Kuning termasuk dalam kategori aman aman, karena tidak mampu untuk dibobol dengan mudah. (2) Walaupun *Website* OJS dari Universitas Lancang Kuning sudah termasuk kategori aman, namun serangan-serangan lainnya mungkin bisa terjadi. (3) Diperlukannya penerapan sistem monitoring untuk melindungi server dari *website* OJS Universitas Lancang Kuning, contohnya seperti menerapkan *Firewall* maupun *Intrusion Detection System* (IDS).	OWASP ASVS versi 4. Namun yang membedakan dari penelitian ini yaitu Penelitian ini menggunakan *Framework* Manajemen Risiko ISO 3100 dan menggunakan tools OWASP ASVS versi terbaru yaitu versi 4.0.3 serta menggunakan OWASP ZAP versi 2.11.0
3	"Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis *Website* pada STMIK ROSMA Dengan Menggunakan OWASP TOP 10" (Yudiana et al., 2021)	Hasil dari pengujian Sistem Informasi E-Office STMIK ROSMA menggunakan OWASP ZAP adalah terdapat 13 kerentanan dan berdasarkan OWASP TOP 10 adalah terdapat 4 kerentanan yaitu *Sensitive Data Exposure*, *Security Misconfiguration*, *Cross Site Scripting*, dan *Insecure Deserialization*. Sehingga dapat disimpulkan Tingkat kerentanan pada Sistem Informasi E-Office STMIK ROSMA adalah Sedang, diharapkan untuk melakukan perbaikan oleh developer atau pihak pengembang.	Penelitian terdahulu ini membahas tentang analisis kualitas keamanan sistem informasi dengan menggunakan tools OWASP TOP 10 dan OWASP ZAP. Namun yang membedakan dari penelitian yaitu penelitian ini menggunakan *Framework* Manajemen Risiko ISO 3100 dan menggunakan OWASP ASVS versi 4.0.3
4	"Mendeteksi Kerentanan Keamanan Aplikasi *Website* Menggunakan Metode OWASP (Open *Web* Application Security Project) untuk Penilaian Risk Rating" (Ghozali et al., 2019)	Hasil dari security assessment menggunakan OWASP Risk Rating Methodology adalah terdapat dua *website* dengan kesimpulan sebagai berikut: 1. Terdapat tujuh risiko, tiga tingkat risiko yang tinggi dua tingkat risiko yang sedang dan dua tingkat risiko yang rendah pada domain http://202.91.11.42/CI. 2. Terdapat delapan risiko, tiga tingkat risiko yang tinggi, dua tingkat risiko yang sedang dan tiga	Penelitian terdahulu ini membahas tentang kerentanan keamanan aplikasi *website* dengan menggunakan tools OWASP Risk Rating Methodology. Namun yang membedakan penelitian ini yaitu penelitian ini menggunakan *Framework*

		tingkat risiko yang rendah pada domain http://202.91.11.42/. 3. Hasil akhirnya adalah *website* http://202.91.11.42/CI dan http://202.91.11.42/ yang menggunakan *framework* Codeigniter dan PHP Native memiliki kelemahan pada Likelihood di tingkat Tengah, sedangkan kelemahan pada Impact berada di tingkat yang Rendah. Dari hasil tersebut penelitian ini tidak dapat memberi jaminan bahwa *website* yang menggunakan *framework* Codeigniter dan PHP Native dapat terhindar dari celah keamanan.	Manajemen Risiko ISO 31000 dengan menggunakan tools OWASP ASVS versi 4.0.3 dan OWASP ZAP versi 2.11.0.
5	Analisis Keamanan *Website* E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard (Setyo Utoro et al, 2020)	Analisis kerentanan aplikasi berbasis *web* dari SMKN 1 Cibatu menggunakan metode PTES yaitu *Penetration Testing Execution Standard* mampu mengungkapkan tingkat kerentanan sistem informasi dengan risiko serangan yang paling tinggi yaitu Cross Site *Script*ing, Cross Site Request Forgery dan Eavesdropping yang berpotensi tinggi untuk terjadinya kebocoran data yang penting. Berdasarkan tahapan pengujian keamanan yang telah dilakukan, metode PTES dapat dijadikan sebagai standar penilaian keamanan aplikasi berbasis *web* pada *website e-learning* pada link alamat belajar.smkn1cibatu.sch.id. Tahapan yang dilakukan terdiri dari *Pre-Engagement Interaction*, *Intelligence Gathering*, *Threat Modelling*, *Vulnerability Analysis*, *Exploitation*, *Post Exploitation* dan *Reporting*	Penelitian terdahulu ini membahas tentang kerentanan keamanan aplikasi *website* dari SMKN 2 Cibatu dengan menggunakan metode PTES dan menggunakan tools Nessus Vulnerability Scanner, NMAP (Network Mapper), Wireshark dan OWASP ZAP. Penelitian ini hanya melakukan analisis kerentanan saja, tidak mengatasi kerentanan tersebut. Namun yang membedakan penelitian ini yaitu penelitian ini menggunakan *Framework* Manajemen Risiko ISO 31000 dengan menggunakan tools OWASP ASVS versi 4.0.3 serta melakukan mitigasi dari risiko atau kerentanan yang muncul

2.2 Teori dasar yang digunakan

2.2.1 Risiko

Risiko merupakan suatu hasil dari kegiatan atau aktivitas yang bersifat tidak terduga dan kemungkinan hasil dari kegiatan tersebut tidak disukai dan tidak diinginkan (operasional sebagai deviasi standar) (Bria, 2012). Pengertian lain, risiko adalah hasil yang diperoleh dari suatu kegiatan yang kemungkinan hasil tersebut menyimpang dari yang diharapkan atau yang direncanakan (Hanafi, 2014).

Selanjutnya pengertian dari risiko, risiko dihubungkan dengan kemungkinan terjadinya akibat buruk yang merugikan dan tidak diinginkan atau tidak terduga (Wedana Yasa et al., 2013). Terdapat pengertian lain yaitu, risiko dapat diartikan sebagai probabilitas yang bersifat merugikan dari suatu kejadian, sedangkan ketidakpastian dinyatakan sebagai gangguan eksogen (exogenous disturbance) (Sherlywati, 2016).

Dari beberapa pengertian yang sudah disebutkan sebelumnya dapat disimpulkan bahwa risiko adalah suatu ketidakpastian yang terjadi dari suatu hasil kegiatan yang tidak terduga dan tidak diinginkan yang menimbulkan suatu hal yang berakibat merugikan.

2.2.2 Manajemen Risiko

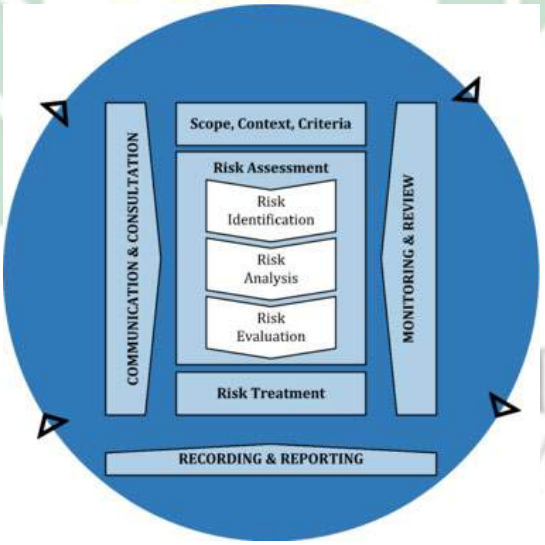
Manajemen risiko merupakan sebuah proses yang sistematis dan terstruktur dalam pengidentifikasian, pengukuran, pemetaan, pengembangan alternatif penanganan risiko, serta pemonitoran dan pengendalian pada penanganan risiko. (Bramantyo Djohanputro, 2008)

Pengertian lain, manajemen Risiko merupakan pelaksanaan fungsi manajemen yang dilakukan guna untuk keperluan penanggulangan risiko, khususnya risiko organisasi/perusahaan, dan masyarakat. Pelaksanaan manajemen risiko terdapat beberapa aktivitas seperti mengorganisir, merencanakan, mengkoordinir, menyusun, mengawasi dan mengevaluasi risiko. (Djojosoedarso, 2003)

Pengertian selanjutnya, manajemen Risiko adalah salah satu bidang keilmuan yang berkaitan dengan cara organisasi dapat menerapkan suatu ukuran dalam pemetaan permasalahan yang ada dengan menggunakan berbagai pendekatan manajemen yang ada secara sistematis dan komprehensif. (Fahmi, 2010)

2.2.3 Manajemen Risiko Berbasis ISO 31000

ISO 31000 adalah satu dari banyaknya pedoman dasar yang menjadi standar keilmuan manajemen risiko. ISO 31000 berisikan panduan tata cara untuk mengelola risiko yang muncul untuk diatasi oleh perusahaan atau organisasi. Penerapan ISO 31000 dapat disesuaikan dengan kebutuhan dari masing-masing organisasi dan dengan masing-masing konteks. Manajemen Risiko berbasis ISO 31000 memiliki beberapa langkah dasar, yaitu: (1) Lingkup Konteks Kriteria; (2) Pengukuran risiko yang terdiri dari identifikasi risiko, analisis risiko dan evaluasi risiko; (3) Perlakuan risiko.



Gambar 1 Diagram *Framework* ISO 31000 (Colle, 2018)

Lingkup, konteks dan kriteria meliputi penentuan lingkup proses, dan pemahaman konteks internal dan eksternal. Organisasi harus melakukan penentuan lingkup kegiatan pada proses manajemen risiko, karena proses manajemen risiko dapat diterapkan pada semua tingkat di organisasi seperti contoh: operasional, strategis, proyek, program atau kegiatan lainnya. Maka penting untuk diperjelasnya sasaran, ruang lingkup proses manajemen risiko, dan keselarasan antara sasaran

organisasi dan ruang lingkupnya (Colle, 2018). Berikut hal-hal yang harus diperhatikan dalam menentukan lingkup:

1. Sasaran dan keputusan yang diperlukan;
2. Hasil yang sesuai;
3. Waktu, lokasi, hal-hal lainnya bersifat detail;
4. Metode dan teknik yang tepat;
5. Sumber daya yang diperlukan;
6. Hubungan dengan proyek, proses dan kegiatan yang berkaitan.

Konteks internal dan eksternal merupakan lingkungan dimana organisasi melakukan penetapan dan pencapaian sasaran. Penetapan konteks pada manajemen risiko harus dilakukan berdasarkan pada pengetahuan terhadap lingkungan internal dan eksternal disaat organisasi beroperasi dan merefleksikan lingkungan yang bersifat detail dari kegiatan manajemen risiko yang diterapkan (Colle, 2018). Pemahaman terhadap konteks merupakan suatu hal yang penting karena:

1. Konteks sasaran dan kegiatan organisasi harus diperhatikan dalam melakukan kegiatan manajemen risiko;
2. Faktor-faktor yang ada pada organisasi dapat menjadi sumber risiko itu sendiri;
3. Sasaran dan lingkup proses manajemen risiko memiliki keterkaitan dengan berbagai sasaran organisasi secara keseluruhan.

Suatu organisasi diharuskan untuk melakukan penetapan kriteria guna untuk kebutuhan evaluasi dari suatu tingkat risiko dan untuk menungjang ketika akan melakukan proses pengambilan keputusan. Pada kriteria risiko dipastikan agar sesuai dengan kerangka manajemen risiko, sasaran, serta ruang lingkup kegiatan yang terkait. Kriteria risiko juga harus mengimplementasikan nilai-nilai, sasaran, dan sumber daya pada organisasi organisasi dengan kebijakan-kebijakan yang berkaitan tentang ilmu manajemen risiko. Kriteria juga harus ditetapkan dengan melakukan pertimbangan bersama pemangku kepentingan (Colle, 2018). Terdapat hal-hal yang harus diperhatikan dalam menyusun kriteria risiko yaitu:

1. Sifat dari ketidakpastian yang berpengaruh pada hasil dan sasaran;

2. Bagaimana konsekuensi dan kemungkinan akan ditentukan dan diukur;
3. Faktor yang berkaitan dengan waktu;
4. Konsisten dalam menggunakan ukuran;
5. Bagaimana cara menentukan tingkat risiko;
6. Bagaimana cara mengombinasikan dan mengurutkan risiko;
7. Kapasitas organisasi.

Risk Assessment atau Pengukuran Risiko pada ISO 31000 adalah salah satu langkah di dalam proses manajemen risiko yang di dalamnya terdiri dari 3 tahap yaitu: Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko. Berikut ini adalah penjelasannya: Pertama yaitu Identifikasi Risiko, melakukan pencarian, menganalisa dan menjabarkan dari risiko yang didapatkan untuk menunjang dan bisa juga menghambat dalam mencapai sasaran dari suatu organisasi (Colle, 2018). Hal penting yang harus diperhatikan dalam melakukan identifikasi risiko yaitu:

1. Sumber risiko yang bersifat nyata dan tidak nyata;
2. Terjadinya kejadian dan penyebabnya;
3. Adanya peluang dan ancamannya;
4. Adanya kemampuan dan kerentanannya;
5. Perubahan yang terjadi pada konteks internal maupun eksternal;
6. Indikator dari masing-masing risiko;
7. Sumber daya, sifat dan nilai aset;
8. Konsekuensi yang timbul dan dampak dari risiko terhadap sasaran;
9. Keandalan sumber informasi dan keterbatasan ilmu pengetahuan;
10. Faktor-faktor yang ada dengan waktu yang terkait;
11. Asumsi-asumsi dari para pihak yang terlibat.

Kedua yaitu Analisis Risiko, untuk melakukan pemahaman dari sifat dan karakteristik risiko termasuk tingkatan dari risiko tersebut. Analisis risiko berkaitan dengan suatu pertimbangan yang terperinci tentang ketidakpastian, konsekuensi, sumber risiko, skenario, peristiwa, kemungkinan, keefektifan dan pengendaliannya (Colle, 2018). Analisis risiko harus memperhatikan sebagai berikut:

1. Kemungkinan terjadinya suatu kejadian dan konsekuensinya;
2. Sifat dan besar dari konsekuensinya;

3. Kompleksitas dan keterkaitannya;
4. Waktu dan ukuran yang digunakan;
5. Keefektifan dari pengendalian yang digunakan;
6. Sensitivitas dan tingkat kepercayaan dari analisis.

Langkah selanjutnya dan yang terakhir di dalam pengukuran risiko yaitu evaluasi risiko, membantu melakukan pengambilan keputusan apa yang akan dilakukan nantinya dari masing-masing risiko yang telah didapatkan. Evaluasi risiko membandingkan hasil-hasil yang telah didapatkan pada analisis risiko sebelumnya untuk menetapkan apakah langkah tindak lanjut perlu dilakukan atau tidak terhadap masing-masing risiko. Pada penelitian ini Evaluasi Risiko berisikan respon yang akan dilakukan dari risiko yang muncul.

Langkah selanjutnya dan langkah terakhir yang digunakan penelitian ini pada manajemen risiko berbasis ISO 31000 adalah perlakuan risiko. Perlakuan risiko bertujuan untuk menerapkan dan memilih strategi mitigasi dalam melakukan perlakuan risiko. Perlakuan risiko mencakup proses-proses seperti berikut:

1. Pemilihan opsi untuk perlakuan risiko nantinya;
2. Menentukan perencanaan dan bagaimana implementasinya terhadap perlakuan risiko;
3. Menilai efektivitas dari perlakuan risiko;
4. Pengambilan keputusan;
5. Pelaksanaan perlakuan risiko tingkat lanjut.

2.2.4 Alat Bantu *Risk Assessment* ISO 31000

Pada dokumen ISO 31000 terdapat alat bantu yang dapat digunakan peneliti untuk proses *Risk Assessment* Manajemen Risiko, dimana setiap alat bantu memiliki keunggulan dan kelemahan yang berbeda-beda. Hal ini menunjukkan bahwa tidak semua alat bantu dapat digunakan disemua tahapan, dan penerapan alat bantu tersebut disesuaikan dengan kebutuhan masing-masing.

Pada Pengukuran Risiko Manajemen Risiko ISO 31000 terdapat beberapa langkah yang dicantumkan pada dokumen ISO 31000, yaitu: Identifikasi Risiko, Analisis Risiko (yang terdiri dari Konsekuensi, Probabilitas dan Tingkat Risiko)

dan Evaluasi Risiko. Dari masing-masing alat bantu tersebut berisikan tiga pernyataan yaitu: SA, A dan NA. SA berarti sangat dapat diterapkan, A berarti dapat diterapkan dan NA berarti tidak dapat diterapkan.

Tabel 2 Penerapan Alat Bantu Pengukuran Risiko pada dokumen ISO 31000

No	Alat bantu dan Teknik	Proses Pengukuran Risiko				
		Identifikasi Risiko	Analisis Risiko			Evaluasi Risiko
			Konsekuensi	Probabilitas	Tingkat Risiko	
1	Curah pendapat	SA	NA	NA	NA	NA
2	Wawancara terstruktur atau semi-struktur	SA	NA	NA	NA	NA
3	Delphi	SA	NA	NA	NA	NA
4	Daftar periksa	SA	NA	NA	NA	NA
5	Analisis pendahuluan potensi bahaya	SA	NA	NA	NA	NA
6	Studi potensi bahaya dan operabilitas (HAZOP)	SA	SA	A	A	A
7	Analisis potensi bahaya dan titik kendali kritis (HACCP)	SA	SA	NA	NA	SA
8	Penilaian risiko lingkungan	SA	SA	SA	SA	SA
9	Struktur “apa-jika” " (SWIFT)	SA	SA	SA	SA	SA
10	Analisis skenario	SA	SA	A	A	A
11	Analisis dampak bisnis	A	SA	A	A	A
12	Analisis akar penyebab	NA	SA	SA	SA	SA
13	Analisis modus kegagalan dan dampak	SA	SA	SA	SA	SA
14	Analisis pohon kesalahan	A	NA	SA	A	A
15	Analisis pohon kejadian	A	SA	A	A	NA
16	Analisis sebab dan konsekuensi	A	SA	SA	A	A

17	Analisis sebab-dan-akibat	SA	SA	NA	NA	NA
18	Analisis lapisan proteksi (LOPA)	A	SA	A	A	NA
19	Pohon keputusan	NA	SA	SA	A	A
20	Analisis keandalan manusia	SA	SA	SA	SA	A
21	Analisis dasi kupu-kupu	NA	A	SA	SA	A
22	Pemeliharaan yang terpusat pada keandalan	SA	SA	SA	SA	SA
23	Analisis rangkaian selinap	A	NA	NA	NA	NA
24	Analisis Markov	A	SA	NA	NA	NA
25	Simulasi Monte carlo	NA	NA	NA	NA	SA
26	Statistik Bayesian dan jaring Bayes	NA	SA	NA	NA	SA
27	Kurva FN	A	SA	SA	A	SA
28	Indeks risiko	A	SA	SA	A	SA
29	Matriks Konsekuensi/probabilitas	SA	SA	SA	SA	A
30	Analisis biaya/manfaat	A	SA	A	A	A
31	Analisis keputusan multikriteria (MCDA)	A	SA	A	SA	A
	1) SA = Sangat dapat diterapkan 2) NA = Tidak dapat diterapkan 3) A = Dapat diterapkan					

2.2.5 *Open Web Application Security Project*

Open Web Application Security Project atau yang biasa di singkat OWASP adalah organisasi non-profit yang bekerja di bidang peningkatan keamanan *software* atau perangkat lunak. Proyek ini dipimpin oleh komunitas-komunitas dengan ratusan cabang yang ada di banyak negara serta memiliki puluhan ribu anggota, melakukan seminar pendidikan dan pelatihan. Organisasi OWASP menjadi sumber pengetahuan tentang keamanan bagi pengembang aplikasi berbasis *website* (OWASP Foundation, 2021).

OWASP membuat banyak proyek diantaranya yang dikenal banyak orang yaitu: OWASP *Top Ten*, *Security Knowledge Framework,* OWASP *Software Assurance Maturity Model* (SAMM), *Dependency Track*, *Mobile Security Testing Guide*, OWASP *Application Security Verification Standard* dan OWASP *Zed Attack Proxy*. Proyek dari perusahaan OWASP tersebut akan terus berkembang dan meningkat seiring berjalannya waktu dan pengetahuan, agar semua proyek yang ada dapat digunakan dengan baik.

2.2.6 OWASP ASVS 4.0.3

OWASP ASVS (*Application Security Verification Standard*) adalah salah satu proyek yang ada di perusahaan OWASP. OWASP ASVS sudah mengalami beberapa pembaharuan dan yang terbaru adalah versi 4.0.3 yang dirilis pada bulan oktober 2021. OWASP ASVS menyediakan kontrol keamanan dasar untuk aplikasi berbasis *website* dan juga menyediakan daftar persyaratan bagi pengembang aplikasi untuk melakukan pengembangan yang aman.

