PENETRATION TESTING PADA SEBUAH WEBSITE PERUSAHAAN EDUCATION DEVELOPMENT DENGAN FRAMEWORK OWASP TOP-10

PENETRATION TESTING ON AN EDUCATION DEVELOPMENT COMPANY'S WEBSITE WITH A TOP-10 OWASP FRAMEWORK

Ahmad Hasan Mutawakkil Alallah[1], Muhamad Nasrullah[2], Muhammad Ilham Alhari[3]
E-mail: [1]hasanmtwkl@student.telkomuniversity.ac.id, [2]emnasrul@telkomuniversity.ac.id,
[3]ilhamalhari@telkomuniversity.ac.id
[1,2] Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

Abstrak

Perkembangan teknologi informasi yang pesat memberikan berbagai kemudahan, termasuk dalam penyebaran informasi melalui *website*. Namun, kemajuan ini juga meningkatkan risiko keamanan siber, seperti pencurian data, kerugian finansial, dan penurunan reputasi perusahaan akibat peretasan. *Website* XYZ, yang menyediakan layanan edukasi dan menyimpan data sensitif seperti pembelian paket *bootcamp*, belum pernah dilakukan pengujian keamanan sistem. Maka dari itu, kebutuhan akan keamanan siber semakin penting untuk melindungi data-data sensitif dari ancaman peretasan. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada website XYZ menggunakan metode penetration testing berdasarkan framework Open Web Application Security Project (OWASP) Top 10 – 2021. Hasil pengujian menunjukkan adanya beberapa celah keamanan utama, di antaranya kelemahan validasi input pada fitur pembelian barang, tidak adanya header keamanan penting, penggunaan komponen usang, serta tidak adanya mekanisme rate limiting pada login berulang. Risiko lain meliputi penggunaan file JavaScript pihak ketiga yang tidak aman dan kurangnya pemantauan aktivitas login mencurigakan. Rekomendasi perbaikan mencakup validasi input yang lebih ketat, pembaruan komponen secara berkala, penerapan rate limiting, penambahan header keamanan, serta pengamanan sumber file pihak ketiga. Dengan implementasi perbaikan ini, risiko serangan dapat diminimalkan, data sensitif terlindungi, dan kepercayaan pelanggan terhadap layanan website XYZ meningkat. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan pertahanan keamanan website XYZ dari ancaman siber.

Kata kunci: *Website, Kejahatan Cyber, Penetration Testing, Kali Linux*.

Abstract

The rapid development of information technology offers various conveniences, including the dissemination of information through websites. However, this progress also increases cybersecurity risks, such as data breaches, financial losses, and damage to a company's reputation caused by hacking. Website XYZ, which provides educational services and stores sensitive data such as bootcamp package purchases, has never undergone a security test. Thus, cybersecurity measures to protect sensitive data from hacking threats are critical. This study analyzes security vulnerabilities on the XYZ website using penetration testing based on the Open Web Application Security Project (OWASP) Top 10 – 2021 framework. The results reveal several significant vulnerabilities, including input validation weaknesses in the product purchase feature, missing critical security headers, outdated components, and the lack of a rate limiting mechanism for repeated login attempts. Additional risks include insecure third-party JavaScript files and inadequate monitoring of suspicious login activities. Recommended improvements involve stricter input validation, regular component updates, rate limiting, security headers, and securing third-party file sources. These measures aim to reduce cybersecurity risks, safeguard sensitive data, and enhance customer trust in Website XYZ's services. This research is expected to contribute to improving the security defense of website XYZ from cyber threats.

