Skripsi _Agung_Ramadhan SI Revisi.pdf

by Eunwoo Choi

Submission date: 14-Sep-2026 10:05AM (UTC+0700)
Submission ID: 3031340294
File name: Skripsi__Agung_Ramadhan_SI_Revisi.pdf (833.44K)
Word count: 10335
Character count: 71647

PENGUJIAN KEAMANAN *WEBSITE* SISTEMASI UNISI MENGGUNAKAN METODE *PENETRATION TESTING*

DISUSUN OLEH :

AGUNG RAMADHAN
403211010040

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS ISLAM INDRAGIRI
TEMBILAHAN

2025

PENGUJIAN KEAMANAN *WEBSITE* SISTEMASI UNISI MENGGUNAKAN METODE *PENETRATION TESTING*

SECURITY TESTING OF THE UNISI SYSTEMASI WEBSITE USING THE PENETRATION TESTING METHOD

Diajukan untuk memenuhi salah satu syarat
memperoleh derajat Sarjana S1

DISUSUN OLEH :

AGUNG RAMADHAN
403211010040

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS ISLAM INDRAGIRI
TEMBILAHAN

2025

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, Tugas Akhir ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Tembilahan, Juli 2026

Meterai
Rp. 10.000

Agung Ramadhan
NIM.403211010040

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah Swt. atas segala limpahan rahmat, karunia, kesehatan, dan kemudahan yang diberikan-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Pengujian Keamanan Website Sistemasi UNISI Menggunakan Metode Penetration Testing"**. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan dan memperoleh gelar Sarjana pada Program Studi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri.

Penyusunan skripsi ini bukanlah proses yang berjalan tanpa hambatan. Berbagai keterbatasan, kendala teknis, dan kesulitan selama pelaksanaan pengujian keamanan menjadi bagian yang harus dilalui oleh penulis. Namun, berkat doa, bantuan, arahan, dukungan, serta motivasi dari berbagai pihak, penelitian dan penyusunan skripsi ini akhirnya dapat diselesaikan dengan baik. Oleh karena itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Najamuddin, Lc., M.A., selaku Rektor Universitas Islam Indragiri, yang telah memberikan dukungan dan fasilitas selama penulis menjalani proses pendidikan.
2. Bapak Dr. Bayu Rianti, S.Si., M.Kom., selaku Dekan Fakultas Teknik dan Ilmu Komputer Universitas Islam Indragiri, yang telah memberikan dukungan serta kesempatan kepada penulis untuk menyelesaikan pendidikan.
3. Ibu Fitri Yunita, S.Si., M.Kom., selaku Ketua Program Studi Sistem Informasi, yang telah memberikan arahan, dukungan, dan pelayanan

akademik selama penulis menempuh pendidikan di Program Studi Sistem Informasi.

4. Bapak Abdul Muni, S.Kom., M.Kom, selaku Dosen Pembimbing I, yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, arahan, masukan, serta motivasi kepada penulis selama pelaksanaan penelitian dan penyusunan skripsi ini.
5. Bapak Dr. Bayu Rianti, S.Si., M.Kom, selaku Dosen Pembimbing II, yang telah memberikan bimbingan, koreksi, saran, dan arahan sehingga skripsi ini dapat diselesaikan dengan baik.
6. Seluruh dosen dan staf Fakultas Teknik dan Ilmu Komputer Universitas Islam Indragiri, khususnya Program Studi Sistem Informasi, yang telah memberikan ilmu pengetahuan, pengalaman, pelayanan, dan bantuan kepada penulis selama menjalani proses perkuliahan.
7. Pihak pengelola website Sistemasi Universitas Islam Indragiri yang telah memberikan izin, informasi, dan kesempatan kepada penulis untuk melaksanakan penelitian serta melakukan pengujian keamanan website sesuai dengan ruang lingkup yang telah ditentukan.

Ibu saya Saidah Ahmad yang selalu memberikan kasih sayang, doa, nasihat, pengorbanan, semangat, serta dukungan moral dan material kepada penulis. Setiap proses dan pencapaian yang diperoleh penulis tidak terlepas dari doa dan perjuangan kedua orang tua.

8. Seluruh keluarga yang senantiasa memberikan perhatian, dukungan, dan motivasi kepada penulis selama menjalani proses perkuliahan hingga penyelesaian skripsi ini.

9. Sahabat dan teman-teman seperjuangan Program Studi Sistem Informasi yang telah memberikan bantuan, semangat, kebersamaan, serta menjadi tempat bertukar pikiran selama proses perkuliahan dan penyusunan skripsi.
10. Semua pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan bantuan, doa, dukungan, dan kontribusi dalam pelaksanaan penelitian serta penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki berbagai kekurangan dan belum sepenuhnya sempurna, baik dari segi penulisan, metode pengujian, maupun pembahasannya. Keterbatasan ruang lingkup dan kemampuan penulis tentu memengaruhi hasil penelitian yang diperoleh. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun sebagai bahan evaluasi dan perbaikan untuk penelitian pada masa yang akan datang.

Akhir kata, penulis berharap skripsi ini dapat memberikan manfaat bagi pembaca, pengelola website Sistemasi Universitas Islam Indragiri, Fakultas Teknik dan Ilmu Komputer, serta pihak-pihak yang berkepentingan dalam pengembangan keamanan sistem informasi. Penelitian ini juga diharapkan dapat menjadi salah satu referensi bagi penelitian selanjutnya, khususnya yang berkaitan dengan pengujian keamanan website menggunakan metode *penetration testing*.

Indragiri Hilir, …… 2026

Agung Ramadhan

INTISARI

Website Sistemasi UNISI digunakan untuk mendukung kegiatan akademik, sehingga aspek keamanannya perlu diperhatikan agar data dan layanan di dalam sistem tidak mudah disalahgunakan. Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan, mengetahui tingkat risiko, serta memberikan rekomendasi perbaikan pada website Sistemasi UNISI. Metode yang digunakan adalah penetration testing dengan bantuan tools OWASP ZAP melalui fitur Automated Scan.

Hasil pengujian menunjukkan bahwa terdapat 19 alert yang terbagi dalam kategori risiko sedang, rendah, dan informasional. Beberapa kerentanan yang ditemukan meliputi tidak adanya token Anti-CSRF, belum diterapkannya Content Security Policy, tidak tersedia header anti-clickjacking, penggunaan pustaka JavaScript yang rentan, cookie tanpa atribut SameSite dan HttpOnly, serta penggunaan HTTPS yang belum konsisten. Temuan tersebut menunjukkan bahwa website Sistemasi UNISI masih memiliki beberapa kelemahan yang perlu segera diperbaiki.

Rekomendasi yang diberikan meliputi penerapan token Anti-CSRF, pengaturan header keamanan, pembaruan pustaka JavaScript, penguatan konfigurasi cookie, serta penerapan HTTPS secara menyeluruh. Perbaikan tersebut diharapkan dapat meningkatkan perlindungan sistem dan mengurangi risiko serangan terhadap website Sistemasi UNISI.

Kata kunci: keamanan website, penetration testing, OWASP ZAP, kerentanan, Sistemasi UNISI.

DAFTAR ISI

KATA PENGANTAR ii

DAFTAR ISI viii

DAFTAR TABEL x

DAFTAR GAMBAR xi

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 2

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 4

1.6 Sistematika Penulisan 4

BAB II TINJAUAN LITERATUR 7

2.1 Website 7

2.2 Sistem Informasi 8

2.3 Penetration Testing 8

2.4 OWASP 9

2.5 OWASP ZAP 10

2.6 Keamanan Website 17

2.7 Keamanan Siber (Cybersecurity) 18

2.8 Penelitian Terdahulu 20

BAB III METODE PENELITIAN 26

3.1 Alur Penelitian 26

3.2 Metode Pengumpulan Data 27
3.2.1 Studi Literatur 27
3.3 Perencanaan 28
3.4 Pengintaian 28
3.5 Scanning 29
3.6 Pengujian Kerentanan Website 29
3.6.1 Tested Website Determination 30
3.6.2 Software Installation 30
3.6.3 Vulnerabillity Testing 30
3.7 Kesimpulan 30
3.8 Solusi 31
3.9 Bahan dan Alat Penelitian 31

BAB IV HASIL DAN PEMBAHASAN 33

4.1 Implementasi Hasil 33
4.2 Analisa Hasil Penelitian 33
4.3 Hasil OWASP ZAP 34

BAB V KESIMPULAN DAN SARAN 42

5.1 Kesimpulan 42
5.2 Saran 43

DAFTAR PUSTAKA 44

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian Terdahulu 20

Tabel 3.1 Bahan dan Alat Penelitian..... 31

Tabel 4.1 Hasil *Report* OWASP ZAP 34

DAFTAR GAMBAR

Gambar 2.1 Logo *Software* OWASP ZAP 11

Gambar 2.2 Proses ZAP Tahap 1 11

Gambar 2.3 Proses ZAP Tahap 2 11

63

Gambar 3.1 Alur Penelitian 26

Gambar 4.1 Tampilan Halaman Dashboard OWASP ZAP..... 33

Gambar 4.2 Tampilan Hasil *Report* OWASP ZAP 34

BAB I

PENDAHULUAN

1.1 Latar Belakang

Universitas Islam Indragiri (UNISI), yang terletak di Kabupaten Indragiri Hilir, Riau, mengintegrasikan nilai-nilai Islam dengan ilmu pengetahuan dan teknologi untuk memberikan pendidikan berkualitas [1]. Dalam mendukung kegiatan akademik dan pengembangan keilmuan, UNISI menyediakan berbagai platform digital, salah satunya adalah Sistemasi UNISI, yaitu *website* jurnal referensi yang menjadi pusat akses publikasi ilmiah dari sivitas akademika UNISI

Sebagai *platform* terbuka yang dapat diakses oleh pengguna dari dalam maupun luar institusi, Sistemasi UNISI berperan penting dalam diseminasi pengetahuan dan penguatan reputasi akademik universitas [2]. Namun, penggunaan teknologi berbasis web juga membawa potensi risiko keamanan, seperti akses ilegal, pencurian data, atau penyisipan konten berbahaya [3]. Oleh karena itu, penting untuk melakukan evaluasi terhadap keamanan website jurnal ini guna melindungi integritas data dan menjaga kredibilitas institusi.

Dalam konteks keamanan siber, website jurnal seperti Sistemasi UNISI tetap rentan terhadap berbagai ancaman, termasuk serangan injeksi, eksploitasi celah sistem, serta gangguan terhadap fungsionalitas situs [4]. Serangan semacam ini dapat menyebabkan pencemaran konten, kebocoran data penulis, hingga kerusakan sistem yang menghambat akses publik terhadap publikasi ilmiah. Untuk itu, perlu dilakukan langkah-langkah pencegahan yang komprehensif agar platform jurnal ini dapat berfungsi secara optimal dan aman [5].

Uji penetrasi (*penetration testing*) adalah metode efektif untuk mengidentifikasi kerentanan keamanan dalam sistem informasi. Proses ini mencakup analisis kerentanan hingga simulasi serangan untuk mengevaluasi tingkat ketahanan sistem [6]. Alat seperti OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*) digunakan secara luas dalam pengujian keamanan aplikasi web [7]. Dengan fitur seperti deteksi ancaman SQL *injection* dan CSRF, OWASP ZAP membantu memperbaiki celah keamanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab [8].

Dalam pengujian terhadap *website* Sistemasi UNISI, penerapan penetration testing menggunakan OWASP ZAP bertujuan untuk menemukan celah-celah keamanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Alat ini tidak hanya mendeteksi kerentanan, tetapi juga mendukung integrasi dengan pengembangan perangkat lunak untuk menjaga keamanan sejak awal hingga akhir [10]. Selain sebagai alat deteksi, OWASP ZAP juga memungkinkan integrasi dengan proses pengembangan berkelanjutan untuk menjaga keamanan situs dari waktu ke waktu. Penelitian ini dilakukan untuk menganalisis tingkat keamanan website Sistemasi UNISI, mengidentifikasi risiko yang ada, serta memberikan rekomendasi teknis sebagai langkah peningkatan perlindungan dan keamanan sistem.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut:

1. Tingkat keamanan *website* Sistemasi UNISI dalam menghadapi ancaman cyber saat ini.

2. Potensi ancaman keamanan yang dapat dihadapi oleh *website* Sistemasi UNISI.
3. Upaya meningkatkan keamanan website Sistemasi UNISI melalui metode penetration testing dan implementasi rekomendasi perbaikan.