OWASP ASVS adalah daftar persyaratan atau pengujian keamanan aplikasi yang dapat digunakan oleh arsitek, pengembang, penguji, profesional keamanan, vendor alat, dan konsumen untuk menentukan, membangun, menguji, dan memverifikasi aplikasi aman. OWASP ASVS memiliki beberapa klausul yang berkaitan dengan beberapa komponen yang ada pada aplikasi berbasis *website*. Total klausul yang ada pada OWASP ASVS adalah 14 klausul.

Tabel 3 Klausul OWASP ASVS 4.0.3

No	Klausul
1	*Architecture, Design and Threat Modeling*
2	*Authentication*
3	*Session Management*
4	*Access Control*
5	*Validation, Sanitization and Encoding*
6	*Stored Cryptography*
7	*Error Handling and Logging*
8	*Data Protection*

9	*Communication*
10	*Malicious Code*
11	*Business Logic*
12	Files *and Resources*
13	*API and Web Service*
14	*Configuration*

2.2.7 OWASP ZAP

OWASP ZAP (*Open Web Application Security Project - Zed Attack Proxy*) merupakan salah satu project lain dari OWASP selain OWASP ASVS. OWASP ZAP adalah tools yang digunakan mencari kerentanan dari suatu *website*. Celah-celah yang ada pada suatu *website* dapat dicari kerentanannya menggunakan tools ini, tentunya akan sangat sesuai dengan penelitian ini dalam melakukan analisis ancaman keamanan *website*. OWASP ZAP memiliki 160 macam Alert yang apabila dilihat secara detail pada *Alert Detail* terdapat 4 status (*alpha*, *beta*, *release*, *deprecated*), 4 risk (*low*, *medium*, *high*, *informational*) dan 3 *type* (*active*, *passive*, *websocket passive*), namun penelitian ini hanya berfokus pada risk saja. Data-data tersebut tersedia dan dapat diakses pada *Documentation* – ZAP *Alert Detail*.

Tabel 4 Tingkat Risiko OWASP ZAP

Tingkat Risiko
Informational
Low
Medium
High

Cara kerja dari OWASP ZAP yaitu dengan melakukan *scanning* atau pencarian apakah komponen yang dibutuhkan sudah terpasang pada "HTTP" dari sebuah *website* guna untuk mencari potensi kerentanan pada suatu *website*, apabila sudah dilakukan *scanning* maka tingkat risiko dari suatu permasalahan tersebut

akan muncul sesuai dengan dokumentasi yang ada pada OWASP ZAP yang sudah melakukan berbagai pengujian dan pengetesan pada banyak *website*. Jadi cara kerjanya yaitu melakukan *scanning* pada HTTP di suatu *website*.

2.2.8 Keamanan Sistem Informasi

Keamanan Sistem Informasi adalah bagaimana cara melakukan pencegahan penipuan (*cheating*) ataupun melakukan pendeteksian penipuan yang akan terjadi pada sistem berbasis informasi, dimana informasi yang dimaksud tidak memiliki arti fisik (Ghozali et al., 2019).

Tujuan dari adanya keamanan sistem informasi adalah untuk melakukan pencegahan dari ancaman yang merugikan terhadap sistem yang ada pada suatu perusahaan atau instansi pendidikan. Ancaman yang merugikan tersebut dapat berupa kerusakan, penipuan, kehilangan data penting (G.J Simson & Gene Spafford, 2005).

Selanjutnya, tujuan dari keamanan sistem informasi adalah untuk melindungi kerahasiaan data berupa dokumen, foto, audio, video dan lain sebagainya dalam layanan sistem informasi yang diterapkan oleh perusahaan yang mengimplementasikan teknologi informasi serta melindungi integritas dan ketersediaan informasi (Akbar et al., 2018).

2.2.9 *Web*

Web adalah layanan yang dapat terhubung dengan fasilitas *hypertext* dan bertujuan untuk untuk menampilkan data berupa suara, teks, animasi, gambar serta format multimedia lainnya pada pengguna komputer atau *user* (Kustiyahningsih & Anamisa, 2011).

Pengertian lain, *web* merupakan suatu sistem dengan dokumen yang terkait di dalamnya dan digunakan sebagai media untuk menampilkan informasi dalam bentuk seperti gambar, teks, video, suara, dan perangkat multimedia lainnya yang sejenis pada jaringan internet (Sibero, 2013).

Dari pengertian-pengertian sebelumnya, disimpulkan bahwa pengertian *web* adalah suatu layanan hypertext yang digunakan sebagai media menampilkan

informasi dengan format berupa text, suara, gambar, video, animasi dan format multimedia lainnya pada jaringan internet.

2.2.10 *Website*

Website adalah kumpulan dari banyaknya halaman *web* yang saling terhubung dan dokumen-dokumen yang berkaitan. *Web* memiliki beberapa komponen, dimulai dari halaman atau *"page"* lalu kumpulan dari banyaknya halaman disebut *"homepage"*. *Homepage* berada pada posisi terluar dari *website*, dengan berbagai macam halaman di dalamnya. Beberapa *web* yang sudah ada memiliki halaman di dalam *homepage* yang disebut *"child page"*, *child page* berisikan *hyperlink* yang terhubung dengan halaman lain (Gregorius Agung, 2000).

Pengertian lain, *website* adalah suatu sistem yang dapat berkaitan dengan beberapa dokumen-dokumen yang dapat digunakan sebagai media dan berfungsi untuk menampilkan suatu informasi seperti gambar, tulisan, multimedia, dan lain sebagainya melalui jaringan internet (Alexander F. K. Sibero, 2011).

Pengertian selanjutnya, *website* adalah aplikasi yang berisikan dokumen-dokumen dengan format multimedia (animasi, tulisan, video, gambar) dan di dalamnya menggunakan protokol HTTP (*Hypertext Transfer Protocol*) dan dapat diakses menggunakan browser (M.Rudyanto Arief, 2011).

Pengertian selanjutnya, *Website* merupakan kumpulan banyak halaman *web* yang dimanfaatkan oleh manusia untuk menampilkan suatu informasi berupa teks, gambar diam ataupun yang bergerak, suara, animasi, atau bahkan gabungan dari format itu semuanya, yang bersifat dinamis ataupun statis yang membentuk suatu rangkaian kerangka *web* yang saling berkaitan, dan dapat terhubung satu dengan yang lainnya (Bintu Humairah Bekti, 2015).

2.2.11 *Hypertext Transfer Protocol*

Hypertext Transfer Protocol atau disingkat HTTP merupakan sebuah protokol pada jaringan yang berfungsi agar dua user yang terdiri dari *client* dan *server* dapat melakukan komunikasi dua arah dengan baik dengan cara *request* dan *response*. Pada HTTP juga dapat menentukan jenis dari pesan dan bagaimana cara

mengirimkannya, serta interaksi *web server* terhadap perintah (Priyanto Hidayatullah, 2017)**.**

Pengertian lainnya, *Hypertext Transfer Protocol* atau yang biasa disingkat HTTP adalah sebuah protokol di suatu jaringan yang terdapat pada lapisan aplikasi yang dapat digunakan untuk suatu jenis sistem informasi yang bersifat terdistribusi, kolaboratif, dan *hypermedia* (Handoko, 2017).

Dari pengertian diatas dapat disimpulkan bahwa, *Hypertext Transfer Protocol* atau HTTP adalah sebuah protokol jaringan pada lapisan aplikasi agar *client* dan *server* dapat berkomunikasi dengan cara *request-response* dan bersifat terdistribusi, kolaboratif dan *hypermedia*.

2.3 Integrasi Keilmuan

Pada penelitian ini, dilakukan integrasi keilmuan dengan melakukan wawancara kepada salah satu narasumber yang berkompeten dalam Agama Islam yaitu ustadzah Wiwin Luqna Hunaida, M.Pd.I yang merupakan seorang Dosen pada Fakultas Tarbiyah dan Keguruan pada Universitas Islam Negeri Sunan Ampel. Berdasarkan hasil yang didapatkan pada saat wawancara, diperoleh ayat-ayat Al-Qur'an yang berkaitan dengan manajemen risiko ada pada kisah Yusuf yang mentakwilkan mimpi sang raja pada masanya. Kisah tersebut terdapat pada Al-Qur'an Surat Yusuf ayat 43,

خُضْرٍ سُنْۢبُلٰتٍ وَّسَبْعَ عِجَافٌ سَبْعٌ يَّأْكُلُهُنَّ سِمَانٍ بَقَرٰتٍ سَبْعَ اَرٰى اِنِّيْٓ الْمَلِكُ وَقَالَ
تَعْبُرُوْنَ لِلرُّءْيَا كُنْتُمْ اِنْ رُءْيَايَ فِيْ اَفْتُوْنِيْ الْمَلَاُ يٰٓاَيُّهَا يٰبِسٰتٍۗ وَّاُخَرَ

Artinya :

Dan raja berkata (kepada para pemuka kaumnya), "Sesungguhnya aku bermimpi melihat tujuh ekor sapi betina yang gemuk dimakan oleh tujuh ekor sapi betina yang kurus; tujuh tangkai (gandum) yang hijau dan (tujuh tangkai) lainnya yang kering. Wahai orang yang terkemuka! Terangkanlah kepadaku tentang takwil mimpiku itu jika kamu dapat menakwilkan mimpi." (43)

Selanjutnya penjelasan tentang Yusuf yang mentakwilkan mimpi sang raja dijelaskan pada Al-Qur'an Surat Yusuf ayat 46 sampai ayat 49:

سُنْۢبُلٰتٍ وَّسَبْعِ عِجَافٌ سَبْعٌ يَّأْكُلُهُنَّ سِمَانٍ بَقَرٰتٍ سَبْعِ فِيْ اَفْتِنَا الصِّدِّيْقُ اَيُّهَا يُوْسُفُ
يَعْلَمُوْنَ لَعَلَّهُمْ النَّاسِ اِلَى اَرْجِعُ لَّعَلِّيْٓ يٰبِسٰتٍۙ وَّاُخَرَ خُضْرٍ

Artinya :

"Yusuf, wahai orang yang sangat dipercaya! Terangkanlah kepada kami (takwil mimpi) tentang tujuh ekor sapi betina yang gemuk yang dimakan oleh tujuh (ekor sapi betina) yang kurus, tujuh tangkai (gandum) yang hijau dan (tujuh tangkai) lainnya yang kering agar aku kembali kepada orang-orang itu, agar mereka mengetahui." (46)

تَأْكُلُوْنَ مِمَّا قَلِيْلًا اِلَّا سُنْۢبُلِهٖ فِيْ فَذَرُوْهُ حَصَدْتُّمْ فَمَا دَاَبًاۚ سِنِيْنَ سَبْعَ تَزْرَعُوْنَ قَالَ

Dia (Yusuf) berkata, “Agar kamu bercocok tanam tujuh tahun (berturut-turut) sebagaimana biasa; kemudian apa yang kamu tuai hendaklah kamu biarkan di tangkainya kecuali sedikit untuk kamu makan.” (47)

تُحْصِنُوْنَ مِمَّا قَلِيْلًا اِلَّا لَهُنَّ قَدَّمْتُمْ مَا يَّأْكُلْنَ شِدَادٌ سَبْعٌ ذٰلِكَ بَعْدِ مِنْۢ يَأْتِيْ ثُمَّ

Kemudian setelah itu akan datang tujuh (tahun) yang sangat sulit, yang menghabiskan apa yang kamu simpan untuk menghadapinya (tahun sulit), kecuali sedikit dari apa (bibit gandum) yang kamu simpan. (48)

يَعْصِرُوْنَ وَفِيْهِ النَّاسُ يُغَاثُ فِيْهِ عَامٌ ذٰلِكَ بَعْدِ مِنْۢ يَأْتِيْ ثُمَّ

Setelah itu akan datang tahun, di mana manusia diberi hujan (dengan cukup) dan pada masa itu mereka memeras (anggur).” (49)

Dalam tafsir Al-Mishbah, M. Quraish Shihab menafsirkan bahwa Nabi Yusuf mengetahui arti dari tujuh ekor sapi adalah tujuh tahun masa pertanian. Sapi yang gemuk melambangkan kesuburan sedangkan sapi kurus melambangkan masa sulit dalam pertanian. Lalu bulir-bulir gandum melambangkan jumlah pangan yang tersedia, setiap bulirnya berarti setahun.

Dari cerita Nabi Yusuf A.S dan Sang Raja pada zaman itu menceritakan tentang adanya dua buah masa yaitu: masa selama tujuh tahun pertama di suatu daerah mengalami masa pertanian yang sangat subur dan menghasilkan banyak hasil panen, dan masa selama tujuh tahun kedua mengalami masa sulit dengan banyaknya kekeringan yang terjadi. Terdapat suatu risiko yang terjadi saat mengalami kesuburan pertanian yaitu kekeringan pertanian, Nabi Yusuf A.S memberikan solusi untuk memanajemen risiko yang muncul tersebut dengan cara menyimpan sisa hasil panen pada tujuh tahun pertama untuk dipersiapkan pada tujuh tahun kedua supaya saat mengalami masa kekeringan sang raja dan masyarakat masih bisa bertahan hidup.

Hal ini membuktikan bahwa setiap kegiatan atau aktivitas yang kita lakukan terdapat risiko dibaliknya, risiko tersebut tentunya bersifat merugikan. Manusia diberi akal oleh Allah SWT untuk berpikir bagaimana cara menyelesaikan

permasalahan yang ada, pada studi kasus ini adalah risiko tersebut. Manajemen risiko sangat diperlukan supaya dapat melakukan pencegahan dan mitigasi dari risiko yang muncul. Dengan adanya cerita dari Nabi Yusuf A.S kita dapat menjadi pribadi lebih baik lagi, dengan selalu menambah ilmu pengetahuan dan wawasan agar kita dapat mengatasi masalah atau risiko yang muncul dalam menjalani kehidupan.

Selanjutnya diperkuat dengan Surat Al-Baqarah ayat 60 yang menceritakan tentang nabi musa yang memukul batu menggunakan tongkat sehingga mengeluarkan dua belas mata air.

عَشْرَةَ اثْنَتَا مِنْهُ فَانْفَجَرَتْ الْحَجَرَ ۖ بِّعَصَاكَ اضْرِبْ فَقُلْنَا لِقَوْمِهٖ مُوْسٰى اسْتَسْقٰى وَاِذِ
فِى تَعْثَوْا وَلَا اللّٰهِ رِّزْقِ مِنْ وَاشْرَبُوْا كُلُوْا ۖ مَّشْرَبَهُمْ اُنَاسٍ كُلُّ عَلِمَ قَدْ ۖ عَيْنًا
مُفْسِدِيْنَ الْاَرْضِ

Dan (ingatlah) ketika Musa memohon air untuk kaumnya, lalu Kami berfirman, “Pukullah batu itu dengan tongkatmu!” Maka memancarlah daripadanya dua belas mata air. Setiap suku telah mengetahui tempat minumnya (masing-masing). Makan dan minumlah dari rezeki (yang diberikan) Allah, dan janganlah kamu melakukan kejahatan di bumi dengan berbuat kerusakan (60)

Pada Tafsir dari Kementrian Agama RI menjelaskan bahwa ayat tersebut Allah SWT menceritakan bagaimana Nabi Musa A.S berdoa kepada Allah meminta pertolongan berupa air minum bagi para pengikutnya yang terdiri dari dua belas suku. Allah mengabulkan doa tersebut dan memerintahkan Nabi Musa memukul tongkatnya ke batu besar yang ada pada padang pasir dan seketika memancarlah dua belas sumber mata air dari batu tersebut. Sesungguhnya Allah kuasa untuk memancarkan air dari batu tanpa dipukul menggunakan tongkat lebih dahulu, tetapi Allah hendak memperlihatkan kepada para hambanya untuk selalu berusaha dan bekerja untuk mencapai tujuan tertentu sesuai proses hubungan antara sebab dan akibat. Ayat ini juga menjelaskan tentang bagaimana cara melakukan manajemen terhadap segala hal yang kita dapatkan, supaya kita dapat memanfaatkan sesuatu yang kita dapat menjadi maksimal.

Ayat selanjutnya diperjelas pada Al-Qur'an Surah Al-Maidah ayat 2 yang berbunyi:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تُحِلُّوْا شَعَاۤىِٕرَ اللّٰهِ وَلَا الشَّهْرَ الْحَرَامَ وَلَا الْهَدْيَ وَلَا الْقَلَاۤىِٕدَ وَلَآ اٰۤمِّيْنَ الْبَيْتَ الْحَرَامَ يَبْتَغُوْنَ فَضْلًا مِّنْ رَّبِّهِمْ وَرِضْوَانًا ۗوَاِذَا حَلَلْتُمْ فَاصْطَادُوْا ۗوَلَا يَجْرِمَنَّكُمْ شَنَاٰنُ قَوْمٍ اَنْ صَدُّوْكُمْ عَنِ الْمَسْجِدِ الْحَرَامِ اَنْ تَعْتَدُوْا ۘوَتَعَاوَنُوْا عَلَى الْبِرِّ وَالتَّقْوٰى ۖوَلَا تَعَاوَنُوْا عَلَى الْاِثْمِ وَالْعُدْوَانِ ۚوَاتَّقُوا اللّٰهَ ۗاِنَّ اللّٰهَ شَدِيْدُ الْعِقَابِ

Wahai orang-orang yang beriman! Janganlah kamu melanggar syiar-syiar kesucian Allah, dan jangan (melanggar kehormatan) bulan-bulan haram, jangan (mengganggu) hadyu (hewan-hewan kurban) dan qala'id (hewan-hewan kurban yang diberi tanda), dan jangan (pula) mengganggu orang-orang yang mengunjungi Baitulharam; mereka mencari karunia dan keridaan Tuhannya. Tetapi apabila kamu telah menyelesaikan ihram, maka bolehlah kamu berburu. Jangan sampai kebencian(mu) kepada suatu kaum karena mereka menghalang-halangimu dari Masjidilharam, mendorongmu berbuat melampaui batas (kepada mereka). Dan tolong-menolonglah kamu dalam (mengerjakan) kebajikan dan takwa, dan jangan tolong-menolong dalam berbuat dosa dan permusuhan. Bertakwalah kepada Allah, sungguh, Allah sangat berat siksaan-Nya. (2)

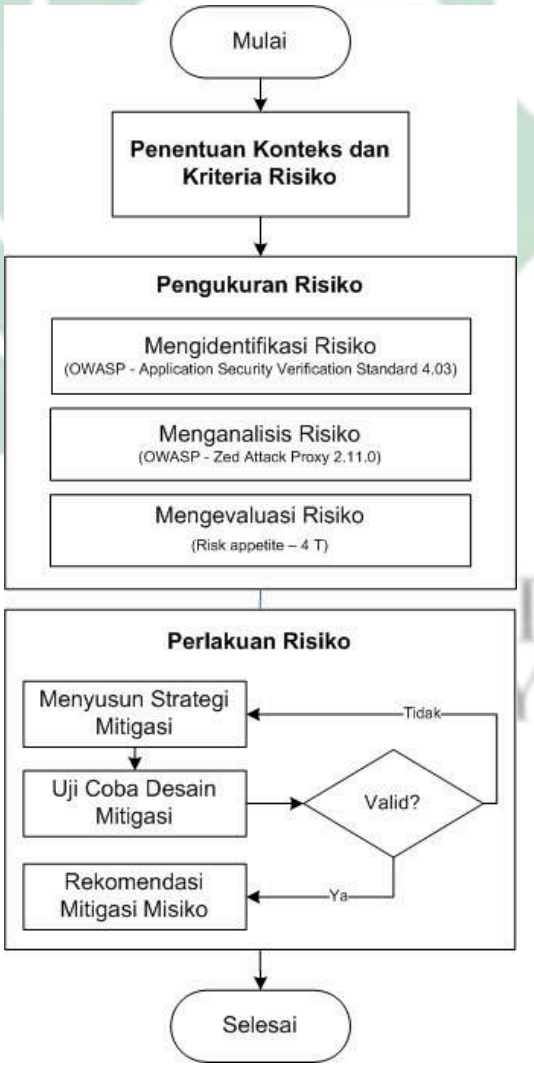
Menurut Tafsir Kementerian Agama RI menjelaskan bahwa ayat tersebut berisikan hukum-hukum yang ditetapkan Allah yan berkaitan dengan tata cara pelaksanaan haji. Hal ini menjelaskan secara detail dengan cara melakukan manajemen dalam hal mempersiapkan diri untuk melaksanakan ibadah haji, seperti apa saja yang harus dipenuhi dan apa saja yang dilarang untuk dilakukan, semua itu harus dipatuhi dan harus dilakukan. Manusia harus dapat melakukan manajemen diri dari setiap kegiatan dan perbuatan yang mereka lakukan, karena setiap apa yang kita perbuat pasti terdapat risiko-risiko kehidupan yang muncul, dengan dilakukannya manajemen diri kita semua dapat mengatasi segala risiko yang muncul di dalam kehidupan kita.

