Jurnal Bumigora Information Technology (BITe)
Vol. 7, No. 1, Juni 2025, Hal. 25∼38
E-ISSN: 2685-4066, DOI: 10.30812/bite/v7i1.5032

Analisis Keamanan Website Perguruan Tinggi di Nusa Tenggara Barat terhadap Serangan *SQL Injection*, *Cross Site Scripting*, dan *Insecure Direct Object Reference* melalui Pengujian Penetrasi

Security Analysis of University Websites in West Nusa Tenggara against SQL Injection, Cross Site Scripting, and Insecure Direct Object Reference Attacks through Penetration Testing

Dhira Wahyu Febrian*, **Raphael Bianco Huwae**, **Ahmad Zafrullah Mardiansyah**
Universitas Mataram, Mataram, Indonesia

Informasi Artikel:
Diterima: 20 Maret 2025, Direvisi: 31 Mei 2025, Disetujui: 2 Juni 2025

Abstrak-
Latar Belakang: Di era digital, keamanan siber merupakan aspek penting bagi perguruan tinggi dalam melindungi informasi akademik dan data pengguna. Fokus dari penelitian ini adalah mengidentifikasi dan menganalisis kerentanan keamanan pada *website* perguruan tinggi di Nusa Tenggara Barat terhadap tiga jenis serangan, yaitu SQL *Injection*, *Cross Site Scripting* (XSS), dan *Insecure Direct Object Reference* (IDOR), yang dapat membahayakan integritas data dan sistem informasi perguruan tinggi.
Tujuan: Tujuan penelitian ini adalah untuk mengevaluasi tingkat kerentanan dan tingkat keparahan risiko dari ketiga jenis serangan tersebut pada *website* institusi pendidikan tinggi.
Metode: Penelitian ini menggunakan **metode** pengujian penetrasi, serta melakukan penilaian tingkat keparahan kerentanan berdasarkan *Common Vulnerability Scoring Syste*m (CVSS) versi 3.1.
Hasil: Hasil penelitian ini adalah sebanyak 50% dari sepuluh *website* perguruan tinggi yang diuji rentan terhadap serangan XSS, 30% rentan terhadap SQL *Injection*, dan 20% rentan terhadap IDOR. Tingkat keparahan tertinggi terdapat pada kerentanan SQL *Injection* dengan skor CVSS 9.0 kategori kritikal.
Kesimpulan: Implikasi dari hasil penelitian ini menunjukkan bahwa institusi perguruan tinggi perlu segera memperkuat keamanan sistem dengan validasi input yang ketat, penerapan WAF, serta mekanisme otorisasi yang memadai untuk mencegah eksploitasi kerentanan serupa di masa mendatang.

Kata Kunci: Keamanan Siber, Keamanan Website, Penetrasi Testing, SQL Injection.

Abstract-
Background: *In the digital era, cybersecurity is important for universities in protecting academic information and user data. The focus of this research is to identify and analyze the security vulnerabilities of higher education websites in West Nusa Tenggara against three types of attacks, namely SQL Injection, Cross Site Scripting (XSS), and Insecure Direct Object Reference (IDOR), which can compromise the integrity of higher education data and information systems.*
Objective: *This research aims to evaluate the level of vulnerability and severity of the risk of the three types of attacks on the websites of higher education institutions.*
Methods: *This research uses penetration testing methods, and assesses the severity of vulnerabilities based on the Common Vulnerability Scoring System (CVSS) version 3.1.*
Result: *This research results show that 50% of the ten college websites tested are vulnerable to XSS attacks, 30% to SQL Injection, and 20% to IDOR. The highest severity was found in the SQL Injection vulnerability with a CVSS score of 9.0 critical category.*
Conclusion: *The implications of the results of this study indicate that higher education institutions need to immediately strengthen system security with strict input validation, WAF implementation, and adequate authorization mechanisms to prevent future exploitation of similar vulnerabilities.*

Keywords*: Cyber Security, Penetration Testing, SQL Injection, Web Security.*

How to Cite: D. W. Febrian, R. B. Huwae, & A. Z. Mardiansyah, "Analisis Keamanan Website Perguruan Tinggi di Nusa Tenggara Barat terhadap Serangan *SQL Injection*, *Cross Site Scripting*, dan *Insecure Direct Object Reference* melalui Pengujian Penetrasi," *Jurnal Bumigora Information Technology (BITe)*, vol. 7, no. 1, Jun 2025. doi: 10.30812/bite/v7i1.5032.

Penulis Korespondensi:

Dhira Wahyu Febrian,
PUniversitas Mataram, Mataram, Indonesia,
Email: dhiraxioo@gmail.com

1. PENDAHULUAN

Memasuki era digital, transformasi teknologi telah mengubah berbagai aspek kehidupan, salah satunya pada institusi perguruan tinggi. Perguruan tinggi kini tidak hanya berfungsi sebagai pusat pendidikan, tetapi juga menjadi sumber utama informasi digital yang dapat diakses di mana saja dan di kapan saja [1]. Digitalisasi layanan, seperti sistem informasi akademik dan *e-learning*, menjadikan *website* sebagai elemen utama dalam menyediakan informasi yang cepat, akurat, dan mudah diakses, serta mengelola seluruh proses pembelajaran, termasuk presensi dan penilaian tugas [2]. Seiring dengan meningkatnya penggunaan *website*, ancaman terhadap keamanan siber juga semakin berkembang. Sepanjang tahun 2020, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 9.749 serangan web *defacement*, yang menunjukkan tingginya risiko keamanan pada situs *website*, termasuk situs perguruan tinggi. Dari jumlah tersebut, 84 persen (8.205 insiden) terjadi pada halaman muka, sementara 16 persen (1.544 insiden) menyasar halaman tersembunyi atau sub-menu *website* [3]. Hal ini menegaskan pentingnya perhatian terhadap keamanan siber untuk melindungi integritas dan keandalan informasi digital di perguruan tinggi. Jenis Serangan siber yang paling banyak di laporkan menurut survei dari Badan Siber dan Sandi Negara (BSSN) yaitu SQL *Injection*, *Cross-Site Scripting* (XSS), Dan *Insecure Direct Object Reference* (IDOR), dengan total 128 serangan pada tahun 2021 [4]. Selain itu, lembaga riset siber *Communication & Information System Security Research Center* (CISSReC) mengungkapkan bahwa sebanyak 26 *website* kampus perguruan tinggi di Indonesia diretas dan disusupi perjudian *online* [5]. Termasuk *website* Universitas Mataram, yang untuk kesekian kalinya menjadi target peretasan *hacker* [6]. Kondisi ini menegaskan pentingnya pengujian penetrasi secara berkala untuk mengidentifikasi dan mengatasi kerentanan keamanan pada *website*, terutama dalam melindungi data dan reputasi institusi perguruan tinggi.

