

# Analisis Celah Keamanan *Website* Poltekkes Kemenkes Sorong Menggunakan Metode *Penetration Testing*

Gunawan Yudi Jayanto<sup>1\*</sup>  
Julius Panda Putra Naibaho<sup>2</sup>  
Alex De Kweldju<sup>3</sup>

<sup>1</sup>Fakultas Teknik, Teknik Informatika, Universitas Papua, Jl. Gunung Salju Amban, Manokwari,  
Papua Barat 98314, Indonesia

<sup>1</sup>yudigunawanmkw@gmail.com, <sup>2</sup>j.naibaho@unipa.ac.id

<sup>3</sup>a.dexweldju@unipa.ac.id

**\*Penulis Korespondensi:**

Gunawan Yudi Jayanto  
yudigunawanmkw@gmail.com

## Abstrak

Waktu ini, teknologi informasi mempunyai sangat diperlukan, di era digital keamanan siber menjadi salah satu faktor utama suatu institusi untuk dapat bertahan dan diakui kredibilitasnya, termasuk institusi pendidikan, Website Poltekkes Sorong digunakan sebagai portal utama atau media untuk menyebarkan informasi akademik, interaksi antara mahasiswa dan publik, Namun keberadaan celah keamanannya merupakan suatu yang memungkinkan serangan siber untuk dilakukan yang dapat membahayakan kerahasiaan data. Penelitian ini bertujuan buat melakukan analisis terhadap celah keamanan website Poltekkes Kemenkes Sorong, pengujian yang dilakukan menggunakan metode penetration testing yang beberapa tahap meliputi pengumpulan informasi scanning, analisa kerentanan. Sehingga penelitian ini dapat memberikan panduan dan praktis bagi pengelola sistem informasi di Poltekkes Kemenkes Sorong untuk mengurangi resiko serangan siber dan melindungi data sensitif yang dipegang oleh institusi.

**Kata Kunci:** Keamanan Website; Kerentanan Web Acunetix; Penilaian Kerentanan Owasp Zap; Uji Penetrasi

## Abstract

Currently, information technology is very necessary, in the digital era cybersecurity is one of the main factors for an institution to survive and be recognized for its credibility, including educational institutions, the Poltekkes Sorong Website is used as the main portal or media to disseminate academic information, interaction between students and the public, However, the existence of security gaps is something that allows cyber attacks to be carried out which can endanger data confidentiality. This study aims to analyze the security gaps in the Poltekkes Kemenkes Sorong website, the testing carried out using the penetration testing method which has several stages including collecting scanning information, vulnerability analysis. So that this study can provide guidance and practice for information system managers at Poltekkes Kemenkes Sorong to reduce the risk of cyber attacks and protect sensitive data held by the institution.

**Keywords:** Acunetix Web Vulnerability; Owasp Zap Vulnerability Assessment; Penetration Testing; Website Security.

---

## 1. Pendahuluan

Pada era digital yang semakin berkembang keamanan informasi menjadi salah satu aspek krusial bagi setiap organisasi, termasuk lembaga pendidikan, *Website* merupakan sumber informasi yang terus berkembang mengikuti perkembangan teknologi dimasa sekarang, dan penggunaan website telah banyak diterapkan di berbagai bidang[1]. *Website* banyak digunakan sebagai media penyimpanan data, dan informasi yang dapat diakses secara publik maupun secara rahasia[2]. Penyimpanan data pribadi yang terdapat didalam sebuah *website* harus bersifat aman, sehingga *website* tersebut harus memiliki sistem keamanan yang baik dan dapat menjamin keamanan data yang tersimpan pada server *website* tersebut[3]. Website tidak hanya berfungsi sebagai sarana penyebaran informasi, tetapi juga sebagai medium penting dalam pelaksanaan administrasi akademik pendaftaran dan interaksi antara pihak kampus dengan mahasiswa serta publik. Salah

satu jenis media informasi daring adalah situs web. Website adalah gabungan *page* yang tersusun bersama domain atau subdomain khusus, yang diakses lewat jaringan internet[4]. Dokumen HTML yang dapat dilihat melalui protokol http atau https disebut halaman web. Situs web, aplikasi, dan blog merupakan contoh sistem informasi. Setiap organisasi, berapa pun ukurannya, terutama lembaga pendidikan, harus mengutamakan keamanan informasi. Sebagai lembaga pendidikan, universitas rentan terhadap serangan siber [5]. dengan situs web resmi universitas menjadi salah satu targetnya [6]. Website saat ini tidak hanya menyebarkan informasi tetapi juga digunakan dalam pelaksanaan administrasi akademik pendaftaran, serta interaksi dengan siswa maupun publik. Metode pengelolaan sumber daya jaringan disebut keamanan jaringan, dan tujuannya adalah untuk membatasi akses jaringan sehingga hanya pengguna yang berwenang yang dapat menggunakan jaringan [7]. *Penetration testing* dapat digunakan untuk mengurangi frekuensi kejadian yang tidak diinginkan, salah satunya adalah untuk mengidentifikasi serangan injeksi, terutama injeksi pada database atau server yang bisa ditemukan dalam kasus *SQL Injection*. Website Poltekkes Kemenkes Sorong, sebagai salah satu institusi pendidikan kesehatan, juga dituntut untuk memastikan keamanan data dan transaksi yang dilakukan melalui websitenya. Namun, dengan bertambahnya *technology* resiko siber juga semakin tinggi. Untuk solusinya, dilakukan teknik pengujian penetrasi yang dirancang untuk menilai kelemahan atau kekurangan pada situs web Poltekkes Kemenkes Sorong.

Penelitian untuk menemukan kelemahan keamanan pada situs web sistem informasi kampus, lakukan pengujian penetrasi [8]. Metode Kali Linux digunakan untuk teknik ini, *Penetration Testing* adalah kegiatan yang dilakukan oleh seseorang tertentu dengan cara menemukan celah kelemahan sistem yang akan menjadi sasaran serangan oleh orang ataupun pihak yang belum dikenal kebajikannya. Orang yang melakukan metode ini disebut dengan pentester. *Penetration testing* bertujuan untuk melihat jenis-jenis serangan apa yang dapat terjadi karena adanya celah-celah kelemahan tersebut[9][10][11]. Program sumber terbuka untuk virtualisasi disebut Virtualbox. Melalui penggunaan teknologi virtualisasi, orang dapat merasakan komputer dan sistem operasinya seolah-olah mereka hadir secara fisik. [12]. Kali Linux, sistem operasi sumber terbuka yang dibangun di atas Debian Linux, dikembangkan oleh Offensive Security [13]. Kali Linux digunakan untuk memenuhi persyaratan pengujian penetrasi dan sistem keamanan pada komputer. Kali Linux memiliki tampilan dasar dan mudah dioperasikan, sehingga populer di kalangan pemula yang mempelajari pengujian penetrasi dalam sistem, jaringan, dan aplikasi [14][15]. SQL adalah Structured Query Language, singkatannya adalah SQL. Bahasa tingkat keempat adalah SQL, artinya bahasa tersebut digunakan untuk menyajikan temuan atau mengubah fakta yang tidak diinginkan. Penyuntikan SQL, menurut White Hat, adalah teknik hacking. Secara singkat, fungsi dari serangan *SQL injection* adalah hacker dapat melihat database sebuah website. Serangan ini terjadi ketika input user tidak di-validated, sehingga user dapat memodifikasi perintah SQL yang dieksekusi oleh database. Jika form input data di website Poltekkes Kemenkes Sorong tidak dijaga, risiko dari *SQL Injection* adalah penyerang dapat dmaccan database website tersebut. Database yang terkena dampaknya merupakan tempat penyimpanan data-data sensitif seperti data mahasiswa dan data dosen[16].