BAB III
METODOLOGI PENELITIAN

Pada bab tiga ini membahas tentang langkah-langkah yang akan dilakukan untuk menentukan metode yang digunakan penelitian ini. Bab ini terdiri dari: diagram alur penelitian, metode penelitian, sasaran penelitian, lingkup konteks kriteria, pengukuran risiko, dan perlakuan risiko.

3.1 Diagram Alur Penelitian

Penelitian ini menggunakan beberapa tahapan proses dalam pelaksanaannya, dan digambarkan dalam bentuk diagram sebagai berikut:



Gambar 2 Diagram Alur Penelitian

3.2 Metode Penelitian

Penelitian ini menggunakan pendekatan metodologi penelitian Kualitatif. Metodologi Penelitian merupakan suatu keilmuan yang bertujuan untuk memperoleh hasil penelitian yang lebih mendalam mengenai sistematika dan langkah-langkah penelitian (Drs. Syahrum & Drs. Salim, 2017). Pengertian Penelitian kualitatif sendiri yaitu penelitian yang memiliki tujuan untuk memahami fenomena yang dialami oleh suatu subyek penelitian secara menyeluruh dan dengan cara deskripsi dalam bentuk kalimat deskriptif, pada konteks tertentu serta dengan menggunakan berbagai metode ilmiah (Moleong, 2010).

Pengertian selanjutnya yaitu menurut Kirl dan Miller, penelitian kualitatif merupakan tradisi dalam ilmu pengetahuan sosial secara fundamental bergantung pada pengamatan manusia, dalam kawasan maupun istilah. Dari pengertian-pengertian yang sudah dipaparkan sebelumnya dapat disimpulkan penelitian kualitatif merupakan salah satu prosedur penelitian yang dilakukan untuk mengungkap masalah secara holistik-kontekstual dan menghasilkan data yang bersifat deskriptif pada konteks tertentu dengan menggunakan berbagai metode ilmiah dan bergantung pada pengamatan yang dilakukan oleh manusia. (Moleong 2010)

Tujuan dari penelitian kualitatif adalah untuk melakukan riset yang berfokus pada perolehan data dengan dilakukannya suatu tahapan-tahapan atau langkah-langkah dan juga dapat didapatkan melalui komunikasi terbuka, percakapan dan wawancara. Penelitian kualitatif dapat dilakukan dengan beberapa cara, seperti contoh melakukan pengamatan secara langsung pada obyek penelitian, melakukan survei terbuka yang berkaitan dengan obyek pembahasan dari suatu penelitian, melakukan wawancara secara mendalam dan detail terhadap suatu narasumber yang berkaitan dengan obyek yang dibahas pada penelitian ini.

3.3 Sasaran Penelitian

Dalam penelitian ini yang menjadi sasarannya adalah admin dan segala perangkat dari Rumah Jurnal Saintek Universitas Islam Negeri Sunan Ampel yang bertugas untuk mengoperasikan atau bertanggung jawab atas keberlangsungan dan penggunaan *website* tersebut. Fitur-fitur pada *website* OJS Rumah Jurnal Saintek

Universitas Islam Negeri Sunan Ampel juga akan dilibatkan saat implementasi manajemen risiko berbasis ISO 31000 dari segi struktur halaman, konfigurasi *web* server dan lain-lain.

3.4 Lingkup Konteks Kriteria

Langkah pertama yang dilakukan pada penelitian ini yaitu menentukan lingkup, konteks dan kriteria. Penelitian ini menggunakan klausul-klausul yang ada pada OWASP ASVS yang terdiri dari 14 klausul. Penggunaan 14 klausul OWASP ASVS pada langkah ini karena risiko-risiko yang muncul pada langkah selanjutnya tidak akan jauh-jauh dari 14 klausul tersebut dan OWASP ASVS akan menjadi dasar dari pencarian risiko. Hal itu dapat terjadi karena beberapa faktor, yang pertama yaitu karena OWASP ASVS memiliki standar keamanan yang cukup lengkap dan khusus untuk aplikasi berbasis *web*, oleh sebab itu penggunaan 14 klausul OWASP ASVS menjadi maksimal, dan alasan selanjutnya yaitu pencarian risiko nantinya akan menggunakan tools OWASP ZAP yang berada pada satu organisasi yang sama dan kemungkinan memiliki keterkaitan di dalamnya.

Tabel 5 Desain Lingkup Konteks Kriteria Risk Register ISO 31000

No	Lingkup Konteks Kriteria
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

3.5 Pengukuran Risiko

Pengukuran risiko menjadi proses yang penting pada manajemen risiko berbasis ISO 31000 karena kegiatan manajemen risiko yang utama ada pada langkah ini. Pada pengukuran risiko terbagi menjadi 3, yaitu: identifikasi risiko, analisis risiko dan evaluasi risiko.

3.5.1 Identifikasi Risiko

Langkah pertama yang dilakukan pada pengukuran risiko yaitu identifikasi risiko. Identifikasi risiko yang dilakukan adalah melakukan pencarian dari kemungkinan-kemungkinan yang muncul pada suatu *website*. Pencarian risiko pada langkah ini memanfaatkan tools yaitu OWASP ZAP. OWASP ZAP adalah tools yang dapat melakukan pencarian kerentanan-kerentanan pada suatu *website* dari segi keamanannya. Saat OWASP ZAP dijalankan maka kerentanan-kerentanan akan muncul dan kerentanan itulah yang menjadi risiko.

Risiko yang muncul selanjutnya dilakukan pengkategorian dari masing-masing risiko berdasarkan Lingkup Konteks Kriteria yang sudah ditentukan sebelumnya yaitu berdasarkan pada OWASP ASVS versi 4.0.3 yang terdiri dari 14 klausul. Pencarian dilakukan menggunakan kata kunci yang berkaitan dengan risiko tersebut, setelah ditemukannya masing-masing risiko berdasarkan Lingkup Konteks Kriterianya masukkan kedalam tabel. Selanjutnya yaitu pemberian ID risiko pada masing-masing risiko yang telah ditemukan. Berikut adalah tabel desain identifikasi risiko.

Tabel 6 Desain Identifikasi Risiko Risk Register ISO 31000

No	Lingkup, Konteks, Kriteria	Identifikasi Risiko	ID Risiko
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

13			
14			

3.5.2 Analisis Risiko

Langkah selanjutnya yaitu analisis risiko. Setelah mengetahui risiko-risiko yang muncul pada OWASP ZAP langkah selanjutnya adalah melakukan pencarian tingkat risiko pada masing-masing risiko. OWASP ZAP sudah menyediakan fitur untuk melakukan pencarian tingkat risiko berdasarkan perhitungan yang sudah dilakukan sebelumnya pada penelitian yang dilakukan oleh organisasi tersebut. Selanjutnya setelah melakukan pencaria risiko yaitu melakukan pencarian dari deskripsi dari masing-masing risiko. Deskripsi risiko ini berisikan arti dari risiko yang muncul dan alasan mengapa risiko tersebut muncul. Langkah terakhir yaitu tingkat risiko dan deskripsi tersebut dimasukkan kedalam tabel berdasarkan masing-masing risikonya. Berikut adalah tabel desain analisis risiko.

Tabel 7 Desain Analisis Risiko Risk Register ISO 31000

ID Risiko	**Identifikasi Risiko**	**Analisis Risiko**	
		Tingkat Risiko	**Deskripsi**

3.5.3 Evaluasi Risiko

Langkah terakhir pada langkah pengukuran risiko adalah evaluasi risiko. Setelah risiko, tingkat risiko dan deskripsinya sudah ditemukan langkah selanjutnya yaitu menentukan respon apa yang akan dilakukan oleh masing-masing risiko. Pada manajemen risiko berbasis ISO 31000 terdapat 4 respon, yaitu: Transfer, Terminate, *Tolerate*, dan *Treat*. Setelah ditentukan respon apa yang diberikan pada masing-masing risiko yaitu melakukan perlakuan risiko sesuai dengan respon apa yang

diberikan pada masing-masing risiko. Dilakukan penentuan aturan dari masing-masing respon untuk dapat diterapkan pada risiko yang telah muncul dan dapat digunakan untuk menilai risiko tersebut mendapatkan evaluasi risiko yang mana. Berikut adalah tabel desain evaluasi risiko.

Tabel 8 Desain Evaluasi Risiko Risk Register ISO 31000

ID Risiko	Identifikasi Risiko	Analisis Risiko		Evaluasi Risiko
		Tingkat Risiko	Deskripsi	

3.6 Perlakuan Risiko

Terdapat tiga langkah yang ditentukan pada penelitian ini untuk melakukan perlakuan risiko. Tiga langkah tersebut yaitu:

3.6.1 Menyusun Strategi Mitigasi

Pada langkah menyusun strategi mitigasi ini aktivitas yang dilakukan adalah mencari referensi-referensi menyusun strategi mitigasi. Referensi-referensi tersebut menggunakan isi dari OWASP ASVS versi 4.0.3 dan OWASP ZAP pada fitur *Solution*, masing-masing risiko akan dicari solusi penyelesaiannya menggunakan referensi tersebut, setelah ditemukan deskripsi dan cara-cara mitigasi risiko berdasarkan risiko yang dicari pada masing-masing referensi tersebut disatukan menjadi satu pemahaman dan satu strategi mitigasi. Selanjutnya data-data tersebut dimasukkan kedalam tabel perlakuan risiko.

3.6.2 Uji Coba Desain Mitigasi

Langkah selanjutnya yaitu melakukan uji coba desain mitigasi. Setelah ditemukannya deskripsi dari strategi mitigasi dilakukan pencarian mitigasi secara

teknis agar dapat diimplementasikan pada masing-masing risiko. Mitigasi secara teknis ini berkaitan dengan *source code, sintax, coding* dan konfigurasi lainnya. Pencarian *source code, sintax, coding* tersebut dilakukan pada beberapa referensi di internet yang terpercaya untuk menyelesaikan masing-masing risiko. Setelah ditemukannya *source code, sintax, coding* dilakukan uji coba apakah saat melakukan implementasi *source code* muncul *error* dan dilakukan scan ulang menggunakan OWASP ZAP, apabila tidak muncul *error* dan hasil setelah dilakukan scan ulang menggunakan OWASP ZAP ternyata risiko tersebut sudah hilang maka uji coba berhasil.

3.6.3 Rekomendasi Mitigasi Risiko

Langkah terakhir yaitu rekomendasi mitigasi risiko. Dari data-data yang didapatkan dari langkah-langkah sebelumnya berupa deskripsi strategi mitigasi pada langkah menyusun strategi mitigasi dan mitigasi secara teknis serta hasilnya pada langkah uji coba desain mitigasi, digabungkan dan menjadi rekomendasi mitigasi risiko dari masing-masing risiko yang muncul supaya dapat terselesaikan permasalahan keamanan *website* tersebut. Data-data tersebut dimasukkan kedalam tabel perlakuan risiko.

Tabel 9 Desain Perlakuan Risiko Risk Register ISO 31000

ID Risiko	Strategi Mitigasi	Mitigasi secara Teknis	Hasil

BAB IV
HASIL DAN PEMBAHASAN

Pada bab 4 ini berisikan isi dari penelitian ini, semua hasil yang telah diperoleh selama dilakukannya penelitian ini dibahas pada bab ini. Hasil dan Pembahasan pada bab ini terdiri dari: Lingkup Konteks Kriteria, Pengukuran Risiko (yang terdiri dari Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko), Perlakuan Risiko dan Pembahasan.

4.1 Lingkup Konteks Kriteria

Pada Lingkup Konteks Kriteria ini menggunakan OWASP ASVS 4.0.3 untuk datanya. OWASP ASVS 4.0.3 memiliki 14 klausul yang berkaitan dengan komponen-komponen yang ada pada aplikasi berbasis *web* atau *website*. Berikut adalah deskripsi lengkap dari 14 klausul OWASP ASVS 4.0.3.

Tabel 10 Hasil Lingkup Konteks Kriteria

No	Lingkup Konteks Kriteria
1	*Architecture, Design and Threat Modeling*
2	*Authentication*
3	*Session Management*
4	*Access Control*
5	*Validation, Sanitization and Encoding*
6	*Stored Cryptography*
7	*Error Handling and Logging*
8	*Data Protection*
9	*Communication*
10	*Malicious Code*
11	*Business Logic*
12	File*s and Resources*
13	*API and Web Service*
14	*Configuration*

Architecture, Design and Threat Modeling (1), pada klausul ini membahas tentang keamanan dari segi arsitektur, desain dan pemodelan saat melakukan pengembangan suatu aplikasi atau *website*. Para pengembang harus memperhatikan keamanan-keamanan yang akan disematkan ke dalam *website* untuk menjaga agar

website yang mereka buat atau *code* yang mereka sematkan pada *website* tersebut tidak dirusak atau disalahgunakan oleh penjahat digital.

Authentication (2), klausul ini berkaitan dengan proses validasi identitas terhadap suatu pengguna untuk dapat mengakses *website* yang bersangkutan. Kontrol akses harus dicantumkan pada *website* untuk mengenali target pengguna terkait perizinan yang akan menggunakan *website* tersebut, dan agar *website* tersebut tidak jatuh ke tangan penjahat digital yang mengancam keamanan *website*.

Session Management (3), komponen ini digunakan untuk mengontrol pada saat pengguna melakukan sebuah koneksi pada suatu *website* dan kemudian informasi koneksi tersebut dapat tersimpan agar pengguna dapat langsung terhubung dengan *website* yang bersangkutan tanpa harus melakukan koneksi ulang. Komponen ini bisa menjadi celah keamanan apabila tidak dimanajemen dengan baik karena berkaitan dengan data koneksi pengguna saat melakukan koneksi pada *website* yang bersangkutan.

Access Control (4), pada klausul ini membahas tentang otorisasi yaitu mengontrol perizinan suatu akses ke sumber daya agar yang dapat mengakses sumber daya tersebut hanya orang-orang atau para pengguna yang diizinkan dan memiliki akses. Komponen ini harus diperhatikan supaya akses sumber daya suatu *website* tidak digunakan oleh pengguna yang tidak bertanggung jawab untuk melakukan kejahatan.

Validation, Sanitization and Encoding (5), komponen ini menjadi kelemahan keamanan *website* yang paling banyak terjadi yaitu kegagalan untuk melakukan validasi terhadap suatu input yang datang dari pengguna. Penjahat digital dapat melakukan serangan dari inputan ini dengan mengirim kode-kode berbahaya yang merusak *website* tersebut. Dengan dilakukannya validasi terhadap inputan yang dilakukan oleh pengguna, serangan tersebut dapat dicegah.

Stored Cryptography (6), suatu *website* harus bisa menghargai kerahasiaan data penggunanya saat melakukan penyimpanan data. Penyimpanan data yang disediakan oleh suatu *website* harus mengutamakan keamanan penyimpanan data

agar data yang tersimpan pada suatu penyimpanan tersebut dapat diakses kembali oleh pengguna sesuai dengan apa yang disimpan sebelumnya.

Error Handling and Logging (7), pada saat suatu *website* mengalami *error* sering terjadi munculnya data-data penting pada *error* tersebut, *Error Handling and Logging* sangat diperlukan pada kasus ini. Pengembang aplikasi harus melakukan kontrol terhadap *error-error* yang kemungkinan muncul pada suatu *website* agar *error* tersebut tidak menjadi celah keamanan.

Data Protection (8), kerahasiaan, integritas dan ketersediaan adalah 3 elemen kunci untuk perlindungan data yang baik. Kerahasiaan, data harus dilindungi dari aktivitas yang mencurigakan baik pada saat proses pengiriman maupun saat data sudah tersimpan. Integritas, data harus dilindungi agar tidak dapat dibuat, diubah atau dihapus oleh pengguna yang tidak berwenang. Ketersediaan, data harus tersedia untuk pengguna yang berwenang sesuai dengan kebutuhannya.

Communication (9), komunikasi antara pengembang aplikasi dan pengguna harus sering dilakukan demi tercapainya tujuan keamanan yang baik. Pengembang aplikasi dapat melakukan pelatihan atau rekomendasi yang dapat dilakukan oleh pengguna untuk meningkatkan keamanan *website* khususnya dari segi data mereka. Contohnya yaitu pengembang aplikasi merekomendasikan kepada pengguna untuk membuat sebuah password yang rumit dan tidak mudah ditebak oleh siapapun untuk meningkatkan keamanan password tersebut.

Malicious Code (10), saat melakukan pengembangan, para pengembang aplikasi harus memperhatikan *code* yang digunakan. *Code* yang digunakan haruslah aman dan tidak berbahaya ataupun memicu terjadinya bahaya. *Website* harus memiliki *security policy* yang baik untuk menjaga dari segala serangan. Contoh serangan *Malicious Code* adalah *virus, trojan, horse, logic bomb, ransomware* dan lain sebagainya.

Business Logic (11), pada klausul ini membahas tentang alur bisnis. Alur bisnis suatu *website* harus bersifat berurutan, diproses secara berurutan dan tidak dapat terlewat. Logika bisnis mencakup batasan untuk mendeteksi dan mencegah serangan yang bersifat otomatis, seperti mentransfer dana kecil terus menerus.

Logika bisnis harus mempertimbangkan dari segi kasus penyalagunaan dan pelaku kejahatan, dan memiliki perlindungan terhadap *spoofing, tampering, information disclosure dan privilege attacks.*

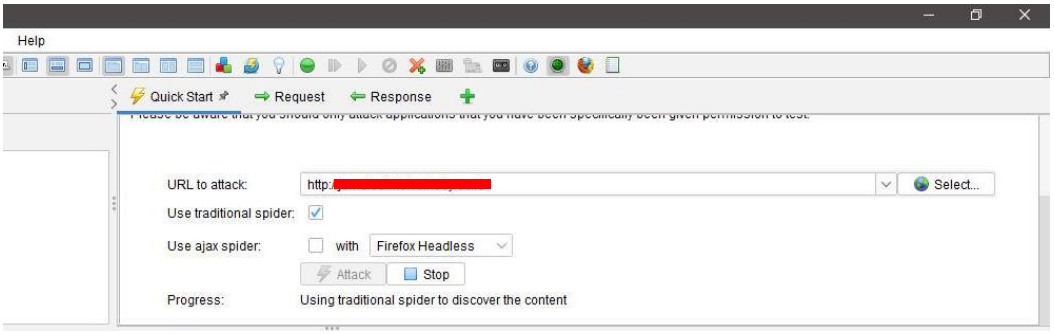
File*s and Resources* (12), *website* pasti berkaitan dengan data dan file dengan pengguna yang mengoperasikannya. Penggunaan data dan file haruslah terpercaya dengan sumber yang jelas, apabila data dan file yang diperoleh dari sumber yang tidak terpercaya atau bahkan berbahaya maka akan menjadi celah keamanan *website* tersebut. Contohnya adalah mencantumkan alamat domain lain yang terpercaya.

API and Web Service (13), klausul ini membahas tentang interface dan pelayanan *website*. *Website* dipastikan menggunakan API yang terpercaya seperti JSON atau XML atau GraphQL dan harus memastikan otentikasi yang memadai, *session management*, otorisasi semua layanan *web*. *Website* juga harus melakukan validasi terhadap input di semua parameter dan kontrol keamanan yang efektif untuk semua jenis API.

Configuration (14), *website* harus melalui tahap konfigurasi yang baik seperti menggunakan perangkat konfigurasi yang terpercaya, aman dan dapat dilakukan otomatisasi untuk mempermudah apabila terdapat suatu yang tidak aman, dapat diselesaikan dengan *source code* dan *script* secara otomatis. Selanjutnya melakukan manajemen konfigurasi sedemikian rupa agar komponen yang kadaluarsa atau tidak aman tidak dicantumkan oleh *website*.

4.2 Pengukuran Risiko

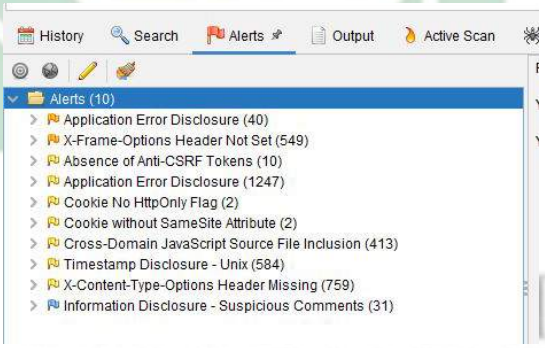
Langkah selanjutnya pada penelitian ini adalah dengan melakukan pengukuran risiko. Pengukuran risiko yang dilakukan menggunakan aplikasi atau *tools* yaitu OWASP ZAP. Caranya yaitu dengan menuliskan alamat *website* yang akan dilakukan pengukuran risiko lalu klik '*attack*' maka secara otomatis akan muncul risiko kerentanan keamanan dari *website* yang bersangkutan.



