JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 05 NOMOR 02 JULI 2025
ISSN 2774 – 5775 | eISSN 2774-5767

ANALISIS KERENTANAN *WEBSITE* MELALUI PENDEKATAN *PENETRATION TESTING* BERDASARKAN STANDAR OWASP TOP 10 STUDI KASUS SIMPELMAS UNIVERSITAS XYZ

Mizar Ismu Arief[1)], Dede Syahrul Anwar[2)], Agus Supriatman[3)]
[1,2,3]Prodi Teknik Informatika, Fakultas Teknik, Universitas Perjuangan Tasikmalaya

Correspondence author: M.I. Arief, 2103010101@unper.ac.id, Ciamis, Indonesia

Abstract

SIMPELMAS was a web-based information system used by the LP2M of XYZ University to manage research and community service data. A hacking incident on the simpelmas.universitas-xyz.ac.id subdomain indicated security vulnerabilities that needed further investigation. This research aimed to analyse the vulnerability level of the subdomain using a penetration testing approach based on the Open Web Application Security Project (OWASP) Top 10 2021 edition standards. A black-box testing method was implemented through data collection, vulnerability scanning, exploitation testing, and report preparation stages, utilising OWASP ZAP, Burp Suite, and SQLMap tools. The results revealed two principal vulnerabilities: Security Misconfiguration in the form of active APP_DEBUG on the production server, and Identification and Authentication Failures due to the absence of login attempt restrictions (rate limiting). This research provides technical recommendations for mitigation and can serve as a reference for security improvements in similar information systems within academic environments.

Keywords: security vulnerabilities, web-based information system, owasp top 10

Abstrak

SIMPELMAS adalah sistem informasi berbasis web yang digunakan LP2M Universitas XYZ untuk pengelolaan data penelitian dan pengabdian masyarakat. Insiden peretasan pada subdomain simpelmas.universitas-xyz.ac.id mengindikasikan adanya celah keamanan yang perlu diteliti. Penelitian ini menganalisis kerentanan subdomain tersebut menggunakan pendekatan *penetration testing* berdasarkan standar OWASP Top 10 edisi 2021. Metode blackbox testing diterapkan melalui tahapan pengumpulan data, pemindaian kerentanan, pengujian eksploitasi, dan penyusunan laporan dengan memanfaatkan tools OWASP ZAP, Burp Suite, dan SQLMap. Hasil penelitian menemukan dua kerentanan utama: Security Misconfiguration berupa aktifnya APP_DEBUG di server produksi dan Identification and Authentication Failures karena tidak adanya pembatasan percobaan login. Penelitian ini menyediakan rekomendasi teknis untuk mitigasi dan dapat menjadi rujukan perbaikan keamanan sistem informasi di lingkungan akademik.

Kata Kunci: sistem informasi berbasis web, celah keamanan, owasp top 10

A. PENDAHULUAN

Pemanfaatan teknologi informasi telah menjadi pilar fundamental dalam operasional perguruan tinggi modern, mendukung berbagai aspek mulai dari administrasi akademik hingga pelaksanaan Tridarma Perguruan Tinggi. Di Universitas XYZ, Lembaga Penelitian dan Pengabdian kepada Masyarakat (LP2M) memainkan peran sentral dalam mengoordinasikan aktivitas penelitian dan pengabdian masyarakat. Untuk menunjang tugas ini, LP2M mengandalkan Sistem Informasi Penelitian dan Pengabdian kepada Masyarakat (SIMPELMAS), sebuah platform berbasis web yang dirancang untuk memfasilitasi pengelolaan hibah internal, penelitian mandiri, dan pengabdian masyarakat oleh para dosen. Sistem ini tidak hanya menyederhanakan proses pengajuan proposal dan pelaporan kemajuan bagi dosen, tetapi juga membantu LP2M dalam pemantauan, rekapitulasi data, dan penyajian informasi terstruktur yang esensial untuk akreditasi institusi.

Meskipun infrastruktur pendukung SIMPELMAS dikelola oleh Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi (UPT TIK) dengan berbagai lapisan proteksi, keamanan pada level aplikasi inti menghadapi tantangan signifikan. SIMPELMAS dibangun menggunakan kerangka kerja Laravel versi 6, yang tidak lagi menerima pembaruan keamanan resmi, sehingga berpotensi menyimpan kerentanan yang belum teridentifikasi. Situasi ini diperburuk oleh kurangnya dokumentasi pengembangan yang memadai dan fakta bahwa pengujian keamanan secara mendalam belum pernah dilakukan. Kerentanan sistem ini terbukti nyata ketika subdomain SIMPELMAS mengalami insiden peretasan pada 21 Oktober 2024, yang menyebabkan perubahan pada halaman *website* dan hilangnya data. Insiden ini terdokumentasi dalam arsip aktivitas peretasan global di situs defacer.id, yang mencatat bahwa simpelmas.universitas-xyz.ac.id diretas oleh "saTaoz" dari tim Jawa Barat Cyber (saTaoz, 2024). Serangan ini merupakan contoh nyata dari fenomena *Web Defacement*, yaitu tindakan modifikasi tampilan halaman web oleh pihak tidak berwenang.