Keywords: *Website, Cybercrime, Penetration Testing, Kali Linux.*

1. PENDAHULUAN

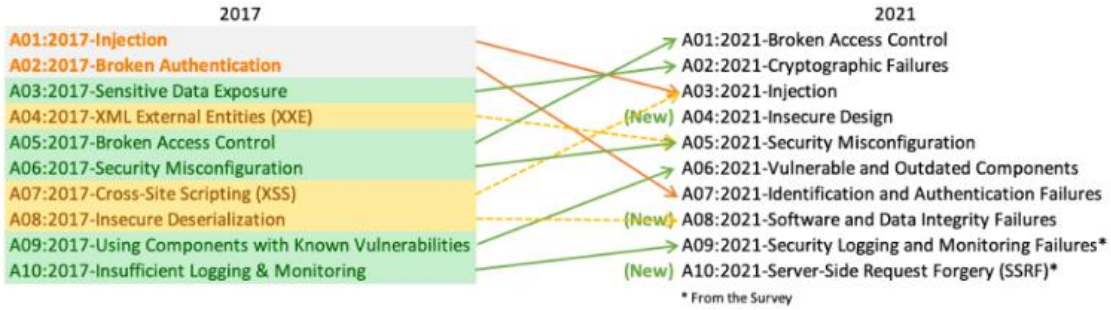
Pada era yang makin modern ini, perkembangan dalam teknologi informasi yang pesat merupakan suatu fenomena bagi masyarakat [1]. Salah satu contoh hasil dari perkembangan ini adalah terciptanya *website*, perkembangan teknologi *website* semakin mengarah pada kemudahan dan kecepatan dalam pertukaran data, yang mencakup sistem siber-fisik, *internet of things*, *cloud computing* dan *cognitive computing*[2]. Seiring dengan kemajuan ini, muncul berbagai kekhawatiran dari sisi pengguna maupun pengembang. Kekhawatiran tersebut terkait dengan kerentanan keamanan yang bisa menimbulkan ancaman, berdampak pada kerugian finansial dan merusak reputasi perusahaan[3].

PT XYZ merupakan perusahaan yang berfokus pada penyediaan layanan pendidikan, seperti konsultasi, pelatihan, pengembangan kepemimpinan, riset, dan pendampingan berkelanjutan. Sebagai *website* penyedia *workshop*, *course*, dan pelatihan, terdapat *billing details* yang berisi data pribadi saat proses *check* out pembelian *course*, sehingga keamanan website mereka menjadi esensial. Selain itu, pada *website* XYZ ini sebelumnya belum pernah dilakukan pengujian penetrasi. Maka pentingnya melakukan pengujian penetrasi, sebagai deteksi kerentanan agar sistem keamanan *website* diperbarui secara berkala untuk membantu dalam pencegahan serangan oleh *hacker*[4].

Pada penelitian ini akan dilakukan uji penetrasi untuk mencari tahu apakah protokol keamanan yang digunakan berfungsi dengan baik, serta mencari celah kerentanan yang dimiliki *website* XYZ. Dalam melakukan uji penetrasi, peneliti berpedoman pada OWASP Top 10 – 2021. OWASP Top 10 ini berisikan 10 daftar teratas celah keamanan web yang perlu diperhatikan oleh pengembang, untuk menghindari penyerang mengeksploitasi kerentanan tersebut[5].

2. METODOLOGI

Peneliti mengadopsi *framework* OWASP Top 10 - 2021 dalam melakukan pengujian penetrasi ini dan pengujian ini dilakukan secara *black box testing*. OWASP Top 10 – 2021 ini berisi 10 daftar kerentanan teratas yang mengancam keamanan pada web[6].

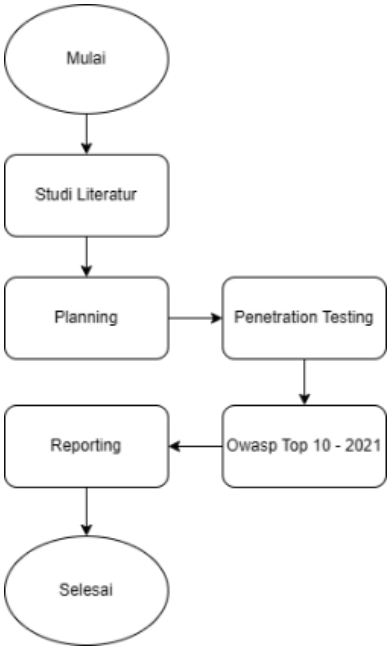


Gambar 1 OWASP Top 10 - 2021

Adapun alur penelitian yang digunakan dalam proses ini terdiri dari serangkaian tahapan yang disusun secara sistematis untuk memastikan setiap langkah penelitian dilakukan secara terstruktur, efisien, dan sesuai dengan tujuan yang telah ditentukan.

2.1 Alur Penelitian

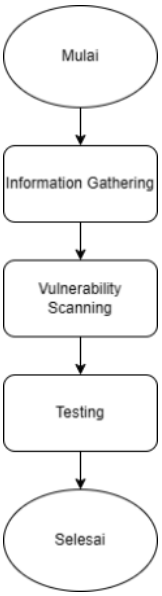
Pada penelitian ini, dilakukan pengumpulan studi literatur yang relevan untuk dijadikan sebagai referensi selama proses penelitian. Pada *planning* dilakukan analisa *website* objek untuk mengeksplorasi fitur-fitur yang ada pada web, Selanjutnya dilakukan *penetration testing* dengan mengacu standar OWAPS Top 10 2021. Lalu, dilanjutkan dengan *reporting* atau penyusunan laporan detail hasil pengujian.