Gambar 3 Alamat *Website* Objek Penelitian

4.2.1. Identifikasi Risiko

Setelah alamat *website* dimasukkan ke dalam OWASP ZAP, maka akan muncul risiko kerentanan keamanan *website* yang bersangkutan. Terdapat 10 risiko kerentanan yang muncul yaitu: *Application Error Disclosure-1, X-Frame-Options Header Not Set, Absense of Anti-CSRF Tokens, Application Error Disclosure-2, Cookie No HttpOnly Flag, Cookie without Samesite Attribute, Cross-Domain Javascript Source* File *Inclusion, Timestamp Disclosure – Unix, X-Content-Type-Options Header Missing, Information Disclosure – Suspicious Comments.*

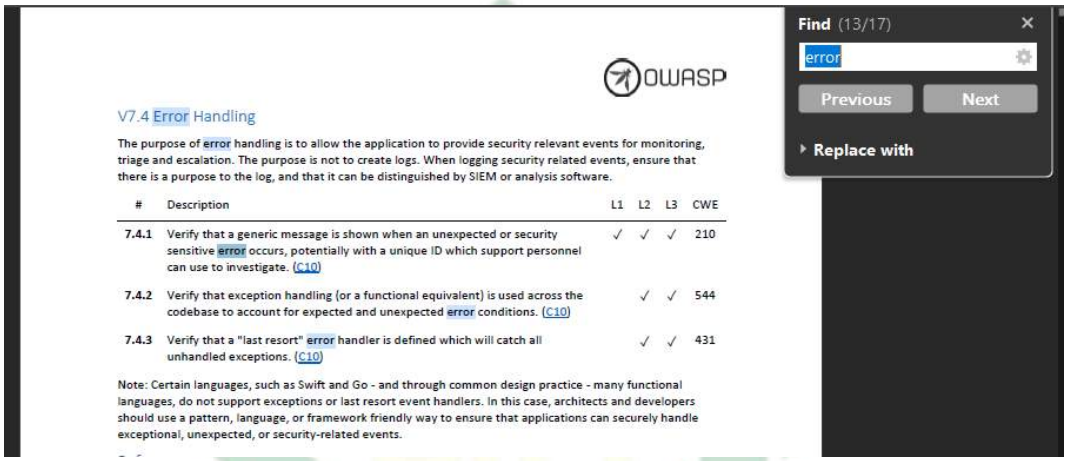


Gambar 4 Hasil Identifikasi Risiko

Langkah selanjutnya yaitu melakukan identifikasi terhadap hasil yang telah diperoleh dan dikategorikan berdasarkan Lingkup Konteks Kriteria yang menggunakan OWASP ASVS 4.0.3. Caranya yaitu dengan melakukan pencarian kata kunci dari nama risiko, deskipsi risikonya atau segala sesuatu yang berkaitan dengan risiko tersebut. Pada kasus ini hanya ada beberapa Lingkup Konteks Kriteria saya yang sesuai dengan hasil identifikasi.

4.2.1.1 *Application Error Disclosure-1*

Pada risiko ini membahas tentang *error*, OWASP ASVS versi 4.0.3 memiliki klausul yang membahas tentang *error* yaitu pada klausul tujuh yang membahas tentang *Error Handling and Logging*, namun masih belum diketahui bagian mananya risiko ini berkaitan dengan klausul tujuh. Pencarian kata kunci dilakukan dengan kata kunci "*error*" maka akan muncul banyak sekali hasil yang berkaitan dengan *error*.

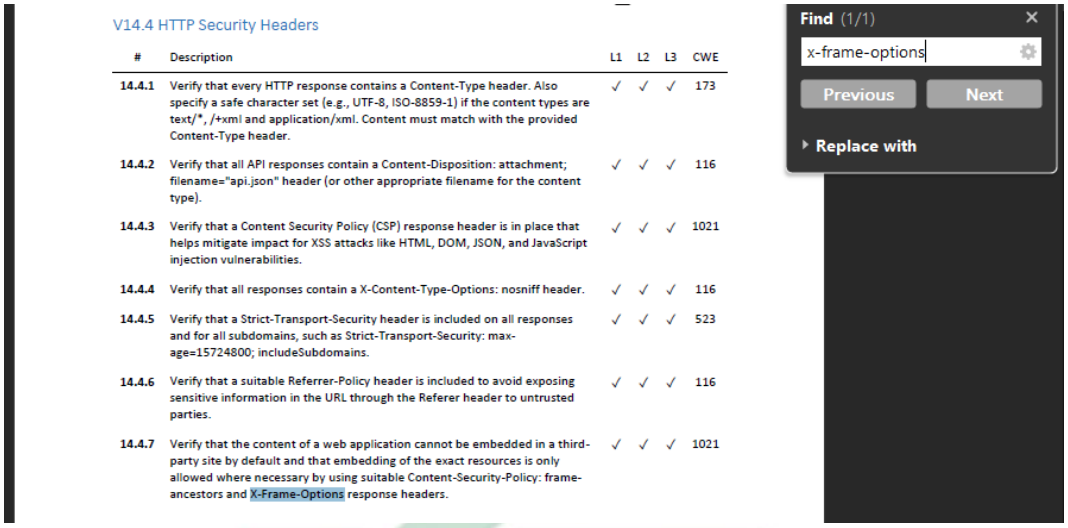


Gambar 5 Identifikasi Risiko *Application Error Disclosure-1*

Dari banyaknya hasil yang muncul, dicarilah hasil yang paling sesuai dengan risiko ini dan hasil yang paling sesuai dengan risiko ini yaitu Klausul (7) *Error Handling and Logging* Sub Klausul (7.4) *Error Handling* lalu pada nomor (7.4.1) yang berisi *"Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate"*. Maka dari hasil tersebut risiko ini berada pada Lingkup Konteks Kriteria ke 7.

4.2.1.2 *X-Frame-Options Header Not Set*

Risiko yang selanjutnya dilakukan identifikasi risiko berdasarkan Lingkup Konteks Kriterianya yaitu *X-Frame-Options Header Not Set*. Sesuai dengan namanya, risiko ini berkaitan dengan Header X-Frame-Options, maka dilakukanlah pencarian menggunakan kata kunci "X-Frame-Options" dan yang mengejutkan bahwa hanya ada satu hasil yang ada pada OWASP ASVS 4.0.3



V14.4 HTTP Security Headers

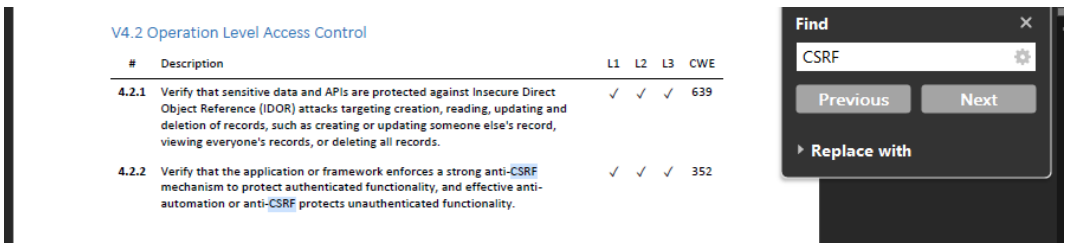
#	Description	L1	L2	L3	CWE
14.4.1	Verify that every HTTP response contains a Content-Type header. Also specify a safe character set (e.g., UTF-8, ISO-8859-1) if the content types are text/*, /+xml and application/xml. Content must match with the provided Content-Type header.	✓	✓	✓	173
14.4.2	Verify that all API responses contain a Content-Disposition: attachment; filename="api.json" header (or other appropriate filename for the content type).	✓	✓	✓	116
14.4.3	Verify that a Content Security Policy (CSP) response header is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.	✓	✓	✓	1021
14.4.4	Verify that all responses contain a X-Content-Type-Options: nosniff header.	✓	✓	✓	116
14.4.5	Verify that a Strict-Transport-Security header is included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.	✓	✓	✓	523
14.4.6	Verify that a suitable Referrer-Policy header is included to avoid exposing sensitive information in the URL through the Referer header to untrusted parties.	✓	✓	✓	116
14.4.7	Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response headers.	✓	✓	✓	1021

Gambar 6 Identifikasi Risiko *X-Frame-Options Header Not Set*

Pencarian yang dihasilkan yaitu Klausul (14) *Configuration* Sub Klausul (14.4) *HTTP Security Headers* dan pada nomor (14.4.7) yang berisi *"Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response header"*. Dengan hasil tersebut maka risiko ini termasuk pada *Configuration* dalam Lingkup Konteks Kriteria

4.2.1.3 *Absense of Anti-CSRF Tokens*

Pada risiko ini membahas tentang *Anti-CSRF Tokens*, maka dilakukanlah pencarian dengan kata kunci tersebut namun tidak muncul hasil apapun. Setelah itu dilakukanlah pencarian kata kunci yang lebih sedikit untuk memperbesar kemungkinan hasil yang diperoleh, kata kunci yang digunakan selanjutnya yaitu "CSRF" dan akhirnya muncullah beberapa hasil yang berkaitan dengan CSRF.



V4.2 Operation Level Access Control

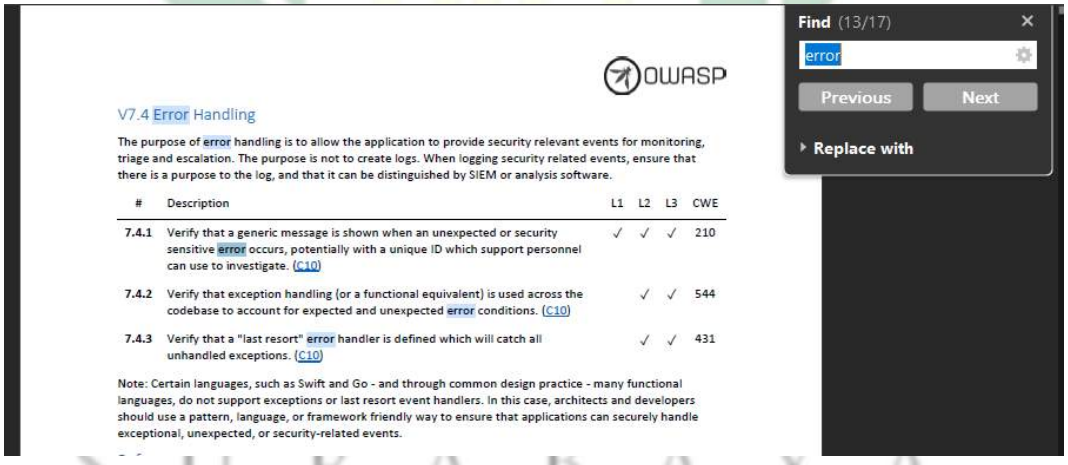
#	Description	L1	L2	L3	CWE
4.2.1	Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	✓	✓	✓	639
4.2.2	Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	✓	✓	✓	352

Gambar 7 Identifikasi Risiko *Absense of Anti-CSRF Tokens*

Pada beberapa hasil yang muncul tersebut dilakukan pencarian lebih lanjut dan yang paling sesuai dengan risiko ini berada pada Klausul (4) *Access Control* Sub Klausul (4.2) *Operation Level Access Control* dan pada nomor (4.2.2) yang berisi *"Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality"*. Oleh sebab itu risiko ini berada pada Lingkup Konteks Kriteria *Access Control*.

4.2.1.4 *Application Error Disclosure-2*

Pada risiko ini membahas tentang *error*, OWASP ASVS versi 4.0.3 memiliki klausul yang membahas tentang *error* yaitu pada klausul 7 yang membahas tentang *Error Handling and Logging*, namun masih belum diketahui bagian mananya risiko ini berkaitan dengan klausul 7. Pencarian kata kunci dilakukan dengan kata kunci "*error*" maka akan muncul banyak sekali hasil yang berkaitan dengan *error*.

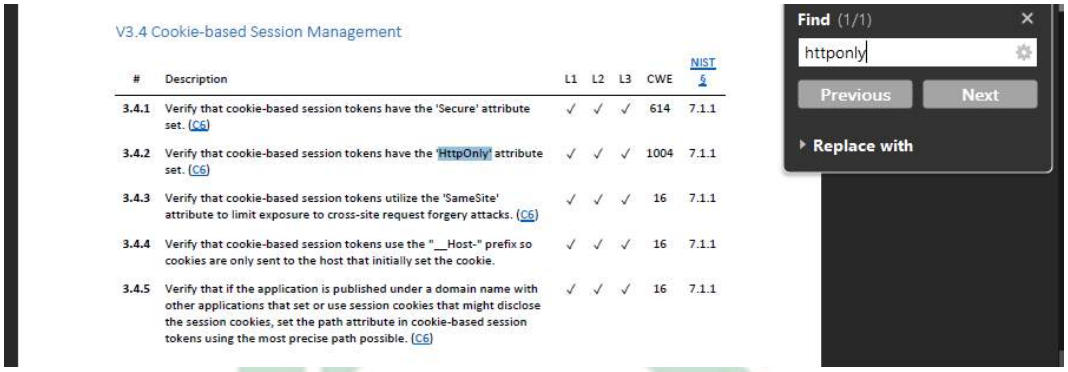


Gambar 8 Identifikasi Risiko *Application Error Disclosure-2*

Dari banyaknya hasil yang muncul, dicarilah hasil yang paling sesuai dengan risiko ini dan hasil yang paling sesuai dengan risiko ini berada pada sub klausul 7.4 yaitu *Error Handling* lalu pada nomor 7.4.1 yang berisi *"Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate"*. Maka dari hasil tersebut risiko ini berada pada Lingkup Konteks Kriteria ke 7.

4.2.1.5 *Cookie No HttpOnly Flag*

Risiko selanjutnya yang dilakukan identifikasi risiko berdasarkan Lingkup Konteks Kriterianya yaitu *Cookie No HttpOnly Flag*. Sesuai dengan namanya risiko ini berkaitan dengan *Cookie* dan HttpOnly, namun apabila kata kunci yang digunakan adalah *Cookie* maka akan muncul banyak hasil dan membuat pencarian menjadi lama, oleh sebab itu kata kunci yang digunakan adalah "Http Only".



V3.4 Cookie-based Session Management

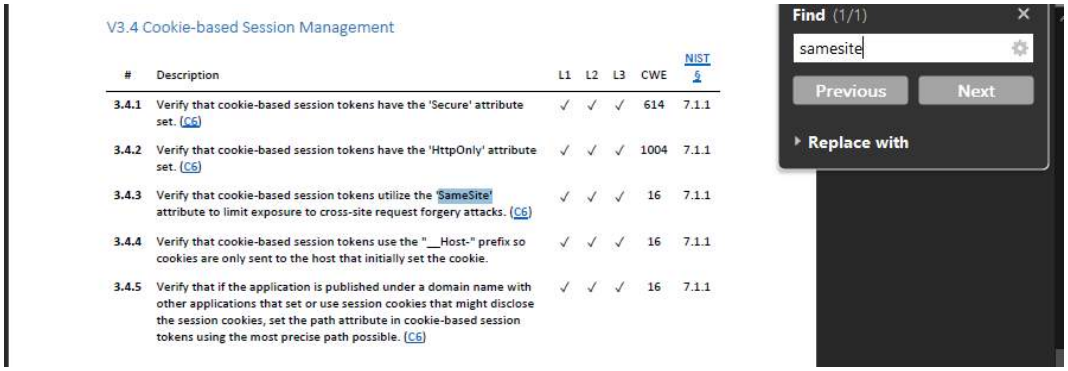
#	Description	L1	L2	L3	CWE	NIST §
3.4.1	Verify that cookie-based session tokens have the 'Secure' attribute set. (C6)	✓	✓	✓	614	7.1.1
3.4.2	Verify that cookie-based session tokens have the 'HttpOnly' attribute set. (C6)	✓	✓	✓	1004	7.1.1
3.4.3	Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks. (C6)	✓	✓	✓	16	7.1.1
3.4.4	Verify that cookie-based session tokens use the "__Host-" prefix so cookies are only sent to the host that initially set the cookie.	✓	✓	✓	16	7.1.1
3.4.5	Verify that if the application is published under a domain name with other applications that set or use session cookies that might disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible. (C6)	✓	✓	✓	16	7.1.1

Gambar 9 Identifikasi Risiko *Cookie* No HttpOnly Flag

Sesuai dengan hasil yang diharapkan, hasil yang muncul hanya satu saja yaitu pada Klausul (3) *Session Management* dengan Sub Klausul (3.4) *Cookie-based Session Management* dan nomor (3.4.2) yang berisikan *"Verify that cookie-based session tokens have the 'HttpOnly' attribute set"*. Dari hasil tersebut dapat disimpulkan bahwa risiko ini berada pada Lingkup Konteks Kriteria yaitu *Session Management*.

4.2.1.6 *Cookie without Samesite Attribute*

Pada risiko ini juga membahas tentang *Cookie* namun pada kasus ini ada yang berbeda yaitu Samesite. Tentunya kata kunci yang digunakan adalah *Samesite* karena untuk mempersempit hasil yang muncul supaya lebih cepat dalam melakukan pencarian. Dan sesuai dengan harapan sebelumnya, saat menggunakan kata kunci "Samesite" muncul satu hasil yang paling sesuai dengan risiko ini.

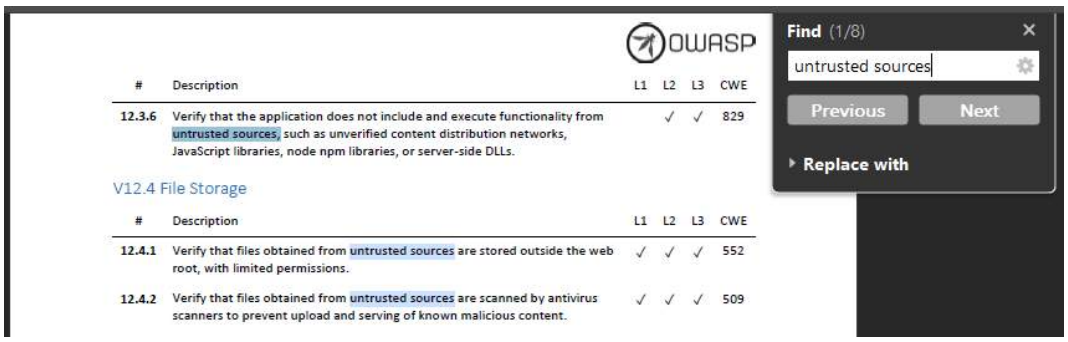


Gambar 10 Identifikasi Risiko *Cookie without Samesite Attribute*

Hasil yang didapatkan saat melakukan pencarian yaitu berada pada Klausul (3) *Session Management* sama seperti risiko sebelumnya, lalu Sub Klausul (3.4) *Cookie-based Session Management* sama juga seperti risiko sebelumnya, namun dengan nomor yang berbeda yaitu (3.4.3) yang berisi tentang *"Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks"*. Oleh sebab itu risiko ini berada pada Lingkup Konteks Kriteria *Session Management.*

4.2.1.7 *Cross-Domain JavaScript Source* File *Inclusion*

Pada risiko ini membahas tentang *Cross-Domain JavaScript Source*, namun pada saat dilakukan pencarian kata kunci dengan kata-kata tersebut, tidak ditemukannya hasil apapun bahkan perkatapun tidak muncul hasil yang sesuai. Lalu dilakukannya pencarian menggunakan kata kunci persamaan kata dari kata tersebut, dan masih tidak ditemukan hasil yang sesuai. Akhirnya setelah memahami maksud dari risiko ini, terdapat kata-kata yang paling relevan dengan risiko ini yaitu "*Untrusted Sources*"

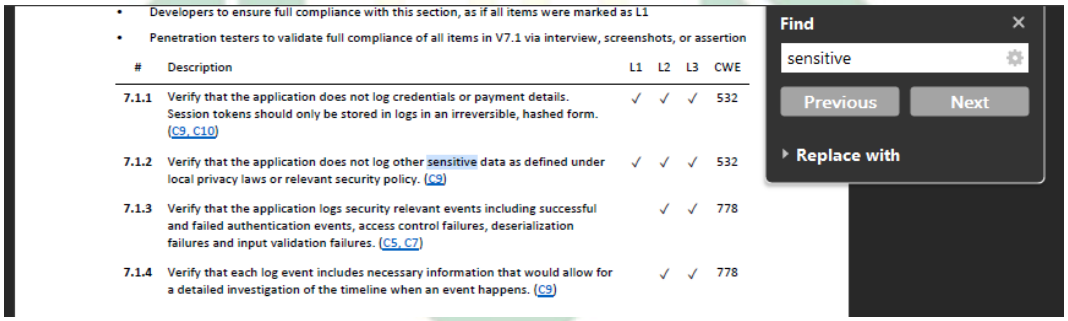


Gambar 11 Identifikasi Risiko Cross-Domain Java*Script* Source File Inclusion

Dari pencarian menggunakan kata kunci tersebut, munculah beberapa hasil dan hasil yang paling sesuai dengan risiko ini yaitu pada Klausul (12) File*s and Resources* lalu pada Sub Klausul (12.3) File *Execution* dan pada nomor (12.3.6) yang berisi *"Verify that* file*s obtained from untrusted sources are validated to be of expected type based on the* file*'s content"*. Oleh sebab itu risiko ini berada pada Lingkup Konteks Kriteria File*s and Resources*.