Serangan yang dikenal sebagai DDoS (Denial of Service) terjadi ketika sejumlah besar permintaan pengguna membanjiri sumber daya pada server. Upaya ini membuat server tidak mampu menangani sejumlah besar permintaan pengguna, yang menyebabkan layanan gagal [17]. Sistem keamanan komputer dapat diserang menggunakan metode *brute force*, yang melibatkan pemilihan semua kemungkinan kunci melalui coba-coba. [18]. Serangan brute-force sering digunakan untuk mendapatkan akses ke data terenkripsi atau host, seperti stasiun kerja, server, atau jaringan. Penyerang menggunakan brute force untuk mendapatkan akses ke akun secara ilegal. Jika pengguna memilih kombinasi kata sandi yang sulit ditebak oleh peretas, metode ini akan memakan waktu yang sangat lama. Tingkat kesulitan pengguna saat membuat kata sandi menentukan berapa lama serangan ini berlangsung. Lamanya waktu yang dibutuhkan oleh

penyerang bertambah seiring dengan kompleksitas kata sandi. Website Poltekkes Kemenkes Sorong dijadikan sebagai objek dalam penelitian ini karena, sama seperti website lembaga pendidikan lainnya, sistem ini mungkin memiliki rentan terhadap serangan siber.

Kerentanan umum seperti SQL Injection (SQLi) dan Cross-Site Scripting (XSS) sering disorot oleh penilaian kerentanan keamanan pada situs web di sektor pendidikan. Studi ini membandingkan studi yang dilakukan pada situs web Poltekkes Kemenkes Sorong dengan studi sejenis yang dilakukan pada lembaga pendidikan lainnya. Menemukan kontribusi unik penelitian ini untuk meningkatkan mitigasi keamanan adalah tujuan utama.

**Tabel 1.** Perbandingan penelitian

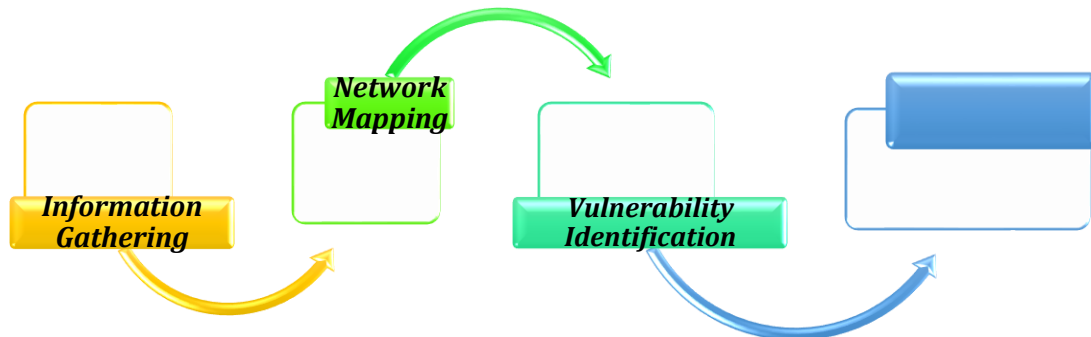
Aspek	Penelitian Poltekkes Kemenkes Sorong	Penelitian Serupa di Domain Pendidikan
<b>Metode Pengujian</b>	Dynamic Analysis & Static Analysis	Umumnya menggunakan Dynamic Analysis
<b>Jenis Celah Keamanan</b>	XSS, SQL Injection, CSRF, Security Misconfiguration	XSS, SQL Injection
<b>Pendekatan Mitigasi</b>	Kombinasi manual dan otomatis melalui CSP (Content Security Policy) dan WAF (Web Application Firewall)	Patch manual dan penggunaan framework yang lebih aman
<b>Automatisasi Keamanan</b>	Implementasi Intrusion Detection System (IDS) berbasis AI untuk mendeteksi pola serangan	IDS jarang digunakan atau hanya berbasis signature
<b>Keamanan Basis Data</b>	Input validation berbasis AI untuk mencegah SQLi	Query parameterized dan escaping input
<b>Keunggulan Implementasi</b>	Menyediakan pemantauan real-time dan penyesuaian kebijakan otomatis	Kebanyakan masih bergantung pada audit berkala

Inovasi dalam mitigasi keamanan makalah ini memberikan kontribusi yang khas dengan menyarankan sejumlah langkah kreatif untuk pertahanan yang lebih baik terhadap XSS dan SQLi, yaitu otomatisasi keamanan bertenaga AI. Penerapan sistem deteksi intrusi (IDS) yang didukung oleh kecerdasan buatan (AI) untuk mengidentifikasi pola serangan secara otomatis, log serangan dianalisis menggunakan pembelajaran mesin, yang memperbarui aturan secara dinamis. Peningkatan keamanan aplikasi website dengan membatasi akses ke situs eksternal, kebijakan keamanan konten (CSP) membantu menghentikan serangan XSS. WAF, atau firewall aplikasi web adaptif, mengubah aturannya sebagai respons terhadap ancaman baru. Perlindungan basis data yang disempurnakan validasi input yang didukung AI mendeteksi pola yang berbahaya sebelum pola tersebut memasuki basis data. Pemantauan kueri SQL secara real-time mendeteksi kegagalan dan mencegah injeksi SQL. Diharapkan dengan penelitian ini pengelola website akan memiliki visi akan langkah apa yang perlu diterapkan dalam meningkatkan keamanan website tersebut baik itu dari segi teknis, update kebijakan, serta penanaman kesadaran pengguna akan *cyber security*.

## 2. Metode Penelitian

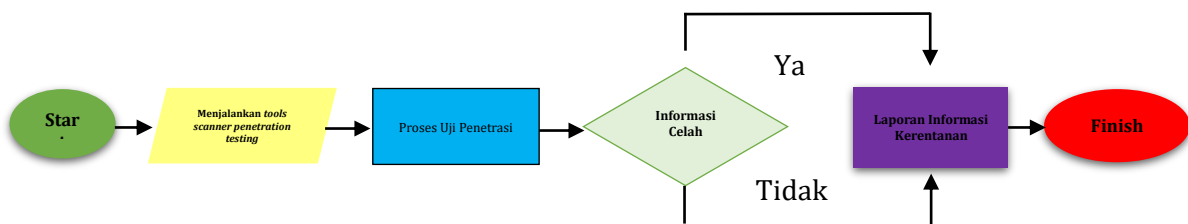
Pendekatan Pengujian Penetrasi digunakan dalam studi ini untuk mengidentifikasi kelemahan keamanan di situs web Poltekkes Kemenkes Sorong. Metode ini dilakukan dengan pendekatan Black Box Testing, di mana penguji tidak memiliki informasi internal tentang sistem sebelum pengujian dilakukan. Selain itu, dilakukan simulasi serangan dunia nyata untuk menguji seberapa besar dampak kerentanan terhadap sistem. Teknik pengujian yang digunakan dalam penelitian

ini yaitu *penetration testing* yang berfungsi untuk menganalisis celah keamanan website Poltekkes Kemenkes Sorong.