Tinjauan pustaka menunjukkan berbagai penelitian terdahulu yang berfokus pada keamanan website, seperti penelitian [7] berfokus pada pengujian penetrasi aplikasi *website* dengan menggunakan serangan SQL *injection* sebagai metode utama. Tujuan dari penelitian ini adalah untuk mengidentifikasi kerentanan keamanan di berbagai aplikasi *website* dan mengevaluasi sejauh mana aplikasi-aplikasi tersebut rentan terhadap serangan SQL *injection*, penelitian [8] menganalisis keamanan *website* pemerintah, khususnya terkait kerentanan yang disebabkan oleh serangan SQL XSS [9]. Untuk mengevaluasi pengujian penetrasi terhadap aplikasi *website* dan Penelitian ini juga menekankan bahwa pengujian dapat dilakukan secara manual maupun otomatis. Manual testing efektif dalam mendeteksi kerentanan kompleks yang tidak dapat diidentifikasi oleh alat otomatis contohnya seperti *Insecure Direct Object Reference* (IDOR), sedangkan automated testing menawarkan efisiensi waktu dan tenaga meskipun kurang akurat dibandingkan dengan metode manual [10] menggunakan metode PTES untuk pengujian penetrasi pada *website* elearning2.binadarma.ac.id, dan penelitian [11] menerapkan metode *black-box* untuk mengidentifikasi kerentanan tanpa akses ke informasi internal sistem. **Terdapat gap** atau kesenjangan yang belum diselesaikan oleh penelitian sebelumnya yaitu sebagian besar studi sebelumnya hanya fokus pada satu atau dua jenis kerentanan keamanan seperti SQL *Injection* atau XSS saja, tanpa mempertimbangkan kerentanan lain seperti IDOR yang sangat bergantung pada logika akses dan lebih sulit terdeteksi secara otomatis. Selain itu, sebagian besar penelitian dilakukan pada website pemerintah atau institusi non-pendidikan tinggi, sehingga belum ada pemetaan khusus mengenai kondisi keamanan siber pada *website* perguruan tinggi di wilayah NTB.

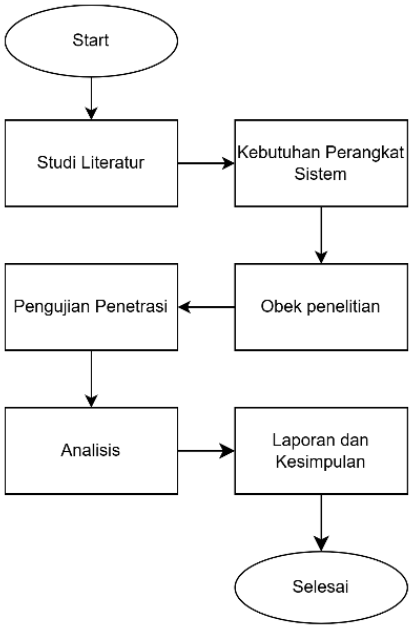
Penelitian ini memiliki **perbedaan signifikan** dibandingkan penelitian sebelumnya, yaitu dengan mengkaji secara bersamaan tiga jenis kerentanan utama SQL XSS, dan IDOR menggunakan pendekatan kombinasi antara

pengujian manual dan otomatis yang diterapkan secara sistematis pada sepuluh *website* perguruan tinggi di wilayah NTB. Selain itu, penelitian ini juga mengukur tingkat keparahan setiap kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS) versi 3.1 guna memberikan penilaian risiko yang lebih terukur. Berdasarkan berbagai studi terdahulu, sebagian besar penelitian hanya berfokus pada satu jenis kerentanan atau dilakukan pada instansi pemerintah dan sektor umum, sehingga penelitian ini mengisi celah tersebut dengan memberikan analisis menyeluruh di lingkungan perguruan tinggi, khususnya di wilayah Indonesia bagian timur, dan menjadi kontribusi baru dalam pemetaan keamanan siber pada sektor perguruan tinggi.

Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis tingkat kerentanan keamanan pada website perguruan tinggi di NTB terhadap tiga jenis serangan siber utama (SQL *Injection*, XSS, dan IDOR), serta menyusun rekomendasi teknis untuk mitigasi. Kontribusi utama penelitian ini adalah memberikan gambaran nyata mengenai kondisi keamanan siber pada institusi pendidikan tinggi di NTB yang belum pernah dibahas sebelumnya. Hasil penelitian ini diharapkan dapat menjadi rujukan bagi pengelola IT kampus untuk meningkatkan proteksi sistem informasi, serta **berkontribusi** pada pengembangan ilmu pengetahuan di bidang keamanan aplikasi *website* dan penetrasi sistem berbasis CVSS.

2. METODE PENELITIAN

Tahap ini membahas metode penelitian yang digunakan untuk melakukan pengujian penetrasi terhadap *website* perguruan tinggi di NTB. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan yang ada, khususnya terhadap serangan SQL XSS, dan IDOR. Berdasarkan Gambar 1, metode penelitian yang diterapkan dalam jurnal meliputi beberapa tahapan, yaitu studi literatur, kebutuhan perangkat sistem, pengujian penetrasi, analisis, serta penyusunan laporan hasil dan penarikan kesimpulan.