4.2.1.8 *Timestamp Disclosure*

Risiko selanjutnya yang dilakukan identifikasi risiko yaitu *Timestamp Disclosure*. Pencarian kata kunci ini agak susah karena dari namanya saat dilakukan search tidak ada hasil yang relevan dengan risiko ini. Setelah dilakukannya pemahaman dari maksud risiko ini dapat diambil kata kunci yaitu *sensitive data*. Dan saat dilakukan search banyak hasil yang merujuk pada risiko ini, namun terdapat satu hasil yang paling relevan dan paling sesuai dengan risiko ini.



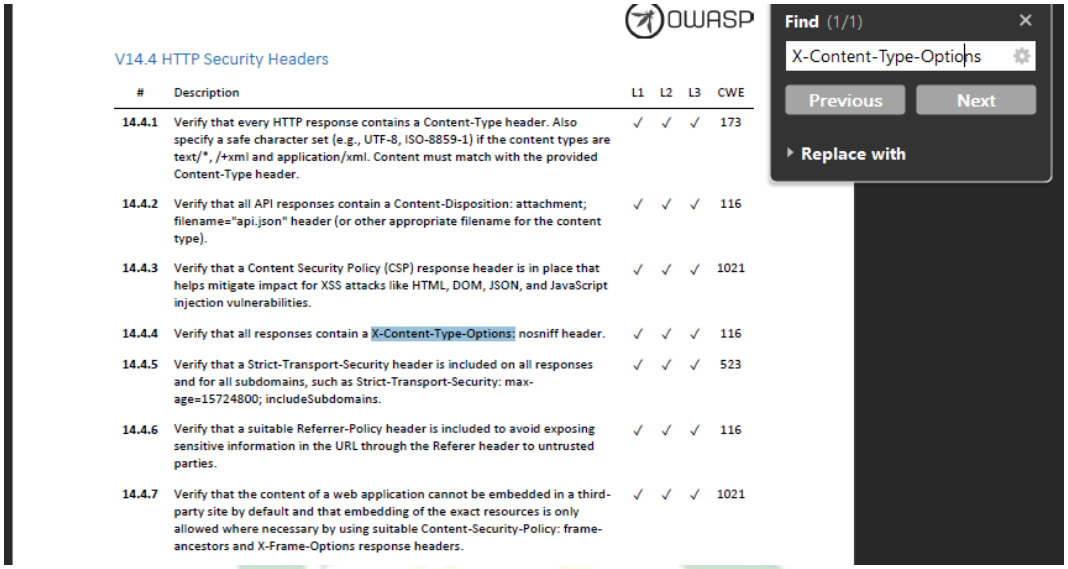
Gambar 12 Identifikasi Risiko *Timestamp Disclosure*

Hasil yang paling relevan dan paling sesuai dengan risiko ini yaitu pada Klausul (7) *Error Handling and Logging* di Sub Klausul (7.1) *Log Content* dan pada nomor 7.1.2 yang berisi tentang *"Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy"*. Dengan alasan itulah risiko ini berada pada Lingkup Konteks Kriteria *Error Handling and Logging.*

4.2.1.9 *X-Content-Type-Options Header Missing*

Pada risiko ini yang dibahas berkaitan dengan X-Content-Type-Options, dan dilakukanlah percarian dengan kata kunci tersebut. Risiko ini mudah sekali dicari karena memiliki kata kunci yang sesuai dengan isi dari OWASP ASVS versi

4.0.3. Dari pencarian kata kunci tersebut muncul satu hasil dan hanya satu yang paling sesuai dengan kasus dari risiko ini.



V14.4 HTTP Security Headers

#	Description	L1	L2	L3	CWE
14.4.1	Verify that every HTTP response contains a Content-Type header. Also specify a safe character set (e.g., UTF-8, ISO-8859-1) if the content types are text/*, /+xml and application/xml. Content must match with the provided Content-Type header.	✓	✓	✓	173
14.4.2	Verify that all API responses contain a Content-Disposition: attachment; filename="api.json" header (or other appropriate filename for the content type).	✓	✓	✓	116
14.4.3	Verify that a Content Security Policy (CSP) response header is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.	✓	✓	✓	1021
14.4.4	Verify that all responses contain a X-Content-Type-Options: nosniff header.	✓	✓	✓	116
14.4.5	Verify that a Strict-Transport-Security header is included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.	✓	✓	✓	523
14.4.6	Verify that a suitable Referrer-Policy header is included to avoid exposing sensitive information in the URL through the Referer header to untrusted parties.	✓	✓	✓	116
14.4.7	Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response headers.	✓	✓	✓	1021

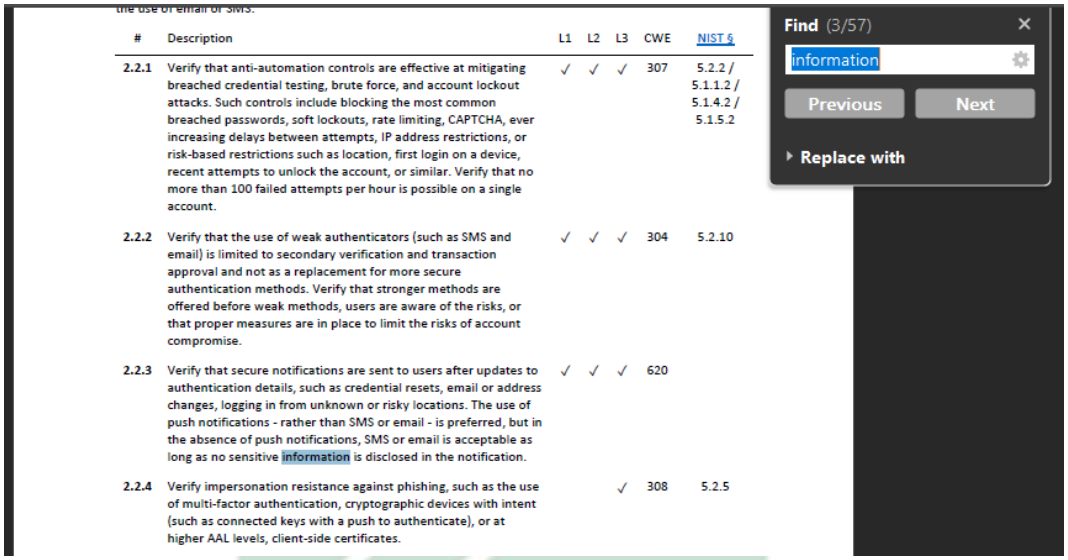
Find (1/1)
X-Content-Type-Options
Previous
Next
Replace with

Gambar 13 Identifikasi Risiko *X-Content-Type-Options Header Missing*

Risiko ini ditemukan pada OWASP ASVS versi 4.0.3 pada Klausul (14) *Configuration* dan dengan Sub Klausul (14.4) *HTTP Security Headers* serta pada nomor 14.4.4 yang membahas tentang *"Verify that all responses contain a X-Content-Type-Options: nosniff header"*. Dengan ditemukannya hasil yang sesuai dengan Klausul yang bersangkutan, risiko ini berada pada Lingkup Konteks Kriteria *Configuration*.

4.2.1.10 *Information Disclosure*

Risiko selanjutnya pada identifikasi risiko ini adalah *Information Disclosure*. Pencarian yang dilakukan pada risiko ini menggunakan kata kunci *Information*, dan yang mengejutkan adalah hasil yang didapatkan sangat banyak dan sulit untuk mencari hasil yang paling sesuai dengan risiko ini. Namun setelah dilakukannya pencarian lebih mendalam, terdapat satu hasil yang paling sesuai dan relevan dengan risiko ini.



the use of email or SMS.

#	Description	L1	L2	L3	CWE	NIST §
2.2.1	Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	✓	✓	✓	307	5.2.2 / 5.1.1.2 / 5.1.4.2 / 5.1.5.2
2.2.2	Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.	✓	✓	✓	304	5.2.10
2.2.3	Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.	✓	✓	✓	620	
2.2.4	Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.			✓	308	5.2.5

Find (3/57)
information
Previous
Next
Replace with

Gambar 14 Identifikasi Risiko *Information Disclosure*

Satu hasil yang paling sesuai dan relevan pada risiko ini yaitu pada Klausul (2) *Authentication* dengan Sub Klausul (2.2) *General Authenticator Security* dan pada nomor 2.2.3 yang berisi *"Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification"*. Berdasarkan dari hasil yang didapatkan, maka risiko ini berada pada Lingkup Konteks Kriteria *Authentication*.

4.2.1.11 Rekap Hasil Identifikasi Risiko

Setelah dilakukannya pencarian risiko yang paling sesuai dan relevan dengan OWASP ASVS versi 4.0.3 yang menjadi Lingkup, Konteks, Kriteria langkah selanjutnya yang akan dilakukan yaitu memberikan kode atau ID untuk masing-masing risiko yang bersangkutan. Pemberian ID risiko ini nantinya akan mempermudah pada saat melakukan langkah selanjutnya, supaya tertata dengan baik, rapi dan mudah dipahami oleh orang lain. Hasilnya dapat dilihat pada tabel berikut ini.

Tabel 11 Hasil Identifikasi Risiko

No	Lingkup, Konteks, Kriteria	Identifikasi Risiko	ID Risiko
1	*Architecture, Design and Threat Modeling*	-	
2	*Authentication*	*Information Disclosure*	*Risk1*
3	*Session Management*	*Cookie No HttpOnly Flag*	*Risk2*
		Cookie without SameSite Attribute	*Risk3*
4	*Access Control*	*Absence of Anti-CSRF Tokens*	*Risk4*
5	*Validation, Sanitization and Encoding*	-	
6	*Stored Cryptography*	-	
7	*Error Handling and Logging*	*Application Error Disclosure-1*	*Risk5*
		Application Error Disclosure-2	*Risk6*
		Timestamp Disclosure	*Risk7*
8	*Data Protection*	-	
9	*Communication*	-	
10	*Malicious Code*	-	
11	*Business Logic*	-	
12	Files *and Resources*	*Cross-Domain JavaScript Source* File *Inclusion*	*Risk8*
13	*API and Web Service*	-	
14	*Configuration*	*X-Frame-Options Header Not Set*	*Risk9*
		X-Content-Type-Options Header Missing	*Risk10*

4.2.2. Analisis Risiko

Langkah selanjutnya melakukan analisis risiko dari hasil yang telah muncul pada aplikasi atau *tools* OWASP ZAP. Pada *tools* tersebut dapat terlihat nama risiko, tingkat risikonya dan deskripsi risiko tersebut. Pada kasus ini terdapat 2 risiko dengan tingkat risiko *medium* yang digambarkan dengan warna jingga, 7 risiko dengan tingkat risiko *low* yang digambarkan dengan warna kuning, dan 1 risiko dengan tingkat risiko *informational* yang digambarkan dengan warna biru.

Selanjutnya terdapat deskripsi yang menjelaskan kasus yang muncul dari masing-masing risiko dan telah diterjemahkan ke dalam bahasa Indonesia dengan penjelasan yang mudah untuk dimengerti. *Tools* ini juga dapat memunculkan bagian yang menyebabkan risiko keamanan muncul berupa halaman *website* yang bersangkutan dan mengarah pada fitur tertentu. Berikut adalah deskripsi yang muncul pada *tools* OWASP ZAP.

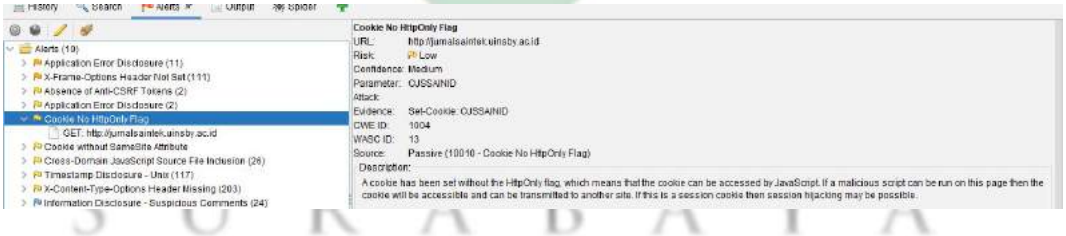
4.2.2.1 *Information Disclosure* (Risk1)

Risk1 pada penelitian ini yaitu *Information Disclosure* dengan tingkat risiko *informational*, pada kasus ini OWASP ZAP menjelaskan bahwa pada *website* yang sedang dianalisis mengandung *comment*, *comment* pada suatu *website* ditakutkan akan membantu *hacker* atau *penjahat digital* dalam menjalankan rencana jahat mereka dalam melakukan *hack* pada *website* yang bersangkutan karena ditakutkan terdapat informasi yang penting di dalamnya.

Gambar 15 Analisis Risiko *Information Disclosure* (Risk1)

4.2.2.2 *Cookie No HttpOnly Flag* (Risk2)

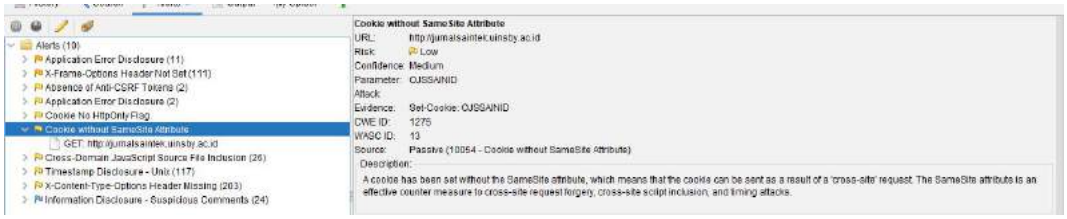
Risk2 yaitu *Cookie No HttpOnly Flag* dengan tingkat risiko *low*, *cookie* tidak di setting pada *HttpOnly* hal ini berarti *cookie* dapat diakses oleh Java*script*. Jika *script* berbahaya dapat dijalankan pada halaman ini, maka *cookie* dapat diakses dan ditransmisikan ke situs lain. Jika ini adalah *cookie* session, maka pembajakan session kemungkinan bisa terjadi.



Gambar 16 Analisis Risiko *Cookie No HttpOnly Flag* (Risk2)

4.2.2.3 *Cookie without Samesite Attribute* (Risk3)

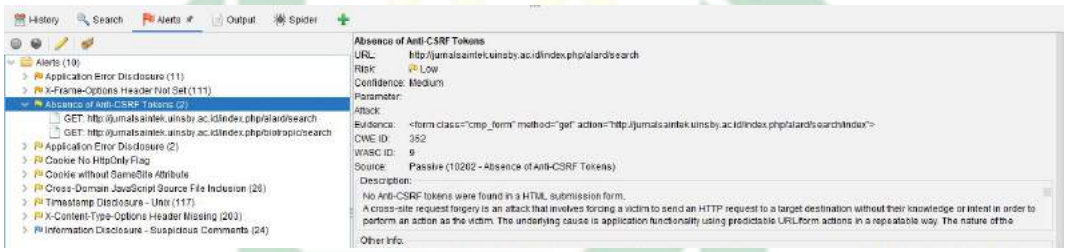
Risiko selanjutnya dengan ID Risiko – Risk3 yaitu *Cookie without Samesite Attribute* dengan tingkat risiko *low*, *cookie* di setting pada Samesite namun attributenya di setting ke “none”, yang berarti *cookie* dapat dikirim sebagai hasil dari *cross-site request*. *Samesite Attribute* adalah tindakan balasan yang efektif untuk *cross-site request forgery, cross-site inclusion, dan timing attack.*



Gambar 17 Analisis Risiko *Cookie without Samesite Attribute* (Risk3)

4.2.2.4 *Absense of Anti-CSRF Tokens* (Risk4)

Selanjutnya Risk4 yaitu *Absense of Anti-CSRF Tokens* dengan tingkat risiko *low*, tidak adanya token anti CSRF yang ditemukan dalam HTML submission form. CSRF atau Cross-Site Request Forgery adalah serangan yang memungkinkan penjahat digital melakukan permintaan HTTP seperti *Get, Post, Delete*, dan *Put* yang tidak sah atas nama korban saat diautentikasi ke *website*. Pembajakan *session* juga mendukung serangan CSRF.



Gambar 18 Analisis Risiko *Absense of Anti-CSRF Tokens* (Risk4)

4.2.2.5 *Application Error Disclosure-1* (Risk5)

Risk5 yaitu *Application Error Disclosure*-1 dengan tingkat risiko *medium*, terdapat 2 kasus risiko pada tipe ini, dan untuk kasus risiko ini yaitu terdapat halaman yang memunculkan *Directory Listing* yang berisikan file-file yang kemungkinan penting. *Directory Listing* ini mencantumkan file-file yang ada pada *website* yang bersangkutan dapat dimanfaatkan penjahat digital untuk mendownloadnya, mengubahnya, dan menghapusnya.

Gambar 19 Analisis Risiko *Application Error Disclosure-1* (Risk5)

4.2.2.6 *Application Error Disclosure-2* (Risk6)

Risiko selanjutnya yaitu Risk6 yaitu *Application Error Disclosure-2* dengan tingkat risiko *low*, pada kasus ini dikarenakan munculnya *error* 500, *error* 500 kemungkinan dapat memunculkan data-data sensitif yang penting dan seharusnya tidak dimunculkan, ini menjadi celah keamanan pada *website* tersebut dan kemungkinan dapat dimanfaatkan penjahat digital untuk menggunakan data yang bersifat sangat penting tersebut dengan tidak bertanggung jawab untuk berbuat jahat.

Gambar 20 Analisis Risiko *Application Error Disclosure-2* (Risk6)

4.2.2.7 *Timestamp Disclosure* (Risk7)

Risk7 yaitu *Timestamp Disclosure* dengan tingkat risiko *low*, pada kasus ini OWASP ZAP menjelaskan bahwa *website* yang sedang kita analisis mengandung *timestamp* atau stempel waktu yang muncul secara terbuka. *Timestamp* atau stempel waktu adalah urutan angka yang berisikan waktu kapan suatu peristiwa terjadi, untuk kasus ini yang berarti waktu dari suatu data. Urutan angka tersebut kemungkinan berisikan pukul, tanggal, bulan, tahun dan informasi sejenisnya.

Gambar 21 Analisis Risiko *Timestamp Disclosure* (Risk7)

4.2.2.8 *Cross-Domain JavaScript Source* File *Inclusion* (Risk8)

Risiko selanjutnya Risk8 yaitu *Cross-Domain JavaScript Source* File *Inclusion* dengan tingkat risiko *low*, pada kasus ini OWASP ZAP membaca bahwa aplikasi atau *website* kita mengandung link atau domain lain. Apabila link domain yang ada pada *website* tersebut adalah domain yang berbahaya, maka akan membahayakan pula pengguna *website* kita karena *website* kita yang telah membagikan link domain *website* tersebut.

Gambar 22 Analisis Risiko *Cross-Domain JavaScript Source* File *Inclusion* (Risk8)

4.2.2.9 *X-Frame-Options Header Not Set* (Risk9)

Risk9 yaitu *X-Frame-Options Header Not Set* dengan tingkat risiko *medium*, *Header X-Frame-Options* tidak ada. Fungsi dari *Header X-Frame-Options* adalah untuk melindungi *website* dari serangan 'ClickJacking'. ClickJacking adalah sebuah jenis serangan *website* yang membuat penggunanya secara tidak sengaja mengklik elemen pada halaman *web* yang tidak ingin diklik.

Gambar 23 Analisis Risiko *X-Frame-Options Header Not Set* (Risk9)

4.2.2.10 *X-Content-Type-Options Header Missing* (Risk10)

Risiko selanjutnya Risk10 yaitu *X-Content-Type-Options Header Missing*, Header X-Content-Type-Options tidak ada, hal tersebut menyebabkan kemungkinan munculnya serangan XSS atau *Cross Site Scripting*. XSS atau *Cross Site Scripting* adalah serangan *website* yang menggunakan *code* berbahaya yang dapat dieksekusi oleh halaman yang bersangkutan, serangan tersebut dapat mencuri session pengguna dan menyamar sebagai pengguna tersebut.

Gambar 24 Analisis Risiko *X-Content-Type-Options Header Missing* (Risk10)

4.2.2.11 Hasil Rekap Analisis Risiko

Dari hasil yang telah didapatkan dari OWASP ZAP saat melakukan analisis risiko, langkah selanjutnya yaitu menuliskan hasil yang telah didapatkan yaitu dari Tingkat Risiko dan juga Deskripsi sesuai dengan masing-masing risiko. Hasilnya berada pada tabel 10 berikut ini.