Fenomena *Web Defacement* seperti yang terjadi pada SIMPELMAS bukanlah insiden yang jarang terjadi, terutama pada situs pemerintahan dan pendidikan. Meskipun dalam kasus ini dampaknya berupa modifikasi konten, risiko serangan serupa dapat berkembang menjadi lebih serius, seperti penyalahgunaan situs untuk menampilkan konten ilegal (misalnya, iklan judi daring), yang dikenal sebagai *Web Defacement Slot.* Serangan semacam ini tidak hanya menimbulkan dampak negatif pada reputasi instansi tetapi juga berpotensi menyebabkan hilangnya kepercayaan pengguna. Menyadari risiko ini, diperlukan pendekatan proaktif untuk mengidentifikasi dan memitigasi celah keamanan sebelum dapat dieksploitasi kembali.

Untuk menjaga keamanan data dan informasi dalam menghadapi ancaman tersebut, metode *penetration testing* (uji penetrasi) dapat diterapkan. Metode ini merupakan rangkaian langkah sistematis untuk menguji tingkat keamanan suatu sistem, melibatkan analisis mendalam guna mengidentifikasi potensi kerentanan seperti kesalahan konfigurasi, kelemahan perangkat lunak/keras, atau kekurangan dalam logika proses (Dharmawan, 2022). Dalam penerapannya pada sebuah *website*, penggunaan standar tertentu menjadi panduan penting untuk menganalisis keamanannya (Dharmawan, 2022).

Di tengah pesatnya perkembangan domain keamanan siber, kepatuhan terhadap standar keamanan yang mapan selama pengujian penetrasi menjadi sangat krusial. Kerangka kerja seperti ISO, ISSAF, NIST CSF, dan OWASP berfungsi sebagai tolok ukur penting bagi para profesional. Analisis komparatif menunjukkan bahwa OWASP (*Open Web Application Security Project*), khususnya daftar Top 10, unggul karena

diperbarui secara berkala oleh para ahli global untuk merefleksikan risiko aplikasi web terkini dengan pembaruan signifikan pada tahun 2021 dan sifatnya yang *open-source* serta bebas biaya, menjadikannya pilihan tepat, terutama bagi organisasi dengan anggaran terbatas (Tinambunan et al., 2024). Dengan mengadopsi model OWASP Top 10, organisasi dapat memfokuskan upaya pada risiko keamanan terbesar dan menutupi celah yang ada, sementara kerangka kerja lain seperti NIST CSF dapat melengkapinya dengan panduan pengelolaan keamanan informasi yang lebih holistik (Tinambunan et al., 2024).

Beberapa penelitian terdahulu telah mengaplikasikan metode serupa dalam konteks keamanan sistem informasi. Sebagai contoh, Dharmawan, Prihati, dan Listijo (2022) berjudul "*Penetration testing* menggunakan owasp top 10 pada domain xyz.ac.id" melakukan *penetration testing* menggunakan OWASP Top 10 tahun 2017 pada domain xyz.ac.id dan disebutkan bahwa berhasil mengidentifikasi celah keamanan seperti SQL Injection dan Cross-Site Scripting (Dharmawan, 2022).

Penelitian lain oleh Febry Septian, Muhammad Hadi Arfian, Jefry Sunupurwa Asri, dan Budi Tjahjono (2024) berjudul "Pengujian Keamanan *Website* dengan Metode *Penetration testing* (Studi Kasus: Universitas Esa Unggul" disebutkan bahwa menggunakan OWASP Top 10 2021 dan menemukan kerentanan berisiko tinggi seperti broken access control dan security misconfiguration (Septian et al., 2024).

Selanjutnya, Yusuf dan Suharsono (2023) dengan penelitian yang berjudul "Pengujian keamanan dengan metode owasp top 10 pada *website eform helpdesk*" disebutkan bahwa penelitian tersebut juga menggunakan OWASP Top 10 2021 pada *website eform helpdesk* dan menemukan enam celah keamanan, termasuk *Broken Access Control*, *Cryptographic Failures*, dan *Injection* (Yusuf & Suharsono, 2023).

Demikian pula, penelitian Tinambunan, Junaidi, dan Rizki (2024) yang berjudul "Pengujian sistem informasi akademik universitas melalui pendekatan *penetration testing* berdasarkan owasp top 10" berhasil mengidentifikasi 23 celah keamanan pada Sistem Informasi Akademik Universitas X dengan pendekatan *penetration testing* berdasarkan OWASP Top 10, di mana 20 di antaranya sesuai kategori OWASP Top 10 termasuk "Broken Access Control" dan "Injection" (Tinambunan et al., 2024).

Penelitian-penelitian ini menunjukkan efektivitas OWASP Top 10 sebagai panduan dalam mendeteksi berbagai kerentanan pada aplikasi web di lingkungan akademik maupun lainnya.

Berdasarkan latar belakang dan tinjauan penelitian terdahulu, tujuan dari penelitian ini adalah untuk: (1) Mengidentifikasi potensi celah keamanan pada subdomain simpelmas.universitas-xyz.ac.id menggunakan metode *penetration testing* berbasis OWASP Top 10 tahun 2021; (2) Menganalisis tingkat risiko dari setiap celah keamanan yang ditemukan; dan (3) Memberikan rekomendasi mitigasi teknis untuk memperbaiki celah keamanan tersebut guna meningkatkan keamanan sistem secara menyeluruh.