Gambar 1. Alur metode penelitian

2.1. Studi Literatur

Studi literatur dilakukan dengan meneliti berbagai jurnal, penelitian, dan literatur lain yang berkaitan dengan *vulnerability assessment* serta metode pengujian penetrasi dalam mengidentifikasi celah keamanan pada sistem. Kajian ini mencakup pemahaman mendalam mengenai berbagai jenis kerentanan yang umum ditemukan dalam aplikasi *website*, seperti SQL XSS, dan IDOR. SQL *Injection* adalah jenis serangan yang mengeksploitasi celah keamanan pada sistem basis data dengan menyisipkan perintah SQL berbahaya ke dalam input aplikasi

website, sehingga memungkinkan penyerang untuk membaca, mengubah, atau bahkan menghapus data sensitif dalam database [12]. Sementara itu, *Cross Site Scripting* (XSS) adalah serangan yang memungkinkan penyerang menyuntikkan skrip berbahaya ke dalam halaman *website* yang dikunjungi oleh pengguna lain, yang dapat digunakan untuk mencuri data pengguna [13]. Sedangkan IDOR adalah kerentanan yang terjadi ketika aplikasi *website* memberikan akses langsung ke objek tanpa otorisasi yang memadai, memungkinkan penyerang mengakses atau memodifikasi data milik pengguna lain dengan hanya mengubah parameter dalam URL atau permintaan API [14].

Dalam penelitian ini, berbagai alat digunakan untuk mengumpulkan informasi dan menguji keamanan *website* target seperti Wappalyzer, Nmap, Xray, SQLmap, Burpsuite, digunakan untuk mengidentifikasi teknologi yang digunakan oleh *website*, seperti framework, server, dan pustaka JavaScript yang dapat menjadi potensi titik serangan. Nmap berfungsi sebagai alat pemindaian jaringan guna mengidentifikasi *port* yang terbuka serta layanan yang berjalan di dalamnya, yang dapat memberikan gambaran awal mengenai kemungkinan eksploitasi. Selanjutnya, Xray digunakan sebagai alat pemindaian kerentanan untuk mendeteksi kelemahan keamanan yang mungkin terdapat pada *website* target. Untuk pengujian penetrasi, penelitian ini memanfaatkan SQLmap, yang secara otomatis mendeteksi dan mengeksploitasi kerentanan SQL *Injection*, serta Burp Suite, yang digunakan dalam analisis keamanan aplikasi *website*, termasuk memeriksa keamanan *input* serta mendeteksi serangan XSS dan IDOR.

2.2. Kebutuhan Perangkat Sistem

Pada tahap ini, kebutuhan perangkat sistem yang diperlukan untuk perangkat lunak perangkat lunak pengujian keamanan yang memerlukan sumber daya tinggi secara efisien dan tanpa gangguan dan Perangkat lunak yang digunakan dalam penelitian ini meliputi Kali Linux, VirtualBox, xray, SQLmap, Burp Suite, Wappalyzer, dan Nmap, yang digunakan untuk pengujian sistem.

2.3. Objek Penelitian

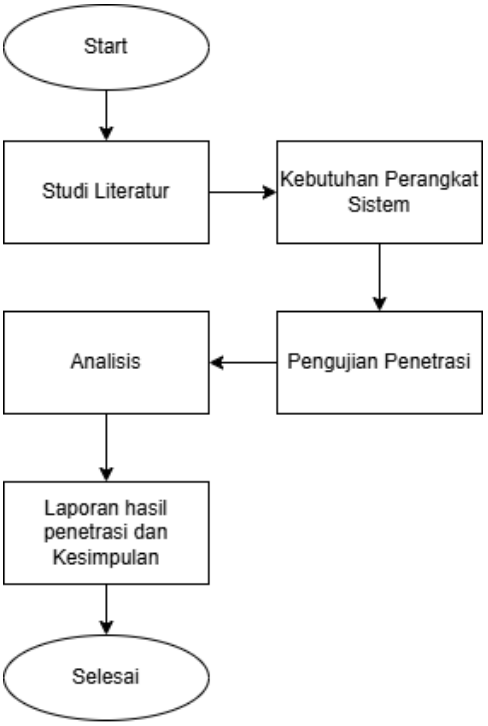
Penelitian ini melibatkan pengujian penetrasi terhadap website, yang menjadi objek penelitian yaitu perguruan tinggi yang ada di wilayah NTB. Pengujian dilakukan untuk menganalisis kerentanan sistem terhadap ancaman SQL XSS, dan IDOR. Berikut adalah daftar perguruan tinggi yang menjadi target penelitian pada Tabel 1.

Tabel 1. Objek penelitian

No	Perguruan Tinggi
1.	Universitas ABC
2.	Universitas DEF
3.	Universitas GHI
4.	Universitas JKL
5.	Universitas MNO
6.	Akademi ABC
7.	Universitas PQR
8.	Institut ABC
9.	Universitas STU

2.4. Pengujian Penetrasi

Pengujian penetrasi dilakukan untuk menganalisis kerentanan keamanan SQL XSS dan IDOR pada sistem *website* perguruan tinggi yang menjadi objek penelitian. Proses pengujian ini dirancang dengan beberapa tahapan yang saling terintegrasi, sebagaimana dijelaskan pada alur pengujian penetrasi pada Gambar 2. Pada Gambar 2, Pengintaian Sistem merupakan tahapan awal dalam pengujian penetrasi yang bertujuan untuk mengumpulkan informasi terkait *website* yang akan di uji. Pada proses ini melibatkan penggunaan *tool* wappalyzer untuk mengidentifikasi terkait teknologi yang digunakan oleh *website* perguruan tinggi yang menjadi target dan Nmap untuk pemindaian aktif terhadap server target guna mengidentifikasi *port* terbuka.



Gambar 2. Alur pengujian penetrasi

Pemindaian Kerentanan dilakukan dengan kombinasi metode otomatis dan manual untuk mendeteksi potensi kelemahan keamanan, seperti SQL XSS, dan IDOR. Pemindaian untuk SQL *Injection* dan *Cross Site Scripting* (XSS) dilakukan secara otomatis menggunakan *tools* seperti XRay dan Burp Suite, di mana XRay memindai berbagai *endpoint* dengan *payload* tertentu untuk mendeteksi respon kerentanan, sementara Burp Suite memanfaatkan fitur Burp *Scanner* untuk mengeksplorasi parameter dinamis serta menghasilkan laporan terstruktur. Pengujian kerentanan dilakukan untuk memvalidasi dan menganalisis risiko dari celah keamanan yang terdeteksi. Pengujian SQL *Injection* dilakukan menggunakan SQLmap, yang mengirimkan berbagai *payload* ke parameter rentan untuk mengeksploitasi query basis data, seperti mengambil data sensitif atau mengendalikan database. Untuk *Cross Site Scripting* (XSS), digunakan Burp Suite yang menyuntikkan script berbahaya ke elemen *input* rentan guna mengidentifikasi potensi eksekusi kode di sisi pengguna. Pengujian dilakukan secara sistematis pada setiap potensi kerentanan, dengan mendokumentasikan langkah eksploitasi, *payload*, dan hasil yang diperoleh untuk memastikan analisis mendalam serta rekomendasi perbaikan yang akurat.