Tabel 12 Hasil Analisis Risiko

ID Risiko	Identifikasi Risiko	Analisis Risiko	
		Tingkat Risiko	Deskripsi
Risk1	*Information Disclosure*	*Informational*	*Website* mengandung *comment* yang kemungkinan

			terdapat informasi penting yang dapat membantu *hacker* dalam melakukan *hack*
Risk2	*Cookie No HttpOnly Flag*	*Low*	*Cookie* tidak di setting pada *HttpOnly*, yang berarti *cookie* dapat diakses oleh Java*Script*. Jika *script* berbahaya dapat dijalankan di halaman ini, maka *cookie* akan dapat diakses dan dapat ditransmisikan ke situs lain. Jika ini adalah *cookie* session, maka pembajakan session mungkin terjadi.
Risk3	*Cookie without SameSite Attribute*	*Low*	*Cookie* telah disetel dengan SameSite attributenya disetel ke *none*, yang berarti bahwa *cookie* dapat dikirim sebagai hasil dari *cross-site* request. The SameSite attribute adalah tindakan balasan yang efektif untuk pemalsuan cross-site request, cross-site *script* inclusion, dan timing attacks.
Risk4	*Absence of Anti-CSRF Tokens*	*Low*	Tidak ada token Anti CSRF yang ditemukan dalam HTML submission form
Risk5	*Application Error Disclosure-1*	*Medium*	Halaman ini memunculkan directory listing yang berisikan file-file yang kemungkinan penting.
Risk6	*Application Error Disclosure-2*	*Low*	Halaman ini berisi pesan *error* yang mungkin mengungkapkan informasi sensitif seperti lokasi file yang menghasilkan pengecualian yang tidak tertangani. Informasi ini dapat digunakan untuk meluncurkan serangan lebih lanjut terhadap aplikasi *web*.
Risk7	*Timestamp Disclosure*	*Low*	Timestamp muncul pada *website*.
Risk8	*Cross-Domain JavaScript Source File Inclusion*	*Low*	*Website* berisi domain dari *website* lain
Risk9	*X-Frame-Options Header Not Set*	*Medium*	*Header X-Frame-Options* tidak ada. Fungsi dari *Header X-Frame-Options* adalah untuk melindungi *website* dari serangan *ClickJacking*. *ClickJacking* adalah sebuah

			jenis serangan *website* yang membuat penggunanya secara tidak sengaja mengklik elemen pada halaman *web* yang tidak ingin di klik.
Risk10	*X-Content-Type-Options Header Missing*	*Low*	Header X-Content-Type-Options tidak ada, hal tersebut menyebabkan munculnya serangan XSS atau Cross Site *Script*ing. XSS atau Cross Site *Script*ing adalah serangan *website* menggunakan code berbahaya yang dapat dieksekusi oleh halaman *website*, serangan tersebut dapat mencuri session client dan menyamar sebagai client tersebut.

4.2.3. Evaluasi Risiko

Pada tahap terakhir pada pengukuran risiko adalah dengan melakukan evaluasi risiko. Aktivitas pada tahap ini adalah dengan melakukan evaluasi terhadap risiko yang telah diidentifikasi dan dianalisis sebelumnya dan melakukan pengambilan keputusan apa yang akan dilakukan terhadap risiko-risiko tersebut, yang berarti pada tahap evaluasi risiko ini menentukan hasil nantinya pada saat melakukan perlakuan risiko karena tahap ini akan menentukan risiko mana yang perlu dilakukan mitigasi dan yang tidak perlu. Terdapat 4 jenis pengambilan keputusan pada tahap evaluasi risiko ini yaitu: *Tolerate*, *Treat*, Transfer dan Terminate serta diperlukannya aturan dari masing-masing keputusan tersebut.

Tabel 13 Aturan Evaluasi Risiko

Tingkat Risiko	Aturan
Informational	*Tolerate*
Low	*Tolerate* (Jika data yang terkait bukanlah data sensitif) atau *Treat* (Jika data yang terkait adalah data sensitif)
Medium	*Treat*
High	*Transfer*
Very High	*Terminate*

Tolerate yaitu mentoleransi risiko yang ada dan tidak melakukan mitigasi apapun dengan alasan tingkat risiko yang dihasilnya rendah untuk kasus ini tingkat risikonya adalah *informational dan low* karena data yang terkait pada risiko tersebut bukanlah data yang sensitif, namun terdapat beberapa risiko dengan tingkat risiko *low* yang tetap dilakukan mitigasi atau *treat*.

Treat yaitu melakukan mitigasi dengan sumber daya manusia sendiri tanpa perlu bantuan dari pihak ketiga atau pihak lainnya dengan alasan tingkat risiko yang dihasilkan cukup berbahaya pada kasus ini tingkat risikonya adalah *low* dan *medium*. Pada kasus ini terdapat beberapa risiko yang memiliki tingkat risiko low perlu dilakukan mitigasi karena data yang terkait pada risiko tersebut adalah data sensitif.

Transfer yaitu melakukan mitigasi risiko dengan menggunakan bantuan dari pihak ketiga atau pihak lain karena sumber daya manusia yang dimiliki tidak berhasil melakukan mitigasi risiko secara mandiri oleh sebab itu perlu bantuan dari pihak yang mengerti dengan risiko terkait dan tingkat risiko yang tinggi yaitu *high*. Namun pada kasus ini tidak ditemukan risiko dengan tingkat risiko high sehingga tidak ada evaluasi risiko dengan pengambilan keputusan menggunakan Transfer.

Terminate yaitu melakukan penghapusan fitur pada aplikasi yang bersangkutan dengan alasan karena tingkat risiko yang sangat tinggi yaitu *very high* dan sangat berbahaya untuk *website* apabila masih tetap dipertahankan. Namun pada kasus ini tidak ditemukan risiko yang memiliki tingkat risiko *very high*, oleh sebab itu pada evaluasi risiko ini tidak menggunakan keputusan Terminate.

4.2.3.1 *Information Disclosure* (Risk1)

Pertama yaitu risk1 yang membahas tentang *Information Disclosure*. Risiko ini mendapatkan evaluasi risiko *Tolerate* karena risiko ini memiliki tingkat risiko *Informational*, pada aturan yang telah dibuat pada penelitian ini apabila terdapat risiko yang memiliki tingkat risiko *informational* maka evaluasi yang diberikan yaitu *Tolerate*. *Tolerate* ini artinya tidak dilakukan mitigasi risiko terhadap risiko yang bersangkutan.

4.2.3.2 *Cookie No HttpOnly Flag* (Risk2)

Risiko yang kedua yaitu *Cookie No HttpOnly Flag*. Risiko ini mendapatkan evaluasi risiko *Treat* karena risiko ini memiliki tingkat risiko *Low* dan risiko ini berkaitan dengan data sensitif yaitu *Cookie*. *Cookie* pada dasarnya dapat menyimpan data riwayat kunjungan ke suatu *website* untuk mempermudah penggunanya supaya tidak perlu melakukan login ulang. Dengan alasan tersebut maka risiko ini harus dilakukan mitigasi supaya tidak terjadi pencurian data *cookie* tersebut.

4.2.3.3 *Cookie without SameSite Attribute* (Risk3)

Risiko yang selanjutnya yaitu *Cookie without SameSite Attribute*. Sama seperti risiko sebelumnya yang membahas tentang *cookie*, *cookie* juga menyimpan data dari penggunanya melalui browser. Pada kasus ini walaupun sama-sama membahas tentang *cookie*, namun mitigasi yang dilakukan berbeda. Risiko ini dapat dimanfaatkan hacker untuk melakukan *cross-site request forgery*, *cross-site script inclusion*, dan *timing attacks*. Oleh sebab itu risiko ini mendapat evaluasi risiko *Treat*.

4.2.3.4 *Absence of Anti-CSRF Tokens* (Risk4)

Risiko yang keempat yaitu *Absence of Anti-CSRF Tokens*. Risiko ini mendapatkan evaluasi risiko *Tolerate* karena pada dasarnya *Anti-CSRF Tokens* ditambahkan kedalam inputan pada saat login, terdapat beberapa kasus penyerangan dimana hacker melakukan kecurangan saat login. Oleh sebab itu diperlukannya *Anti-CSRF Tokens* namun pada kasus *website* yang menjadi obyek penelitian ini terdeteksi pada inputan *Search* yang tidak perlu ditambahkan *Anti-CSRF Tokens*. Dengan alasan itulah risiko ini mendapatkan evaluasi risiko *Tolerate*.

4.2.3.5 *Application Error Disclosure-1* (Risk5)

Risiko yang kelima yaitu *Application Error Disclosure-1*. Risiko ini mendapatkan evaluasi risiko *Treat* karena tingkat risiko pada risiko ini *medium*. Sesuai dengan aturan yang telah dibuat sebelumnya bahwa apabila terdapat risiko yang memiliki tingkat risiko *medium*, maka evaluasi risiko yang didapatkan yaitu *Treat*. Mitigasi perlu dilakukan pada risiko ini karena dapat berbahaya apabila

dibiarkan karena pada risiko ini memunculkan file-file yang menjadi komponen pada *website* ini. File-file tersebut juga dapat dimanipulasi dan dapat merusak *website*.

4.2.3.6 *Application Error Disclosure-2* (Risk6)

Risiko selanjutnya yaitu *Application Error Disclosure-2*. Risiko ini berbeda dengan risiko sebelumnya walaupun namanya terlihat sama tingkat risikonya juga berbeda yaitu *Low*, kasus yang terjadi pada risiko ini yaitu munculnya pesan *error* 500 yang ada pada suatu fitur. Pesan *error* yang muncul pada fitur tersebut sudah ditangani oleh halaman *error* yang sudah tersedia pada *website* tersebut dan tidak memunculkan data-data yang sensitif. Jadi evaluasi risiko yang didapatkan pada risiko ini yaitu *Tolerate*.

4.2.3.7 *Timestamp Disclosure* (Risk7)

Risiko selanjutnya yaitu Risk7 - *Timestamp Disclosure*. Risiko ini mendapatkan evaluasi risiko *Tolerate* karena timestamp yang dimunculkan pada *website* ini bukanlah data yang sensitif. Pada OWASP ZAP sendiri terdapat deskripsi bahwa diperlukannya pengecekan secara manual apakah timestamp tersebut merupakan data sensitif atau bukan, dan setelah dilakukan pengecekan ternyata timestamp tersebut bukanlah data sensitif. Oleh sebab itu risiko ini mendapatkan evaluasi risiko *Tolerate*.

4.2.3.8 *Cross-Domain JavaScript Source* File *Inclusion* (Risk8)

Risiko kedelapan yaitu *Cross-Domain JavaScript Source* File *Inclusion*. Risiko ini mendapatkan evaluasi risiko *Tolerate*, risiko ini menjelaskan bahwa terdapat domain lain atau pihak ketiga yang dicantumkan pada *website* ini, pada OWASP ZAP memjelaskan bahwa harus dipastikan domain tersebut bukanlah domain yang berbahaya. Alasan risiko ini mendapatkan evaluasi risiko *Tolerate* karena domain yang dicantumkan pada *website* ini bukanlah domain yang berbahaya karena domain tersebut dari twitter, dimana twitter adalah domain yang terpercaya dan bukan domain yang berbahaya.

4.2.3.9 *X-Frame-Options Header Not Set* (Risk9)

Risiko selanjutnya yaitu *X-Frame-Options Header Not Set*. Risiko ini mendapatkan evaluasi risiko *Treat* karena risiko ini memiliki tingkat risiko *Medium*, dari aturan yang telah dibuat sebelumnya bahwa risiko dengan tingkat risiko *Medium* maka mendapatkan evaluasi *Treat*. Risiko ini menjelaskan tentang Header X-Frame-Options yang tidak terpasang pada konfigurasi *web* server dari *website* tersebut. Risiko ini cukup berbahaya karena dapat membuat pengguna mengeklik sesuatu yang tidak sengaja dia klik.

4.2.3.10 *X-Content-Type-Options Header Missing* (Risk10)

Risiko yang kesepuluh dan yang terakhir yaitu *X-Content-Type-Options Header Missing*. Risiko ini mendapatkan evaluasi risiko *Treat* karena risiko ini berkaitan dengan XSS atau *Cross Site Scripting*. *Cross Site Scripting* adalah tindakan dimana hacker dapat melakukan eksekusi *script* berbahaya yang dimasukkan kedalam *website* untuk merusak *website* tersebut. Risiko ini berbahaya apabila dibiarkan saja, oleh sebab itu risiko ini perlu dilakukannya mitigasi risiko.

4.2.3.11 Hasil Rekap Evaluasi Risiko

Dari aturan evaluasi risiko sebelumnya dan masing-masing risiko telah dilakukan evaluasi risiko, hasil yang didapatkan direkap kedalam tabel. Didalam tabel tersebut sesuai dengan risiko-risiko sebelumnya dan hasil evaluasi risiko yang didapatkan pada masing-masing risiko. Berikut adalah tabel hasil evaluasi risiko.

Tabel 14 Hasil Evaluasi Risiko

ID Risiko	Identifikasi Risiko	Analisis Risiko		Evaluasi Risiko
		Tingkat Risiko	Deskripsi	
Risk1	*Information Disclosure*	*Informational*	*Website* mengandung *comment* yang kemungkinan terdapat informasi penting yang dapat membantu *hacker* dalam melakukan *hack*	*Tolerate*
Risk2	*Cookie No HttpOnly Flag*	*Low*	*Cookie* tidak di setting pada *HttpOnly*, yang berarti *cookie* dapat diakses oleh Java*Script*. Jika *script* berbahaya dapat	*Treat*

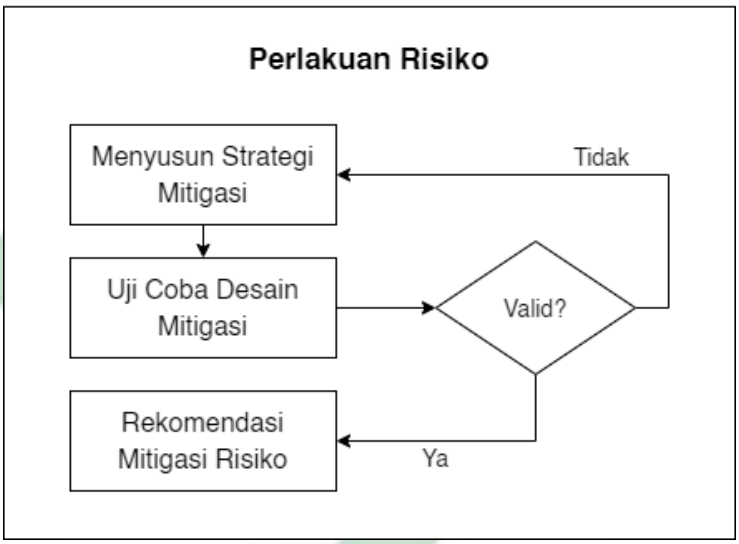
			dijalankan di halaman ini, maka *cookie* akan dapat diakses dan dapat ditransmisikan ke situs lain. Jika ini adalah *cookie* session, maka pembajakan session mungkin terjadi.	
Risk3	*Cookie without SameSite Attribute*	*Low*	*Cookie* telah disetel dengan SameSite attributenya disetel ke *none*, yang berarti bahwa *cookie* dapat dikirim sebagai hasil dari *cross-site* request. The SameSite attribute adalah tindakan balasan yang efektif untuk cross-site request forgery, cross-site *script* inclusion, dan timing attacks.	*Treat*
Risk4	*Absence of Anti-CSRF Tokens*	*Low*	Tidak ada token Anti CSRF yang ditemukan dalam HTML submission form	*Tolerate*
Risk5	*Application Error Disclosure-1*	*Medium*	Halaman ini memunculkan directory listing yang berisikan file-file yang kemungkinan penting.	*Treat*
Risk6	*Application Error Disclosure-2*	*Low*	Halaman ini berisi pesan *error* yang mungkin mengungkapkan informasi sensitif seperti lokasi file yang menghasilkan pengecualian yang tidak tertangani. Informasi ini dapat digunakan untuk meluncurkan serangan lebih lanjut terhadap aplikasi *web*.	*Tolerate*
Risk7	*Timestamp Disclosure*	*Low*	Timestamp muncul pada *website*.	*Tolerate*

Risk8	*Cross-Domain JavaScript Source File Inclusion*	*Low*	*Website* berisi domain dari *website* lain	*Tolerate*
Risk9	*X-Frame-Options Header Not Set*	*Medium*	*Header X-Frame-Options* tidak ada. Fungsi dari *Header X-Frame-Options* adalah untuk melindungi *website* dari serangan *ClickJacking*. *ClickJacking* adalah sebuah jenis serangan *website* yang membuat penggunanya secara tidak sengaja mengklik elemen pada halaman *web* yang tidak ingin di klik.	*Treat*
Risk10	*X-Content-Type-Options Header Missing*	*Low*	Header X-Content-Type-Options tidak ada, hal tersebut menyebabkan munculnya serangan XSS atau Cross Site *Script*ing. XSS atau Cross Site *Script*ing adalah serangan *website* menggunakan code berbahaya yang dapat dieksekusi oleh halaman *website*, serangan tersebut dapat mencuri session client dan menyamar sebagai client tersebut.	*Treat*

Berdasarkan data yang ada pada tabel hasil evaluasi risiko terdapat 10 risiko yang diantaranya adalah 5 risiko mendapatkan evaluasi risiko *Tolerate* dan 5 risiko mendapatkan evaluasi risiko *Treat*. Perlakuan risiko nantinya akan dilakukan pada risiko yang memiliki evaluasi risiko *Treat*. Jadi risiko yang dilakukan perlakuan risiko yaitu *Risk2, Risk3, Risk5, Risk9* dan *Risk10*.

4.3 Perlakuan Risiko

Pada perlakuan risiko ini terdiri dari 3 sub bab yaitu: Menyusun Strategi Mitigasi, Uji Coba Desain Mitigasi dan Rekomendasi Mitigasi Risiko. Pada sub bab Menyusun Strategi Mitigasi referensi yang digunakan berdasarkan pada OWASP ASVS versi 4.0.3 dan OWASP ZAP pada fitur *Solution*. Pada sub bab Uji Coba Desain Mitigasi melakukan pencarian mitigasi secara teknis berdasarkan strategi mitigasi sebelumnya supaya dapat diimplementasikan, lalu dilakukan uji coba apakah mitigasi tersebut sudah sesuai, tidak muncul *error* dan pada OWASP ZAP sudah terselesaikan maka dinyatakan berhasil. Pada Rekomendasi Mitigasi Risiko ditetapkannya rekomendasi mitigasi yang sudah dinyatakan berhasil.



Gambar 25 Alur Perlakuan Risiko

4.3.1 Menyusun Strategi Mitigasi

Penyusunan strategi mitigasi ini menggunakan beberapa referensi, referensi-referensi yang digunakan untuk menyusun strategi mitigasi dari penelitian ini yaitu dari OWASP ASVS versi 4.0.3 dan OWASP ZAP pada fitur *Solution*. Dari kedua sumber tersebut digabung menjadi satu hasil berupa deskripsi yang nantinya akan menjadi strategi mitigasi dari perlakuan risiko ini.

4.3.1.1 *Cookie No HttpOnly Flag* (Risk2)

Strategi mitigasi dari risiko ini didapatkan dari OWASP ASVS versi 4.0.3 pada Klausul (3) *Session Management* dengan Sub Klausul (3.4) *Cookie-based Session Management* dan nomor (3.4.2) yang berisikan *"Verify that cookie-based*

session tokens have the 'HttpOnly' attribute set". Apabila diterjemakan menjadi bahasa indonesia yang berarti "Verifikasi bahwa *cookie*-based session tokens memiliki set atribut *HttpOnly*".

Pada referensi yang kedua didapatkan dari OWASP ZAP pada fitur *solution* yang berisi *"Ensure that the HttpOnly flag is set for all cookies"* yang apabila diterjemakan ke dalam bahasa indonesia berarti "Pastikan bahwa flag HttpOnly disetel untuk semua *cookie*". Dari kedua referensi tersebut sama-sama menjelaskan untuk melakukan verifikasi bahwa *cookie* memiliki set atribut *HttpOnly*.

4.3.1.2 *Cookie without SameSite Attribute* (Risk3)

Risiko selanjutnya untuk strategi mitigasinya didapatkan dari OWASP ASVS versi 4.0.3 Klausul (3) *Session Management* pada Sub Klausul (3.4) *Cookie-based Session Management* nomor (3.4.3) yang berisi tentang *"Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks"* yang apabila diterjemahkan ke dalam bahasa indonesia menjadi "Verifikasi bahwa *cookie*-based session tokens menggunakan atribut *Samesite* untuk membatasi paparan terhadap serangan cross-site request forgery"

Pada referensi yang kedua didapatkan dari OWASP ZAP pada fitur *solution* yang berisikan "*Ensure that the Samesite attribute is set to either 'lax' or ideally 'strict' for all cookies*" yang diterjemahkan menjadi bahasa indonesia yaitu "pastikan atribut Samesite diatur ke '*lax*' atau idelnya '*strict*' untuk semua *cookie*". Dari kedua referensi tersebut dapat disimpulkan untuk melakukan verifikasi bahwa *cookie* menggunakan set atribut *Samesite* agar terhindar dari penyerangan seperti *cross-site request forgery, cross-site inclusion, dan timing attack.*

4.3.1.3 *Application Error Disclosure* (Risk5)

Strategi mitigasi dari risiko ini didapatkan dari OWASP ASVS 4.0.3 Klausul (7) *Error Handling and Logging* Sub Klausul (7.4) *Error Handling* lalu pada nomor (7.4.1) yang berisi *"Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate"* yang diterjemahkan menjadi bahasa

indonesia yaitu "Verifikasi bahwa pesan umum ditampilkan ketika kesalahan sensitif keamanan atau tak terduga terjadi, berpotensi dengan ID unik yang dapat digunakan personel pendukung untuk menyelidiki"

Referensi selanjutnya dari OWASP ZAP pada fitur *Solution* yang berisi *"Review the source code of this page. Implement custom error pages"* yang diterjemahkan menjadi "Tinjau source code halaman ini. Terapkan halaman kesalahan khusus". Pada kasus dari risiko ini *error* yang muncul berupa list dari file-file komponen *website* tersebut atau biasa disebut directory listing, dan cara mitigasinya yaitu adalah melakukan tinjau *source code* pada halaman yang bersangkutan dan menerapkan halaman kesalahan khusus atau menghilangkan *directory listring* tersebut.