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang perlu diperhatikan, di antaranya:

1. Pengujian *penetration test* hanya menggunakan *tools* OWASP ZAP.
2. Penelitian ini hanya untuk menganalisis kerentanan pada *website* Sistemasi UNISI.
3. Penelitian akan membatasi diri pada penggunaan metode uji penetrasi sebagai alat utama untuk mengidentifikasi kerentanan keamanan. Metode ini akan digunakan untuk mensimulasikan serangan yang mungkin dilakukan oleh penyerang asing, tanpa melibatkan serangan yang sebenarnya.

1.4 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

1. Mengidentifikasi kerentanan keamanan pada *website* Sistemasi UNISI melalui uji penetrasi menggunakan OWASP ZAP, untuk menemukan potensi celah keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab.
2. Menganalisis efektivitas metode uji penetrasi dalam meningkatkan keamanan situs web, khususnya pada *platform* berbasis web di lingkungan akademik seperti Sistemasi UNISI di Fakultas Teknik dan Ilmu Komputer Universitas Islam Indragiri.

3. Memberikan rekomendasi perbaikan dan langkah pencegahan berdasarkan hasil uji penetrasi yang dilakukan, untuk meningkatkan keamanan dan mengurangi risiko ancaman *cyber* pada *website* Sistemasi UNISI.

1.5 Manfaat Penelitian

1. Penelitian ini membantu meningkatkan keamanan *website* SISTEMASI UNISI dengan mengidentifikasi kerentanan, sehingga dapat meminimalkan risiko serangan siber dan kerusakan sistem.
2. Penelitian ini menjaga keamanan dan kerahasiaan data penting seperti data mahasiswa, nilai, KRS, proposal, tugas akhir, yudisium, dan wisuda dengan menutup celah keamanan yang ada.
3. Penelitian ini memperkuat pemahaman tentang penetration testing sebagai metode efektif untuk mengamankan situs web dan mendukung studi keamanan informasi di lingkungan akademik.

1.6 Sistematika Penulisan

Sistematika penulisan terbagi dalam lima bab, meliputi pendahuluan, landasan teori, metode penelitian, hasil dan pembahasan, dan penutup. Berikut penjelasan singkat ke lima bab tersebut :

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB 2 TINJAUAN LITERATUR

Pada bab ini menjelaskan teori-teori terkait landasan pelaksanaan penelitian, meliputi teori *website*, *penetration testing* dengan menggunakan *tools* OWASP ZAP, dan penelitian terdahulu yang relevan untuk mendukung penelitian ini.

BAB 3 METODE PENELITIAN

Pada bab ini menjelaskan secara metodis proses penelitian, mencakup penjelasan-penjelasan tentang pendekatan penelitian, prosedur penelitian, keabsahan data, tempat dan waktu penelitian, narasumber, teknis analisis data penelitian, alat analisis data penelitian serta instrument penelitian. Tujuannya secara tidak langsung memberikan gambaran tentang ruang lingkup dan batasan penelitian kepada para pembaca.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan pelaksanaan dan hasil pengujian keamanan website Sistemasi UNISI menggunakan metode penetration testing dengan bantuan tools OWASP ZAP. Pembahasan meliputi tahapan pengujian melalui fitur Automated Scan, proses memasukkan alamat website sebagai target pengujian, analisis hasil penelitian, serta hasil pemindaian kerentanan yang ditemukan. Bab ini juga menguraikan jenis ancaman, tingkat risiko, deskripsi kerentanan, dampak yang dapat ditimbulkan, dan solusi perbaikan berdasarkan hasil laporan OWASP ZAP.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini menjelaskan kesimpulan yang diperoleh berdasarkan hasil pengujian keamanan website Sistemasi UNISI menggunakan metode penetration testing dengan tools OWASP ZAP. Kesimpulan memuat hasil identifikasi kerentanan, tingkat risiko keamanan, efektivitas penggunaan OWASP ZAP, serta rekomendasi perbaikan untuk meningkatkan keamanan website. Selain itu, bab ini juga memuat saran berupa penerapan Content Security Policy, penambahan header keamanan, peningkatan pengelolaan cookie, serta penggunaan protokol HTTPS secara konsisten.

BAB II

TINJAUAN LITERATUR

2.1 *Website*

Terdapat dua konsep utama yang menjelaskan tentang situs web. Pertama, situs web merupakan kumpulan halaman yang memuat informasi dalam berbagai format seperti teks, gambar, animasi, dan suara. Halaman tersebut dapat memiliki sifat statis atau dinamis, dan terhubung membentuk sebuah struktur yang saling terkait dalam jaringan situs [12]. Kedua, aplikasi berbasis web merupakan jenis aplikasi yang dapat diakses melalui peramban web tanpa perlu proses instalasi, bergantung pada internet, dan tidak terikat pada sistem operasi. Fleksibilitasnya memungkinkan pengguna untuk mengakses dan memanfaatkan fungsinya secara daring [13].

Sebuah *website* terdiri dari serangkaian *file* yang saling terhubung dan disimpan dalam satu *folder*. *Website* berfungsi sebagai tempat untuk mengumpulkan *file-file* halaman web, yang mencakup gambar, skrip CSS, audio, dan berbagai jenis *file* lainnya. Dengan banyaknya *file* yang membentuk sebuah website, diperlukan pengelolaan *file* yang baik untuk memastikan kinerjanya optimal [14].

Situs web, sebagai kumpulan halaman dengan berbagai jenis informasi, dapat memiliki karakteristik yang bervariasi dari statis hingga dinamis, serta terhubung membentuk struktur yang mengarah pada jaringan situs secara keseluruhan. Di sisi lain, aplikasi berbasis web tidak memerlukan instalasi dan dapat diakses melalui peramban web, memanfaatkan internet, dan tidak bergantung pada sistem operasi tertentu, memungkinkan pengguna untuk mengakses dan menggunakan

layanannya secara *online* [13]. Dua konsep ini memberikan gambaran tentang struktur dan fungsionalitas situs web serta aplikasi web berbasis *browser* dalam menyajikan informasi dan layanan secara daring kepada pengguna.

2.2 Sistem Informasi

Sistem informasi adalah sebuah sistem dalam organisasi yang mengintegrasikan kebutuhan untuk memproses transaksi sehari-hari, mendukung kegiatan manajerial dan strategi organisasi, serta menyediakan laporan-laporan yang dibutuhkan oleh pihak eksternal tertentu [15].

2.3 *Penetration Testing*

Penetration testing adalah upaya yang dilakukan secara sah untuk mengeksploitasi sistem komputer dengan tujuan membuat sistem tersebut menjadi aman [16]. *Penetration test*ing yang dilakukan dengan baik dapat menghasilkan rekomendasi untuk mengatasi dan memperbaiki masalah yang ditemukan selama pengujian [17].

*Penetration test*ing adalah serangkaian proses yang melibatkan prosedur dan teknik untuk mengevaluasi keamanan sistem komputer atau jaringan dengan melakukan simulasi penyerangan [18]. Tujuan utamanya adalah untuk mengidentifikasi potensi kerentanan dalam sistem sehingga celah-celah keamanan tersebut dapat ditemukan dan kemudian ditutup atau diperbaiki. *Penetration test*ing dilakukan sebagai langkah preventif untuk mengatasi risiko peretasan pada suatu sistem [19].

2.4 OWASP

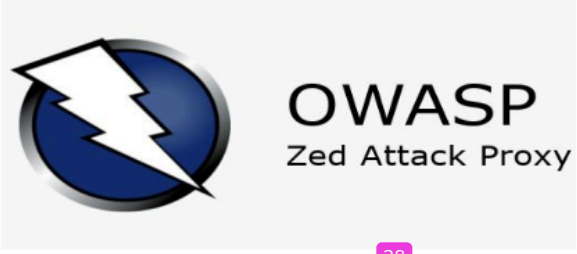
Open Web Application Security Project (OWASP) adalah sebuah *framework* yang bersifat *open source* dengan fokus utama pada perbaikan keamanan perangkat lunak aplikasi [20]. OWASP merupakan sebuah organisasi yang didedikasikan untuk menemukan dan mengatasi kerentanan keamanan dalam aplikasi web. Berdasarkan standar yang dikeluarkan oleh OWASP, ada sebelas langkah yang dapat dilakukan untuk menilai dan menguji keamanan pada sebuah *website*, termasuk *Information Gathering*, *Configuration Management*, *Secure Transmission*, *Authentication, Session Management*, *Authorization*, *Cryptography*, *Data Validation*, *Denial of Service*, dan *Error Handling*. Langkah-langkah ini membantu dalam mengidentifikasi dan mengatasi celah keamanan yang mungkin ada dalam aplikasi web sehingga dapat meningkatkan tingkat keamanan secara keseluruhan [21].

Menurut Mulyanto, dkk [22], *Open Web Application Security Project* (OWASP) adalah sebuah organisasi internasional nirlaba yang didirikan oleh *Open Web Application Security Project* (OWASP) *Foundation* pada tanggal 21 April 2004 di Amerika Serikat. Fokus utama dari OWASP adalah meningkatkan keamanan perangkat lunak dan berkomitmen untuk membantu organisasi dalam pengembangan, perolehan, operasi, dan pemeliharaan aplikasi yang dapat dipercaya, dengan tujuan memastikan keamanan dalam pembuatan dan pengembangan aplikasi. Misi OWASP adalah melindungi perangkat lunak sehingga individu dan organisasi dapat membuat keputusan yang tepat terkait dengan risiko keamanan.

2.5 OWASP ZAP

OWASP Zed Attack Proxy (ZAP) adalah alat pengujian penetrasi *open-source* yang tersedia secara gratis dan dikelola di bawah naungan *Open Web Application Security Project* (OWASP) [23]. ZAP dirancang khusus untuk menguji aplikasi web dan memiliki fleksibilitas serta kemampuan untuk diperluas. Secara esensial, ZAP berfungsi sebagai "*proxy man-in-the-middle*" berada di antara browser pengujian dan aplikasi web yang sedang diuji. Ini memungkinkan ZAP untuk mencegat dan memeriksa pesan yang dikirim antara *browser* dan aplikasi web, dapat mengubah kontennya jika diperlukan, dan kemudian meneruskan paket tersebut ke tujuan. ZAP dapat digunakan sebagai aplikasi mandiri atau sebagai proses daemon. OWASP ZAP (*Zed Attack Proxy*) digunakan secara luas dalam pengujian penetrasi untuk menemukan kerentanan atau celah keamanan dalam aplikasi *website*, dan menyediakan fitur pemindaian otomatis yang berguna dalam proses ini [21].

OWASP ZAP adalah alat pemindai kerentanan yang dikembangkan oleh organisasi OWASP (*Open Web Application Security Project*). Alat ini merupakan salah satu proyek paling aktif dalam lingkup OWASP, dan terus mengalami pengembangan. OWASP ZAP adalah perangkat sumber terbuka, yang berarti bahwa siapa pun dapat mengakses, menggunakan, dan berkontribusi pada pengembangan alat ini. Hal ini menjadikannya salah satu alat yang sangat berharga dalam mengidentifikasi dan mengatasi kerentanan keamanan pada aplikasi web [24].



Gambar 2.1 Logo *Software* OWASP ZAP

Zed Attack Proxy (ZAP) adalah alat pengujian penetrasi sumber terbuka gratis yang dikelola di bawah payung *The Software Security Project* (SSP). ZAP dirancang khusus untuk menguji aplikasi web dan fleksibel serta dapat diperluas [25]. Pada intinya, ZAP dikenal sebagai "*proxy man-in-the-middle*" yang berdiri di antara *browser* penguji dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang dikirim antara browser dan aplikasi web, memodifikasi konten jika diperlukan, dan kemudian meneruskan paket-paket tersebut ke tujuan. Ini dapat digunakan sebagai aplikasi yang berdiri sendiri, dan sebagai proses daemon.



Gambar 2.2 Proses ZAP Tahap 1

Jika ada proksi jaringan lain yang sudah digunakan, seperti di banyak lingkungan perusahaan, ZAP dapat dikonfigurasi untuk menyambung ke proksi tersebut.