Gambar 2 Alur Penelitian

2.2 *Penetration Testing*

Pada proses penetration testing ini terdapat beberapa tahapan. Peneliti melakukan *information gathering* atau melakukan pengumpulan informasi dengan beberapa alat yang membantu dalam memahami lebih dalam terkait target pengujian, lalu dilakukan *vulnerability scanning* untuk mengidentifikasi celah keamanan, dan dilakukan *testing* untuk pengujian kerentanan.



Gambar 3 Tahapan *Penetration Testing*

2.3 Alat dan Bahan

Dalam melakukan penelitian ini, peneliti menggunakan beberapa alat dan bahan yang sesuai dengan tujuan penelitian ini, berikut merupakan *software* dan *hardware* yang digunakan untuk menunjang jalannya penelitian.

Tabel 1 Software

Komponen	Spesifikasi
System Software	Windows 11 dan Kali Linux

Application Software	Oracle VM Virtualbox

Tabel 2 Hardware

Komponen	**Spesifikasi**
Processor	11th Gen Intel® Core™ i5-11400H
Graphic Card	NVIDIA GeForce RTX 3050Ti
RAM	8.00 GB
Storage Memory	500 GB
Wi-Fi	10 Mbps

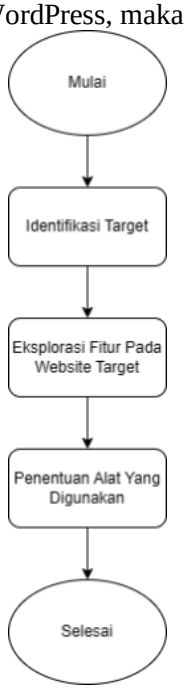
3. HASIL DAN PEMBAHASAN

3.1 Studi Literatur

Pada tahapan studi literatur ini merupakan pengumpulan sumber pustaka yang meliputi jurnal, sumber bacaan, dan artikel ilmiah yang relevan dengan topik yang diteliti. Proses ini dilakukan untuk membantu peneliti dalam memahami topik yang akan diteliti. Setelah dilakukan pengumpulan, peneliti memutuskan untuk menggunakan *framework* OWASP Top 10 – 2021, yang dimana berisi daftar 10 teratas kerentanan yang mengancam keamanan website[7]. Selain itu, *framework* ini juga merupakan langkah awal dalam peningkatan keamanan aplikasi.[8]

3.2 *Planning*

Pada tahapan *planning* ini merupakan perencanaan awal untuk memastikan tujuan pengujian sesuai aspek keamananan secara menyeluruh[9]. Peneliti melakukan identifikasi target yang diuji, seperti menentukan batasan yang diuji, lalu melakukan eksplorasi fitur-fitur yang meliputi interaksi antar halaman, pencarian area yang rentan, dilanjutkan dengan dengan alat yang sesuai seperti web target dengan CMS WordPress, maka digunakan alat WPScan.



Gambar 4 Alur *Planning*

3.3 *Penetration Testing*

Pada tahapan *penetration testing* ini dilakukan percobaan mengeksploitasi ke dalam sistem untuk mengetahui kemungkinan adanya celah kerentanan dalam sistem.[10]. *Penetration testing* ini dilakukan secara *black box testing* dikarenakan pengujian dilakukan tanpa mengetahui struktur internal dan kode web[11]. Pengujian ini menyesuaikan dengan kategori yang terdapat pada daftar 10 kerentanan OWASP Top 10. Pengujian ini melibatkan beberapa alat dari

operational system (OS) Kali Linux, dikarenakan Kali Linux menawarkan alat pengujian keamanan serta cukup memudahkan penggunaan dalam memaksimalkan pengujian[12].

3.3.1 *Information Gathering*

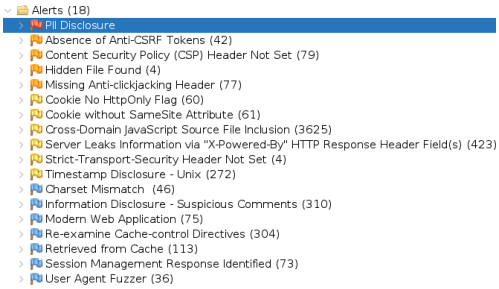
Pada tahap *information gathering* merupakan proses memahami target, pengumpulan informasi, serta membantu dalam meningkatkan efisiensi dalam penguujian[13]. Peneliti menggunakan beberapa perintah di sistem operasi Kali Linux dan alat. Perintah-perintah ini mencakup Whois, Nslookup, dan Nmap. Dengan memanfaatkan kombinasi perintah dan alat ini, peneliti dapat mengumpulkan data yang komprehensif dan akurat mengenai infrastruktur jaringan dan potensi kerentanannya.