Laporan Pengujian Kerentanan, data dari proses pemindaian kerentanan dan pengujian kerentanan dianalisis untuk menyusun laporan sebagai referensi tim IT perguruan tinggi dalam meningkatkan keamanan *website*. Data dikelompokkan berdasarkan jenis, sumber kerentanan, dan solusi mitigasi. Laporan disajikan dengan terminologi teknis yang mudah dipahami, mencakup hasil pengujian penetrasi dan penilaian keamanan sebagai panduan perbaikan bagi pengelola *website*.

2.5. Analisis

Pada tahap analisis, temuan terkait indikasi kerentanan yang sudah diuji akan dianalisis menggunakan kalkulator CVSS versi 3.1 untuk menilai tingkat keparahan, dampak, dan langkah mitigasi yang diperlukan. CVSS berfungsi sebagai kerangka kerja standar yang memungkinkan penilaian kuantitatif terhadap kerentanan keamanan, sehingga memudahkan organisasi dalam memprioritaskan penanganan kerentanan berdasarkan skor yang dihasilkan. Skor CVSS dihitung berdasarkan metrik dasar, temporal, dan lingkungan, yang mencakup faktor-faktor seperti kompleksitas serangan, dampak pada kerahasiaan, integritas, ketersediaan, serta lingkungan spesifik di mana kerentanan tersebut ditemukan [15]. Hasil akhirnya memberikan evaluasi tingkat kerentanan

keamanan *website* perguruan tinggi, yang dapat digunakan sebagai dasar untuk mengambil langkah-langkah mitigasi yang tepat.

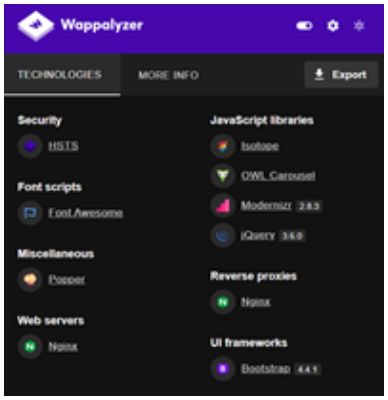
2.6. Laporan Pengujian Penetrasi dan Kesimpulan

Pada tahap terakhir yaitu laporan hasil penetrasi dan kesimpulan, *Output* yang dihasilkan berupa ringkasan kerentanan keamanan pada *website* perguruan tinggi, yang digunakan sebagai acuan untuk Tindakan perbaikan.

3. HASIL DAN PEMBAHASAN

3.1. Pengintaian Sistem

Pengintaian sistem dilakukan dengan menggunakan dua tools, yaitu wappalyzer dikenal lebih developer friendly dan dokumentatif digunakan untuk pengintaian secara pasif, yang memungkinkan identifikasi teknologi pada website, seperti framework, Content management System (CMS), bahasa pemrograman, dan server, tanpa memberikan beban tambahan pada server target. dan Nmap untuk pemindaian lebih dalam secara aktif terhadap server target guna mengidentifikasi port tebuka. Berdasarkan Gambar 3, hasil pengintaian menggunakan Wappalyzer menunjukkan teknologi yang digunakan pada website target, seperti HSTS untuk keamanan, server Nginx, serta berbagai library dan framework seperti Font Awesome, Isotope, OWL Carousel, Modernizr 2.8.3, jQuery 3.6.0, dan Bootstrap 4.4.1. Informasi ini menjadi dasar untuk analisis lebih lanjut pada tahap pemindaian dan pengujian kerentanan. Selanjutnya, berdasarkan Gambar 4, hasil pengintaian menggunakan Nmap menunjukkan top 10 port pada server target. Beberapa port terbuka yang teridentifikasi antara lain port 21 (FTP), 22 (SSH), 80 (HTTP), dan 443 (HTTPS), serta beberapa port yang berstatus filtered, yang menandakan perlindungan firewall. Data ini digunakan untuk menilai potensi celah keamanan yang dapat dieksploitasi pada tahap pengujian penetrasi selanjutnya.