Gambar 2.3 Proses ZAP Tahap 2

ZAP menyediakan fungsionalitas untuk berbagai tingkat keahlian, mulai dari pengembang, penguji yang baru mengenal pengujian keamanan, hingga spesialis pengujian keamanan. ZAP memiliki versi untuk setiap OS utama dan Docker, jadi *user* tidak terikat pada satu OS. Fungsionalitas tambahan tersedia secara bebas dari berbagai *add-on* di ZAP *Marketplace*, dapat diakses dari dalam klien ZAP. Karena ZAP bersifat *open-source*, kode sumbernya dapat diperiksa untuk melihat secara tepat bagaimana fungsionalitas tersebut diimplementasikan. Siapa pun dapat secara sukarela mengerjakan ZAP, memperbaiki bug, menambahkan fitur, membuat permintaan tarik untuk melakukan perbaikan ke dalam proyek, dan membuat *add-on* untuk mendukung situasi khusus.

Daftar OWASP *Top Ten* adalah alat yang diakui secara luas untuk mengidentifikasi kerentanan dalam aplikasi web. Karena panduan keamanan khusus untuk *blockchain* saat ini masih kurang, memetakan kerangka kerja yang ada, seperti OWASP, ke dalam *blockchain* dapat membantu mengidentifikasi potensi kerentanan dalam sistem *blockchain*. Meskipun Daftar OWASP *Top Ten* dirancang untuk menggambarkan kerentanan yang dihadapi oleh pengembang aplikasi web, sembilan dari sepuluh kerentanan OWASP juga berlaku untuk sistem blockchain. Pengecualiannya adalah XML *External Entities* (XXE), yang tidak berlaku karena tidak adanya penggunaan XML dalam *blockchain* [26].

Ancaman keamanan terhadap aplikasi mobile semakin meningkat dengan pesat. Kelemahan dan cacat keamanan dalam aplikasi mobile memberikan peluang bagi peretas untuk masuk dan mengakses informasi sensitif. Analisis kebutuhan defensif harus menjadi bagian integral dari SDLC (*Software Development Life Cycle*) yang aman untuk *mobile.* Pengembang perlu

mempertimbangkan kerahasiaan informasi dan integritas data, serta memverifikasi keamanan sejak awal siklus pengembangan daripada memperbaiki lubang keamanan setelah serangan dan kebocoran data terjadi. Menghilangkan kerentanan keamanan yang diketahui sejak awal akan membantu pengembang meningkatkan keamanan aplikasi dan mengurangi kemungkinan eksploitasi. Namun, banyak pengembang perangkat lunak kurang memiliki pengetahuan dan keterampilan keamanan yang diperlukan pada tahap pengembangan, sehingga pendidikan *Secure Mobile Software Development* sangat diperlukan bagi insinyur perangkat lunak mobile. Dalam makalah ini, kami mengusulkan analisis kebutuhan keamanan yang dipandu berdasarkan rekomendasi risiko keamanan OWASP *Mobile Top Ten* untuk pengembangan perangkat lunak mobile Android dan keterkaitannya dengan kontrol pengembangan dalam SDLC. Membangun aplikasi yang aman dan kebal terhadap risiko OWASP *Mobile Top Ten* akan menjadi pendekatan yang efektif untuk memberikan pedoman keamanan mobile yang sangat berguna [27]. Adapun acaman yang dapat diidentifikasi oleh OWASP ZAP sebagai berikut:

1) *Injection*

Serangan injeksi dapat terjadi ketika aplikasi tidak melakukan validasi dan penyaringan input pengguna secara memadai, sehingga penyerang memiliki peluang untuk memasukkan perintah yang seharusnya tidak dijalankan oleh sistem. Pada kasus SQL, lemahnya proses validasi input dapat dimanfaatkan untuk melewati mekanisme autentikasi maupun mengeksekusi perintah tertentu pada basis data tanpa izin. Permasalahan serupa juga dapat muncul pada teknologi blockchain.

Sebelum peluncuran mainnet EOS, peneliti dari Qihoo 360 menemukan kelemahan pada proses parsing smart contract EOS yang memungkinkan terjadinya penulisan buffer di luar batas [28]. Kerentanan tersebut berpotensi dimanfaatkan untuk mengganggu atau mengambil alih sistem melalui eksekusi smart contract berbahaya.

2) Kerentanan CSRF

Kerentanan CSRF (*Cross-Site Request Forgery*) adalah jenis serangan keamanan yang memanfaatkan kepercayaan yang diberikan oleh web browser kepada sebuah situs web. Dalam serangan CSRF, seorang penyerang mengirimkan permintaan yang tidak diinginkan dari pengguna yang sudah terautentikasi ke situs web yang ditargetkan. Ini terjadi ketika pengguna terautentikasi di suatu situs (misalnya media sosial, bank, atau situs *e-commerce*) dan secara tidak disadari mengirim permintaan HTTP ke situs lain yang dieksploitasi oleh penyerang [29].

3) Kerentanan otentikasi yang rusak

Kerentanan otentikasi yang rusak memungkinkan penyerang menyamar sebagai pengguna sah. Implementasi otentikasi yang benar sangat penting dalam sistem blockchain karena penggunaan kriptografi kunci publik menciptakan permukaan serangan yang besar. Contoh kasus terjadi pada cryptocurrency LISK, di mana desain yang kurang memperhatikan keamanan memungkinkan serangan pada otentikasi. Alamat pengguna dihasilkan dengan hashing kunci publik dan memotong hasilnya menjadi 64 bit, yang membuat alamat tidak langsung terikat dengan kunci publik dan rentan terhadap serangan. Alamat di LISK hanya

terikat dengan kunci publik saat pengguna melakukan transaksi, sehingga banyak akun yang hanya menerima nilai tetap rentan terhadap serangan. Penyerang hanya perlu melakukan 2^{64} operasi pembuatan kunci untuk menemukan pasangan kunci privat/publik yang cocok dengan alamat tertentu, mengurangi kompleksitas dengan faktor M jika menargetkan salah satu dari M alamat. Serangan ini cukup layak dilakukan dan beberapa akun rentan memegang jutaan dolar.

4) *Sensitive Data Exposure*

Sensitive data exposure adalah data berharga yang harus dijaga kerahasiaannya tidak terlindungi dengan baik. Teknologi blockchain rentan terhadap kerentanan ini karena kurangnya pemahaman tentang teknologinya. Blockchain bersifat tidak dapat diubah, artinya data yang disimpan tidak dapat dihapus tanpa kontrol dari semua node di jaringan. Kebanyakan blockchain juga bersifat publik, memungkinkan siapa saja untuk mengunduh dan menyimpan salinan lengkap data dalam buku besar.

Dalam jangka pendek, kombinasi ini membuat blockchain rentan terhadap upaya penambangan data. Banyak organisasi berspesialisasi dalam menambang blockchain untuk data publik yang dapat digabungkan menjadi informasi berguna yang dapat digunakan untuk penegakan hukum, spionase perusahaan, dan tujuan lainnya. Dalam jangka panjang, semua kriptografi dapat ditembus. Komputasi kuantum di masa depan akan memungkinkan dekripsi data yang disimpan di blockchain yang dienkripsi dengan algoritma enkripsi asimetris klasik. Jika data harus

dirahasiakan selamanya, seperti data pribadi yang dilindungi oleh undang-undang privasi seperti GDPR atau HIPAA, data tersebut sebaiknya tidak pernah disimpan di blockchain publik, bahkan dalam format terenkripsi.

5) *XML External Entities (XXE)*

Kerentanan *XML External Entities (XXE)* didasarkan pada referensi entitas eksternal di dalam dokumen XML, yang dapat mengekspos file *internal* sensitif di server web. Namun, karena *blockchain* tidak berbasis XML, kerentanan ini umumnya tidak berlaku pada teknologi blockchain.

6) *SQL Injection*

SQL injection adalah serangan keamanan di mana penyerang memanfaatkan kerentanan pada aplikasi web yang menggunakan SQL (*Structured Query Language*) untuk memanipulasi database. Serangan ini terjadi ketika aplikasi web tidak memvalidasi input pengguna dengan benar sebelum mengirimkannya ke server database. Sebagai hasilnya, penyerang dapat menyisipkan atau "injeksi" kode SQL yang berbahaya ke dalam pernyataan SQL yang dieksekusi oleh database. Dampak dari serangan SQL injection dapat sangat serius, termasuk pengungkapan atau pencurian data sensitif, modifikasi atau penghapusan data, bahkan pengambilalihan kontrol penuh terhadap server database. Beberapa bentuk serangan SQL injection meliputi penggunaan tanda kutip, komentar SQL, dan teknik-teknik lain untuk mengubah logika pernyataan SQL yang dieksekusi [30].

7) *Broken Access Control*

Broken access control berbeda dengan broken *authentication* di mana penyerang berpura-pura menjadi pengguna yang tidak sah, *broken access control* memungkinkan pengguna jahat mengakses fungsi yang dilindungi secara tidak sah. Mekanisme kontrol akses yang buruk adalah salah satu kerentanan utama dalam *smart contract Ethereum*. Contoh nyata adalah dompet multi-tanda tangan berbasis *smart contract Parity* yang dieksploitasi dua kali karena kerentanan kontrol akses. Pada serangan pertama, penyerang mengambil alih kontrak dompet Parity dan menguras dana. Pada serangan kedua, fungsi serupa dalam kontrak perpustakaan yang digunakan oleh semua dompet Parity diserang, diambil alih, dan dihancurkan, membuat semua dompet Parity tidak dapat digunakan dan menyebabkan sekitar 1% dari seluruh Ether hilang selamanya.

2.6 Keamanan *Website*

Keamanan suatu *website* adalah prioritas utama bagi pengelola dan pengguna situs. Seringkali, pengguna hanya mempertimbangkan desain tampilan dan konten untuk menarik pengunjung, tanpa memperhatikan aspek keamanan. Namun, mengabaikan keamanan *website* dapat berdampak serius pada pengguna sendiri, karena data penting dalam *website* dapat diretas atau tampilan *website* dapat dimodifikasi oleh pihak yang tidak berwenang. Keamanan *website* yang baik adalah melindungi komputer, aplikasi, dan jaringannya untuk menjaga keamanan informasi yang terdapat di dalamnya. Dengan demikian, penting untuk memahami bahwa keamanan bukan hanya tanggung jawab pengelola, tetapi juga setiap pengguna yang berinteraksi dengan *website* tersebut [22].

Menurut Editya dan Mulyati [31], keamanan adalah salah satu aspek utama dalam konteks sistem jaringan internet. Pada dasarnya, internet dibangun melalui jaringan komputer yang saling terhubung. Dalam hal ini, jumlah pengguna yang terhubung dalam suatu jaringan memiliki dampak signifikan terhadap keamanan data dan informasi yang dikirim dan diterima. Keamanan informasi menjadi krusial karena dapat rentan terhadap berbagai serangan dan potensi penyalahgunaan data. Oleh karena itu, menjaga keamanan dalam lingkungan internet menjadi suatu keharusan yang tidak bisa diabaikan.

2.7 Keamanan Siber (*Cybersecurity*)

Keamanan siber memainkan peran kunci dalam melindungi infrastruktur digital, data, dan informasi pada era teknologi informasi saat ini. Salah satu manfaat utamanya adalah mengamankan data pribadi dan sensitif dari akses ilegal, memastikan keaslian data, dan menjaga ketersediaan sistem bagi pengguna yang sah. Selain itu, keamanan siber juga membantu meningkatkan kepercayaan dalam transaksi *online*, mencegah serangan malware, dan melindungi infrastruktur vital seperti sistem energi dan keuangan dari ancaman siber. Dengan mengurangi risiko serangan siber, keamanan siber juga berkontribusi pada pemenuhan peraturan keamanan data, pengurangan risiko pencurian identitas, dan meningkatkan kesadaran keamanan di organisasi. Melalui manfaat ini, keamanan siber menjadi sangat penting dalam menjaga integritas sistem informasi di dunia digital yang terus berkembang [32].