Penelitian ini berbeda dengan penelitian sebelumnya karena fokusnya secara spesifik pada subdomain simpelmas Universitas XYZ, yang memiliki peran krusial dalam pengelolaan data penelitian dan pengabdian masyarakat. Keunggulan dan kebaruan penelitian ini terletak pada penggunaan standar OWASP Top 10 tahun 2021 yang lebih mutakhir untuk menghadapi ancaman keamanan terbaru, serta evaluasi terhadap efektivitas langkah-langkah keamanan yang telah ada pada sistem target, seperti firewall, VPN, Docker, WAF, dan Cloudflare. Dengan demikian, posisi penelitian ini adalah untuk menguji secara komprehensif sistem yang sudah beroperasi dan memiliki lapisan pertahanan awal, namun belum pernah diaudit keamanannya secara mendalam pasca

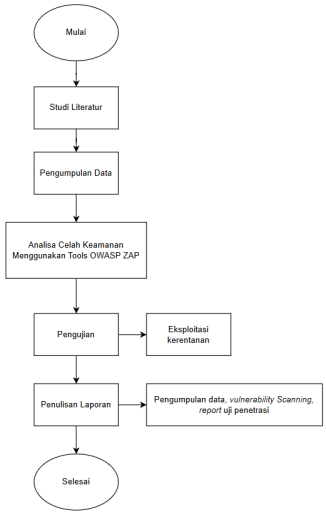
insiden peretasan dan mengingat versi platform yang digunakan sudah usang

Kontribusi yang diharapkan dari penelitian ini adalah memberikan gambaran nyata mengenai kondisi keamanan SIMPELMAS Universitas XYZ, menyediakan dasar bagi LP2M dan tim teknis universitas untuk melakukan perbaikan yang terukur, serta menjadi studi kasus yang relevan bagi institusi pendidikan tinggi lain yang mengelola sistem serupa. Selain itu, penelitian ini juga berkontribusi pada khazanah ilmiah terkait penerapan praktis OWASP Top 10 2021 dalam audit keamanan sistem informasi akademik.

Adapun keterbatasan (*limitation*) dalam penelitian ini meliputi: (1) Pengujian keamanan difokuskan pada kerentanan yang tercakup dalam OWASP Top 10 tahun 2021, sehingga potensi kerentanan di luar daftar tersebut mungkin tidak teridentifikasi secara mendalam; (2) Pengujian dilakukan dengan pendekatan *black-box testing*, di mana penguji tidak memiliki akses ke kode sumber aplikasi, yang mungkin membatasi analisis pada beberapa jenis kerentanan tertentu; dan (3) Ruang lingkup pengujian terbatas pada subdomain simpelmas.universitas-xyz.ac.id dan tidak mencakup keseluruhan infrastruktur jaringan Universitas XYZ.

B. METODE PENELITIAN

Penelitian ini mengikuti alur sistematis yang mencakup: studi literatur, pengumpulan data, analisis kerentanan, pengujian, dan pelaporan. Tahapan ini dirancang untuk mempermudah identifikasi dan evaluasi kerentanan pada subdomain Simpelmas. Tahapan penelitian dapat dilihat pada gambar 1,



Gambar 1. Metode Penelitian

Pengumpulan Data

Tahap ini bertujuan untuk memperoleh informasi teknis terkait target sistem, mencakup alamat IP, layanan aktif, konfigurasi jaringan, dan data pendukung lainnya. Proses dilakukan melalui teknik information gathering dan footprinting menggunakan beberapa metode berikut:

1. Whois

Untuk memperoleh informasi registrasi domain dan IP (Allo & Widiasari, 2024).

2. Nmap

"nmap -sS -sV -O -A -T4 --host-timeout 30m -F <TARGET_IP>" pada Nmap ini menggunakan *scan* SYN untuk mengetahui apakah *port* terbuka, mendeteksi versi layanan, mendeteksi sistem operasi, dan menjalankan *scan* yang lengkap dengan kecepatan sedang. Selain itu, command ini menggunakan timeout 30 menit untuk setiap host dan menggunakan daftar *port* yang paling umum digunakan untuk mempercepat proses *scan* (Dwiyatno, 2020).

3. *Google dorking*

Karena subdomain simpelmas menggunakan halaman login sebagai titik awal, pengumpulan data tambahan diperlukan untuk menyusun wordlist guna mendukung brute force login. Metode yang digunakan yaitu *Google dorking* dengan memanfaatkan teknik pencarian lanjutan di Google untuk menemukan informasi publik

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 05 NOMOR 02 JULI 2025
ISSN 2774 – 5775 | eISSN 2774-5767

terkait dengan Simpelmas (Dirgantara et al., 2025). Contoh dorking:

a. "site:simpelmas.universitas-xyz.ac.id" filetype:pdf
untuk mencari dokumen yang mungkin berisi data pengguna.
b. "site:*.universitas-xyz.*"
untuk menemukan subdomain yang berhubungan dengan Universitas XYZ, termasuk sistem yang membutuhkan autentikasi.

Hal ini membantu dalam memetakan cakupan sistem yang relevan untuk penelitian

4. *Bypass* Login Sederhana

Pada sistem yang ditemukan dari hasil *google dorking* dan memiliki login sederhana, eksplorasi dilakukan untuk mencoba *bypass* autentikasi dengan memanfaatkan parameter login yang lemah atau manipulasi permintaan sederhana. Tujuannya adalah untuk mengakses halaman dashboard yang mungkin berisi informasi lebih lanjut.

Memindai dan Analisa Celah Keamanan

Pemindaian kerentanan dilakukan menggunakan OWASP ZAP, dengan fitur pemindaian otomatis terhadap subdomain Simpelmas. Hasil analisis meliputi jenis celah keamanan, tingkat risiko (tinggi, sedang, rendah), serta kategorisasi berdasarkan OWASP Top 10.