Gambar 3. Pengintaian sistem *wappylyzer*

```
┌──(initiald㉿initialD)-[~]
└─$ nmap --top-ports 10  103.13.207.173
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 10:41 CST
Nmap scan report for ip103-13-207-173.cloudhost.web.id (103.13.207.173)
Host is up (0.021s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

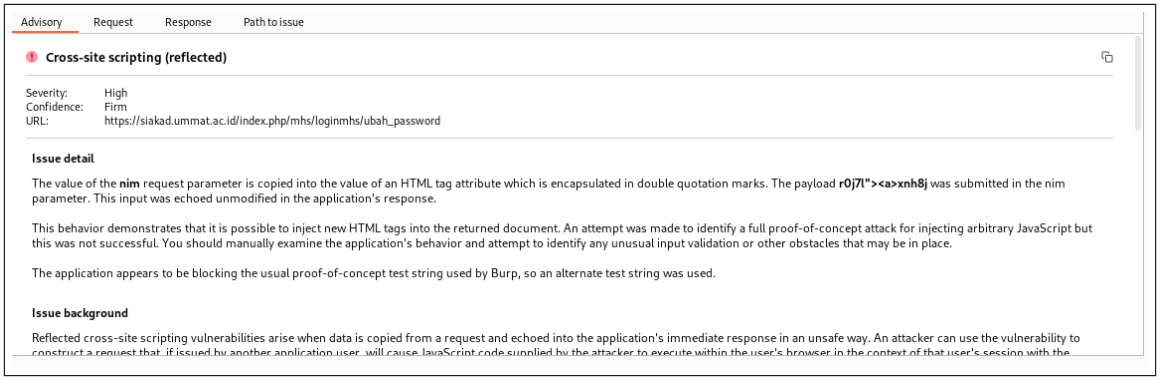
Gambar 4. Pengintaianp *Port* nmap

3.2. Pemindaian Kerentanan

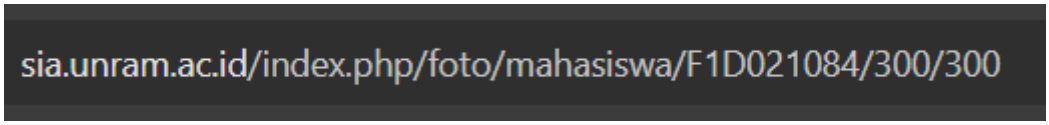
Pemindaian kerentanan dilakukan menggunakan Xray yang efektif untuk pemindaian endpoint API dan web modern untuk mendeteksi celah keamanan pada website perguruan tinggi, terutama kerentanan SQL *Injection* dan *Cross Site Scripting* (XSS). Sementara itu, pendekatan manual digunakan untuk mengidentifikasi kerentanan IDOR dengan memeriksa *endpoint* sensitif secara mendalam. Berdasarkan gambar 5. di atas, merupakan hasil dari pemindaian kerentanan SQL *injection* website menggunakan Xray, hasil pemindaian menunjukkan kerentanan SQL *Injection* pada *website* menggunakan Xray. *Tool* ini mendeteksi parameter injeksi pada URL, *payload* yang digunakan, serta data permintaan (*Request*) yang menunjukkan adanya celah keamanan dalam *input* parameter "kata" pada *endpoint* tersebut.

Gambar 5. Hasil pemindaian kerentanan sql *injection* xray

Gambar 6, hasil pemindaian menunjukkan kerentanan *Cross Site Scripting* (XSS) pada *website* menggunakan Burpsuite. Kerentanan ditemukan pada parameter "nim". Permintaan (*Request*) yang ditampilkan mengonfirmasi injeksi berhasil terhadap *input* parameter tersebut, yang memungkinkan eksekusi kode JavaScript di sisi *client*. Gambar 7 merupakan hasil dari pemindaian kerentanan *Insecure Direct Object Reference* (IDOR) secara manual. Pemindaian ini dilakukan dengan cara mengubah parameter ID yang terdapat dalam URL.



Gambar 6. Hasil pemindaian kerentanan *cross site scripting* (xss) burpsuite

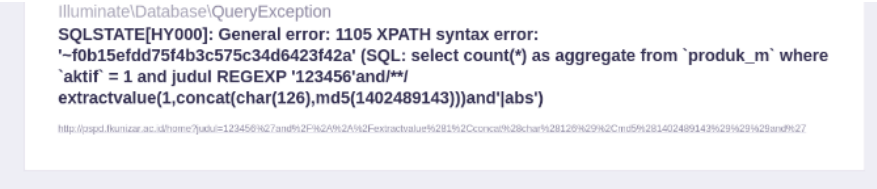


Gambar 7. Pemindaian manual *insecure direct object reference* (IDOR)

3.3. Pengujian Kerentanan

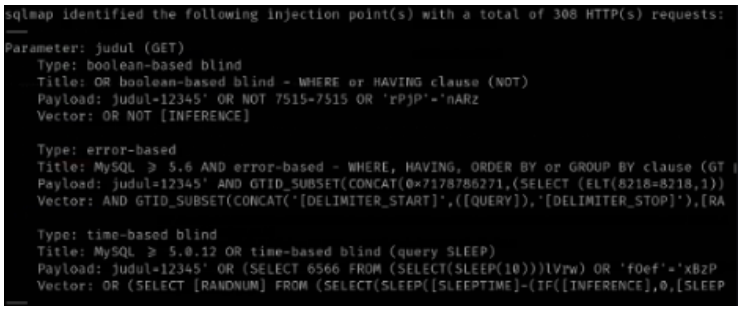
Pengujian kerentanan dilakukan setalah mendapatkan hasil dari pemindaian kerentanan. Pada tahap Pengujian SQL *Injection* dimulai dengan pengecekan *false positive*, dilanjutkan dengan SQLMap, hingga parameter terbukti injectable. Untuk *Cross Site Scripting* (XSS), *payload* disuntikkan melalui BurpSuite dan

divalidasi dengan eksekusi pada HTML. *Pada* IDOR, endpoint diuji dengan memanipulasi parameter ID untuk mengakses data tanpa otorisasi. Gambar 8, pengujian SQL *Injection* dengan cara manual untuk memeriksa apakah parameter rentan terhadap injeksi SQL atau hanya memberikan hasil *false positive*. Hasil menunjukkan adanya respons *error database* yang menandakan parameter memang rentan terhadap SQL *Injection*.

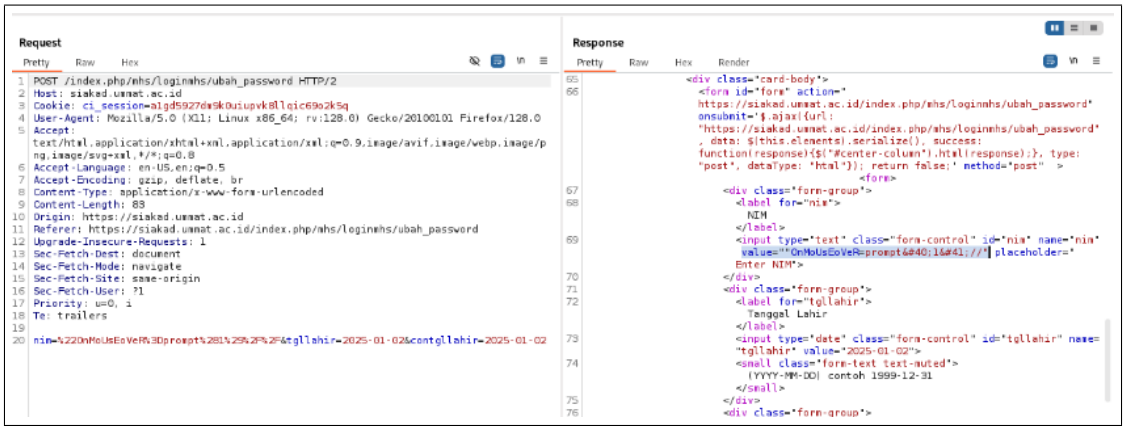


Gambar 8. Validasi kerentanan sql *injection*

Gambar 9, validasi menggunakan sqlmap ternyata benar bahwa parameter rentan terhadap SQL *Injection* melalui teknik *boolean-based*, *error-based*, dan *time-based blind*. *Payload* yang digunakan berhasil menunjukkan adanya kelemahan pada *endpoint* yang diuji, mengindikasikan potensi eksploitasi lebih lanjut terhadap sistem database. Berdasarkan pengujian pada Gambar 10, *payload* "on-mouseover" berhasil disuntikkan ke dalam elemen HTML pada *response* server. Hal ini mengindikasikan adanya potensi kerentanan *Cross Site Scripting* (XSS), yang memungkinkan penyerang untuk menyisipkan skrip berbahaya dan memanipulasi perilaku halaman *website*.

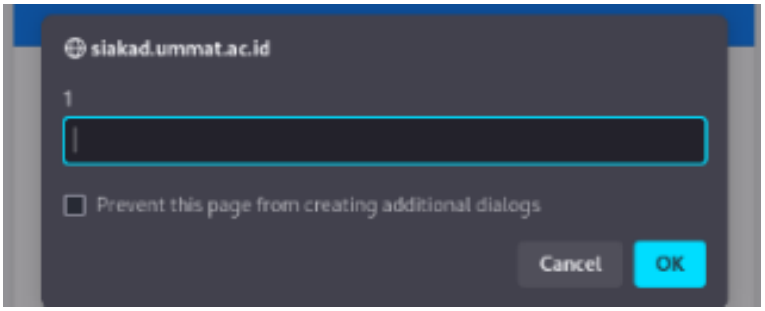


Gambar 9. Hasil pengujian sqlmap



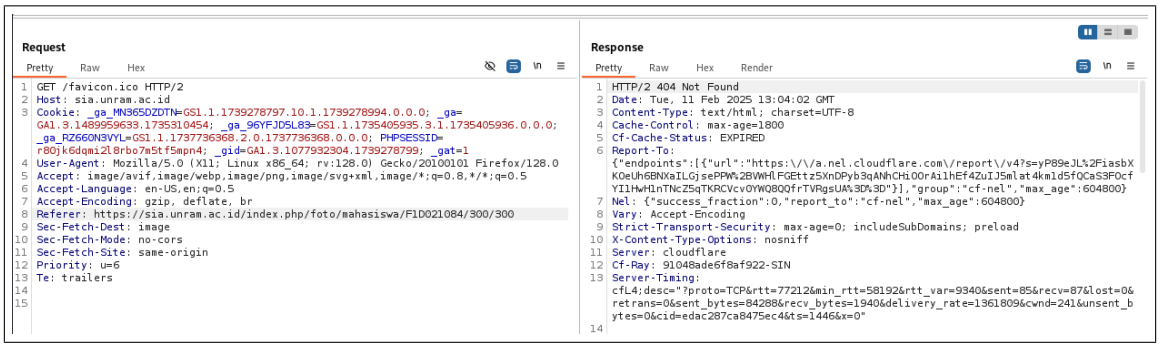
Gambar 10. *Payload cross site scripting* (XSS) tersuntik