Tujuan utama keamanan siber adalah melindungi infrastruktur digital, data, dan informasi dari serangan yang berpotensi merusak, mencuri, atau mengganggu. Beberapa tujuan kunci dari keamanan siber meliputi:

1. Perlindungan Data Sensitif: Mencegah akses yang tidak sah atau pencurian terhadap data sensitif seperti informasi pribadi, informasi keuangan, dan rahasia perusahaan.
2. Mempertahankan Integritas Data: Menjaga keaslian dan integritas data agar tidak terpengaruh oleh manipulasi atau perubahan yang tidak sah.
3. Menjamin Ketersediaan Layanan: Memastikan bahwa sistem dan layanan digital tersedia untuk pengguna yang berhak dan tidak terganggu oleh serangan atau gangguan.
4. Meningkatkan Kepercayaan: Memberikan kepercayaan kepada pengguna dalam melakukan transaksi online dan interaksi digital lainnya dengan aman dan terpercaya.
5. Mencegah Ancaman Malware: Mengidentifikasi, mencegah, dan menghilangkan serangan malware yang dapat merusak sistem dan mencuri informasi sensitif.
6. Menjaga Infrastruktur Kritis: Melindungi infrastruktur kritis seperti sistem energi, keuangan, dan layanan publik dari serangan siber yang dapat mengganggu operasional dan keamanan.
7. Pematuhan Regulasi: Memastikan bahwa organisasi mematuhi peraturan dan undang-undang terkait keamanan data serta melindungi privasi pengguna.
8. Meningkatkan Kesadaran Keamanan: Mengedukasi pengguna dan staf organisasi tentang praktik keamanan digital untuk mengurangi risiko serangan siber.

9. Perlindungan Reputasi dan Efisiensi Operasional: Mengurangi dampak serangan siber untuk menjaga reputasi bisnis, efisiensi operasional, dan kelangsungan operasi organisasi.
10. Mengamankan Jaringan dan IoT: Menjaga keamanan jaringan komputer dan perangkat In*ternet of Things* (IoT) dari serangan dan eksploitasi yang dapat merusak atau mencuri data.

2.8 Penelitian Terdahulu

Tabel 2.1 Perbandingan Penelitian Terdahulu

Peneliti	Hasil Penelitian	Komentar
Yum Thurfah Afifa Rosaliah, Jayanta Jayanta, Bayu Hananto (2021)	Penelitian ini menemukan beberapa celah keamanan signifikan, termasuk masalah pada *Broken Authentication*, *Sensitive Data Exposure*, dan *Security Misconfiguration*, mengindikasikan ketidakamanan dalam otentikasi, perlindungan data sensitif, dan konfigurasi keamanan. Selain itu, temuan tambahan melibatkan celah keamanan *Clickjacking*, menunjukkan adanya kerentanan tambahan yang perlu diperhatikan dan diatasi.	Dari penelitian tersebut, peneliti hanya menggunakan satu metode yaitu OWASP ZAP, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.
Bahrun Ghozali, Kusrini Kusrini, Sudarmawan Sudarmawan (2019)	Hasil penelitian mengidentifikasi tingkat risiko berdasarkan faktor *Likelihood* dan *Impact*, menghasilkan tiga tingkat risiko: *high*, *medium*, dan *low*. Temuan ini memberikan wawasan berharga untuk pengelola dan pengembang	Dari penelitian tersebut, peneliti hanya menggunakan satu metode yaitu OWASP ZAP, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.

Peneliti	Hasil Penelitian	Komentar
	sistem, memungkinkan pengambilan tindakan proaktif untuk mencegah dan mengatasi risiko keamanan. Penelitian ini berkontribusi pada pengelolaan risiko keamanan sistem informasi krusial di tingkat pemerintahan.	
Hery Sofyan, dkk (2023)	Hasil penelitian ini menemukan satu kerentanan dengan level tinggi, tiga dengan level medium, dan enam dengan level rendah, sehingga secara umum tingkat kerentanan *website* berada pada level medium.	Dari penelitian tersebut, peneliti hanya menggunakan satu metode yaitu OWASP ZAP, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.
Fahmi Fachri, Abdul Fadlil, Imam Riadi (2021)	Tentang keamanan web server melalui penetration test menemukan empat kelemahan tingkat tinggi, empat tingkat menengah, dan dua tingkat rendah pada Sistem Informasi Akademik perguruan tinggi. Temuan mencakup keberadaan port terbuka yang memudahkan peretas untuk masuk dan mengeksploitasi informasi. Uji coba simulasi serangan berhasil mendapatkan *username* dan *password*, menyoroti kerentanan signifikan dalam keamanan *web server*. Temuan ini memberikan dasar untuk perbaikan dan penguatan keamanan sistem.	Dari penelitian tersebut, peneliti hanya menggunakan satu metode yaitu SQL Lite, tanpa melakukan perbandingan dengan metode *penetration testing* yang lainnya, sehingga dampak yang lain tidak teridentifikasi secara maksimal.
Sabrina Asiah	Hasil pengujian menunjukkan	Dari penelitian tersebut,

Peneliti	Hasil Penelitian	Komentar
Febriani, Abdul Muni, Bayu Riyanto, Muhammad Jalil, Chrismondari (2024)	bahwa situs web SIAKAD CLOUD memiliki 14 kerentanan dengan tingkat keparahan sedang hingga rendah, serta 4 kerentanan pada tingkat informasi. Secara keseluruhan, 18 kerentanan teridentifikasi, yang kemudian diikuti dengan rekomendasi perbaikan. Meskipun kerentanannya tergolong rendah, penelitian ini menyarankan agar administrator situs web SIAKAD CLOUD melakukan langkah-langkah perbaikan guna memperkuat pertahanan dari ancaman serangan yang lebih besar	peneliti hanya mengidentifikasi kerentanan menggunakan satu metode pengujian tanpa membandingkannya dengan metode atau alat lainnya seperti OWASP ZAP atau Nmap. Hal ini membuat potensi ancaman yang lebih kompleks atau spesifik tidak terdeteksi secara maksimal, sehingga rekomendasi perbaikan kurang menyeluruh.
Syarif Hidayatulloh, Desky Saptadiaji (2021)	Hasil penelitian menunjukkan bahwa website Universitas ARS memiliki 13 kerentanan yang berhasil teridentifikasi melalui proses pemindaian. Dari jumlah tersebut, satu kerentanan berada pada tingkat ancaman sedang, sementara 12 lainnya berada pada tingkat ancaman rendah. Berdasarkan analisis terhadap hasil pengujian, dapat disimpulkan bahwa website Universitas ARS memiliki tingkat keamanan yang sangat baik. Website ini memenuhi ketiga aspek keamanan informasi, yakni kerahasiaan, integritas, dan ketersediaan, serta didukung oleh web	Dari penelitian tersebut, peneliti hanya mengidentifikasi kerentanan berdasarkan hasil pemindaian tanpa melakukan eksplorasi lebih lanjut dengan metode lain, seperti uji penetrasi manual atau simulasi serangan nyata. Hal ini dapat membatasi analisis mendalam terhadap kerentanan tingkat ancaman sedang dan mengabaikan potensi ancaman lain yang mungkin tidak terdeteksi oleh alat pemindaian

Peneliti	Hasil Penelitian	Komentar
	server dan perangkat lunak sistem informasi akademik yang aman	
Yunanri W, Yuliadi, Fahri Hamdani, Yasinta Bella Fitriana, dan Nabil Oper (2023)	Penelitian menunjukkan bahwa website Universitas Teknologi Sumbawa (UTS) memiliki keamanan yang baik terhadap serangan Distributed Denial of Service (DDoS). Meskipun pengujian dilakukan dengan berbagai intensitas serangan menggunakan Low Orbit Ion Cannon (LOIC), mulai dari 500, 1000, 5000, hingga 10.000 paket, website tetap dapat diakses meskipun mengalami kelambatan. Penelitian juga merekomendasikan penerapan teknik blacklist IP dan penggunaan firewall untuk meningkatkan perlindungan terhadap serangan DDoS di masa mendatang.	Penelitian ini hanya menggunakan satu alat, yaitu Low Orbit Ion Cannon (LOIC), untuk menguji ketahanan website terhadap serangan DDoS. Akan lebih baik jika peneliti membandingkan hasilnya dengan alat lain, seperti HOIC atau Slowloris, untuk memberikan gambaran lebih komprehensif mengenai keamanan website. Selain itu, meskipun rekomendasi seperti teknik blacklist IP dan firewall diberikan, penelitian tidak menjelaskan implementasi spesifik atau efektivitas solusi tersebut dalam menghadapi serangan yang lebih kompleks.
Betta Wahyu Retna Mulya, Avinanta Tarigan (2018)	Celah keamanan pada sistem jaringan komputer adalah kelemahan yang dapat dimanfaatkan oleh penyerang untuk mengancam kerahasiaan, integritas, atau ketersediaan sistem. Penanganan celah ini memerlukan analisis menggunakan metode CVSS dan FMEA untuk menentukan skala prioritas berdasarkan tingkat kerentanan. Hasil analisis menunjukkan bahwa	Penelitian ini memberikan hasil yang cukup komprehensif dengan memanfaatkan penggabungan metode CVSS dan FMEA untuk menentukan prioritas mitigasi risiko. Namun, penelitian ini belum membandingkan efektivitas metode tersebut dengan pendekatan lainnya, seperti OCTAVE atau FAIR, yang juga sering digunakan dalam analisis risiko keamanan.

Peneliti	Hasil Penelitian	Komentar
	prioritas penanganan di Politeknik Kota Malang dimulai dari server singa, diikuti server sierra, dino, dan leopard, dengan tingkat kerentanan 40–60%. Penggabungan metode ini efektif untuk menentukan peringkat mitigasi risiko berdasarkan dampak potensial kerentanan.	Selain itu, deskripsi tentang implementasi langkah mitigasi pada setiap server kurang mendalam, sehingga sulit untuk menilai sejauh mana solusi yang diusulkan dapat mengatasi kerentanan yang teridentifikasi secara optimal.
Wahyudin, Heri Kuswara, Resti, Sopiyan Dalis (2024)	Penelitian menunjukkan bahwa website sakupos.com, yang berbasis point of sales, memiliki 10 kerentanan keamanan yang terdeteksi melalui pengujian menggunakan OWASP ZAP. Dari hasil scanning, ditemukan 7 kerentanan dengan tingkat risiko Medium, 2 kerentanan dengan tingkat risiko Low, dan 1 kerentanan dengan tingkat risiko Informational. Penelitian ini juga memberikan rekomendasi solusi untuk mencegah potensi serangan berdasarkan hasil analisis tingkat kerentanan. Temuan ini menunjukkan pentingnya vulnerability assessment untuk meningkatkan keamanan website dan memitigasi risiko serangan siber.	Penelitian ini berhasil mengidentifikasi kerentanan pada website sakupos.com dan memberikan rekomendasi perbaikan yang relevan. Namun, metode pengujian hanya menggunakan OWASP ZAP tanpa membandingkannya dengan alat lain seperti Burp Suite atau Nessus, sehingga validasi hasil dan cakupan deteksi kerentanan mungkin kurang optimal. Selain itu, penelitian ini tidak menjelaskan implementasi solusi atau evaluasi efektivitas dari rekomendasi yang diberikan, sehingga tidak dapat dipastikan apakah langkah yang disarankan dapat mengurangi risiko secara signifikan. Pendekatan yang lebih komprehensif akan memberikan gambaran yang lebih lengkap tentang keamanan website.
Christian Alderi	Penelitian menekankan	Penelitian ini memberikan

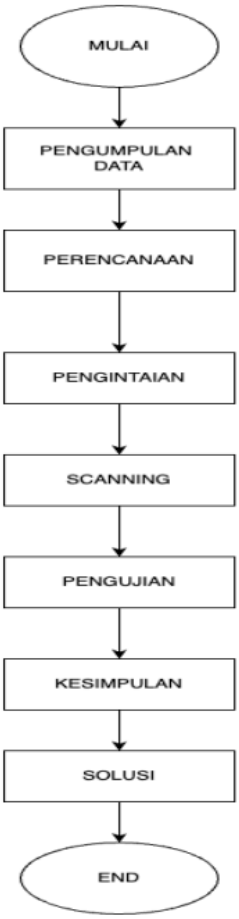
Peneliti	Hasil Penelitian	Komentar
Jeffta Soeweh, dkk (2022)	pentingnya langkah preventif, seperti penilaian kerentanan menggunakan framework OWASP Top 10, untuk meminimalkan dampak buruk serangan siber. Berdasarkan laporan BSSN tahun 2021, serangan siber terhadap sektor pendidikan tinggi terus meningkat, sehingga institusi seperti FMIPA UNSRAT perlu meningkatkan keamanan siber dan melindungi infrastruktur informasi vital. Penelitian ini memberikan rekomendasi untuk memperkuat keamanan website FMIPA UNSRAT, dengan harapan dapat mencegah serangan siber dan melindungi informasi penting institusi.	pemahaman yang baik tentang urgensi langkah preventif untuk melindungi infrastruktur informasi di sektor pendidikan tinggi. Namun, penelitian hanya berfokus pada penilaian kerentanan dengan framework OWASP Top 10 tanpa menyebutkan metode tambahan seperti penetration testing atau monitoring berkelanjutan, yang dapat memberikan wawasan lebih dalam tentang ancaman nyata. Selain itu, tidak ada informasi mengenai implementasi atau uji coba rekomendasi keamanan yang diberikan, sehingga efektivitas langkah-langkah tersebut tidak dapat diverifikasi. Penambahan analisis risiko atau studi kasus serangan siber di institusi serupa dapat meningkatkan relevansi dan kontribusi penelitian ini.