**Gambar 1.** Langkah-Langkah Metode Uji Penetrasi

Diagram alir ini menggambarkan bagaimana prosedur penelitian dilakukan secara metodis. Diagram alir ini memudahkan pelaksanaan berbagai prosedur uji penetrasi [18].



**Gambar 2.** Diagram Alir Pengujian Penetrasi

Diagram alir yang mengilustrasikan proses pengujian penetrasi disajikan dalam Gambar 2, diikuti dengan pengujian penetrasi yang dilakukan pada platform target.

**Tabel 2.** Langkah-Langkah Tahapan Penelitian

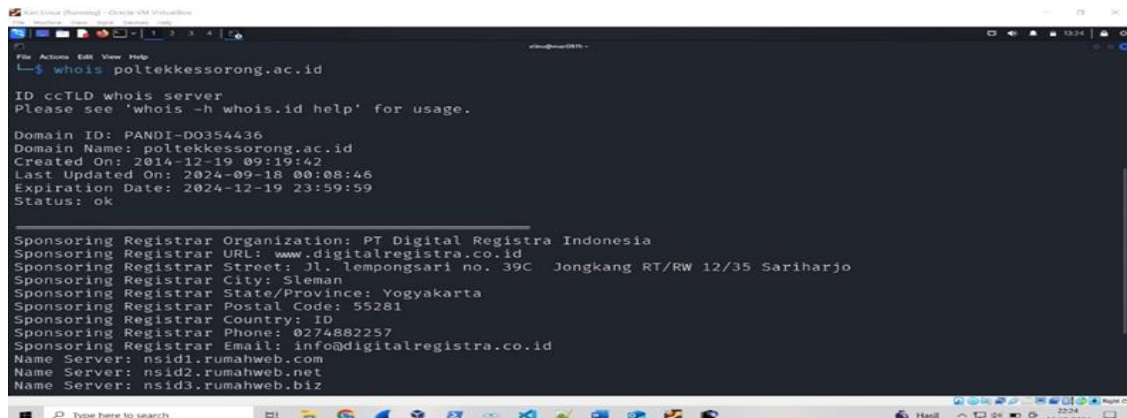
Nama Tahapan	Tools	Keterangan
<i>Information Gathering</i>	Whois	Mencari Informasi Website
<i>Network Mapping</i>	Nmap	Scan Port
<i>Vulnerability Identification</i>	Acunatix	Scan Kerentanan
<i>Vulnerability Assessment</i>	Owasp Zap	Mengidentifikasi Kerentanan

Penelitian ini dilakukan dalam beberapa tahap utama sesuai dengan framework Penetration Testing Execution Standard (PTES). Tahapan pengujian Sistem Informasi terdiri dari beberapa langkah, berikut ini adalah langkah-langkah yang dilakukan saat melakukan pengujian sistem informasi. Penjelasan tabel di atas adalah sebagai berikut [19].

1. Pengumpulan informasi, meliputi data umum tentang sistem informasi target, seperti email, informasi domain, dan alamat IP.
2. Pemetaan jaringan, proses yang digunakan untuk menentukan nama, jenis, dan versi port yang terbuka.

3. Identifikasi kerentanan, menemukan kelemahan atau kerentanan dalam sistem informasi target dikenal sebagai.
4. Penilaian kerentanan, proses menemukan, menilai, dan mengkategorikan kelemahan dalam perangkat keras, jaringan, dan sistem.

*Information Gathering* atau pengumpulan informasi, merupakan langkah yang dilakukan untuk mendapatkan informasi dan data dari target dalam rangka pengecekan website poltekkessorong.ac.id. Penelitian ini menggunakan whois tool untuk mendapatkan hasil penggalan data dan informasi, dan hasil pengumpulan informasi ditunjukkan pada gambar 3 [20].



```
whois poltekkessorong.ac.id

ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

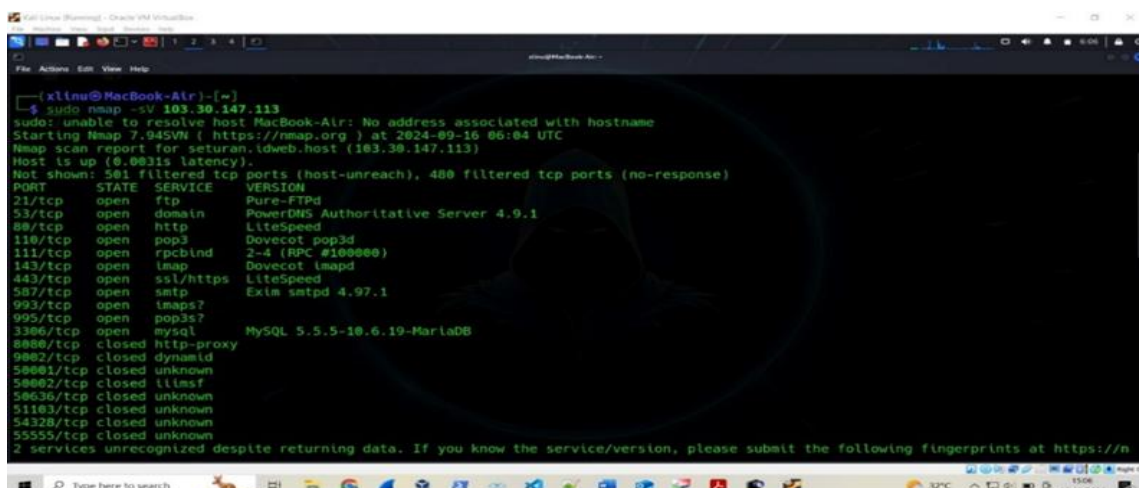
Domain ID: PANDI-DO354436
Domain Name: poltekkessorong.ac.id
Created On: 2014-12-19 09:19:42
Last Updated On: 2024-09-18 00:08:46
Expiration Date: 2024-12-19 23:59:59
Status: ok

Sponsoring Registrar Organization: PT Digital Registra Indonesia
Sponsoring Registrar URL: www.digitalregistra.co.id
Sponsoring Registrar Street: Jl. lempongsari no. 39C Jongkang RT/RW 12/35 Sariharjo
Sponsoring Registrar City: Sleman
Sponsoring Registrar State/Province: Yogyakarta
Sponsoring Registrar Postal Code: 55281
Sponsoring Registrar Phone: 0274882257
Sponsoring Registrar Email: info@digitalregistra.co.id
Name Server: nsid1.rumahweb.com
Name Server: nsid2.rumahweb.net
Name Server: nsid3.rumahweb.biz
```

Gambar 3. Information Gathering Whois

Dari hasil scanning menggunakan Whois terlihat beberapa informasi mengenai website potekkessorong.ac.id mulai dari waktu pembuatan domain, waktu kadaluarsa atau expired website poltekkessorong.ac.id, serta layanan web hosting yang digunakan.