Gambar 11, tampilan dialog yang muncul menunjukkan bahwa situs website telah berhasil dieksploitasi melalui kerentanan *Cross Site Scripting* (XSS). *Payload* yang disuntikkan berhasil dieksekusi di sisi *client*, menyebabkan munculnya jendela dialog (*alert box*). Hal ini mengonfirmasi bahwa *input* tidak divalidasi atau disanitasi dengan benar sebelum dimasukkan ke dalam halaman *website*.

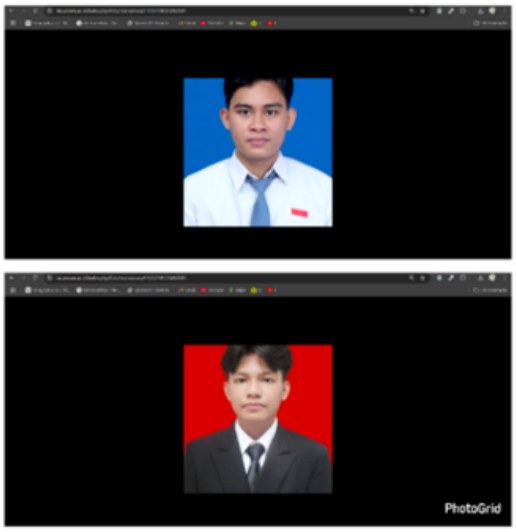


Gambar 11. Tampilan *Website* terkena *cross site scripting* (XSS)

Berdasarkan Gambar 12 dan Gambar 13, IDOR ditemukan saat mengubah parameter ID dari ****21084 menjadi ****21057, yang menyebabkan tampilan foto berubah ke milik ID ****21057, meskipun *request* di Burp Suite tetap menunjukkan ID ****021084. Ini terjadi karena sistem tidak menerapkan validasi otorisasi yang memadai dalam mengakses sumber daya. Saat pengguna mengubah parameter ID dalam URL, server tetap memproses permintaan tanpa memverifikasi apakah pengguna memiliki izin yang sesuai untuk mengakses foto tersebut.



Gambar 12. *Request* burpsuite



Gambar 13. Pengujian IDOR

3.4. Laporan Pengujian Penetrasi

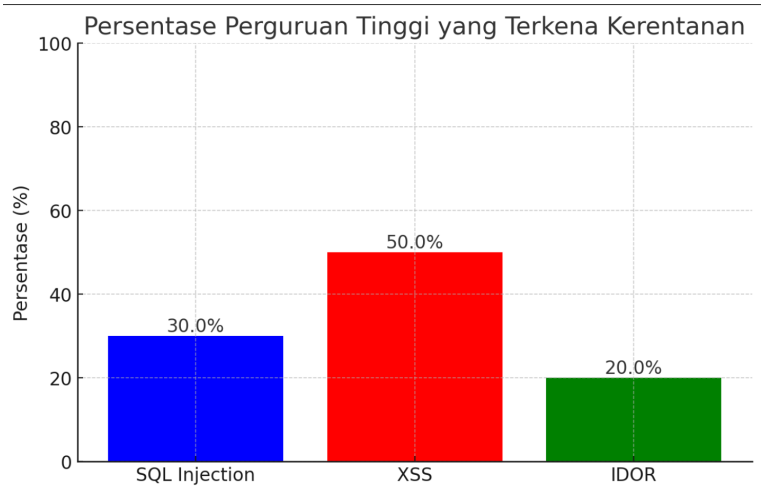
Pada laporan pengujian penetrasi merupakan rangkuman dari hasil pengujian penetrasi yang menyajikan hasil pengujian penetrasi terhadap 10 *website* perguruan tinggi yang menunjukkan tingkat kerentanan terhadap

masing-masing ancaman keamanan pada Tabel 2, dan grafik persentase perguruan tinggi yang terkena kerentanan pada Gambar 13. Tabel 2 merangkum dampak dari masing-masing jenis kerentanan yang teridentifikasi. Sementara itu, Tabel 3 menampilkan skor CVSS Versi 3.1 untuk setiap kerentanan yang ditemukan guna memberikan gambaran tingkat keparahan risiko.

Tabel 2. Hasil penelitian

No.	Perguruan Tinggi	SQL Injection	Cross Site Scripting	Insecure Direct Object Refeference
1.	Universitas ABC	✓	-	-
2.	Universitas DEF	-	✓	✓
3.	Universitas GHI	-	-	✓
4.	Universitas JKL	-	-	-
5.	Universitas MNO	-	✓	-
6.	Akademi ABC	-	✓	-
7.	Universitas PQR	✓	-	-
8.	Institut ABC	-	✓	-
9.	Universitas STU	✓	-	-
10.	Politeknik ABC	-	✓	-

Berdasarkan hasil penelitian pada Tabel 2, ditemukan tiga jenis kerentanan utama dalam pengujian penetrasi terhadap *website* perguruan tinggi, yaitu SQL *Injection*, *Cross-Site Scripting* (XSS), dan IDOR. Terdapat satu perguruan tinggi yang tidak memiliki ketiga jenis kerentanan tersebut, yang berarti sistem keamanannya lebih baik dibandingkan dengan perguruan tinggi lainnya. Hal ini bisa menjadi indikator bahwa institusi tersebut telah menerapkan praktik keamanan yang lebih ketat. Gambar 14 menunjukkan **temuan penelitian** ini adalah terdapat tiga jenis kerentanan utama yang ditemukan dalam pengujian penetrasi terhadap website perguruan tinggi di NTB, yaitu SQL *Injection*, *Cross Site Scripting* (XSS), dan IDOR. Dari sepuluh perguruan tinggi yang diteliti, lima di antaranya (50%) rentan terhadap XSS, tiga perguruan tinggi (30%) rentan terhadap SQL *Injection*, dan dua perguruan tinggi (20%) mengalami kerentanan IDOR.



Gambar 14. Diagram Perguruan Tinggi Yang Terkena Kerentanan

Hasil penelitian ini **sejalan atau didukung** oleh penelitian [7], yang menunjukkan bahwa sebagian besar *website* yang diuji mengalami kerentanan SQL *Injection*, Penelitian [8] juga mendukung temuan ini, di mana ditemukan kerentanan SQL *Injection* dan XSS pada situs pemerintah. Perbedaan tingkat kerentanan yang lebih rendah pada penelitian ini kemungkinan disebabkan oleh penggunaan sistem pengamanan tambahan seperti Web Application Firewall (WAF) atau CMS dengan fitur keamanan bawaan. Dengan demikian, hasil penelitian ini memperkuat urgensi perlunya peningkatan mekanisme validasi *input* dan kontrol akses pada *website* perguruan tinggi.

Tabel 3. CVSS Versi 3.1