BAB III

METODE PENELITIAN

3.1 Alur Penelitian

Proses pengujian penetrasi pada setiap situs web memiliki pendekatan yang efektif karena menggunakan standar keamanan yang komprehensif, yang disesuaikan dengan konfigurasi situs web dan server [37]. Penelitian ini terdiri dari ZAP lima tahapan untuk menganalisis kerentanan keamanan pada situs web Sistemasi UNISI dengan menggunakan kerangka kerja OWASP ZAP. Tahapan tersebut meliputi, perencanaan, pengintaian, *scanning*, *report*, solusi dan kesimpulan. Alur penelitian ini ditampilkan pada Gambar 3.1.



Gambar 3.1 Alur Penelitian

3.2 Metode Pengumpulan Data

Untuk melakukan penelitian ini penulis menggunakan 2 metode untuk mengumpulkan data yaitu, sebagai berikut:

3.2.1 Observasi

Metode observasi dilakukan dengan cara melakukan pengamatan secara langsung terhadap website Sistemasi UNISI yang menjadi objek penelitian. Observasi bertujuan untuk memperoleh gambaran mengenai kondisi website, struktur halaman, fitur yang tersedia, mekanisme autentikasi pengguna, proses input dan pengolahan data, serta fungsi-fungsi yang dapat diakses melalui website.

Pada tahap ini, penulis juga mengidentifikasi bagian-bagian website yang berpotensi menjadi titik pengujian keamanan, seperti halaman login, form input, parameter URL, pengelolaan sesi pengguna, serta fitur lain yang berhubungan dengan interaksi pengguna dan sistem. Hasil observasi digunakan untuk menentukan ruang lingkup dan skenario pengujian yang akan dilakukan pada tahap penetration testing. Seluruh proses pengamatan dan pengujian dilakukan dalam batas ruang lingkup penelitian serta dengan memperhatikan izin dan keamanan sistem yang menjadi objek penelitian.

3.2.2 Studi Literatur

Metode studi literatur dilakukan dengan cara melakukan penelaahan terhadap berbagai literatur yang relevan dengan topik penelitian. Penelaahan ini meliputi jurnal ilmiah, buku, prosiding konferensi, tugas

akhir, dan sumber-sumber digital lainnya. Hasil dari studi literatur ini akan digunakan sebagai landasan dalam pengembangan penelitian lebih lanjut.

3.3 Perencanaan

Perencanaan Tahap perencanaan adalah langkah awal dalam melakukan *penetration testing*. Pada tahap ini, Peneliti menentukan ruang lingkup pengujian dan menyusun rencana pengujian yang mencakup tujuan, sumber daya yang dibutuhkan, dan waktu pelaksanaan. Hal ini melibatkan pemahaman tentang sistem yang akan diuji, seperti infrastruktur dan aplikasi yang terlibat, serta potensi ancaman yang perlu diuji. Pada tahapan ini, Peneliti juga harus memastikan bahwa semua pihak yang terlibat memiliki pemahaman yang sama mengenai tujuan dan metode yang akan digunakan dalam pengujian.

Dalam penelitian ini, penulis melakukan observasi terhadap website Sistemasi UNISI. Observasi dilakukan untuk mengumpulkan data dan informasi yang diperlukan sebagai dasar penelitian. Proses observasi ini juga bertujuan untuk memantau perubahan serta perkembangan pada website Sistemasi UNISI, khususnya setelah pergantian website yang dilakukan pada tahun 2023. Selama masa tersebut, penulis mencatat adanya perubahan signifikan pada website, terutama terkait pembaruan fitur, tampilan, dan desain dari versi lama ke versi baru. Pengamatan dilakukan secara berkelanjutan untuk mengidentifikasi dampak dari perubahan tersebut terhadap keamanan website.

3.4 Pengintaian

Pengintai adalah tahap pengumpulan informasi awal tentang target. Pada tahap ini, Peneliti mengumpulkan data sebanyak mungkin mengenai website atau

sistem yang akan diuji tanpa melakukan tindakan yang dapat membahayakan sistem. Informasi ini meliputi struktur jaringan, teknologi yang digunakan, dan rincian yang relevan lainnya yang bisa digunakan untuk merencanakan serangan lebih lanjut. Pengumpulan informasi ini dapat dilakukan melalui teknik seperti pemindaian DNS, pencarian informasi publik, atau eksplorasi metadata.

3.5 *Scanning*

Setelah tahap pengintai, Peneliti melanjutkan dengan scanning untuk menemukan kerentanannya. Proses ini mencakup penggunaan alat dan teknik untuk menganalisis sistem dan aplikasi untuk mendeteksi potensi celah keamanan. Scanning dapat dilakukan untuk mengidentifikasi port yang terbuka, kerentanannya dalam aplikasi web, serta memeriksa apakah ada konfigurasi yang tidak aman. Alat seperti OWASP ZAP, yang Peneliti sebutkan, sangat efektif dalam tahap ini untuk memeriksa potensi kelemahan seperti *SQL injection* atau *Cross-Site Scripting* (XSS), dan lain-lain.

3.6 Pengujian Kerentanan *Website*

Setelah *scanning* dan identifikasi kerentanan, Peneliti menyusun laporan yang merinci temuan selama proses *penetration testing*. Laporan ini mencakup informasi tentang kerentanannya, penilaian terhadap tingkat risiko yang ditimbulkan, serta bukti-bukti eksploitasi yang mungkin ditemukan selama uji penetrasi. Tujuan dari laporan ini adalah untuk memberikan pemangku kepentingan pemahaman yang jelas mengenai potensi ancaman yang ada dan dampaknya terhadap keamanan sistem

3.6.1 *Tested Website Determination*

Penelitian ini mengkaji *website* dalam lingkup organisasi akademik yang digunakan pada Universitas Islam Indragiri, untuk keperluan publikasi UNISI yaitu, https://sistemasi.ftik.unisi.ac.id.

3.6.2 *Software Installation*

Menginstal aplikasi OWASP ZAP versi 2.11.1 pada sistem operasi Windows 11 sangat berguna untuk meningkatkan keamanan situs web. Aplikasi ini membantu dalam mendeteksi dan menganalisis kerentanan yang mungkin ada pada situs web. Untuk mendapatkan aplikasi ZAP secara resmi, pengguna dapat mengunduhnya melalui situs web OWASP di alamat https://www.zaproxy.org/.

3.6.3 *Vulnerabillity Testing*

Pengujian kerentanan dilakukan menggunakan aplikasi OWASP ZAP, di mana proses pengujian mencakup penentuan URL situs web sebagai target utama. Aplikasi OWASP ZAP kemudian melakukan pemindaian otomatis terhadap situs web tersebut menggunakan opsi pemindaian *spider* tradisional. Pemindaian ini memungkinkan OWASP ZAP untuk menjelajahi dan mengidentifikasi potensi kerentanan pada struktur dan konten situs web target secara menyeluruh.

3.7 Kesimpulan

Kesimpulan adalah bagian akhir dari proses penetration testing. Pada tahap ini, Peneliti menyimpulkan hasil uji penetrasi secara keseluruhan, memberikan ringkasan tentang tingkat keamanan sistem yang diuji, dan menilai efektivitas langkah-langkah perbaikan yang telah dilakukan. Peneliti juga dapat

mengidentifikasi langkah selanjutnya yang diperlukan untuk memastikan keamanan berkelanjutan dari sistem, seperti pengujian ulang atau implementasi kontrol keamanan tambahan.

3.8 Solusi

Setelah proses pemindaian selesai, hasil yang diperoleh mencakup informasi mengenai kerentanan yang ditemukan, termasuk peringatan, tingkat risiko, dan detail lainnya. Peringatan ini memberikan indikasi mengenai masalah keamanan yang terdeteksi, sedangkan tingkat risiko mengukur potensi dampak dari kerentanan tersebut. Detail tambahan yang disediakan membantu dalam memahami konteks dan spesifikasi kerentanan yang ditemukan, serta dapat digunakan untuk merumuskan langkah-langkah perbaikan yang diperlukan.

Berdasarkan kerentanan yang terdeteksi pada *website* Sistemasi UNISI, penulis selanjutnya mengembangkan solusi untuk mengatasi masalah-masalah keamanan yang diidentifikasi. Solusi ini dirancang untuk memperbaiki kerentanan yang ditemukan, sehingga meningkatkan keamanan situs dan melindungi data serta integritas sistem dari potensi ancaman.

3.9 Bahan dan Alat Penelitian

Bahan dan alat dalam penelitian menggunakan *software* dan *hardware* sebagai bahan literature penelitian, untuk spesifikasi *software* dan *hardware* dapat dilihat pada tabel 3.1 dibawah ini:

Tabel 3.1 Bahan dan Alat Penelitian

Hardware **dan Sistem Operasi**	***Software***
Lenovo 82h7 Processor : 11th Gen Intel(R) Cor (TM) i7-	OWASP ZAP : Untuk mengecek *kerentanan website.*

1165G7 @ 2.80 GHz RAM : 8 GB System type : 64-bit Operating system, x64-based processor	

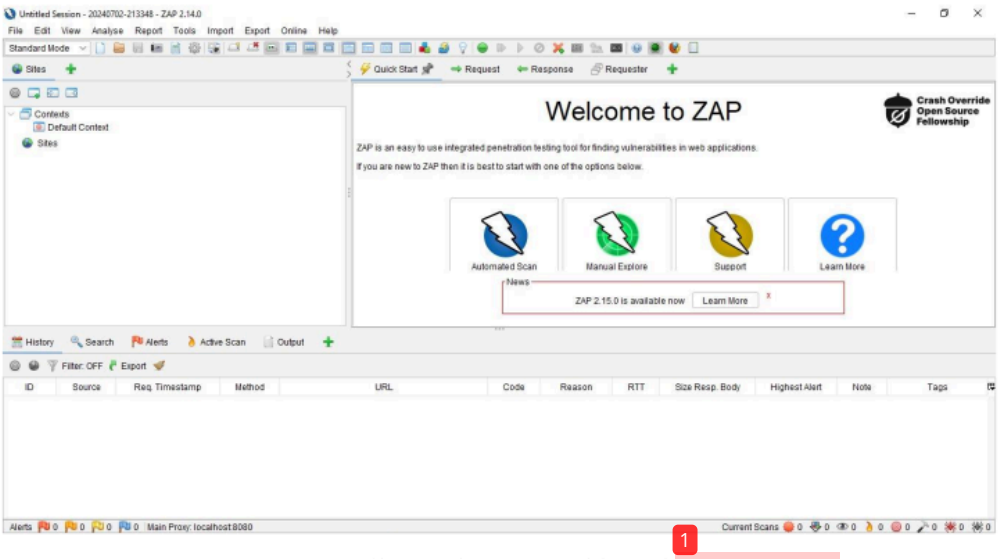
BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Hasil

Berikut langkah-langkah pengecekkan keamanan *website* menggunakan *tools* OWASP ZAP:

1. Membuka aplikasi OWASP ZAP.



Gambar 4.1 Tampilan Halaman Dashboard OWASP ZAP

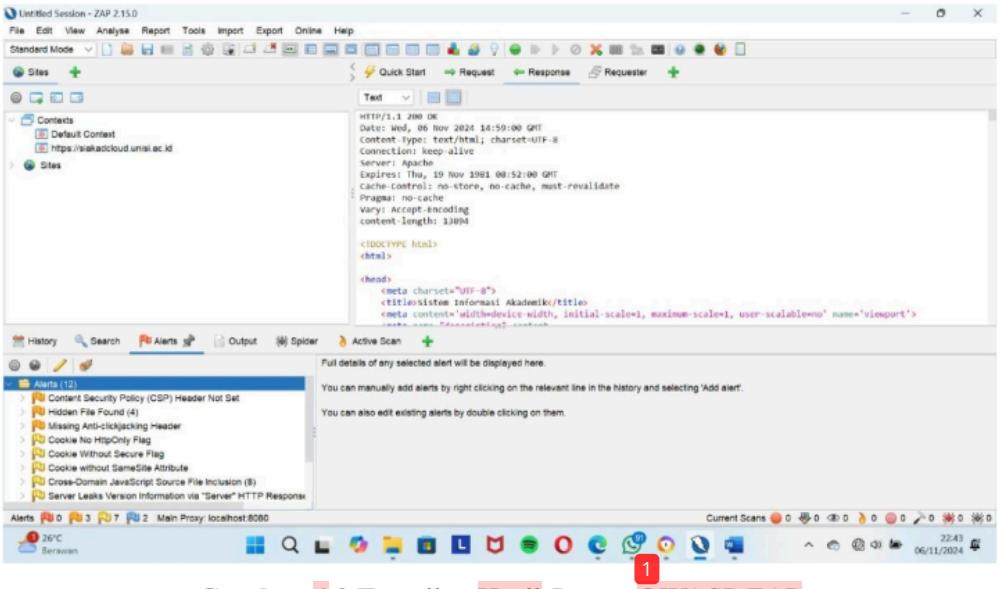
2. Memilih fitur *Automated Scan* pada OWASP ZAP.
3. Memasukkan *link website* Sistemasi UNISI pada kolom *URL to Attack*.

4.2 Analisa Hasil Penelitian

Tahap dalam melakukan analisis menggunakan metode *penetration testing* yang dapat secara langsung memonitor celah-celah keamanan *website* Sistemasi UNISI. Penelitian ini menggunakan *tools* yaitu OWASP ZAP.

4.3 Hasil OWASP ZAP

Penelitian menggunakan *tools* OWASP ZAP untuk *spidering* (menelusuri seluruh situs web) dan *scraping* untuk mengidentifikasi struktur dan konten web secara lebih mendalam pada *website* OWASP ZAP.



Gambar 4.2 Tampilan Hasil *Report* OWASP ZAP

Pada gambar 4.2 merupakan tampilan hasil dari *report tools* OWASP ZAP. Dimana pada tampilan tersebut diketahui terdapat 19 *alert* dari hasil pengecekkan keamanan *website* menggunakan *tools* OWASP ZAP. Berikut adalah hasil *report tools* OWASP ZAP:

Tabel 4.1 Hasil *Report* OWASP ZAP

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
Absence of Anti-CSRF Tokens(216)	*Medium*	Tidak ada token Anti-CSRF yang ditemukan dalam formulir pengiriman HTML. Pemalsuan permintaan lintas situs adalah serangan yang melibatkan pemaksaan korban untuk mengirimkan permintaan HTTP ke tujuan target tanpa sepengetahuan atau	Fase: Arsitektur dan Desain Gunakan pustaka atau kerangka kerja yang telah diperiksa yang tidak memungkinkan kelemahan ini terjadi atau sediakan konstruksi yang membuat kelemahan ini lebih mudah dihindari. Sebagai contoh, gunakan paket anti-CSRF seperti OWASP

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
		niat mereka untuk melakukan tindakan sebagai korban. Penyebab utamanya adalah fungsionalitas aplikasi yang menggunakan URL/formulir yang dapat diprediksi dengan cara yang berulang-ulang. Sifat dari serangan ini adalah CSRF mengeksploitasi kepercayaan yang dimiliki oleh sebuah situs web terhadap pengguna. Sebaliknya, skrip lintas situs (XSS) mengeksploitasi kepercayaan yang dimiliki pengguna terhadap situs web. Seperti XSS, serangan CSRF tidak selalu bersifat lintas situs, tetapi bisa saja. Pemalsuan permintaan lintas situs juga dikenal sebagai CSRF, XSRF, serangan sekali klik, session riding, deputi bingung, dan ombak laut. Serangan CSRF efektif dalam beberapa situasi, termasuk: • Korban memiliki sesi aktif di situs target. • Korban diautentikasi melalui HTTP auth di situs target. • Korban berada di jaringan lokal yang sama dengan situs target. CSRF terutama digunakan untuk melakukan tindakan terhadap situs target dengan menggunakan hak istimewa korban, tetapi teknik terbaru telah ditemukan untuk mengungkapkan informasi dengan mendapatkan akses ke respon. Risiko pengungkapan informasi meningkat secara dramatis	CSRFGuard. Fase: Implementasi Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar pertahanan CSRF dapat dilewati dengan menggunakan skrip yang dikendalikan oleh penyerang. Fase: Arsitektur dan Desain Buatlah nonce unik untuk setiap formulir, letakkan nonce ke dalam formulir, dan verifikasi nonce setelah menerima formulir. Pastikan bahwa nonce tidak dapat diprediksi (CWE-330). Perhatikan bahwa hal ini dapat dilewati dengan menggunakan XSS. Identifikasi operasi yang sangat berbahaya. Ketika pengguna melakukan operasi berbahaya, kirimkan permintaan konfirmasi terpisah untuk memastikan bahwa pengguna memang bermaksud melakukan operasi tersebut. Perhatikan bahwa hal ini dapat dilewati dengan menggunakan XSS. Gunakan kontrol Manajemen Sesi ESAPI. Kontrol ini mencakup komponen untuk CSRF. Jangan gunakan metode GET untuk permintaan apa pun yang memicu perubahan status. Fase Implementasi Periksa header HTTP Referer untuk melihat apakah permintaan berasal dari halaman yang diharapkan. Hal ini dapat merusak fungsionalitas yang sah, karena pengguna atau proksi mungkin telah menonaktifkan pengiriman Referer untuk

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
		ketika situs target rentan terhadap XSS, karena XSS dapat digunakan sebagai platform untuk CSRF, yang memungkinkan serangan beroperasi dalam batas-batas kebijakan yang [illegible].	alasan privasi.
Content Security Policy (CSP) Header Not Set (312)	*Medium*	Tidak ada token Anti-CSRF yang ditemukan dalam formulir pengiriman HTML. Pemalsuan permintaan lintas situs adalah serangan yang melibatkan pemaksaan korban untuk mengirim permintaan HTTP ke tujuan target tanpa sepengetahuan atau niat mereka untuk melakukan tindakan sebagai korban. Penyebab utamanya adalah fungsionalitas aplikasi yang menggunakan URL/formulir yang dapat diprediksi dengan cara yang berulang-ulang. Sifat dari serangan ini adalah CSRF mengeksploitasi kepercayaan yang dimiliki oleh sebuah situs web terhadap pengguna. Sebaliknya, skrip lintas situs (XSS) mengeksploitasi kepercayaan yang dimiliki pengguna terhadap situs web. Seperti XSS, serangan CSRF tidak selalu bersifat lintas situs, tetapi bisa saja. Pemalsuan permintaan lintas situs juga dikenal sebagai CSRF, XSRF, serangan sekali klik, session riding, deputi bingung, dan ombak laut. Serangan CSRF efektif dalam beberapa situasi, termasuk: • Korban memiliki sesi aktif di situs target. • Korban diautentikasi	Fase: Arsitektur dan Desain Gunakan pustaka atau kerangka kerja yang telah diperiksa yang tidak memungkinkan kelemahan ini terjadi atau sediakan konstruksi yang membuat kelemahan ini lebih mudah dihindari. Sebagai contoh, gunakan paket anti-CSRF seperti OWASP CSRFGuard. Fase: Implementasi Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar pertahanan CSRF dapat dilewati dengan menggunakan skrip yang dikendalikan oleh penyerang. Fase: Arsitektur dan Desain Buatlah nonce unik untuk setiap formulir, letakkan nonce ke dalam formulir, dan verifikasi nonce setelah menerima formulir. Pastikan bahwa nonce tidak dapat diprediksi (CWE-330). Perhatikan bahwa hal ini dapat dilewati dengan menggunakan XSS. Identifikasi operasi yang sangat berbahaya. Ketika pengguna melakukan operasi berbahaya, kirimkan permintaan konfirmasi terpisah untuk memastikan bahwa pengguna memang bermaksud melakukan operasi tersebut. Perhatikan bahwa hal ini dapat dilewati dengan menggunakan XSS.

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
		melalui HTTP auth di situs target. • Korban berada di jaringan lokal yang sama dengan situs target. CSRF terutama digunakan untuk melakukan tindakan terhadap situs target dengan menggunakan hak istimewa korban, tetapi teknik terbaru telah ditemukan untuk mengungkapkan informasi dengan mendapatkan akses ke respon. Risiko pengungkapan informasi meningkat secara dramatis ketika situs target rentan terhadap XSS, karena XSS dapat digunakan sebagai platform untuk CSRF, yang memungkinkan serangan beroperasi dalam batas-batas kebijakan yang sama.	Gunakan kontrol Manajemen Sesi ESAPI. Kontrol ini mencakup komponen untuk CSRF. Jangan gunakan metode GET untuk permintaan apa pun yang memicu perubahan status. Fase Implementasi Periksa header HTTP Referer untuk melihat apakah permintaan berasal dari halaman yang diharapkan. Hal ini dapat merusak fungsionalitas yang sah, karena pengguna atau proksi mungkin telah menonaktifkan pengiriman Referer untuk alasan privasi.
Missing Anti-clikcjaking Header	*Medium*	Respons tidak menyertakan *Content-Security-Policy* dengan arahan *'frame-ancestors'* atau *X-Frame-Options* untuk melindungi dari serangan *'ClickJacking'*.	*Browser Web modern* mendukung *header HTTP Content-Security-Policy* dan *X-Frame-Options*. Pastikan salah satunya diatur di semua halaman web yang dikembalikan oleh situs/aplikasi. Jika mengharapkan halaman dibingkai hanya oleh halaman di server (misalnya itu adalah bagian dari FRAMESET) maka akan ingin menggunakan SAMEORIGIN, jika Anda tidak pernah mengharapkan halaman dibingkai, harus menggunakan DENY. Atau, pertimbangkan untuk menerapkan arahan "frame-ancestors" Kebijakan amanan Konten.
Vulnerable JS Library	*Medium*	Perpustakaan yang teridentifikasi tampaknya rentan.	Upgrade to the latest version of the affected library.
Big Redirect	*Low*	Server telah merespons	

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
Detected (Potential Sensitive Information Leak)		dengan pengalihan yang tampaknya memberikan respons yang besar. Hal ini dapat mengindikasikan bahwa meskipun server mengirimkan pengalihan, server juga merespons dengan konten tubuh (yang mungkin termasuk detail sensitif, PII, dll.).	Pastikan tidak ada informasi sensitif yang bocor melalui tanggapan pengalihan. Tanggapan pengalihan seharusnya hampir tidak memiliki konten.
Cookie Without SameSite Attribute	*Low*	Cookie telah diatur tanpa atribut SameSite, yang berarti bahwa cookie dapat dikirim sebagai hasil dari permintaan 'lintas situs'. Atribut SameSite adalah tindakan balasan yang efektif untuk pemalsuan permintaan lintas situs, penyertaan skrip lintas situs, dan serangan waktu.	Pastikan atribut SameSite diatur ke 'longgar' atau idealnya 'ketat' untuk semua cookie.
Cross-Domain JavaScript Source File Inclusion	*Low*	Halaman ini menyertakan satu atau beberapa file skrip dari domain pihak ketiga.	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi.
Sever Leaks Version Infrmation via "Server" HTTP Response Header Field	*Low*	Server web/aplikasi membocorkan informasi versi melalui header respons HTTP "Server". Akses ke informasi tersebut dapat memfasilitasi penyerang mengidentifikasi kerentanan lain yang menjadi subjek server web/aplikasi.	Pastikan server web, server aplikasi, load balancer, dll. Anda dikonfigurasi untuk menekan header "Server" atau memberikan detail umum.
Strict-Transport-Security Header Not Set	*Low*	HTTP Strict Transport Security (HSTS) adalah mekanisme kebijakan keamanan web di mana server web menyatakan bahwa agen pengguna yang mematuhi (seperti browser web) harus berinteraksi dengannya hanya menggunakan koneksi HTTPS yang aman (yaitu HTTP yang dilapisi melalui TLS/SSL). HSTS adalah protokol trek standar IETF dan ditentukan dalam RFC 6797.	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menerapkan Ketat-Transport-Security.
X-Content-Type-	*Low*	Header Anti-MIME-	Pastikan bahwa aplikasi/server