*Network Mapping* atau Nmap adalah alat penejelajahan jaringan sumber terbuka. Alat ini memindai jaringan besar dengan cepat dan memberikan berbagai informasi. Tabel port bisa dibilang merupakan fitur Nmap yang paling berguna karena memberikan penghitungan port yang tersedia dan statusnya, apakah port tersebut terbuka, tertutup atau terlindungi (terfilter). Bersamaan dengan tabel port, Nmap menyediakan informasi DNS, perkiraan sistem operasi dan alamat MAC dll. Gunakan alat Nmap v.7.9 untuk melakukan *footprinting* menggunakan objek domain poltekkessorong.ac.id, ip yang di gunakan adalah 103.30.147.113 dengan menuliskan perintah `sudo nmap -sV 103.30.147.113` ditunjukkan pada gambar 4.



```
xlinu@MacBook-Air:~$ sudo nmap -sV 103.30.147.113
sudo: unable to resolve host MacBook-Air: No address associated with hostname
Starting Nmap 7.94SV ( https://nmap.org ) at 2024-09-18 06:04 UTC
Nmap scan report for seturan.idweb.host (103.30.147.113)
Host is up (0.0031s latency).
Not shown: 501 filtered tcp ports (host-unreach), 400 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Pure-FTPd
53/tcp    open  domain         PowerDNS Authoritative Server 4.9.1
80/tcp    open  http           LiteSpeed
110/tcp   open  pop3           Dovecot pop3d
111/tcp   open  rpcbind        2-4 (RPC #100000)
143/tcp   open  imap           Dovecot imapd
443/tcp   open  ssl/https      LiteSpeed
587/tcp   open  smtp           Exim smtpd 4.97.1
993/tcp   open  lmtps?
995/tcp   open  pop3s?
3306/tcp  open  mysql          MySQL 5.5.5-10.6.19-MariaDB
8080/tcp  closed http-proxy
9002/tcp  closed dynamid
50001/tcp closed unknown
50002/tcp closed llimsf
50636/tcp closed unknown
51163/tcp closed unknown
54328/tcp closed unknown
55555/tcp closed unknown
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://n
```

Gambar 4. Proses Pengujian Port Dengan Network Mapping

### 3. Hasil

Dari hasil *footprinting* berikut ini adalah ringkasan informasi yang dikumpulkan setelah pemindaian Nmap. 103.30.147.113 adalah alamat IP yang digunakan poltekkessorong.ac.id. Berikut ini adalah ikhtisar sejumlah port terbuka di situs web poltekkessorong.ac.id [21].

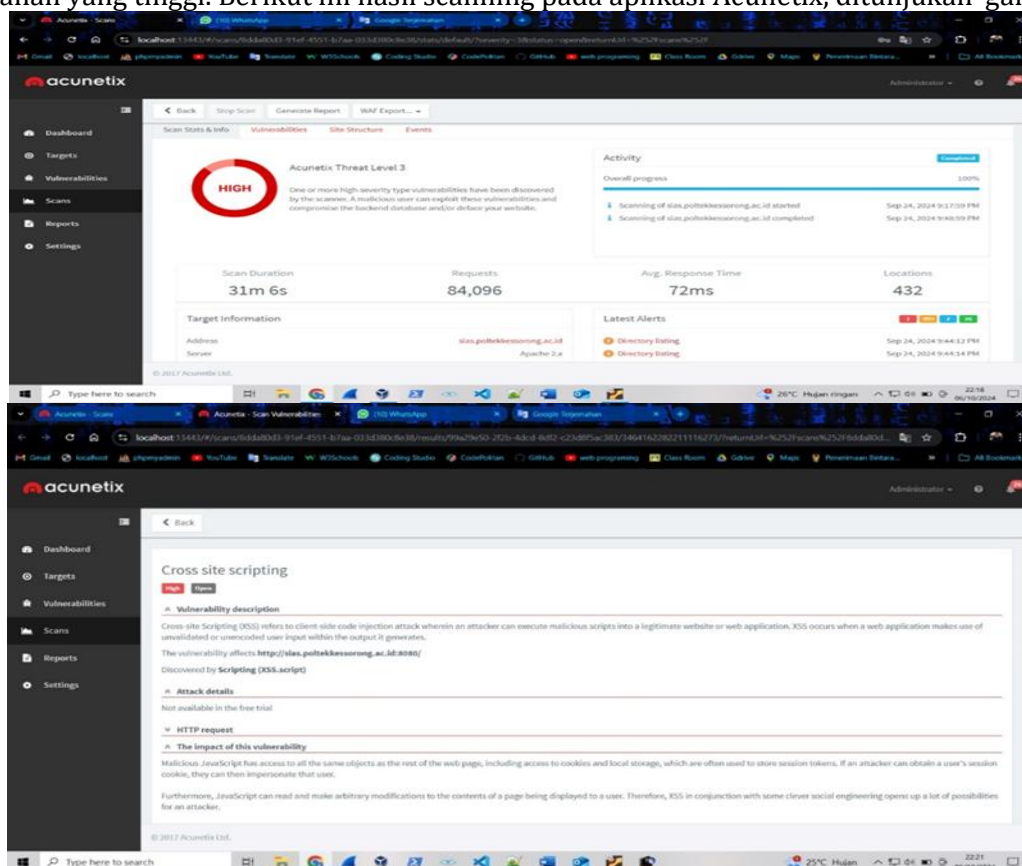
**Tabel 3.** Hasil *footprinting* informasi Port yang terbuka

No	Port	Protokol	Status	Service	Keterangan
1	21	tcp	open	ftp	FTP adalah <i>File Transfer Protocol</i> , yaitu protocol atau metode untuk mentransfer file antar komputer melalui jaringan internet.
2	53	tcp	open	domain	Domain pada port 53 adalah nama domain yang diubah menjadi alamat IP numerik oleh protokol DNS ( <i>Domain Name System</i> ), yang digunakan untuk komunikasi antara klien dan server DNS.
3	80	tcp	open	http	HTTP pada port 80 adalah <i>protokol Situs web diakses melalui Hypertext Transfer Protocol (HTTP)</i> . web secara default, merupakan gerbang komunikasi untuk permintaan dan respons HTTP antara server dan komputer klien.
4	110	tcp	open	pop3	POP3 pada port 110 adalah protokol yang digunakan untuk mengakses email secara tak terenkripsi.
5	111	tcp	open	rpcbind	RPCbind ( <i>Remote Procedure Call Bind</i> ) adalah layanan yang berjalan pada port 111 dan berfungsi untuk menetapkan alamat Internet sebagai program yang berjalan di komputer jarak jauh.
6	143	tcp	open	imap	IMAP ( <i>Internet Message Access Protocol</i> ) pada port 143 adalah protokol email yang digunakan untuk mengakses email yang disimpan di server tanpa enkripsi.
7	443	tcp	open	ssl/https	Port 443 ssl/https adalah port jaringan khusus yang digunakan untuk layanan <i>Hypertext Transfer Protocol Secure</i> , atau HTTPS. Data yang dikirim antara browser dan server dienkripsi menggunakan HTTPS, varian HTTP yang aman. Data tidak dapat diakses dengan mudah oleh orang yang tidak berwenang saat port 443 digunakan.
8	587	tcp	open	smtp	SMTP pada port 587 adalah protokol standar untuk mengirim dan menerima email secara terenkripsi menggunakan SMTP Secure (SMTPS).