No	Perguruan Tinggi	Kerentanan	Skor CVSS 3.1
1.	Universitas ABC	*SQL Injection*	*9.0 (Critical)*
2.	Universitas DEF	*Cross Site Scripting (XSS)*	*5.4 (Medium)*
3.	Universitas DEF	*Insecure Direct Object Reference (IDOR)*	*5.3 (Medium)*
4.	Universitas GHI	*Insecure Direct Object Reference (IDOR)*	*7.5 (High)*
5.	Universitas MNO	*Cross Site Scripting (XSS)*	*6.1 (Medium)*
6.	Akademi ABC	*Cross Site Scripting (XSS)*	*6.1 (Medium)*
7.	Universitas PQR	*SQL Injection*	*9.0 (Critical)*
8.	Institut ABC	*Cross Site Scripting (XSS)*	*6.1 (Medium)*
9.	Universitas STU	*SQL Injection*	*9.0 (Critical)*
10.	Politeknik ABC	*Cross Site Scripting (XSS)*	*6.1 (Medium)*

Berdasarkan Tabel 4, CVSS Versi 4.0, ditemukan bahwa SQL *Injection* memiliki tingkat keparahan tertinggi dengan skor 9.0 (*Critical*) pada Universitas ABC, Universitas PQR, dan Universitas STU, yang menunjukkan potensi eksploitasi serius terhadap data. *Cross-Site Scripting* (XSS) menjadi kerentanan yang paling sering ditemukan, dengan tingkat keparahan *Medium* (5.4 - 6.1) yang terdapat pada Universitas DEF, Universitas MNO, Akademi ABC, Institut ABC, dan Politeknik ABC, mengindikasikan kurangnya sanitasi *input* yang memadai. *Insecure Direct Object Reference* (IDOR) ditemukan pada Universitas DEF dan Universitas GHI, dengan tingkat keparahan *Medium* hingga *High* (5.3 - 7.5), yang menunjukkan adanya kelemahan dalam kontrol akses terhadap data *sensitive*.

Tabel 4. Efek dan Pencegahan Kerentanan

No	Kerentanan	Efek	Pencegahan
1.	SQL Injection	Penyerang dapat membaca, memodifikasi, atau menghapus data pada basis data melalui injeksi perintah SQL yang tidak tervalidasi.	Memvalidasi input dari pengguna dengan ketat. Gunakan *parameterized query* atau *prepared statements* untuk menghindari injeksi perintah. Selain itu, implementasikan *Web Application Firewall (WAF)* untuk mendeteksi dan memblokir pola serangan SQL Injection.
2.	Cross Site Scripting (XSS)	Penyerang dapat menyuntikkan skrip berbahaya yang dieksekusi pada browser pengguna, mencuri data sensitif atau melakukan aksi berbahaya lainnya.	Memvalidasi dan membersihkan semua input dan output yang berasal dari pengguna. Gunakan escape karakter khusus yang berpotensi berbahaya. Selain itu, terapkan *Content Security Policy* (CSP) untuk membatasi sumber daya eksternal yang dapat dimuat oleh *website*.
3.	IDOR	Penyerang dapat mengakses atau memodifikasi data milik pengguna lain dengan memanipulasi parameter pada URL atau *request*.	Memastikan setiap akses ke data diperiksa dengan mekanisme otorisasi yang ketat di sisi server. Gunakan pengidentifikasi yang sulit ditebak, seperti UUID, dan tidak mengandalkan validasi di sisi *client*.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan terhadap 10 perguruan tinggi menggunakan berbagai teknik pengujian keamanan, Pengujian keamanan dilakukan dengan *tools* seperti Wappalyzer, Nmap, SQLMap, Burp Suite, dan Xray telah membantu mengidentifikasi kelemahan dalam sistem. Ditemukan bahwa beberapa sistem masih memiliki celah yang dapat dieksploitasi. Sebanyak 30% perguruan tinggi ditemukan rentan terhadap SQL *Injection*, yang memungkinkan penyerang untuk menyisipkan perintah SQL berbahaya dan mendapatkan akses tidak sah ke database. 50% perguruan tinggi mengalami kerentanan *Cross Site Scripting* (XSS), yang dapat dimanfaatkan untuk menjalankan skrip berbahaya di *browser* korban. Selain itu, 20% perguruan tinggi

rentan terhadap IDOR, yang memungkinkan pengguna yang tidak sah mengakses data atau sumber daya yang seharusnya tidak dapat diakses.

Saran untuk penelitian mendatang agar melakukan kolaborasi langsung dengan perguruan tinggi untuk melakukan audit keamanan yang lebih komprehensif, termasuk uji penetrasi berbasis *whitebox* yang mencakup analisis kode sumber untuk mendeteksi potensi kerentanan yang mungkin tidak terdeteksi oleh pengujian otomatis dan hasil audit keamanan ini dijadikan dasar evaluasi berkala oleh tim IT perguruan tinggi.