Pengujian

Eksploitasi dilakukan terhadap celah keamanan yang teridentifikasi sebelumnya, khususnya pada level risiko sedang hingga tinggi. Pengujian dilakukan menggunakan *Burp Suite*, dengan fitur seperti *Repeater* dan *Intruder* untuk memodifikasi permintaan, menguji *payload*, dan melakukan serangan terhadap parameter yang rentan.

Penulisan Laporan

Tahap akhir berupa penyusunan laporan berisi rangkuman temuan dari seluruh tahapan, termasuk hasil pemindaian dan pengujian, serta rekomendasi teknis untuk meningkatkan keamanan sistem.

C. HASIL DAN PEMBAHASAN

Pengujian Keamanan pada SIMPELMAS bertujuan untuk mencegah peretasan yang dilakukan oleh orang yang tidak bertanggung jawab. Hasil dari pengujian akan diberikan kepada pengembang sistem sebagai panduan untuk melakukan perbaikan yang diperlukan. Pengujian ini dilaksanakan dengan menggunakan teknik *penetration testing* berdasarkan standar keamanan OWASP TOP 10. Pada bagian ini akan dipaparkan hasil pengumpulan data, *vulnerability scanning*, dan pengujian.

Pengumpulan Data

Keamanan Dari proses *Information Gathering* yang telah dilakukan pada Simpelmas, hasilnya terungkap dalam bentuk informasi yang terdokumentasi seperti pada tabel 1 berikut

Tabel 1. Hasil Pengumpulan Data

No	Metode/Tools	Hasil Utama
1	Whois	Ditemukan informasi domain universitas-xyz.ac.id: terdaftar sejak 2015, kadaluarsa 2025. Didapat email server, NS, dan nama organisasi
2	CMS Detector	Website menggunakan framework Laravel.
3	Shodan	1X3.1X6.XX.1XX (antis.universitas-xyz.ac.id) 1X3.2X4.XXX.3X (sister.universitas-xyz.ac.id) 1X.7X.XXX.1XX (api-ere*port*.universitas-xyz.ac.id dan ec2-1X-7X-XXX-1XX.ap-southeast-3.compute.amazonaws.com)
4	Hackertarget Subfinder	**Simantap.universitas-xyz.ac.id (1X.7X.XXX.1XX)** **Simpelmas.universitas-xyz.ac.id (1X.7X.XXX.1XX)** Subdomain simpelmas dan simantap berada dalam satu IP server

No	Metode/Tools	Hasil Utama
5	Nmap	**Subdomain simpelmas.universitas-xyz.ac.id** *Port* terbuka: 80 (HTTP), 443 (HTTPS), 8080, dan 8443.
		IP 1X.7X.XXX.1XX *Port* terbuka: 22 (SSH), 80, dan 443. *Port* 8080 menampilkan login Pritunl VPN. Untuk percobaan *port* 22 (SSH), *port* tidak dapat diakses – butuh autentikasi publik key.
6	Dirsearch	**Subdomain simpelmas.universitas-xyz.ac.id** Ditemukan direktori sensitif: /php.php, /register, /_ignition, dll.
		IP 1X.7X.XXX.1XX Ditemukan direktori v1, yang berisi json Message: "API is working"
		IP 1X.7X.XXX.1XX:8080 Banyak folder admin ditemukan, sebagian besar mengarah ke **Unauthorized**.
7	Google Dorking	**site:simpelmas.universitas-xyz.ac.id filetype:pdf** Tidak ada informasi yang terindeks
		site:*.universitas-xyz.*. Ditemukan domain sinaima.universitas-xyz.org, mengandung halaman login admin.
8	Bypass Admin Login	Berhasil akses *dashboard* sinaima.universitas-xyz.org dengan teknik '='or', diperoleh username dan password.

Analis Kebutuhan Sistem

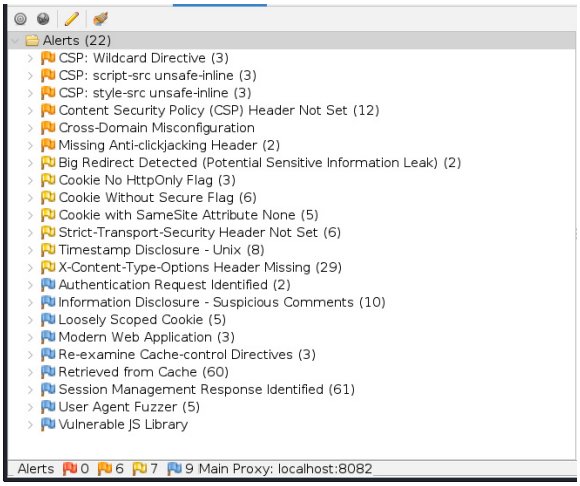
Analisis kebutuhan sistem dilakukan untuk memahami infrastruktur target serta perangkat yang digunakan dalam proses pengujian. Berdasarkan informasi dari pihak UPTIK, diketahui bahwa *subdomain* simpelmas.universitas-xyz.ac.id didukung oleh layanan *AWS*, menggunakan *Cloudflare CDN*, serta dilindungi dengan *firewall*, *Docker*, dan akses melalui *VPN*. Sementara itu, pengujian dilakukan menggunakan perangkat laptop dengan spesifikasi sebagai berikut:

Tabel 2. Spesifikasi Perangkat Penelitian

Kategori	Detail
Perangkat	Laptop
Sistem Operasi	Kali Linux versi 2023.3 (Codename Kali-Rolling)
VPN	ExpressVPN untuk menghindari pemblokiran IP Penguji
Processor	12th Gen Intel® Core™ i5-1235U (12 CPUs), ~1.3GHz
Ram	8 GB
Storage	512 GB
VGA	Intel® UHD Graphics

Vulnerability *Scan*ning

Tahap ini bertujuan untuk mengidentifikasi kerentanan yang terdapat pada subdomain target menggunakan *tool* OWASP ZAP. Pemindaian dilakukan dengan fitur *automated scan,* yang menghasilkan sejumlah alert keamanan pada sistem target.