*Acunetix* adalah alat pengujian keamanan aplikasi web otomatis yang mengaudit aplikasi web anda dengan memeriksa kerentanan seperti *SQL Injection*, *cross-site scripting*, dan kerentanan serupa yang dapat dieksploitasi. Babak pengujian ini dilakukan scanning kerentanan website poltekkessorong.ac.id memakai aplikasi *Acunetix Vulnerability Scanner*[22]. Eksistensi hasil tes



kerentanan website di level 3 high yaitu menandakan bahwa target yang diuji mempunyai tingkat kerentanan yang tinggi. Berikut ini hasil scanning pada aplikasi Acunetix, ditunjukkan gambar 5.



Gambar 5. Pengujian Acunetix

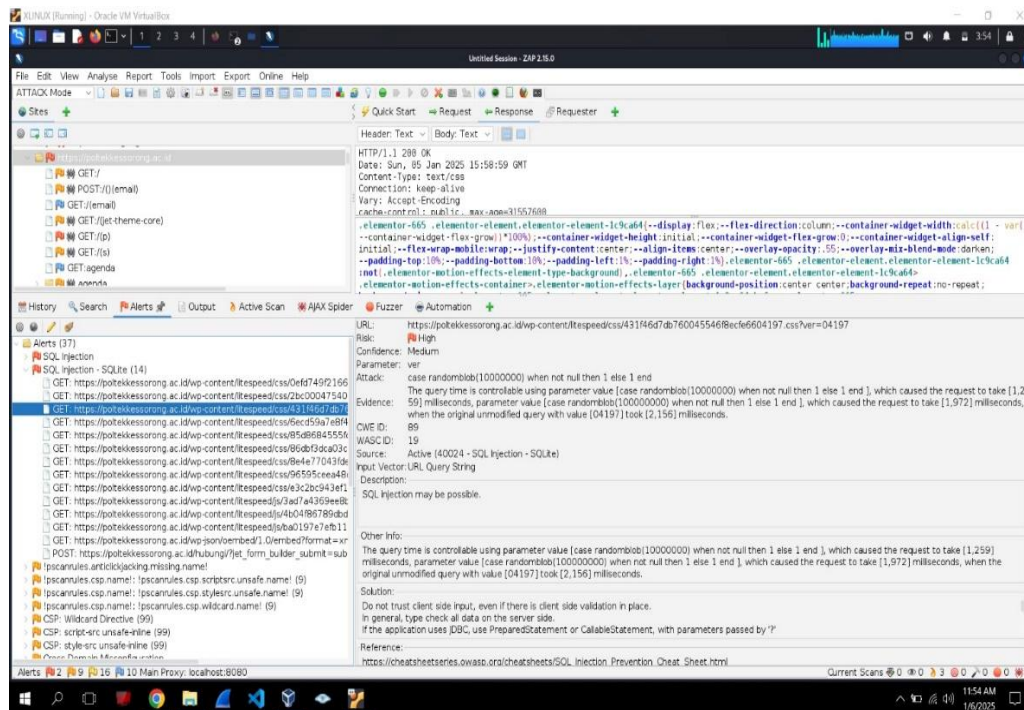
Skrip lintas situs, deskripsi kerentanan *Cross-site Scripting* (XSS) menunjukkan serangan penyuntikan kode sisi klien di mana penyerang dapat menjalankan skrip berbahaya di dalam situs web atau aplikasi web yang sah. XSS terjadi saat aplikasi web menggunakan input pengguna yang tidak divalidasi atau tidak dikodekan dalam output yang dihasilkannya. Kerentanan tersebut mempengaruhi `http://sias.poltekkessorong.ac.id:8080/` ditemukan oleh *scripting* (XSS, script).

Risikonya adalah JavaScript yang jahat akan mengakses semua objek yang sama seperti bagian halaman web lainnya, seperti cookie dan penyimpanan lokal, tempat token sesi disimpan. Ketika penyerang berhasil mendapatkan cookie sesi pengguna, mereka dapat menyamar sebagai pengguna tersebut. Selain itu, JavaScript dapat membaca dan melakukan perubahan sewenang-wenang pada konten halaman yang ditampilkan kepada pengguna. Jadi, penyerang dengan XSS dan sedikit kreativitas dengan sedikit rekayasa sosial dapat melakukan banyak hal.

Kerentanan ini termasuk dalam klasifikasi CWE-79, yang dalam bahasa Inggris dikenal sebagai Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) atau XSS. Berdasarkan skor CVSS versi 3.0, tingkat keparahan kerentanan ini berada pada level sedang dengan nilai 5.3. Vektor serangannya berasal dari jaringan, yang berarti eksploitasi dapat dilakukan dari jarak jauh tanpa akses fisik. Kompleksitas serangannya tergolong rendah, tidak memerlukan hak istimewa apa pun, serta tidak membutuhkan interaksi dari pengguna untuk dapat dieksploitasi. Cakupan dari dampaknya tidak berubah, artinya pengaruhnya tetap terbatas pada komponen yang sama. Dalam hal dampak, kerentanan ini tidak memengaruhi kerahasiaan data, namun dapat menyebabkan gangguan pada integritas, misalnya dengan menyisipkan konten yang tidak sah ke dalam halaman web. Ketersediaan sistem tidak terpengaruh secara langsung

oleh kerentanan ini. Meskipun tidak disediakan informasi rinci lainnya, kerentanan ini tetap perlu diperhatikan karena potensi manipulasi konten yang dapat menyesatkan pengguna.

Owasp zap adalah program yang membantu menemukan kelemahan keamanan dalam aplikasi web. Menurut situs web resmi owasp zap, owasp zap adalah komunitas terbuka yang mendorong pertumbuhan individu dan organisasi. Owasp Zap dapat diinstal pada berbagai sistem operasi, termasuk Windows, Linux, dan Mac OS, ditunjukkan pada gambar 6.



**Gambar 6.** Scanning menggunakan Owasp Zap

*Alerts* merupakan hasil dari proses *active scan*, *alerts* berisikan informasi tentang kerentanan yang pada *website* yang telah discan menggunakan *Owasp Zap*. Terdapat hasil 37 kerentanan yang terbaca pada *tab alerts*. Hasil menunjukkan bahwa terdapat kerentanan pada *website* poltekkessorong.ac.id 2 Tinggi, 9 Sedang, 16 Rendah dan 10 *Informational*, dengan nilai *Confidence* 1 Tinggi, 5 Sedang, 4 Rendah 22.