UCAPAN TERIMA KASIH

Judul untuk ucapan terima kasih dan referensi tidak diberi nomor. Terima kasih disampaikan kepada Tim BITe yang telah meluangkan waktu untuk membuat template ini.

DAFTAR PUSTAKA

[1] H. Himawan, D. Kusuma Wardani, dan R. R. Kartika Kusuma Winahyu, "Pemanfaatan Perpustakaan Digital (E-Library) Sebagai Salah Satu Strategi Peningkatan Kualitas Pendidikan dan Penelitian di Perguruan Tinggi," *Faktor Exacta*, vol. 17, no. 3, p. 212, Sep. 2024. DOI: 10.30998/faktorexacta.v17i3.23824.

[2] A. Y. Pratama dan J. A. Razaq, "Integrasi Sistem Informasi Akademik dan Elearning Moodle dengan Rest API," *Jurnal Manajemen Informatika dan Sistem Informasi*, vol. 6, no. 1, pp. 26–38, Jan. 2023. DOI: 10.36595/misi.v6i1.696.

[3] Tenri, *Situs* Web *Perguruan Tinggi Terbanyak Alami Serangan* Web Defacement. [Online]. Available: https://cyberthreat.id/read/10636/Situs-Web-Perguruan-Tinggi-Terbanyak-Alami-Serangan-Web-Defacement.

[4] O. P. Sandy, *Serangan SQL Injection Jadi Aduan Siber Tertinggi Selama 2021*. [Online]. Available: https://cyberthreat.id/read/13925/Serangan-SQL-Injection-Jadi-Aduan-Siber-Tertinggi-Selama-2021.

[5] M. Gual, *Lembaga riset siber ungkap 26 website kampus diretas situs judi online*. [Online]. Available: https://www.alinea.id/media/lembaga-riset-siber-ungkap-26-website-kampus-diretas-situs-judi-online-b2fv09Jg5.

[6] D. Hawari, *Situs Unram Diretas, Muncul Jokowi2Periode*, Feb. 2019.

[7] A. Alanda *et al.*, "Web Application Penetration Testing Using SQL Injection Attack," *JOIV : International Journal on Informatics Visualization*, vol. 5, no. 3, p. 320, Sep. 2021. DOI: 10.30630/joiv.5.3.470.

[8] N. A. Prasetiyo, R. B. Huwae, dan A. H. Jatmika, "Audit dan Analisis Website Pemerintah Menggunakan Pengujian Penetrasi SQL Injection dan Cross Site Scripting (XSS)," *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*, vol. 6, no. 2, pp. 525–533, Sep. 2024. DOI: 10.29303/jtika.v6i2.425.

[9] S. Nagpure dan S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, PUNE, India: IEEE, Aug. 2017, pp. 1–6. DOI: 10.1109/ICCUBEA.2017.8463920.

[10] R. N. Dasmen *et al.*, "Pengujian Penetrasi pada Website elearning2.binadarma.ac.id dengan Metode PTES (Penetration Testing Execution Standard)," *Jurnal Komputer dan Informatika*, vol. 11, no. 1, pp. 91–95, Mar. 2023. DOI: 10.35508/jicon.v11i1.9809.

[11] M. A. Madani, "Penetration Testing untuk Menguji Sistem Keamanan pada Website," *Jeitech (Journal of Electrical Engineering And Information Technology)*, vol. 2, no. 1, pp. 33–45, 2024.

[12] B. I. Mukhtar dan M. A. Azer, "Evaluating the Modsecurity Web Application Firewall Against SQL Injection Attacks," in *2020 15th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, Egypt: IEEE, Dec. 2020, pp. 1–6. DOI: 10.1109/ICCES51560.2020.9334626.

[13] L. Lei *et al.*, "XSS Detection Technology Based on LSTM-Attention," in *2020 5th International Conference on Control, Robotics and Cybernetics (CRC)*, Wuhan, China: IEEE, Oct. 2020, pp. 175–180. DOI: 10.1109/CRC51253.2020.9253484.

[14] A. R. S. Firdaus dan A. Voutama, "Memanfaatkan Kerentanan Broken Access Control pada Website Orami untuk Membatalkan Pesanan dan Meniru Identitas Pengguna," *TeIKa*, vol. 13, no. 02, pp. 113–120, Oct. 2023. DOI: 10.36342/teika.v13i02.3113.

[15] D. Waltermire *et al.*, "The technical specification for the security content automation protocol (SCAP) version 1.3," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-126r3, Feb. 2018, NIST SP 800–126r3. DOI: 10.6028/NIST.SP.800-126r3.

[Halaman ini sengaja dikosongkan.]