Gambar 1. Kerentanan yang ditemukan owasp zap

Pada Gambar 3, ditampilkan hasil pemindaian OWASP ZAP yang mengindikasikan adanya enam jenis alert dengan tingkat risiko *medium*. Masing-masing *alert* menjelaskan potensi celah yang dapat dimanfaatkan oleh penyerang:

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 05 NOMOR 02 JULI 2025
ISSN 2774 – 5775 | eISSN 2774-5767

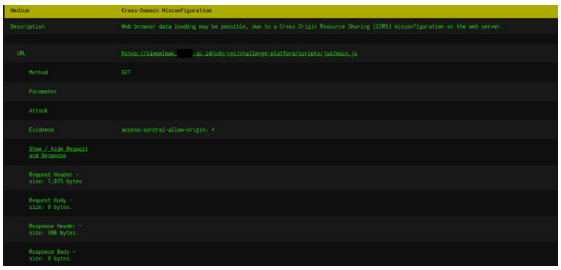
1. CSP: *Wildcard Directive* – Kebijakan *Content Security Policy* menggunakan *wildcard* (*), yang memungkinkan pemuatan sumber daya dari domain manapun tanpa batasan.
2. CSP: *script-src unsafe-inline* – Mengizinkan skrip inline yang membuka kemungkinan eksekusi kode berbahaya secara langsung di browser (potensi XSS).
3. CSP: *style-src unsafe-inline* – Mengizinkan gaya CSS *inline*, yang dapat digunakan untuk mengubah tampilan halaman secara tidak sah.
4. CSP *Header Not Set – Header* CSP tidak ditemukan dalam HTTP *response*, sehingga mengurangi lapisan perlindungan terhadap serangan berbasis *browser*.
5. *Cross-Domain Misconfiguration* – Konfigurasi CORS (*Cross-Origin Resource Sharing*) tidak aman karena mengizinkan akses dari *domain* asing yang tidak terpercaya.
6. *Missing Anti-clickjacking Header* – Ketiadaan *header X-Frame-Options* atau *frame-ancestors* menyebabkan sistem rentan terhadap *clickjacking*, di mana pengguna dapat diarahkan untuk mengklik elemen tersembunyi dalam *iframe*.

Pengujian

Pengujian dilakukan berdasarkan kategori kerentanan dari OWASP *Top* 10 (2021) menggunakan pendekatan *blackbox*. Setiap hasil pengujian diuraikan sebagai berikut:

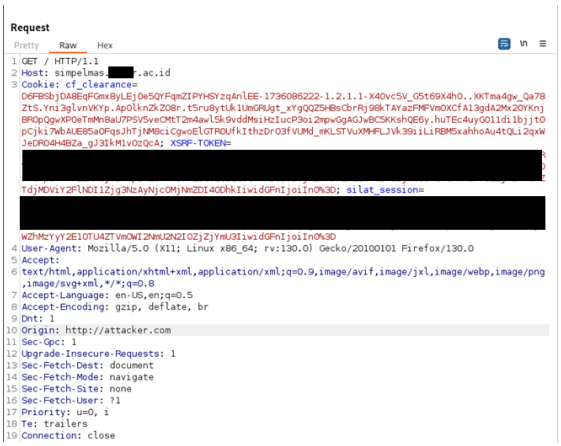
1. A01: Broken Access Control

Hasil *scanning* OWASP ZAP mendeteksi *Cross-Domain Misconfiguration*



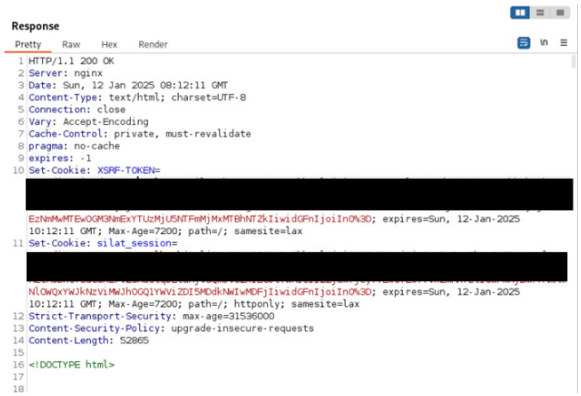
Gambar 2. Kerentanan Cross-Domain Misconfiguration

Gambar 3 menunjukkan temuan awal dari pemindaian otomatis OWASP ZAP yang mengindikasikan potensi konfigurasi lintas *domain* yang tidak aman.