Tabel 3 Hasil *Information Gathering*

Tools	Hasil
Whois	Domain ID: xxxxx-xxxxxxxx, Nama Domain: xxxxxx.xx, Nama *Server*, alamat *registrar*, dan informasi lainnya yang terkait dengan web.
Nslookup	IP *Address:* 104.xx.xx.xxx, *Mail Exchanger*, Informasi SOA (*Start of Authority*) *record.*
Nmap	*Port* 80/HTTP, *Port 443*/SSL HTTP, *Port* 8080/HTTP, *Port* 8443/SSL HTTP.

3.1.2 *Vulnerability Scanning*

Pada tahapan *vulnerability scanning* ini dilakukan pemindaian kerentanan untuk mengevaluasi keamanan web dengan alat yang dapat mendeteksi kerentanan serta saran mitigasi[14], peneliti menggunakan sebuah aplikasi *open-source* yang bernama OWASP ZAP (*Zed Attack Proxy*) untuk membantu dalam proses pengidentifikasian kerentanan keamanan yang terdapat pada situs web target. Adapun hasil dari pemindaian yang dilakukan menggunakan OWASP ZAP terlampir dibawah ini.



Gambar 5 Hasil ZAP

Dari hasil OWASP ZAP, ditemukan 1 kerentanan dengan tingkat *high*, 4 kerentanan dengan tingkat *medium*, 6 kerentanan dengan tingkat *low*, dan 7 kerentanan dengan tingkat *informational*.

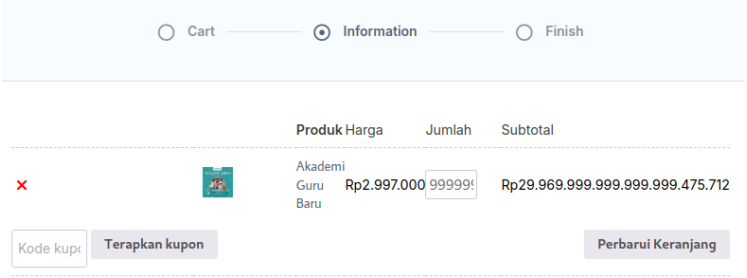
3.1.3 Testing

Pada tahapan *testing* ini dilakukan pengujian kerentanan mengacu pada OWASP Top 10 2021, pengujian juga dilakukan secara *blacbox testing*, dikarenakan peneliti tidak memiliki akses tentang sistem, infrastruktur, maupun *source code* yang digunakan oleh web target.[11]. Tahapan ini melibatkan adanya skenario pengujian untuk membantu dalam pencarian kerentanan dengan efektif[15].

1. A01: *Broken Access Control*

   Dari hasil *scanning* menggunakan OWASP ZAP, ditemukannya kerentanan *hidden file found*, file yang seharusnya tersembunyi namun malah terekspos pada publik. Ditemukan juga

kerentanan pada saat penggunaan alat Burpsuite, dengan skenario pengujian memanipulasi nilai *quantity* pada menu pembelian barang, tidak adanya batas maksimal pada input.



Gambar 6 Hasil A01:2021

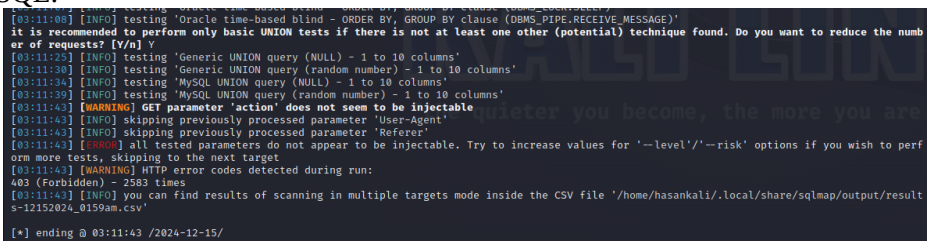
2. A02: *Cryptographic Failure*

Pengujian dilakukan dengan alat Wireshark untuk mengamati interaksi antara klien dengan *server*, serta untuk mengetahui apakah *server* telah menerapkan mekanisme protokol keamanan SSL/TLS dengan baik. Hasilnya, *server* menggunakan TLS 1.2 dan *chiper suite* AES-GCM yang tergolong aman. Dilanjutkan dengan menggunakan alat Testssl.sh untuk melakukan pemeriksaan yang lebih mendalam pada penggunaan protokol keamanan SSL/TLS, hasil dari pengujian tersebut adalah nilai keseluruhan dari server yang diuji mendapatkan nilai 94 dengan predikat "B".