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
Options Header Missing		Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Hal ini memungkinkan versi Internet Explorer dan Chrome yang lebih lama untuk melakukan sniffing MIME pada isi respons, yang berpotensi menyebabkan isi respons ditafsirkan dan ditampilkan sebagai jenis konten selain jenis konten yang dideklarasikan. Versi Firefox saat ini (awal 2014) dan lama akan menggunakan jenis konten yang dideklarasikan (jika sudah diatur), daripada melakukan sniffing MIME.	web mengatur header Content-Type dengan tepat, dan mengatur header X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan browser web yang sesuai standar dan modern yang tidak melakukan MIME sniffing sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan MIME-sniffing.
Cookie No HttpOnly Flag	*Low*	Cookie telah ditetapkan tanpa bendera HttpOnly, yang berarti bahwa cookie dapat diakses oleh JavaScript. Jika skrip berbahaya dapat dijalankan pada halaman ini maka cookie akan dapat diakses dan dapat dikirimkan ke situs lain. Jika ini adalah cookie sesi maka pembajakan sesi mungkin terjadi.	Pastikan bahwa bendera HttpOnly disetel untuk semua cookie.
Secure Pages Include Mixed Content	*Low*	Halaman ini mencakup konten campuran, yaitu konten yang diakses melalui HTTP, bukan HTTPS.	Halaman yang tersedia melalui SSL/TLS harus sepenuhnya terdiri dari konten yang ditransmisikan melalui SSL/TLS. Halaman tidak boleh berisi konten apa pun yang ditransmisikan melalui HTTP yang tidak terenkripsi. Ini termasuk konten dari situs pihak ketiga.
Authentication Request Identified	*Informational*	Permintaan yang diberikan telah diidentifikasi sebagai permintaan autentikasi. Bidang 'Info Lain' berisi satu set baris key=value yang mengidentifikasi bidang yang relevan. Jika permintaan berada dalam konteks yang memiliki	Ini adalah peringatan informasi, bukan kerentanan, sehingga tidak ada yang perlu diperbaiki.

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
		Metode Autentikasi yang disetel ke "Deteksi Otomatis", maka aturan ini akan mengubah autentikasi agar sesuai dengan permintaan yang diidentifikasi.	
Information Disclosure – Sensitive Information in URL	*Informational*	Permintaan tersebut tampaknya berisi informasi sensitif yang bocor dalam URL. Hal ini dapat melanggar PCI dan sebagian besar kebijakan kepatuhan organisasi. Anda dapat mengonfigurasi daftar string untuk pemeriksaan ini untuk menambah atau menghapus nilai yang spesifik untuk lingkungan Anda.	Jangan memberikan informasi sensitif dalam URI.
Information Disclosure – Suspicious Comments	*Informational*	Tanggapan tersebut tampaknya berisi komentar mencurigakan yang dapat membantu penyerang.	Hapus semua komentar yang memberikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.
Modern Web Application	*Informational*	Aplikasi ini tampaknya merupakan aplikasi web modern. Jika Anda perlu menjelajahinya secara otomatis, maka Ajax Spider mungkin lebih efektif daripada yang standar.	Ini adalah peringatan informasi sehingga tidak ada perubahan yang diperlukan.
Re-examine Cache-control Directives	*Informational*	Header kontrol cache belum diatur dengan benar atau tidak ada, sehingga memungkinkan browser dan proxy untuk menyimpan konten dalam cache.	Untuk konten yang aman, pastikan header HTTP kontrol cache diatur dengan "no-cache, no-store, must-revalidate". Jika sebuah aset harus di-cache, pertimbangkan untuk mengatur arahan "public, max-age, immutable".
Session Managemnt Response Identified	*Infromational*	Respons yang diberikan telah diidentifikasi mengandung token manajemen sesi. Bidang 'Info Lain' berisi sekumpulan token header yang dapat digunakan dalam Metode Manajemen Sesi Berbasis Header. Jika	Ini adalah peringatan informasi, bukan kerentanan, sehingga tidak ada yang perlu diperbaiki.

Nama Ancaman	Tingkat Ancaman	Deskripsi	Solusi
		permintaan berada dalam konteks yang memiliki Metode Manajemen Sesi yang disetel ke "Deteksi Otomatis", maka aturan ini akan mengubah manajemen sesi untuk menggunakan token yang diidentifikasi.	
User Controllable HTML Element Attribute (Potential XSS)	*Informational*	Pemeriksaan ini melihat input yang disediakan pengguna dalam parameter string kueri dan data POST untuk mengidentifikasi di mana nilai atribut HTML tertentu dapat dikontrol. Hal ini memberikan deteksi titik panas untuk XSS (skrip lintas situs) yang akan memerlukan tinjauan lebih lanjut oleh analis keamanan untuk menentukan kemampuan eksploitasi.	Validasi semua masukan dan bersihkan keluarannya sebelum menulis ke atribut HTML apa pun.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan analisis dan hasil pemeriksaan menggunakan OWASP ZAP, *website* Sistemasi UNISI menunjukkan beberapa kerentanan yang memerlukan perhatian segera. Berikut adalah beberapa poin penting terkait ancaman keamanan yang dihadapi serta langkah-langkah perbaikan yang dapat dilakukan:

1. Pengujian keamanan menggunakan metode penetration testing dengan tools OWASP ZAP berhasil mengidentifikasi berbagai kerentanan pada website Sistemasi UNISI. Berdasarkan hasil pemindaian ditemukan beberapa celah keamanan dengan tingkat risiko sedang, rendah, dan informasional, yang menunjukkan bahwa website masih memiliki kelemahan yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab
2. Metode penetration testing menggunakan OWASP ZAP terbukti efektif sebagai metode evaluasi keamanan website. Proses pemindaian mampu mendeteksi berbagai jenis kerentanan secara sistematis serta memberikan informasi mengenai tingkat risiko dan penyebab setiap kerentanan, sehingga dapat menjadi dasar dalam menilai kondisi keamanan website Sistemasi UNISI dan membantu proses pengambilan keputusan untuk peningkatan keamanan.
3. Berdasarkan hasil pengujian, rekomendasi perbaikan yang diberikan meliputi penerapan Content Security Policy (CSP), penambahan header keamanan seperti X-Frame-Options, penguatan konfigurasi cookie

menggunakan atribut HttpOnly, Secure, dan SameSite, serta penerapan HTTPS secara konsisten. Implementasi rekomendasi tersebut diharapkan mampu meningkatkan tingkat keamanan website Sistemasi UNISI serta mengurangi risiko terjadinya serangan siber pada masa mendatang.

5.2 Saran

1. Implementasi Kebijakan Keamanan Konten (CSP) dan Pengaturan *Header* Tambahan. Pastikan untuk mengatur kebijakan keamanan konten (*Content Security Policy*) yang ketat guna mencegah serangan seperti *Cross-Site Scripting* (XSS) dan injeksi data. Selain itu, tambahkan header keamanan seperti *X-Frame-Options* dan *X-Content-Type-Options* untuk mengurangi risiko serangan *clickjacking* dan MIME *sniffing*. Mengonfigurasi header ini akan membatasi akses ke sumber daya yang disetujui, sehingga memperkuat keamanan situs.
2. Peningkatan Manajemen *Cookie* dan Penggunaan HTTPS Secara Konsisten. Atur bendera *HttpOnly, Secure*, dan *SameSite* pada semua *cookie* untuk memastikan *cookie* hanya dapat diakses melalui koneksi yang aman dan tidak terpapar pada skrip berbahaya. Selain itu, terapkan protokol HTTPS pada semua halaman web untuk memastikan enkripsi data yang dikirim dan diterima oleh pengguna, mengurangi risiko pencurian data dan pembajakan sesi.

DAFTAR PUSTAKA

[1] B. Rianto dan I. Alsa, "Perancangan Aplikasi Promosi Universitas Islam Indragiri Berbasi Multimedia Interaktif," Selodang Mayang: Jurnal Ilmiah Badan Perencanaan Pembangunan Daerah Kabupaten Indragiri Hilir, vol. 7, no. 1, hlm. 39–43, 2021.

[2] A. Muni, B. Rianto, dan M. Jalil, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Owasp-Zap Di Universitas Islam Indragiri," Teknofile: Jurnal Sistem Informasi, vol. 2, no. 6, hlm. 409–420, 2024.

[3] A. Prahendratno dkk., Strategi Bisnis Digital: Optimalisasi & Otomtisasi Sebuah Bisnis Menggunakaan Media Digital. PT. Sonpedia Publishing Indonesia, 2023.

[4] A. D. Madya, B. D. Haryanto, D. P. Ningsih, dan F. Sinlae, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," Indonesian Journal of Education And Computer Science, vol. 1, no. 3, hlm. 127–135, 2023.

[5] G. Alfaren, "Analisis Serangan Penetration Testing: Sebuah Review Sistematik," Jiifkom (Jurnal Ilmiah Informatika dan Komputer), vol. 1, no. 2, hlm. 21–26, 2022.

[6] M. Huda, Keamanan Informasi. Nulisbuku, 2020.

[7] M. R. Ardiansyah dkk., "Analisis Kerentanan Keamanan Website Menggunakan Metode Ptes (Penetration Testing Execution And Standart)," Nuansa Informatika, vol. 18, no. 2, hlm. 145–153, 2024.

[8] M. Tahir dan M. R. Ardiansyah, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode Ptes (Penetration Testing Execution Standard)," Jurnal Teknik Informatika Unika Santo Thomas, hlm. 118–125, 2024.

[9] F. Tinambunan, A. Junaidi, dan A. M. Rizki, “Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10,” JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 1, hlm. 1062–1069, 2024.

[10] A. F. Hasibuan dan D. Handoko, “Analisis Keretanan Website Dengan Aplikasi Owasp Zap,” Jurnal Ilmu Komputer dan Sistem Informasi, vol. 2, no. 2, hlm. 257–270, 2023.

[11] K. Nisa, M. A. Putra, R. A. Siregar, dan M. D. Irawan, “Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap),” Bulletin of Information Technology (BIT), vol. 3, no. 4, hlm. 216–308, 2022.

[12] J. N. Ginting, “Perancangan dan Pembuatan Sistem Informasi Penerimaan Mahasiswa Baru Berbasis Website,” Jurnal Nasional Teknologi Komputer, vol. 2, no. 2, hlm. 51–59, 2022.

[13] W. Wiyanto, S. Fadhilah, dan A. Siswandi, “E-Tourism Sebagai Media Wisata Kabupaten Bekasi Berbasis Website,” Journal of Practical Computer Science, vol. 2, no. 1, hlm. 1–14, 2022, doi: 10.37366/jpcs.v2i1.1035.

[14] B. Rianto, “WESITE PENYEDIAN INFORMASI RUMAH KOS KAB. INHIL Studi Kasus: Sebagian Rumah Kos Yang Ada Di Tembilahan,” JUTI UNISI, vol. 3, no. 1, hlm. 35–42, 2019.

[15] B. Rianto, L. Lidya, dan G. W. Nurcahyo, “Pemodelan Arsitektur Enterprise Menggunakan Metode Togaf ADM Studi Kasus Dinas Kesehatan Kabupaten Indragiri Hilir,” Jurnal Komputer Terapan, vol. 2, no. 1, hlm. 55–68, 2016.

[16] S. Hidayatulloh dan D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP),” Jurnal Algoritma, vol. 18, no. 1, hlm. 77–86, 2021.