4.3.1.4 *X-Frame-Options Header Not Set* (Risk9)

Strategi mitigasi selanjutnya dari risiko ini didapatkan dari OWASP ASVS 4.0.3 pada Klausul (14) *Configuration* Sub Klausul (14.4) *HTTP Security Headers* pada nomor (14.4.7)*"Verify that the content of a web application cannot be embedded in a third-party site by default and that embedding of the exact resources is only allowed where necessary by using suitable Content-Security-Policy: frame-ancestors and X-Frame-Options response header"* yang diterjemahkan menjadi "Verifikasi bahwa konten aplikasi *web* tidak dapat disematkan di situs pihak ketiga secara default dan bahwa penyematan sumber daya yang tepat hanya diperbolehkan jika diperlukan dengan menggunakan Content- Security Policy: frame-ancestors dan Header X-Frame-Options Respons"

Referensi yang kedua didapatkan dari OWASP ZAP pada fitur *Solution* yang berisi "*Ensure X-Frame-Options Header is set on all web pages and use SAMEORIGIN*" yang apabila diterjemahkan ke dalam bahasa indonesia yaitu "Pastikan Header X-Frame-Options diatur di semua halaman *web* dan gunakan SAMEORIGIN". Dari kedua referensi tersebut dapat disimpulkan bahwa strategi mitigasinya adalah melakukan verifikasi bahwa Header X-Frame-Options perlu ditambahkan pada *website*.

4.3.1.5 *X-Content-Type-Options Header Missing* (Risk10)

Risiko selanjutnya yaitu *X-Content-Type-Options Header Missing* dengan ID Risiko yaitu Risk10. Strategi mitigasi dari risiko ini didapatkan dari OWASP ASVS versi 4.0.3 pada Klausul (14) *Configuration* Sub Klausul (14.4) *HTTP Security Headers* pada nomor (14.4.4) yang membahas tentang *"Verify that all responses contain a X-Content-Type-Options: nosniff header"* yang apabila diterjemahkan menjadi bahasa indonesia menjadi "Verifikasi bahwa semua respons berisi X-Content-Type-Options: header nosniff"

Referensi selanjutnya didapatkan dari OWASP ZAP pada fitur *Solution* yang berisi tentang "*Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to nosniff for all web pages*" apabila diterjemahkan ke dalam bahasa indonesia menjadi "Pastikan aplikasi/server *web* menyetel header Content-Type dengan tepat, dan menyetel header X-Content-Type-Options ke nosniff untuk semua halaman *web*". Dari kedua referensi tersebut dapat disimpulkan untuk melakukan verifikasi bahwa semua respons berisi *X-Content-Type-Options: Header 'nosniff'*.

4.3.2 Uji Coba Desain Mitigasi

Sebelum dilakukannya uji coba desain mitigasi, diperlukannya cara mitigasi risiko dari segi teknisnya karena pada langkah sebelumnya hanya berupa deskripsi saya dan berupa teori sedangkan secara teknisnya pasti berbeda. Mitigasi secara teknisnya mencari dari berbagai macam referensi seperti *stackoverflow* dan lain sebagainya. Dengan deskripsi yang sudah didapatkan dari langkah sebelumnya dapat mempermudah dalam mencari mitigasi secara teknis dari masing-masing risiko.

Setelah ditemukan cara mitigasi dari segi teknisnya, langkah selanjutnya yaitu menerapkan mitigasi teknis tersebut kedalam *website* pada kasus *website* dari penelitian ini yaitu diterapkan ke konfigurasi *web* server dari *website* yang bersangkutan. Setelah ditambahkan di konfigurasi *web* server, dilakukan uji coba apakah muncul *error* di *website* tersebut atau tidak, apabila muncul *error* maka dilakukan pencarian strategi mitigasi yang lain dan apabila tidak muncul *error* dan pada OWASP ZAP sudah selesai maka mitigasi tersebut berhasil.

4.3.2.1 *Cookie No HttpOnly Flag* (Risk2)

Strategi mitigasi pada risiko ini adalah dengan melakukan verifikasi bahwa *cookie* memiliki set atribut *HttpOnly* untuk menghindari terjadinya *cookie* yang dapat diakses Javacript, apabila *script* yang dijalankan adalah berbahaya maka dapat ditransmisikan ke situs lain dan pembajakan *cookie* dan session bisa terjadi. Oleh sebab itu diperlukannya atribut *HttpOnly* pada *cookie* tersebut. Untuk mitigasi secara teknis dicari pada beberapa sumber tertentu seperti *stackoverflow*.

```
Header set X-Frame-Options "SAMEORIGIN"

Header edit Set-Cookie ^(.*) "$1; HttpOnly;SameSite=strict"

        DocumentRoot /var/www/jurnalsaintek

#ProxyPass "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxx/"
#ProxyPassReverse "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxx/"

Header always set X-Content-Type-Options nosniff

<Directory "/var/www/jurnalsaintek/">

        Options FollowSymLinks Includes ExecCGI

        AllowOverride All

#        Options Indexes FollowSymLinks
#        Require all granted

</Directory>
```

Gambar 26 Mitigasi Risiko *Cookie No HttpOnly Flag* (Risk2)

Pada *stackoverflow* terdapat beberapa *source code* yang muncul dan diharuskan ditambahkan pada kofigurasi dari suatu *web* server yang digunakan. Konfigurasinya pun berbeda-beda sesuai dengan jenis *web* servernya, pada kasus penelitian ini *web* server yang digunakan oleh *website* adalah Apache. Konfigurasi yang didapatkan berupa source code *Header Edit Set-Cookie ^(.*) "$1; HttpOnly"*, setelah ditambahkan pada *web* server tidak muncul *error* dan pada OWASP ZAP risiko tersebut sudah terselesaikan maka mitigasi pada risiko ini telah berhasil.

4.3.2.2 *Cookie without SameSite Attribute* (Risk3)

Strategi mitigasi yang ditentukan pada risiko adalah melakukan verifikasi bahwa *cookie* menggunakan set atribut *Samesite* agar terhindar dari penyerangan seperti *cross-site request forgery, cross-site inclusion, dan timing attack*. Dicarilah

referensi mengenai strategi mitigasi ini dalam bentuk teknis atau source code di beberapa sumber salah satunya yaitu *stackoverflow*.

```
Header set X-Frame-Options "SAMEORIGIN"

Header edit Set-Cookie ^(.*) "$1; HttpOnly;SameSite=strict"

        DocumentRoot /var/www/jurnalsaintek

#ProxyPass "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"
#ProxyPassReverse "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"

Header always set X-Content-Type-Options nosniff

<Directory "/var/www/jurnalsaintek/">

        Options FollowSymLinks Includes ExecCGI

        AllowOverride All

#        Options Indexes FollowSymLinks
#        Require all granted

</Directory>
```

Gambar 27 Mitigasi Risiko *Cookie without SameSite Attribute* (Risk3)

Setelah ditemukannya source code dari *stackoverflow* ditambahkan pada *web* server Apache yang digunakan oleh *website* yang bersangkutan. Konfigurasi yang digunakan yaitu berupa source code *Header Edit Set-Cookie ^(.*) "$1; SameSite=strict"*, setelah dilakukannya pemasangan pada source code tersebut, tidak ditemukan *error website* masih bisa dijalankan tanpa kendala dan pada OWASP ZAP risiko tersebut terselesaikan maka mitigasi pada risiko ini telah berhasil.

4.3.2.3 *Application Error Disclosure-1* (Risk5)

Strategi mitigasi pada risiko ini melakukan tinjau *source code* pada halaman yang bersangkutan dan menerapkan halaman kesalahan khusus atau menghilangkan directory listring tersebut. *Error* directory listing ini berbahaya karena dapat memunculkan secara terang-terangan file-file yang ada pada *website* tersebut, dan hacker dapat memanipulasi file-file tersebut. Pencarian source code untuk menghilangkan *error directory listing* ini di beberapa sumber dan yang paling umum yaitu *stackoverflow*.

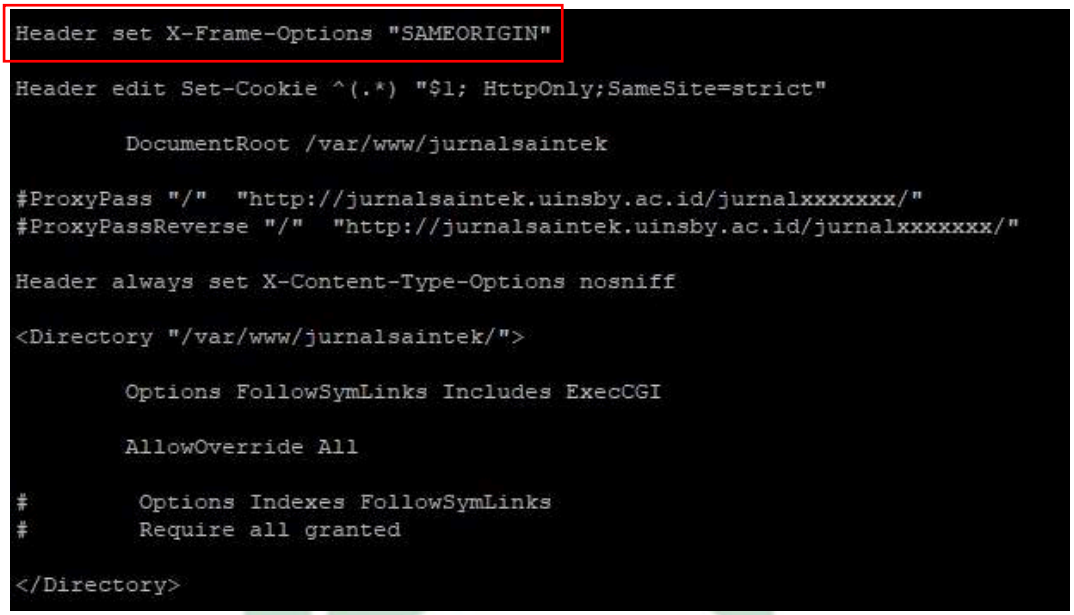
```
Header set X-Frame-Options "SAMEORIGIN"

Header edit Set-Cookie ^(.*) "$1; HttpOnly;SameSite=strict"

        DocumentRoot /var/www/jurnalsaintek

#ProxyPass "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"
#ProxyPassReverse "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"

Header always set X-Content-Type-Options nosniff

<Directory "/var/www/jurnalsaintek/">

        Options FollowSymLinks Includes ExecCGI

        AllowOverride All

#        Options Indexes FollowSymLinks
#        Require all granted

</Directory>
```

Gambar 28 Mitigasi Risiko *Application Error Disclosure* (Risk5)

Setelah ditemukannya *source code* dari *stackoverflow* ternyata *source code* tersebut ditambahkan pada konfigurasi *web* server pada tag directory pada konfigurasi *web* server. Source code yang didapat dari *stackoverflow* adalah dengan menghapus code *Indexes* pada code *Options Indexes FollowSymLinks Includes ExecCGI* akhirnya menjadi *Options FollowSymLinks Includes ExecCGI*, dan source code tersebut ditambahkan di dalam tag directory pada konfigurasi *web* server. Setelah source code tersebut ditambahkan tidak muncul *error* dan *website* masih bisa digunakan dengan normal serta pada OWASP ZAP risiko ini telah terselesaikan maka mitigasi pada risiko ini berhasil.

4.3.2.4 *X-Frame-Options Header Not Set* (Risk9)

Strategi mitigasi pada risiko ini dengan melakukan verifikasi bahwa konten pada *website* tidak dapat disematkan resource apapun oleh pihak ketiga dan apabila penyematan resources dilakukan, hanya diperlukan saja dengan menggunakan Header X-Frame-Options. Penyematan resource tersebut dilakukan oleh hacker untuk membuat penggunanya mengeklik sesuatu yang bukan asli dari *website* tersebut melainkan resource berbahaya dari hacker tersebut.



Gambar 29 Mitigasi Risiko *X-Frame-Options Header Not Set* (Risk9)

Mitigasi secara teknis dilakukan dengan mencari dari *stackoverflow* dan mendapatkan source code yaitu *Header always set X-Frame-Options "SAMEORIGIN"* dan code tersebut ditambahkan pada konfigurasi *web* server dari *website* ini yaitu Apache. Setelah ditambahkannya source code tersebut pada konfigurasi *web* server, tidak muncul *error* dan risiko ini sudah tidak muncul lagi di OWASP ZAP yang mengartikan bahwa mitigasi yang dilakukan pada risiko ini telah berhasil.

4.3.2.5 *X-Content-Type-Options Header Missing* (Risk10)

Strategi mitigasi pada risiko ini yaitu melakukan verifikasi bahwa semua respons berisi *X-Content-Type-Options: Header 'nosniff'*. Header X-Content-Type-Options berfungsi untuk mencegah terjadinya serangan XSS atau *Cross Site Scripting*. XSS atau *Cross Site Scripting* merupakan serangan dengan melakukan eksekusi *script* yang dikirimkan ke *website* dan merusak *website* tersebut. Pencarian mitigasi secara teknis dilakukan pada sumber yang sudah terkenal yaitu *Stackoverflow*.

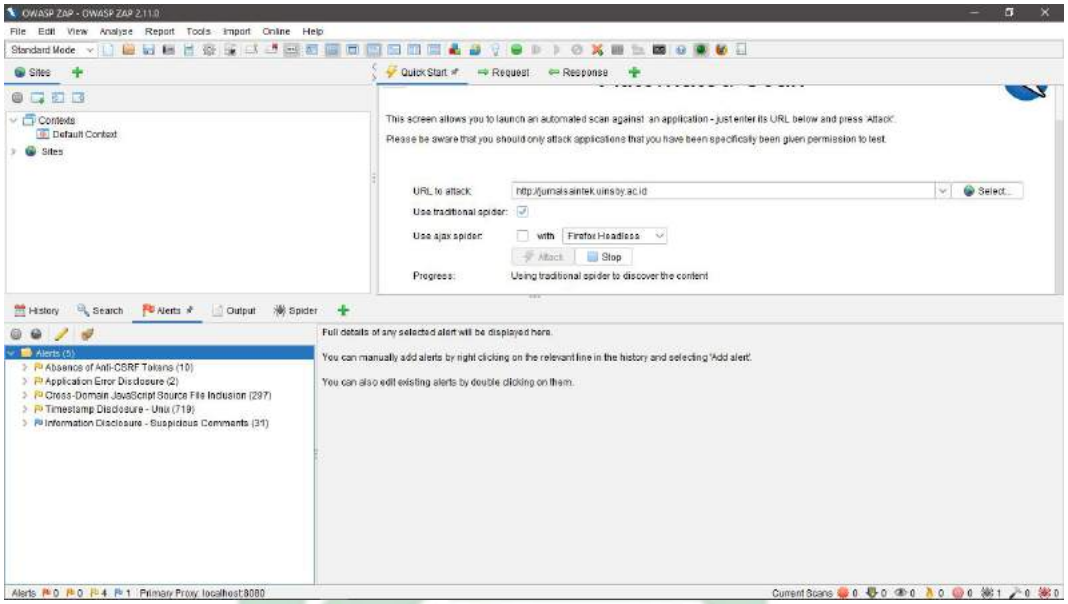
```
Header set X-Frame-Options "SAMEORIGIN"

Header edit Set-Cookie ^(.*) "$1; HttpOnly;SameSite=strict"

        DocumentRoot /var/www/jurnalsaintek

#ProxyPass "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"
#ProxyPassReverse "/"  "http://jurnalsaintek.uinsby.ac.id/jurnalxxxxxxx/"

Header always set X-Content-Type-Options nosniff

<Directory "/var/www/jurnalsaintek/">

        Options FollowSymLinks Includes ExecCGI

        AllowOverride All

#        Options Indexes FollowSymLinks
#        Require all granted

</Directory>
```

Gambar 30 Mitigasi Risiko *X-Content-Type-Options Header Missing* (Risk10)

Setelah dicarinya hasil yang sesuai dengan strategi mitigasi pada risiko ini didapatkan berupa code *Header always set X-Content-Type-Options nosniff*. Source code ini berdasarkan konfigurasi dari *web* server Apache sesuai dengan jenis *web* server yang digunakan oleh *website* pada penelitian ini. Source code ini ditambahkan pada konfigurasi *web* server. Setelah ditambahkan tidak muncul *error* dan pada OWASP ZAP setelah di scan ulang tidak muncul lagi risiko tersebut, maka mitigasi pada risiko ini telah berhasil terselesaikan.

4.3.2.6 Hasil Uji Coba Desain Mitigasi

Berdasarkan hasil yang didapatkan dari implementasi source code dalam upaya melakukan mitigasi risiko, dari lima risiko yang dilakukan implementasi mitigasi risiko menyatakan bahwa lima risiko tersebut telah berhasil diimplementasikan dan berhasil melewati uji coba *error* dan scan ulang menggunakan OWASP ZAP. Pada OWASP ZAP saat dilakukan scan ulang, tidak memunculkan lagi risiko-risiko tersebut yang berarti lima risiko yang telah dilakukan mitigasi berhasil diselesaikan.



Gambar 31 Hasil Uji Coba Desain Mitigasi

4.3.3 Rekomendasi Mitigasi Risiko

Rekomendasi Mitigasi Risiko pada penelitian ini didapatkan pada hasil dari langkah-langkah sebelumnya yaitu Strategi Mitigasi dan Uji Coba Desain Mitigasi. Pada Strategi Mitigasi didapatkan dengan dua referensi yaitu dari OWASP ASVS versi 4.0.3 dan OWASP ZAP pada fitur *Solution*, kemudian disimpulkan dari kedua referensi tersebut menjadi satu kalimat yang paling relevan. Pada Uji Coba Desain Mitigasi melakukan pencarian mitigasi secara teknis dari referensi *Stackoverflow* dan selanjutnya setelah source code ditambahkan pada *web* server *website*, jika tidak muncul *error* dan setelah dilakukan scan ulang di OWASP ZAP terselesaikan maka mitigasi risiko telah berhasil dilakukan.

4.3.3.1 *Cookie No HttpOnly Flag* (Risk2)

Rekomendasi mitigasi risiko pada risiko *Cookie No HttpOnly Flag* ini terdiri dari Strategi Mitigasi dan Mitigasi secara Teknis. Strategi mitigasi risiko ini yaitu melakukan verifikasi bahwa *cookie* telah memiliki set atribut *HttpOnly*. Mitigasi secara teknisnya yaitu dengan melakukan penambahan source code *Header Edit Set-Cookie ^(.*) "$1; HttpOnly"* pada konfigurasi *web* server Apache pada *website* yang bersangkutan.

4.3.3.2 *Cookie without SameSite Attribute* (Risk3)

Rekomendasi mitigasi risiko pada risiko *Cookie No HttpOnly Flag* ini terdiri dari Strategi Mitigasi dan Mitigasi secara Teknis. Strategi mitigasi risiko ini yaitu verifikasi bahwa *cookie* menggunakan set atribut *Samesite* agar terhindar dari penyerangan seperti cross-site request forgery, cross-site inclusion, dan timing attack. Mitigasi secara Teknisnya yaitu dengan melakukan penambahan source code *Header Edit Set-Cookie ^(.*) "$1; SameSite=strict"* pada konfigurasi *web* server Apache pada *website* yang bersangkutan.

4.3.3.3 *Application Error Disclosure-1* (Risk5)

Rekomendasi mitigasi risiko pada risiko *Application Error Disclosure* ini terdiri dari Strategi Mitigasi dan Mitigasi secara Teknis. Strategi mitigasi risiko ini yaitu melakukan tinjau *source code* pada halaman yang bersangkutan dan menerapkan halaman kesalahan khusus atau menghilangkan directory listring tersebut. Mitigasi secara Teknisnya yaitu dengan menghapus *Indexes* pada code *Options Indexes FollowSymLinks Includes ExecCGI* akhirnya menjadi *Options FollowSymLinks Includes ExecCGI*, dan source code tersebut ditambahkan di dalam tag directory pada konfigurasi *web* server dari *website* yang bersangkutan.