Tahapan *Vulnerability Assessment Owasp Zap* yaitu melakukan dokumentasi terkait kerentanan hasil analisis kerentanan yang dilakukan, dan memberikan rekomendasi untuk memperbaiki kerentanan pada *website* poltekkessorong.ac.id

**Tabel 4.** Hasil *Vulnerability Assessment Owasp Zap* poltekkessorong.ac.id

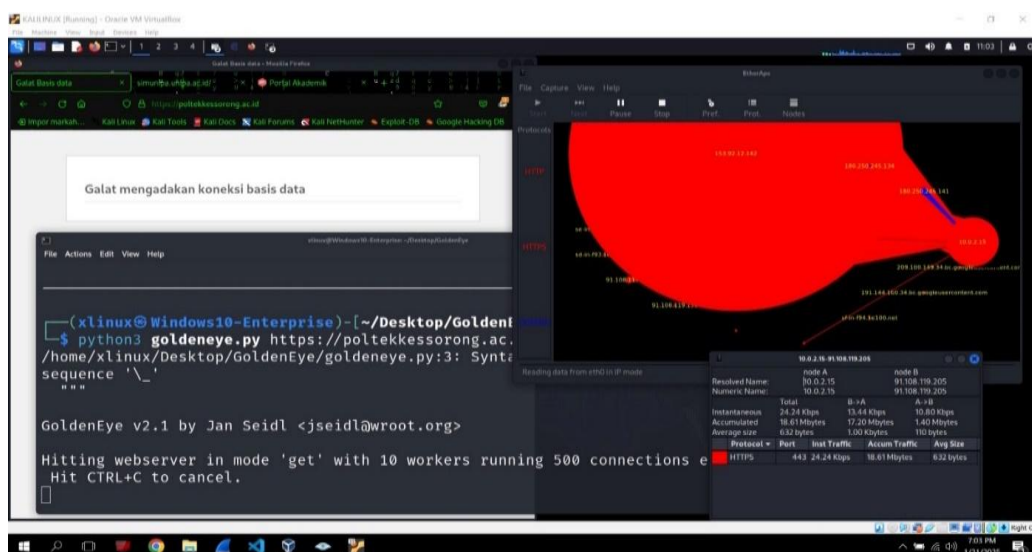
Type Alert	Kerentanan	Deskripsi	Solusi
SQL Injection	High	SQL Injection bisa terjadi	Validasi sisi klien bukanlah cara untuk mengautentikasi input. Secara umum verifikasi jenis semua data (sisi server). Jika aplikasi Anda menggunakan JDBC, gunakan PreparedStatement atau CallableStatement, dengan parameter yang dimasukkan.

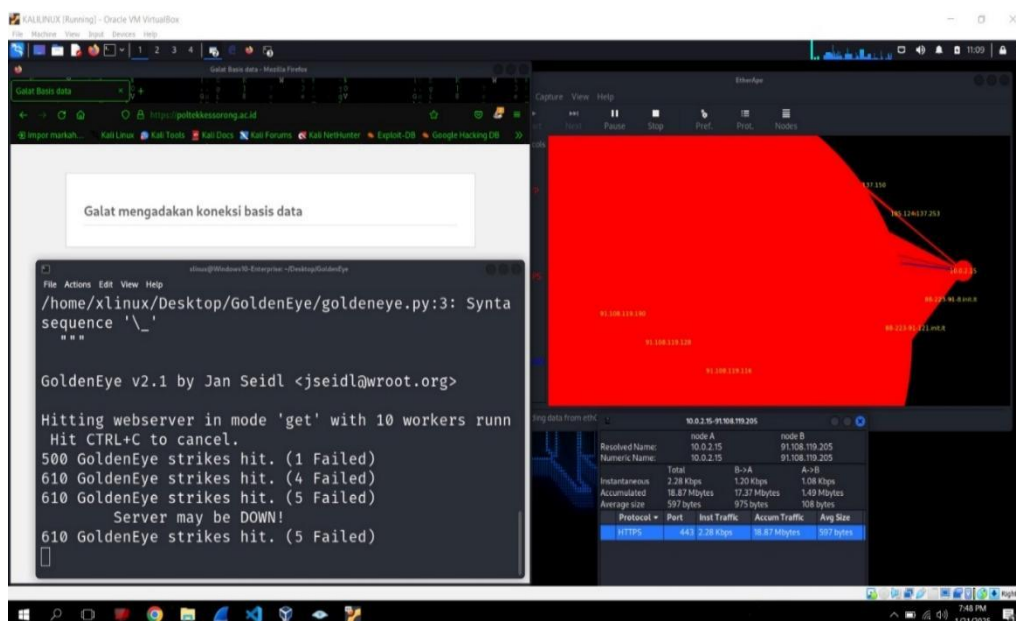


<i>CSP: Wildcard Directive</i>	<i>Medium</i>	Cross Site Scripting (XSS), dan penyuntikan data. Serangan ini digunakan untuk berbagai hal, mulai dari pencurian data hingga merusak situs atau penyebaran malware.	Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menetapkan header Content-Security-Policy dengan benar.
<i>Cross - Domain Misconfiguration</i>	<i>Medium</i>	Pemuatan data peramban web mungkin dapat terjadi, karena adanya kesalahan konfigurasi <i>Cross Origin Resource Sharing</i> (CORS) pada server web.	Jaga data sensitif agar tidak tersedia dengan cara yang tidak diautentikasi (misalnya menggunakan daftar putih alamat IP). Pindahkan header HTTP "Access-Control-Allow-Origin" ke rentang domain yang lebih terbatas, atau hapus semua header CORS secara bersamaan, Opsi terakhir didukung oleh header HTTP modern termasuk header Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya aktif di setiap halaman web yang dikembalikan dari situs/aplikasi Anda.
<i>Missing Anti-clickjacking Header</i>	<i>Medium</i>	Respons tersebut tidak melindungi dari serangan <i>ClickJacking</i> . Respons tersebut harus memiliki Content-Security-Policy dengan direktif <i>frame-ancestors</i> atau direktif <i>X-Frame-Options</i> .	
<i>Big Redirect Detected</i> (Potensi Kebocoran Informasi Sensitif)	<i>Low</i>	Server ini telah mengirimkan pengalihan yang entah bagaimana jelas menghasilkan respons yang sangat besar. Ini mungkin berarti server mengeluarkan pengalihan dan, pada saat yang sama, mengembalikan konten isi (yang dapat berupa informasi sensitif, PII, dan sebagainya.).	Jika pengecualian ini muncul saat pengalihan, pastikan tidak ada konten sensitif yang bocor melalui respons pengalihan. Respons pengalihan tersebut harus berisi sangat sedikit data.
<i>Cookie without Same Site Attribute</i>	<i>Low</i>	Dengan demikian, cookie dikirim tanpa atribut <i>SameSite</i> , yang memungkinkan cookie dikirim sebagai bagian dari permintaan 'lintas situs. Atribut <i>SameSite</i> merupakan tindakan pencegahan yang efektif terhadap pemalsuan permintaan lintas	Tetapkan atribut situs yang sama (sebaiknya ketat) di semua cookie.

<p><i>Strict-Transport-Security Header Not Set</i></p>	<p><i>Low</i></p>	<p>domain, skrip lintas situs, atau serangan pengaturan waktu. HTTP Strict Transport Security (HSTS) adalah mekanisme kebijakan keamanan server web yang memungkinkan server web menyatakan bahwa agen pengguna yang patuh (seperti browser web) dapat berinteraksi dengannya dengan cara yang aman hanya menggunakan HTTPS, HTTP aman melalui TLS/SSL.</p>	<p>Sebaiknya pastikan server web, server aplikasi, penyeimbang beban, dan sebagainya. dikonfigurasi untuk mematuhi Keamanan Transportasi Ketat juga.</p>
<p><i>Information Disclosure Suspicious Comments</i></p>	<p><i>Informational</i></p>	<p>Respons tersebut tampaknya memiliki pujian mencurigakan yang dapat memberikan bantuan kepada penyerang. Kiat, Jika Anda melakukan pencocokan dalam blok skrip (atau berkas), maka pencocokan tersebut akan dilakukan terhadap seluruh skrip, bukan hanya komentar.</p>	<p>Hilangkan komentar apa pun yang dapat mengembalikan informasi yang dapat membantu penyerang dan mengatasi akar penyebab yang ditunjukknya.</p>

Uji serangan yang akan dilakukan pada website poltekkessorong.ac.id adalah serangan *Distributed Denial Of Service* atau DDOS, *tools* yang akan digunakan *GoldenEye* kali linux, ditunjukkan pada gambar 7.