[17] D. F. Priambodo, A. D. Rifansyah, dan M. Hasbi, “Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating,” Teknika, vol. 12, no. 1, hlm. 33–46, 2023.

[18] H. H. Muhammad, A. I. Hadiana, dan H. Ashaury, “Pengamanan Aplikasi Web Dari Serangan Sql Injection Dan Cross Site Scripting Menggunakan Web Application Firewall,” JATI (Jurnal Mahasiswa Teknik Informatika), vol. 7, no. 5, hlm. 3265–3273, 2023.

[19] D. S. Wibowo, M. Nishom, dan T. Abidin, “Pengumpulan Informasi pada Situs Web Dengan Menyusun Kerangka Kerja Keamanan Siber NIST,” Jurnal Informatika: Jurnal Pengembangan IT, vol. 9, no. 1, hlm. 1–6, 2024.

[20] M. Idris, I. Syarif, dan I. Winarno, “Web Application Security Education Platform Based On OWASP API Security Project,” EMITTER international journal of engineering technology, hlm. 246–261, 2022.

[21] G. Guntoro, L. Costaner, dan M. Musfawati, “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), vol. 5, no. 1, hlm. 45–55, 2020.

[22] Y. Mulyanto, E. Haryanti, dan J. Jumirah, “Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement: Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Asesement,” Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 3, no. 3, hlm. 394–400, 2021.

[23] P. Jarupunphol, S. Seatun, dan W. Buathong, “Measuring Vulnerability Assessment Tools’ Performance on the University Web Application.,” Pertanika J Sci Technol, vol. 31, no. 6, 2023.

[24] Y. Yudiana, A. Elanda, dan R. L. Buana, “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), vol. 6, no. 2, hlm. 185–191, 2021.

[25] N. Albalawi, N. Alamrani, R. Aloufi, M. Albalawi, A. Aljaedi, dan A. R. Alharbi, "The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities," Electronics (Basel), vol. 12, no. 12, hlm. 2664, 2023.

[26] H. Poston, "Mapping The OWASP Top Ten to Blockchain," Procedia Comput Sci, vol. 177, hlm. 613–617, 2020.

[27] K. Qian, R. M. Parizi, dan D. Lo, "Owasp Risk Analysis Driven Security Requirements Specification For Secure Android Mobile Software Development," dalam 2018 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, 2018, hlm. 1–2.

[28] S. Khandelwal, "Critical RCE Flaw Discovered In Blockchain-Based EOS Smart Contract System," The Hacker News. Retrieved February, vol. 4, hlm. 2023, 2018.

[29] I. F. Ashari, V. Oktarina, R. G. Sadewo, dan S. Damanhuri, "Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools," Jurnal Sisfokom (Sistem Informasi dan Komputer), vol. 11, no. 2, hlm. 276–281, 2022.

[30] I. Riadi, A. Fadlil, dan M. A. Mu'min, "OWASP Framework-based Network Forensics to Analyze the SQLi Attacks on Web Servers," MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, hlm. 481–494, 2023.

[31] G. H. Editya dan S. Mulyati, "Aplikasi Mobile One Time Password Menggunakan Algoritma MD5 dan SHA1 untuk Meningkatkan Keamanan Website," SKANIKA: Sistem Komputer dan Teknik Informatika, vol. 1, no. 2, hlm. 618–623, 2018.

[32] J. T. Santoso, “Teknologi Keamanan Siber (Cyber Security),” Penerbit Yayasan Prima Agus Teknik, hlm. 1–173, 2023.

[33] Y. T. A. Rosaliah, J. Jayanta, dan B. Hananto, “Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx,” dalam Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya, 2021, hlm. 752–761.

[34] B. Ghozali, K. Kusrini, dan S. Sudarmawan, “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating,” Creative Information Technology Journal, vol. 4, no. 4, hlm. 264–275, 2019.

[35] H. Sofyan, M. Sugiarto, dan B. M. Akbar, “Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN ‘Veteran’ Yogyakarta,” Telematika: Jurnal Informatika dan Teknologi Informasi, vol. 20, no. 2, hlm. 153–162, 2023.

[36] F. Fachri, A. Fadlil, dan I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” J. Inform, vol. 8, no. 2, hlm. 183–190, 2021.

[37] H. S. Abdullah, “Evaluation of open source web application vulnerability scanners,” Academic Journal of Nawroz University, vol. 9, no. 1, hlm. 47–52, 2020.

Skripsi _Agung_Ramadhan SI Revisi.pdf

ORIGINALITY REPORT

50%	46%	20%	27%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Islam Riau Student Paper	12%
2	repository.uin-suska.ac.id Internet Source	5%
3	journal.aira.or.id Internet Source	5%
4	repository.unisi.ac.id Internet Source	2%
5	www.researchgate.net Internet Source	2%
6	www.jurnalteknik.unisla.ac.id Internet Source	2%
7	jsi.politala.ac.id Internet Source	1%
8	ijcs.stmikindonesia.ac.id Internet Source	1%
9	penerbit.stekom.ac.id Internet Source	1%
10	Nurfatun, Muhammad Amirul Mu'min, Dahlan. "Analisis Dan Pengujian Kerentanan Pada Website Kantor Desa Lanta Barat Menggunakan Framework Issaf", Jurnal Sistem dan Informatika (JSI), 2026 Publication	1%
11	jurnal.unity-academy.sch.id Internet Source	1%
12	sads.instiki.ac.id Internet Source	1%
13	usermanual.wiki Internet Source	1%
14	journal.universitaspahlawan.ac.id Internet Source	1%

15	jurnal.upnyk.ac.id Internet Source	1 %
16	jurnal.itscience.org Internet Source	1 %
17	repository.nusaputra.ac.id Internet Source	1 %
18	jurnal.itg.ac.id Internet Source	<1 %
19	jurnalnew.unimus.ac.id Internet Source	<1 %
20	repository.ar-raniry.ac.id Internet Source	<1 %
21	doaj.org Internet Source	<1 %
22	Isa Nur Fathoni, Mohammad Imron, Darso Darso. "Analisis Keamanan Website Ells Amikom Purwokerto Menggunakan Metode Vulnerability Assesment Dengan Kerentanan Tingkat Menengah", Jurnal Minfo Polgan, 2026 Publication	<1 %
23	digilib.ulm.ac.id Internet Source	<1 %
24	Submitted to Universitas Muslim Indonesia Student Paper	<1 %
25	digilib.uinkhas.ac.id Internet Source	<1 %
26	repositori.unibos.ac.id Internet Source	<1 %
27	journal.fkpt.org Internet Source	<1 %
28	repository.pnj.ac.id Internet Source	<1 %
29	Submitted to Sekolah Teknik Elektro & Informatika Student Paper	<1 %
30	Submitted to Politeknik Negeri Bandung Student Paper	<1 %

31	Sri Harjunawati, Syahrial Addin, Ida Hendarsih, Amas Sari Marthanti. "Keberhasilan Manajemen Penjualan Lasser Work Service Zigzag di Semarang Menggunakan Java (Netbeans 7.3)", Profitabilitas, 2021 Publication	<1 %
32	www.roombelajar.com Internet Source	<1 %
33	repository.mercubuana.ac.id Internet Source	<1 %
34	jurnal.teknokrat.ac.id Internet Source	<1 %
35	repository.unissula.ac.id Internet Source	<1 %
36	www.ejournal.itn.ac.id Internet Source	<1 %
37	Betta Wahyu Retna Mulya, Avinanta Tarigan. "PEMERINGKATAN RISIKO KEAMANAN SISTEM JARINGAN KOMPUTER POLITEKNIK KOTA MALANG MENGGUNAKAN CVSS DAN FMEA", ILKOM Jurnal Ilmiah, 2018 Publication	<1 %
38	repository.poliupg.ac.id Internet Source	<1 %
39	journal.lembagakita.org Internet Source	<1 %
40	Ashfa Adlan Haqiqi, Fahmi Fachri. "Analisis Kerentanan Website MAN 2 Kebumen Terhadap Serangan Cross-site Scripting (XSS) Menggunakan Owasp ZAP", Indonesian Journal of Multidisciplinary on Social and Technology, 2026 Publication	<1 %
41	repository.upnvj.ac.id Internet Source	<1 %
42	Submitted to UPN Veteran Jawa Timur Student Paper	<1 %
43	eprints.uad.ac.id Internet Source	<1 %
44	jurnal.nawansa.com Internet Source	<1 %
45	jurnalnasional.ump.ac.id Internet Source	<1 %

46	repository.umsu.ac.id Internet Source	<1 %
47	a-asyam.blogspot.com Internet Source	<1 %
48	digilib.esaunggul.ac.id Internet Source	<1 %
49	jai.front-sci.com Internet Source	<1 %
50	repository.umy.ac.id Internet Source	<1 %
51	Dio Wahyu Saputra, Risqy Siwi Pradini, Mochammad Anshori. "Analisis dan Rekomendasi Keamanan Website Kampus X Menggunakan ISSAF", Jurnal Indonesia : Manajemen Informatika dan Komunikasi, 2025 Publication	<1 %
52	Submitted to Konsorsium PTS Batch 5 Student Paper	<1 %
53	eprints.poltektegal.ac.id Internet Source	<1 %
54	id.123dok.com Internet Source	<1 %
55	repository.mediapenerbitindonesia.com Internet Source	<1 %
56	digilib.unimed.ac.id Internet Source	<1 %
57	e-jurnal.lppmunsera.org Internet Source	<1 %
58	repository.unbari.ac.id Internet Source	<1 %
59	Candra Darmawan, Julius Panda Putra Naibaho, Alex De Kweldju. "Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021", Edumatic: Jurnal Pendidikan Informatika, 2024 Publication	<1 %
60	Submitted to Universitas Pendidikan Ganesha Student Paper	<1 %
	ejournal.unisi.ac.id	

61	Internet Source	<1%
62	repository.yudharta.ac.id Internet Source	<1%
63	digilib.uinsa.ac.id Internet Source	<1%
64	docplayer.info Internet Source	<1%
65	jurnal.univrab.ac.id Internet Source	<1%
66	repository.uinsu.ac.id Internet Source	<1%
67	Submitted to The Illawarra Grammar School Student Paper	<1%
68	dspace.uii.ac.id Internet Source	<1%
69	etd.repository.ugm.ac.id Internet Source	<1%
70	ia801701.us.archive.org Internet Source	<1%
71	journal.arteii.or.id Internet Source	<1%
72	jtika.if.unram.ac.id Internet Source	<1%
73	ojs.amikomsolo.ac.id Internet Source	<1%
74	repository.nurulfikri.ac.id Internet Source	<1%
75	repository.uksw.edu Internet Source	<1%
76	sistemasi.ftik.unisi.ac.id Internet Source	<1%
77	ten.tarbiyah.unmuha.ac.id Internet Source	<1%
78	123dok.com Internet Source	

		<1%
79	Syahrul Dwi Hilda, Nono Heryana, Azhari Ali Ridha. "WEBSITE SECURITY ANALYSIS CURUG VILLAGE GOVERNMENT USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP)", Jurnal Informatika dan Teknik Elektro Terapan, 2024 Publication	<1%
80	Submitted to Universitas Pancasila Student Paper	<1%
81	cdn.juris.id Internet Source	<1%
82	eprints.unram.ac.id Internet Source	<1%
83	jpti.journals.id Internet Source	<1%
84	opengovasia.com Internet Source	<1%
85	repo.darmajaya.ac.id Internet Source	<1%
86	repository.ub.ac.id Internet Source	<1%
87	repository.uinsaizu.ac.id Internet Source	<1%
88	www.pro-linux.de Internet Source	<1%
89	Aland Polma Naek Sihombing, Agung Prabowo, Ibnu Daqiqil Id, Tisha Melia. "Analisis kerentanan keamanan pada sistem informasi akademik berbasis web menggunakan OWASP-ZAP", INFOTECH : Jurnal Informatika & Teknologi, 2026 Publication	<1%
90	Nurasmawati Nurasmawati, Mansur Mansur, Nurmi Hidayasari. "Analisis Kerentanan Keamanan pada Website Kelurahan Rimba Sekampung dengan Menggunakan Framework OWASP ZAP", Jurnal Teknik Industri Terintegrasi, 2025 Publication	<1%
91	repository.radenintan.ac.id Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		