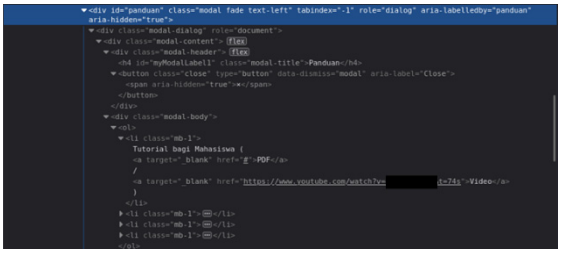
Gambar 3. Modifikasi *Header Origin* pada *Burp Suite*

Gambar 4 memperlihatkan upaya modifikasi *Origin header* menggunakan *Burp Suite* untuk memvalidasi konfigurasi CORS



Gambar 4. Hasil pengujian kerentanan CORS

Gambar 5 merupakan hasil respon dari server, yang menunjukkan tidak terdapat balasan *Access-Control-Allow-Origin*, sehingga kerentanan tersebut dianggap *false positive.* Selanjutnya, penulis melakukan *inspect element* pada halaman *login* dan menemukan tombol tersembunyi.



Gambar 5. Tombol panduan tersembunyi di halaman login

Gambar 6 menampilkan tombol tersembunyi yang mengarah pada dokumentasi sistem berupa video tutorial. Penulis mencoba mengakses beberapa URL yang diperoleh dari dokumentasi tersebut untuk memverifikasi akses kontrol.

Tabel 3. URL Dokumentasi *Website* Simpelmas

URL	Keterangan
https://www.youtube.com/watch?v=XXXX&t=74s	Tutorial bagi Mahasiswa
https://www.youtube.com/watch?v=tXX-XXXX8&t=24s	Tutorial bagi Pembimbing
https://www.youtube.com/watch?v=hXXXVbXXX	Tutorial bagi Reviewer
https://www.youtube.com/watch?v=aXXXFQNXXX	Tutorial bagi Operator

Tabel 3 memuat daftar tautan video dokumentasi dari berbagai peran pengguna (mahasiswa, pembimbing, reviewer, dan operator). Penulis mencoba mengakses beberapa URL yang diperoleh dari dokumentasi tersebut untuk memverifikasi akses kontrol.

Tabel 4. URL Dokumentasi Role Mahasiswa

URL	Isi	Hasil Percobaan
/mahasiswa/proposal	Form upload Pengajuan PKM	Tidak valid
/mahasiswa/rekap	Tabel Rekap Proposal mahasisw	Tidak valid
/master/kalender_view	Kalender pengajuan PKM	Tidak valid
/manajemen/proposal/5	Monitoring progress proposal	Tidak valid

Tabel 5. Dokumentasi Role Pembimbing

URL	Isi	Hasil percobaan
/manajemen/manajemen-pembimbing?tahun=2021	Manajemen Pembimibing	Tidak valid
/manajemen/proposal/5	Monitoring progress proposal	Tidak valid

Tabel 6. Dokumentasi Role Reviewer

URL	Isi	Hasil percobaan
/manajemen/manajemenpembimbing?tahun=2021	Manajemen Reviewer	Tidak valid
/manajemen/nilai/5	Monitoring penilaian	Tidak valid

Tabel 7. Dokumentasi Role Operator

URL	Isi	Hasil percobaan
/master/user	Manajemen Pengguna	Tidak valid
/master/role	Monitoring *Role*	Tidak valid
/master/prodi	Manajemen Fakultas & Prodi	Tidak valid

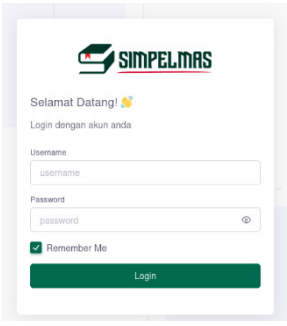
JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 05 NOMOR 02 JULI 2025
ISSN 2774 – 5775 | eISSN 2774-5767

URL	Isi	Hasil percobaan
/master/jenis	Manajemen Jenis PKM	Tidak valid
/master/kalender	Manajemen Kalender PKM	Tidak valid
/rekap/proposal ?tahun=2021	Manajemen Rekap Proposal	Tidak valid
/rekap/proposal-detail?tahun=2021&id=10	Detail Rekap Proposal	Tidak valid
/rekap/kip?tahun=2021&angkatan=2021	Detail Rekap KIP	Tidak valid

Tabel 4 hingga 7 menunjukkan hasil percobaan akses langsung ke *endpoint* berdasarkan dokumentasi sistem. Semua akses dinyatakan tidak valid saat tidak dalam kondisi login. Kesimpulan pengujian : Tidak ditemukan celah *Broken Access Control*.

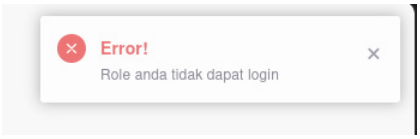
2. A03: Injection

Penulis mencoba teknik *SQL Injection* pada halaman *login*



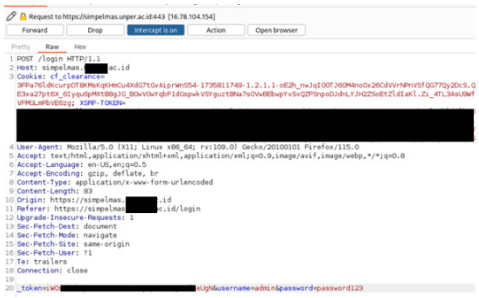
Gambar 6. Tampilan halaman login simpelmas

Gambar 7 merupakan tampilan form login yang menjadi target injeksi.