Gambar 7. Serangan DDoS attack menggunakan GoldenEye

Dari hasil serangan *DDos attack*, *Distributed Denial Of Service* pada website poltekkessorong.ac.id, serangan *GoldenEye* berhasil membanjiri website poltekkessorong.ac.id, dengan lalu lintas yang tidak sah, sehingga server kewalahan dan tidak dapat mengatur seluruh lalu lintas dan menyebabkan situs web menjadi lambat bahkan tidak dapat diakses menyebabkan *server down* pada website poltekkessorong.ac.id. Seperti yang terlihat pada gambar 7 diatas hasil uji serangan *DDoS attack*.

#### 4. Pembahasan

Dengan menggunakan pendekatan pengujian penetrasi, penelitian ini menguji keamanan situs website Poltekkes Kemenkes Sorong. Pengujian difokuskan pada beberapa area utama, termasuk injeksi SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dan pengaturan keamanan server.

Hasil penelitian menunjukkan bahwa pada tahap scanning kerentanan Website pada target poltekkessorong.ac.id yang dilakukan dengan aplikasi Acunetix Web Vulnerability Scanner, hasil pengujian website level 3 high dengan menggunakan aplikasi Acunetix Web Vulnerability Scanner, diperoleh hasil pengujian kerentanan website pada level 3 High bahwa target yang sedang diperiksa memiliki tingkat kerentanan yang tinggi. Deskripsi kerentanan Cross-site Scripting atau XSS adalah serangan injeksi kode sisi klien di mana penyerang dapat mengeksekusi skrip berbahaya ke situs web atau aplikasi web yang sah. Bergantung pada jenis serangan, aplikasi dapat mengalami cross-site scripting (XSS) saat menyertakan input pengguna yang tidak divalidasi atau tidak dikodekan dalam output yang dihasilkannya ke browser web.. Kerentanan tersebut menyerang <http://sias.poltekkessorong.ac.id:8080/> yang ditemukan oleh Scripting atau XSS.script atau gambaran lebih lengkap kerentanan ditunjukan pada Gambar 3. Dampaknya, JavaScript berbahaya memiliki akses ke semua objek yang sama seperti bagian lain dari halaman web, seperti cookie, dan penyimpanan lokal atau tempat umum, tempat cookie disimpan untuk sesi. Jika penyerang mencuri cookie sesi pengguna, mereka akan dapat masuk sebagai pengguna tersebut. Selain itu, JavaScript dapat membaca dan membuat perubahan sewenang-wenang pada apa yang dilihat pengguna di halamannya.. Oleh karena itu, XSS yang dipadukan dengan beberapa rekayasa sosial yang cerdas merupakan even sempurna bagi penyerang.

Dari hasil penelitian yang telah dilakukan pada tahap scanning kerentanan Website pada target poltekkessorong.ac.id dengan menggunakan aplikasi Owasap Zap *Vulnerability Assessment*, memberikan hasil 37 alerts, 2 diantaranya memiliki kerentanan yang tinggi (*high risk*). Hasil dari kerentanan website poltekkessorong.ac.id memiliki SQL Injection yang tinggi, sehingga website poltekkessorong.ac.id tidak aman digunakan untuk menyimpan data penting. Resiko kerentanan website poltekkessorong. Pada tahap terakhir dari tahap dokumentasi risiko dengan rincian deskripsi kerentanan dan penanganan apa yang dapat dilakukan untuk menutup kerentanan yang tepat pada situs web poltekkessorong.ac.id.

Pemanfaatan Kerentanan Untuk menilai dampak kelemahan keamanan pada sistem, simulasi serangan di dunia nyata dilakukan, seperti, *SQL Injection* (SQLi), Menentukan apakah input dapat digunakan untuk mengakses database secara ilegal. *Cross-Site Scripting* (XSS), Menguji kemungkinan serangan skrip yang berbahaya. *Cross-Site Request Forgery* (CSRF), Menentukan kerentanan aplikasi terhadap eksploitasi sesi pengguna. *Broken Authentication & Session Management*, Mengevaluasi kelemahan autentikasi pengguna. *Security Misconfiguration*, Mengidentifikasi kelemahan keamanan server atau aplikasi.

Analisis dampak dan dokumentasi, Menilai tingkat risiko menggunakan skala CVSS (*Common Vulnerability Scoring System*). Mengevaluasi dampak serangan terhadap integritas, ketersediaan, dan kerahasiaan data. Membuat laporan hasil pengujian dan rekomendasi perbaikan. Berikut temuan utama dari pengujian keamanan yang dilakukan adalah, SQL Injection, Data sensitif dapat diakses melalui eksploitasi kueri basis data tanpa perlindungan yang memadai. Cross-Site Scripting (XSS), Parameter dalam URL dan input formulir tidak memiliki validasi yang memadai, yang memungkinkan skrip berbahaya untuk disisipkan. Serangan Stored XSS ditemukan dalam fitur komentar yang menyimpan input tanpa penyaringan yang tepat. Cross-Site Request Forgery (CSRF), Tidak ada implementasi token CSRF pada titik akhir yang mengubah data penting, yang memungkinkan penyerang untuk membuat perubahan tanpa autentikasi tambahan. Konfigurasi Keamanan Server, Server tidak memiliki header keamanan yang lengkap, seperti Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), dan X-Frame-Options. Ada informasi sensitif yang dapat diekstraksi dari respons server, seperti versi PHP yang digunakan.

## 5. Penutup

Website Poltekkes Kemenkes Sorong adalah media informasi dan layanan akademik yang sangat vital bagi mahasiswa, dosen dan staf dalam institusi. Untuk mengungkap potensi risiko kerentanan yang dapat membahayakan keamanan data dan kelangsungan layanan, penelitian ini dilakukan untuk memeriksa celah keamanan pada situs web menggunakan metode Penetration Testing. Melalui proses pengujian yang sistematis, beberapa deskripsi kerentanan ini mengacu pada serangan injeksi kode sisi klien, di mana penyerang dapat mengeksekusi skrip berbahaya ke situs web atau aplikasi web yang sah. XSS terjadi ketika aplikasi web menempatkan input pengguna di output tanpa validasi atau escape. Kerentanan tersebut mempengaruhi <http://sias.poltekkessorong.ac.id.8080/> ditemukan oleh scripting (XSS, script). Penemuan ini menunjukkan bahwa sistem keamanan website masih sangat lemah dalam melindungi data sensitif dan mencegah eksploitasi oleh orang yang tidak bertanggung jawab.