4.3.3.4 *X-Frame-Options Header Not Set* (Risk9)

Rekomendasi mitigasi risiko pada risiko *X-Frame-Options Header Not Set* ini terdiri dari Strategi Mitigasi dan Mitigasi secara Teknis. Strategi mitigasi risiko ini yaitu melakukan verifikasi bahwa Header X-Frame-Options di tambahkan pada *website*. Mitigasi secara teknisnya yaitu dengan menambahkan source code *Header always set X-Frame-Options "SAMEORIGIN"* pada konfigurasi *web* server dari *website* yang bersangkutan.

4.3.3.5 *X-Content-Type-Options Header Missing* (Risk10)

Rekomendasi mitigasi risiko pada *X-Content-Type-Options Header Missing* ini terdiri dari Strategi Mitigasi dan Mitigasi secara Teknis. Strategi mitigasi risiko ini yaitu melakukan verifikasi bahwa semua respons berisi *X-Content-Type-Options: Header 'nosniff'*. Mitigasi secara desainnya yaitu dengan melakukan penambahan source code *Header always set X-Content-Type-Options*

nosniff dimasukkan kedalam tag directory pada konfigurasi *web* server dari *website* yang bersangkutan.

4.3.4 Rekap Hasil Perlakuan Risiko

Dari hasil rekomendasi mitigasi risiko yang telah didapatkan, dimasukkan ke dalam tabel yang nantinya tabel tersebut akan digabungkan dengan yang lain pada tabel risk register nantinya. Tabel ini berisi tentang kumpulan dari trategi mitigasi dan mitigasi secara teknis dari masing-masing risiko. Berikut adalah tabel hasil perlakuan risiko.

Tabel 15 Hasil Perlakuan Risiko

ID Risiko	Strategi Mitigasi	Mitigasi secara Teknis	Hasil
Risk1	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi
Risk2	Melakukan verifikasi bahwa *cookie* telah memiliki set atribut *HttpOnly*	Melakukan penambahan source code *Header Edit Set-Cookie ^(.*) "$1; HttpOnly"* pada konfigurasi *web* server Apache	Berhasil
Risk3	Verifikasi bahwa *cookie* menggunakan set atribut *Samesite*	Melakukan penambahan source code *Header Edit Set-Cookie ^(.*) "$1; SameSite=strict"* pada konfigurasi *web* server Apache	Berhasil
Risk4	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi
Risk5	Melakukan tinjau *source code* pada halaman yang bersangkutan dan menerapkan halaman kesalahan khusus atau menghilangkan directory listring tersebut	Menghapus *Indexes* pada code *Options Indexes FollowSymLinks Includes ExecCGI* menjadi *Options FollowSymLinks Includes ExecCGI*, dan source code tersebut ditambahkan di dalam tag directory pada konfigurasi *web* server	Berhasil
Risk6	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi

Risk7	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi
Risk8	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi	Tidak Dilakukan Mitigasi
Risk9	Melakukan verifikasi bahwa Header X-Frame-Options di tambahkan pada *website*	Menambahkan source code *Header always set X-Frame-Options "SAMEORIGIN"* pada konfigurasi *web* server Apache	Berhasil
Risk10	Melakukan verifikasi bahwa semua respons berisi *X-Content-Type-Options: Header 'nosniff'*.	Menambahkan source code *Header always set X-Content-Type-Options nosniff* pada konfigurasi *web* server Apache	Berhasil

4.4 Pembahasan

Pada subbab pembahasan ini terdiri dari Penerapan Alat Bantu OWASP dan Hasil Mitigasi. Dari masing-masing subbab tersebut berisikan deskripsi dan penjelasannya tersendiri. Pada Penerapan Alat Bantu OWASP menjelaskan tentang alasan digunakannya OWASP sebagai alat bantu dan menjelaskan keselarasan OWASP dan Alat Bantu lainnya yang dicantumkan di Dokumen ISO 31000 berdasarkan Manajemen Risiko ISO 31000. Selanjutnya pada Hasil mitigasi menjelaskan tentang perbandingan sebelum dan sesudah dilakukannya mitigasi risiko.

4.4.1 Penerapan Alat Bantu OWASP

Penelitian ini menggunakan alat bantu yaitu *Open Web Application Security Project* (OWASP) yang terdiri dari OWASP *Application Security Verification Standard* (ASVS) versi 4.0.2 dan OWASP *Zed Attack Proxy* (ZAP). Keunggulan OWASP ASVS versi 4.0.3 yaitu memiliki pembahasan yang berkaitan dengan dasar-dasar keamanan *website* dan aplikasi berbasis *website*. Sehingga OWASP ASVS versi 4.0.3 dirasa cocok diterapkan pada penelitian ini yang membahas tentang keamanan *website*.

OWASP ZAP memiliki fitur yang dapat digunakan untuk memenuhi kebutuhan penelitian ini yaitu dapat melakukan *scanning* pada suatu *website* untuk mencari kerentanan keamanan yang ada pada *website* tersebut. Kerentanan keamanan yang muncul dapat berbeda-beda setiap *website*, kerentanan inilah yang menjadi risiko keamanan *website* pada penelitian ini. OWASP ZAP juga dapat memunculkan tingkat risiko dan deskripsi dari masing-masing risiko dengan penjelasan yang lengkap. OWASP ZAP juga memiliki *Solution* untuk menyelesaikan risiko yang bersangkutan.

Pada studi kasus penelitian ini, alat bantu yang digunakan adalah OWASP yang terdiri dari OWASP ASVS dan OWASP ZAP. Pada *Risk Assessment* atau Pengukuran Risiko yang terdiri dari Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko memiliki kesesuaian dengan OWASP ASVS dan OWASP ZAP. Pada tabel 16 Penerapan Alat Bantu Pengukuran Risiko dilakukan penambahan alat

bantu yaitu OWASP ASVS dan OWASP ZAP pada nomor 32 dan 33, tujuan ditambahkannya alat bantu tersebut untuk melakukan perbandingan terhadap alat bantu lainnya yang dicantumkan pada dokumen ISO 31000.

Pada tabel 16 Penerapan alat bantu OWASP ASVS dapat diperhatikan pada nomor 32, OWASP ASVS dapat dilakukan pada tahap Identifikasi Risiko dengan nilai (A) yang artinya dapat diterapkan. OWASP ASVS ini memiliki keterkaitan dengan risiko-risiko yang muncul pada tahap identifikasi risiko karena OWASP ASVS memiliki dasar-dasar dalam upaya peningkatan keamanan *website* dan risiko-risiko yang muncul merupakan kerentanan keamanan *website* itu sendiri. Jadi secara tidak langsung OWASP ASVS memiliki keterkaitan dengan Identifikasi Risiko

Pada tabel 16 Penerapan alat bantu OWASP ZAP dapat diperhatikan pada nomor 33, OWASP ZAP dapat dilakukan pada tahap Identifikasi Risiko dengan nilai (SA) yang artinya sangat dapat diterapkan dan Analisis Risiko dengan nilai (A) yang artinya dapat diterapkan. OWASP ZAP memiliki kemampuan untuk mengungkap kerentanan-kerentanan keamanan dari suatu *website* lalu kerentanan tersebut nantinya akan menjadi risiko keamanan *website*, hal tersebut sesuai dengan harapan penelitian ini. OWASP ZAP juga memiliki kemampuan untuk memunculkan tingkat risiko dari masing-masing risiko berdasarkan penelitian yang dilakukan oleh Perusahaan OWASP.

Tabel 16 Penerapan Alat Bantu OWASP pada Pengukuran Risiko

No	Alat bantu dan Teknik	Proses Pengukuran Risiko				
		Identifikasi Risiko	Analisis Risiko			Evaluasi Risiko
			Konsekuensi	Probabilitas	Tingkat Risiko	
1	Curah pendapat	SA	NA	NA	NA	NA
2	Wawancara terstruktur atau semi-struktur	SA	NA	NA	NA	NA
3	Delphi	SA	NA	NA	NA	NA

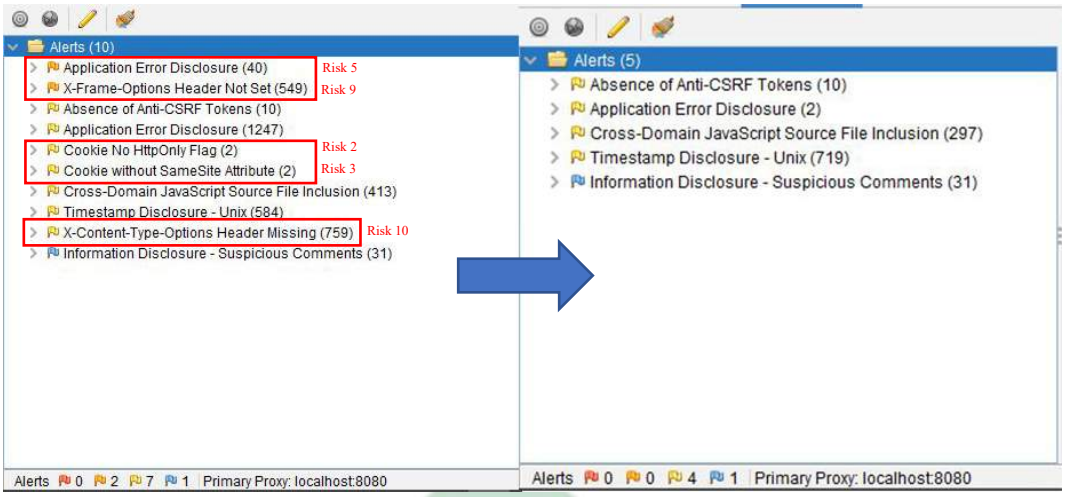
4	Daftar periksa	SA	NA	NA	NA	NA
5	Analisis pendahuluan potensi bahaya	SA	NA	NA	NA	NA
6	Studi potensi bahaya dan operabilitas (HAZOP)	SA	SA	A	A	A
7	Analisis potensi bahaya dan titik kendali kritis (HACCP)	SA	SA	NA	NA	SA
8	Penilaian risiko lingkungan	SA	SA	SA	SA	SA
9	Struktur “apa-jika” " (SWIFT)	SA	SA	SA	SA	SA
10	Analisis skenario	SA	SA	A	A	A
11	Analisis dampak bisnis	A	SA	A	A	A
12	Analisis akar penyebab	NA	SA	SA	SA	SA
13	Analisis modus kegagalan dan dampak	SA	SA	SA	SA	SA
14	Analisis pohon kesalahan	A	NA	SA	A	A
15	Analisis pohon kejadian	A	SA	A	A	NA
16	Analisis sebab dan konsekuensi	A	SA	SA	A	A
17	Analisis sebab-dan-akibat	SA	SA	NA	NA	NA
18	Analisis lapisan proteksi (LOPA)	A	SA	A	A	NA
19	Pohon keputusan	NA	SA	SA	A	A
20	Analisis keandalan manusia	SA	SA	SA	SA	A
21	Analisis dasi kupu-kupu	NA	A	SA	SA	A
22	Pemeliharaan yang terpusat pada keandalan	SA	SA	SA	SA	SA
23	Analisis rangkaian selinap	A	NA	NA	NA	NA
24	Analisis Markov	A	SA	NA	NA	NA
25	Simulasi Monte carlo	NA	NA	NA	NA	SA
26	Statistik Bayesian dan jaring Bayes	NA	SA	NA	NA	SA
27	Kurva FN	A	SA	SA	A	SA

28	Indeks risiko	A	SA	SA	A	SA
29	Matriks Konsekuensi/probabilitas	SA	SA	SA	SA	A
30	Analisis biaya/manfaat	A	SA	A	A	A
31	Analisis keputusan multikriteria (MCDA)	A	SA	A	SA	A
32	OWASP Application Security Verification Standard	A	NA	NA	NA	NA
33	OWASP Zed Attack Proxy	SA	NA	NA	A	NA
	1) SA = Sangat dapat diterapkan 2) NA = Tidak dapat diterapkan 3) A = Dapat diterapkan					

4.4.2 Hasil Uji Mitigasi Risiko

Berdasarkan daftar risiko yang didapatkan pada fase identifikasi risiko (sub bab 4.2.1), terdapat 10 risiko yang didapatkan. Setelah melalui proses analisis (sub bab 4.2.2) dan evaluasi risiko (sub bab 4.2.3) didapatkan 5 risiko yang harus di *treat* atau dilakukannya mitigasi yakni risiko dengan id Risk2, Risk3, Risk5, Risk9 dan Risk10.

Berdasarkan langkah manajemen risiko pada ISO 31000, setelah dilakukan *Risk Assessment* (yang terdiri dari identifikasi, analisis dan evaluasi) maka langkah selanjutnya adalah melakukan risk *treat*ment atau perlakuan risiko. Pada penelitian ini kemudian menyusun langkah perlakuan risiko yaitu strategi mitigasi (sub bab 4.3.1) kemudian dilanjutkan dengan melakukan uji coba terhadap desain mitigasi (sub bab 4.3.2) dan yang terakhir menetapkan rekomendasi mitigasi risiko (sub bab 4.3.3).



Gambar 32 Perbandingan Setelah Mitigasi

Risiko yang dilakukan mitigasi yaitu: Risk2 - *Cookie No HttpOnly Flag* dengan tingkat risiko *Low*, Risk3 - *Cookie without Samesite Attribute* dengan tingkat risiko *Low*, Risk5 - *Application Error Disclosure-1* dengan tingkat risiko *Medium*, Risk9 – *X-Frame-Options Header Not Set* dengan tingkat risiko *Medium* dan terakhir Risk10 – *X-Content-Type-Options Header Missing* dengan tingkat risiko *Low*. Mitigasi risiko yang dilakukan pada lima risiko tersebut telah berhasil dilakukan dan risiko-risiko tersebut telah terselesaikan berdasarkan Strategi Mitigasi dan Mitigasi secara Teknis. Pada Uji Coba Desain Mitigasi risiko-risiko tersebut tidak memunculkan *error* dan saat di scan ulang menggunakan OWASP ZAP risiko tersebut tidak muncul kembali.

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini menggunakan *Framework* Manajemen Risiko ISO 31000 dengan tools OWASP (Open *Web* Application Security Project) yaitu OWASP ASVS (Application Security Verification Standard) versi 4.03 dan OWASP ZAP (Zed Attack Proxy) pada *website* OJS dan didapatkan kesimpulan sebagai berikut:

1. Tahapan manajemen risiko risiko berbasis ISO 31000 untuk website OJS adalah Lingkup Konteks Kriteria, Pengukuran Risiko (terdiri dari Identifikasi Risiko, Analisis Risiko dan Evaluasi Risiko) dan Perlakuan Risiko (terdiri dari Menyusun Strategi Mitigasi, Uji Coba Desain Mitigasi dan Rekomendasi Mitigasi Risiko)
2. Desain mitigasi risiko pada *website* OJS berdasarkan Open Web Application Security Project diambil dari klausul yang ada pada OWASP ASVS versi 4.0.3 dan fitur *Solution* pada OWASP ZAP yang menghasilkan bahwa 5 risiko yang dilakukan mitigasi yaitu *Risk2, Risk3, Risk5, Risk9* dan *Risk10* telah berhasil dilakukan dan risiko kerentanan keamanan pada website OJS telah berhasil diatasi.

5.2 Saran Pengembangan

Penelitian ini menggunakan ilmu manajemen risiko berbasis pada ISO 31000 dan juga menggunakan *framework Open Web Application Security Project* atau OWASP yang terdiri dari OWASP *Application Standar Verification Security* atau ASVS versi 4.0.3 dan Aplikasi dari OWASP untuk mencari Kerentanan dari *website* yang nantinya menjadi risiko pada *website* tersebut. Pada penelitian selanjutnya diharapkan kepada peneliti untuk menggunakan ilmu manajemen risiko yang lain dan menggunakan *framework* yang lain untuk mendapatkan hasil yang lebih kuat dan akurat, mendapatkan ilmu yang bervariatif dan mencari risiko-risiko lain yang belum dicantumkan pada penelitian ini.

DAFTAR PUSTAKA

Akbar, A., Sains, F., Teknologi, D. A. N., Islam, U., Sultan, N., & Kasim, S. (2018). *SISTEM PENILAIAN RISIKO KEAMANAN SISTEM INFORMASI DENGAN PERBANDINGAN METODE SIMPLE ADDICTIVE WEIGHTING (SAW) DAN ANALYTICAL HIERARCHY PROCESS (AHP)*.

Alexander F. K. Sibero. (2011). *Kitab Suci Web Programing*. MediaKom.

Bintu Humairah Bekti. (2015). *Mahir Membuat Website dengan AdobeDreamweaver CS6, CSS dan JQuery*. ANDI.

Bramantyo Djohanputro. (2008). *Manajemen Risiko Korporat*. Penerbit PPM.

Bria, T. A. (2012). Studi tentang risiko yang dihadapi developer dalam bisnis properti. *E-Journal UAJY*, *1*(1), 60. http://e-journal.uajy.ac.id/402/

Colle, A. B. A. (2018). *Diterjemahkan oleh Andi Balladho Aspat Colle dengan bantuan: Google translate dan Buku: J. Susilo, Leo dan R. Kaho, Susilo. 2018. Manajemen Risiko berbasis ISO 31000: 2018 Panduan untuk Risk Leader dan Risk Practitioner . Jakarta: PT. Grasindo*. 21.

Djojosoedarso, S. (2003). *Prinsip-Prinsip Manajemen Resiko dan Asuransi* (Edisi Revi). Salemba Empat.

Fahmi, I. (2010). *Manajemen Resiko*. Alfabeta.

Fikri Kurniawan. (2021). *Pengguna Website di Indonesia Naik 61,6% Sepanjang 2020*. Tekno.Sindonews.Com. https://tekno.sindonews.com/read/389902/207/pengguna-*website*-di-indonesia-naik-616-sepanjang-2020-1617800664

Foundation, O. (2021). *OWASP*. Https://Owasp.Org.

G.J Simson; Gene Spafford. (2005). *Practical UNIX & Internet Security :O'Reilly & Associates Inc. 2nd edition* (2nd editio).

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi *Website* Menggunakan Metode Owasp (Open *Web*

Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

Gregorius Agung. (2000). *Microsoft Frontpage 2000 Webbot*. PT. ElexMedia Komputindo.

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan *Web* Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Hanafi, M. M. (2014). Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management. *Management Research Review*, 1–40. http://repository.ut.ac.id/4789/1/EKMA4262-M1.pdf

Handoko, A. I. P. (2017). *Prototipe Pengendalian Lampu Panggung Menggunakan Web Browser Melalui Jaringan Lokal Berbasis Arduino*. STMIK AKAKOM YOGYAKARTA.

Harimurti, F. (2006). Manajemen Risiko, Fungsi dan Mekanismenya. *Fakultas Ekonomi Universitas Slamet Riyadi*, 105–112.

Kustiyahningsih, Y., & Anamisa, D. R. (2011). *Pemrograman Basis Data Berbasis Web Menggunakan PHP & MySQL*. Graha Ilmu.

M.Rudyanto Arief. (2011). *Pemrograman Web Dinamis Menggunakan PHP dan MYSQL*. C.V ANDI OFFSET.

Moleong, Lexy J. (2010). *Metodologi Penelitian Kualitatif.* Bandung: Remaja Rosdakarya

OWASP. (2021). *Application Security Verification Standard 4.0.3*. *October*, 47.

Priyanto Hidayatullah, J. K. K. (2017). *Pemrograman Web*. Informatika Bandung.

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber. *Jurnal Pertahanan & Bela Negara*, *Vol.7*(No.2), 51–66.

Sherlywati, S. E. (2016). Prosiding Mebc 2016 Fakultas Ekonomi Pengelolaan Risiko Rantai Pasok (Supply Chain Risk Management) Sebagai Keunggulan Bersaing Perusahaan. *Maranatha Economics & Business Conference*, 2–19. http://repository.maranatha.edu/20637/

Sibero, A. F. . (2013). *Web Programing Power Pack*. MediaKom.

Supratman, L. P. (2018). Penggunaan Media Sosial oleh *Digital Native*. *Jurnal ILMU KOMUNIKASI*, *15*(1), 47–60. https://doi.org/10.24002/jik.v15i1.1243

Wedana Yasa, I. W., Sila Dharma, I. G. B., & Ketut Sudipta, I. G. (2013). Manajemen Risiko Operasional Dan Pemeliharaan Tempat Pembuangan Akhir (Tpa) Regional Bangli Di Kabupaten Bangli. *Jurnal Spektran*, *1*(2), 30–38. https://doi.org/10.24843/spektran.2013.v01.i02.p05

Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019). IT Risk Management Based on ISO 31000 and OWASP *Framework* using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), 17–29. https://doi.org/10.5815/ijcnis.2019.12.03

Yudiana, Y., Elanda, A., & Buana, R. L. (2021). Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis *Website* Pada STMIK Rosma Dengan Menggunakan OWASP Top 10. *CESS (Journal of Computer Engineering, System and Science)*, *6*(2), 185. https://doi.org/10.24114/cess.v6i2.24777