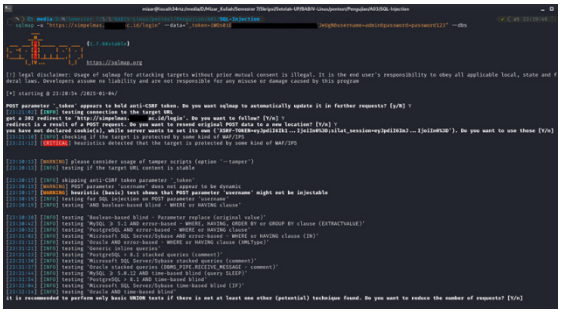
Gambar 7. Hasil *Bypass Login* Manual

Gambar 8 menunjukan bahwa percobaan dengan *payload* '='or' tidak berhasil.



Gambar 8. Intercept Parameter Login *dengan Burp Suite*

Gambar 9 menampilkan parameter *form login* yang berhasil ditangkap.

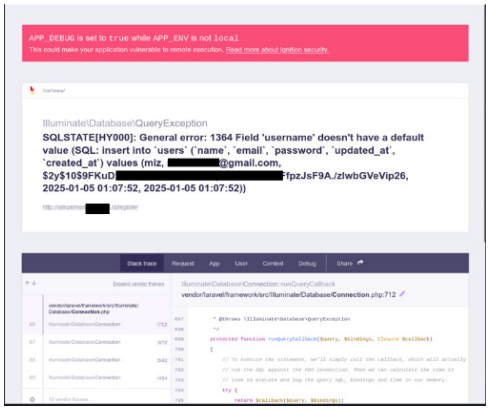


Gambar 9. *Pengujian* SQL Injection *dengan* Payload *Pertama*

Gambar 10. Pengujian *SQL Injection* dengan *Payload* Kedua

Gambar 10 dan Gambar 11 tersebut menunjukkan hasil penggunaan SQLMap, yang keduanya tidak berhasil mengeksploitasi *endpoint login*. Kesimpulan pengujian : Tidak ditemukan celah *Injection*.

3. A05: *Security Misconfiguration*



Gambar 11. *Error APP_DEBUG* Aktif

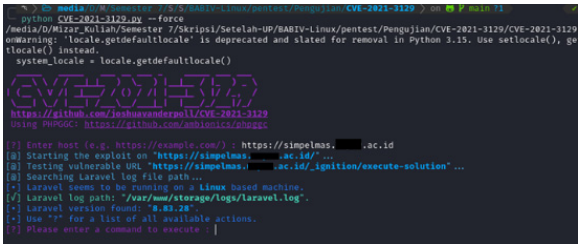
Gambar 12 mengindikasikan bahwa **APP_DEBUG** masih aktif di lingkungan produksi.

Tabel 8. Informasi Sensitif yang Terekspos

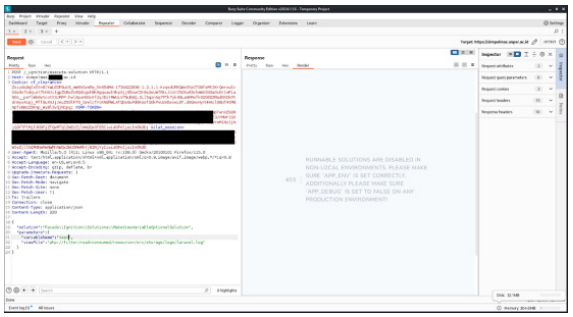
Header	
Path web	/var/www/
x-forwarded-for & x-real-ip	45.8.25.100
Session	
Url	"intended": "http://simpelmas.universitas-xyz.ac.id/master/user"
Environment information	
Laravel Version	8.83.28
PHP Version	7.4.33
Debug	
Connection name	mysql

Tabel 8 menunjukkan informasi penting seperti path direktori, versi Laravel, versi PHP, dan koneksi database yang dapat dimanfaatkan oleh penyerang. Kesimpulan pengujian : Ditemukan celah *Security Misconfiguration*

4. A06: *Vulnerable and Outdated Components*



Gambar 12. Uji Kerentanan CVE-2021-3129



Gambar 13. Eksploitasi Manual Menggunakan *Burp Suite*

Pada gambar 13 dan 14 menunjukan bahwa meskipun *endpoint* dapat diakses, namun eksploitasi gagal karena *patch* sudah diterapkan. Hasil: Kerentanan tidak dapat dieksploitasi.

5. A07: *Identification and Authentication Failures*

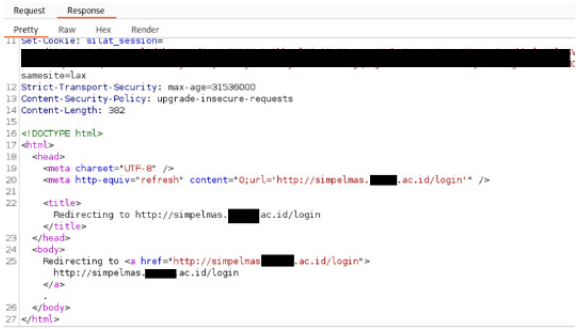
Berdasarkan hasil inspeksi halaman, penulis menemukan indikasi nama pengguna yang valid seperti pada gambar 15. Nama ini kemudian digunakan sebagai target dalam pengujian *brute force*.