Untuk mengatasi kerentanan keamanan yang ditemukan, rekomendasi teknis yang dapat diterapkan, gunakan *prepared statements* atau ORM (*Object-Relational Mapping*) untuk menghindari *SQL Injection*. Terapkan validasi input berbasis konteks, misalnya validasi karakter yang diperbolehkan dalam setiap *input field*, gunakan *Content Security Policy* (CSP) untuk mencegah serangan XSS dengan membatasi sumber daya eksternal yang dapat dijalankan dalam halaman website. Perlindungan Terhadap CSRF, gunakan CSRF token yang unik untuk setiap sesi dan setiap permintaan yang memodifikasi data. Terapkan *SameSite Cookie Attribute* untuk

membatasi akses terhadap cookie sesi dari domain yang berbeda. Peningkatan Keamanan pada Level Server, konfigurasi HTTP *Security Headers* seperti, *Strict-Transport-Security* untuk memaksa penggunaan HTTPS, *X-Frame-Options*, DENY untuk mencegah *clickjacking*, *X-XSS-Protection*, *mode block* untuk menangkal serangan XSS. Sembunyikan informasi server dengan menonaktifkan banner server dan PHP *version exposure*. Peningkatan *logging* dan *monitoring* implementasikan *Intrusion Detection System* (IDS) untuk mendeteksi serangan secara real-time. Gunakan SIEM (*Security Information and Event Management*) untuk analisis log dan peringatan dini terhadap anomali dalam sistem. Lakukan audit keamanan secara berkala untuk memastikan sistem tetap aman dari ancaman baru. Pengembangan solusi keamanan otomatis implementasi sebagai solusi keamanan berbasis API yang dapat terintegrasi dengan sistem website untuk mendeteksi dan menangani ancaman secara real-time. Pendekatan proaktif meningkatkan kesadaran keamanan dengan pelatihan rutin bagi staf pengelola website agar lebih waspada terhadap ancaman siber. Penerapan *Best Practices* Keamanan, memperketat kontrol akses, memperbarui sistem secara berkala, serta mengadopsi standar keamanan terbaru untuk mengurangi risiko eksploitasi. *Monitoring* dan evaluasi Berkelanjutan Menggunakan sistem pemantauan otomatis untuk mendeteksi anomali serta melakukan pengujian keamanan berkala guna memastikan sistem tetap terlindungi. Pendekatan yang berkelanjutan dan terintegrasi sangat diperlukan untuk menjaga keamanan website dari ancaman yang terus berkembang.

Kontribusi penelitian, penelitian ini diharapkan dapat memberikan pemahaman mengenai potensi ancaman yang mengintai website Poltekkes Kemenkes Sorong. Banyak jenis serangan yang dapat dilakukan oleh peretas, serangan yang sering dilakukan seperti, DDoS, XSS, dan juga Injeksi SQL. Semua serangan ini merupakan serangan terkenal di seluruh dunia, dan banyak digunakan oleh peretas. Rekomendasi yang ditawarkan diharapkan dapat membantu menyebarkan informasi tentang bagaimana meningkatkan performa dan keamanan website. Selain itu, penelitian ini diharapkan dapat membantu memperkuat kesadaran pengelola sistem tentang pentingnya monitoring dan evaluasi berkala terhadap keamanan sistem yang digunakannya.

## Referensi

- [1] A. Alanda, D. Satria, M. I. Ardhana, A. A. Dahlan, and H. A. Mooduto, "Web application penetration testing using sql injection attack," *International Journal on Informatics Visualization*, vol. 5, no. 3, pp. 320–326, 2021, doi: 10.30630/ijov.5.3.470.
- [2] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," *IEEE Access*, vol. 10, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.
- [3] M. Aurangzeb *et al.*, "Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage," *Energy Reports*, vol. 11, no. August 2023, pp. 2493–2515, 2024, doi: 10.1016/j.egyr.2024.02.010.
- [4] M. H. Romadhon and Y. Yudhistira, "Sistem Informasi Rental Mobil Berbasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri," vol. 2, no. 1, pp. 30–36, 2021.
- [5] A. Kusumaningrum, H. Wijayanto, and B. D. Raharja, "Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis ( MCDA )," no. 1, pp. 69–78, 2022.



- [6] L. Kestina and G. W. Nurcahyo, "Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability ( Studi Kasus di Bkpsdmd Kabupaten Kerinci )," vol. 3, pp. 9192-9203, 2023.
- [7] A. Bastian, H. Sujadi, and L. Abror, "ANALISIS KEAMANAN APLIKASI DATA POKOK PENDIDIKAN ( DAPODIK ) MENGGUNAKAN PENETRATION TESTING DAN SQL INJECTION," pp. 65-70, 2017.
- [8] Andria, "Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux," *Generation Journal*, vol. 4, no. 2, pp. 69-76, 2020.
- [9] Fikriyadi, Ritzkal, and B. A. Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method," *Jurnal Mantik*, vol. 4, no. 3, pp. 1658-1662, 2020.
- [10] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Algoritma*, vol. 18, no. 1, pp. 77-86, 2021, doi: 10.33364/algoritma/v.18-1.827.
- [11] Y. A. Pohan, Yuhandri Yunus, and Sumijan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *Jurnal Sistim Informasi dan Teknologi*, vol. 3, pp. 1-6, 2021, doi: 10.37034/jsisfotek.v3i1.36.
- [12] H. Alfidzar and B. Parga Zen, "Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna Mendeteksi Serangan DOS Pada Server," *Journal of Informatics, Information System, Software Engineering and Applications*, vol. 4, no. 2, pp. 32-045, 2022.
- [13] F. Setyawan, Rasyidah, and H. Amnur, "Keamanan Jaringan Wireless Dengan Kali Linux," *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no. 1, pp. 16-22, 2022, doi: 10.30630/jitsi.3.1.57.
- [14] A. Wahid, I. Juliady, S. G. Zain, and J. M. Parenreng, "Secure Wireless Sensor Network using Cryptography for Smart Farming Systems," *Internet of Things and Artificial Intelligence Journal*, vol. 2, no. 4, pp. 248-262, 2022, doi: 10.31763/iota.v2i4.554.
- [15] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)*, vol. 6, no. 2, p. 210, 2021, doi: 10.30998/string.v6i2.11477.
- [16] L. A. Nugraha, I. A. Kautsar, and A. S. Fitriani, "SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web," *Smatika Jurnal*, vol. 14, no. 01, pp. 111-123, 2024, doi: 10.32664/smatika.v14i01.1224.
- [17] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service ( DDoS ) menggunakan Metode Data Mining Naïve Bayes," vol. 6, no. 1, pp. 172-180, 2022.
- [18] U. Kristen Satya Wacana Salatiga, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack Artikel Ilmiah Program Studi Teknik Informatika Fakultas Teknologi Informasi," no. 672010194, 2016.
- [19] S. Andriyani, M. F. Sidiq, and B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," *Journal Informatic and Information Technology*, vol. 8798, pp. 1-13, 2023.
- [20] Firda Nurelia Syah Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui

Kali Linux,” *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, vol. 7, no. 1, pp. 52–59, 2023.

- [21] A. M. Akmal, N. Heryana, and Arip Solehudin, “Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment,” *Jurnal Pendidikan dan Konseling*, vol. 4, no. 4, pp. 6298–6309, 2022.
- [22] S. Eko Prasetyo and N. Hassanah, “Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf,” *Jurnal Ilmiah Informatika*, vol. 9, no. 02, pp. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.