Gambar 14. *Username* Valid Berdasarkan Halaman *Website*

Gambar 15 menunjukkan tampilan nama admin yang memiliki potensi sebagai target *login*. Pengujian *brute force* dilakukan dengan *Burp Suite* dan *custom script*. Salah satu respon yang dihasilkan adalah *redirect* otomatis ke halaman *login*, yang menutupi

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 05 NOMOR 02 JULI 2025
ISSN 2774 – 5775 | eISSN 2774-5767

pesan *error* eksplisit namun tetap memungkinkan percobaan terus-menerus.



Gambar 15. Respon *Brute Force* yang Dialihkan ke Halaman Login

Gambar 16 memperlihatkan bahwa sistem melakukan *redirect*, bukan memberikan pesan *error* langsung. Dari 56 kombinasi *username* dan *password* yang diuji, tidak ditemukan percobaan login yang berhasil. Namun, tidak ada pembatasan jumlah percobaan *login* yang diterapkan. Berikut adalah contoh hasil *brute force*:

Tabel 9. Hasil *Brute Force Login*

No	Username	Passowrd	Hasil
1	rixki	123456	Username tidak ada
2	rixxxxeb	123456	Password salah
3	trxxxxxxxni	123456	Password salah
4	arxxxxxxxxna	123	Username tidak ada
5	arxxxxxxxxna	123	Password salah

Tabel 9 merupakan cuplikan dari hasil *brute force*. Dapat terlihat bahwa sistem tidak memberikan *rate limiting* atau pemblokiran meskipun terjadi percobaan *login* berulang. Hasil**:** Sistem memungkinkan *brute force* karena tidak membatasi jumlah percobaan *login* (*rate limiting* tidak diterapkan).

Rekomendasi Perbaikan

Berdasarkan hasil pengujian, disusun rekomendasi perbaikan untuk masing-masing temuan:

1. Nonaktifkan APP_DEBUG di lingkungan produksi untuk mencegah *information disclosure*.
2. Perbarui komponen Laravel untuk menghindari potensi eksploitasi CVE yang sudah diketahui.
3. Terapkan *rate limiting* dan mekanisme penguncian (*lockout*) pada halaman *login* untuk mencegah serangan *brute force*.
4. Lakukan audit berkala terhadap konfigurasi CSP dan header keamanan untuk menghindari *misconfiguration*.

D. PENUTUP

Penelitian ini menganalisis keamanan subdomain Simpelmas Universitas XYZ dengan pendekatan OWASP Top 10 tahun 2021. Berdasarkan hasil pengujian, dapat disimpulkan bahwa secara umum sistem memiliki tingkat kerentanan yang rendah. Namun, dua kategori OWASP yang teridentifikasi sebagai celah potensial adalah Security Misconfiguration dan Identification and Authentication Failures. Ditemukan bahwa fitur APP_DEBUG masih aktif di lingkungan produksi, serta terdapat file phpinfo() yang dapat diakses publik. Selain itu, tidak adanya pembatasan percobaan login (rate limtting) menjadikan halaman login berpotensi menjadi target brute force. Walaupun kerentanan CVE-2021-3129 telah ditambal, penggunaan framework Laravel versi lama tetap menjadi perhatian keamanan.

Untuk meningkatkan keamanan sistem, berikut adalah rekomendasi teknis yang disarankan: (1) Menonaktifkan APP_DEBUG dan memperkuat konfigurasi server; (2) Mengimplementasikan rate limiting pada proses login; (3) Melakukan pembaruan sistem dan framework secara berkala; (4) Menjalankan uji keamanan rutin untuk mendeteksi kerentanan baru.

Saran bagi pengelola sistem di Universitas XYZ meliputi: (1) Melakukan audit keamanan secara berkalan pada seluruh

subdomain; (2) Mengaktifkan autentikasi dua faktor (2FA) pada sistem login; (3) Meningkatkan literasi keamanan siber di kalangan pengembang dan pengelola sistem.

E. DAFTAR PUSTAKA

Allo, A. K., & Widiasari, I. R. (2024). Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning. *JTIK : Jurnal Teknologi Informasi Dan Komunikasi*, *8*(2), 316–323. https://doi.org/10.35870/jtik.v8i2.1723

Dharmawan, A. (2022). Penetration Testing Using OWASP Top 10 On Domain XYZ.ac.id. *Electro Luceat*, *8*(1), 100–108. https://doi.org/10.32531/jelekn.v8i1.455

Dirgantara, R., Kurniati, R., & Hidayasari, N. (2025). Uji Penetrasi Keamanan Website Dinas Komunikasi dan Informatika. *Jurnal Techno.Com*, *24*(1), 260–270. https://doi.org/10.62411/tc.v24i1.12259

Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://doi.org/10.30656/prosisko.v7i2.2522

saTaoz. (2024). *simpelmas.unper.ac.id was hacked*. Defacer.Id. https://defacer.id/mirror/id/129245

Septian, F., Arfian, M. H., Asri, J. S., & Budi Tjahjono. (2024). Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul). *INNOVATIVE: Journal Of Social Science Research*, *4*(5), 3629–3647.

Tinambunan, F., Junaidi, A., & Rizki, A. M. (2024). Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10. *JATI : Jurnal Mahasiswa Teknik Informatika*, *8*(1), 1062–1069. https://doi.org/10.36040/jati.v8i1.8920

Yusuf, R. R., & Suharsono, T. N. (2023). Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk. *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi Dan Teknik*, 402–413. https://doi.org/10.32897/sobat.2023.5.0.3132