Gambar 7 Hasil A02:2021

3. A03: *Injection*

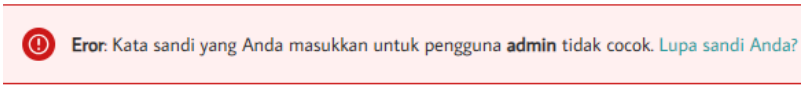
Pengujian dilakukan dengan menggunakan 3 alat kombinasi, yaitu Paramspider untuk mendeteksi parameter yang dapat membantu dalam eksploitasi XSS dan Sql *inject*, Dalfox untuk melakukan eksploitasi XSS (*Cross-Site-Scripting*), dan Sqlmap untuk melakukan eksploitasi Sql *inject*. Hasilnya, Dalfox tidak dapat melakukan XSS dikarenakan tidak ditemukan titik uji potensial, Sqlmap juga tidak menemukan parameter yang bisa dilakukan injeksi SQL.



Gambar 8 Hasil A03:2021

4. A04: *Insecure Design*

Pengujian dilakukan dengan melakukan percobaan login dengan username *default* seperti "admin", lalu muncul *pop-up* yang menyatakan bahwa *passsword* untuk username *admin* tidak cocok. Hal ini merupakan kerentanan yang berasal dari desain login yang tidak mempertimbangkan risiko penyerangan lebih lanjut.



Gambar 9 Hasil A04:2021

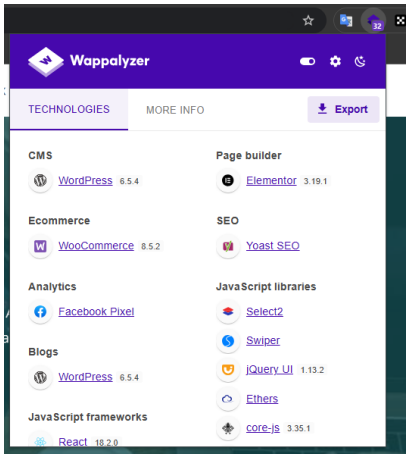
5. A05: *Security Misconfiguration*

Dari hasil *scanning* OWASP ZAP, ditemukan banyak kerentanan yang terkait dengan masalah konfigurasi keamanan, seperti tidak adanya *content security policy header* (CSP), tidak adanya token Anti-CSRF, tidak adanya *header anti-clickjacking*, dan seputar *header* keamanan, lalu pengujian dilanjutkan dengan menggunakan alat Nuclei, dan hasilnya ditemukan tidak adanya beberapa *security headers*.

Gambar 10 Hasil A05:2021

6. A06: *Vulnerable and Outdated Components*

Pengujian dilakukan dengan alat WPScan dan alat berbasis *extension browser* Wappalyzer untuk mengidentifikasi versi komponen yang usang, hasilnya ditemukan banyak plugin dan komponen yang usang.



Gambar 11 Hasil A06:2021

7. A07: *Identification and Authentication Failures*

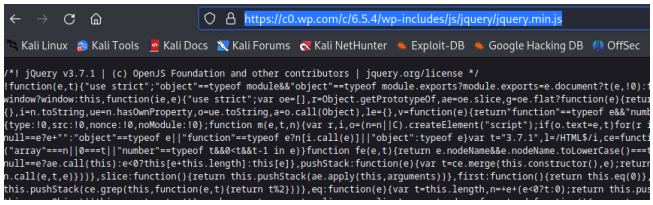
Pengujian ini dengan menggunakan alat Burpsuite untuk melakukan *brute force* dengan 250 payload, hasilnya semua *request* berstatus kode 200, yang berarti server selalu memproses. Tidak adanya proteksi *rate limiting* dan tidak adanya *IP blocking*.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
235	1q2w3e4r	200	1036			96781	
236	jasmine	200	1319			96785	
237	winter	200	1089			96777	
238	prince	200	1433			96777	
239	panties	200	1100			96777	
240	marine	200	1075			96781	
241	ghbdtn	200	1074			96775	
242	fishing	200	1093			96778	
243	cocacola	200	1055			96777	
244	casper	200	1054			96783	
245	james	200	1378			96783	
246	232323	200	1176			96777	
247	raiders	200	1067			96773	
248	888888	200	1117			96783	
249	marlboro	200	1097			96784	
250	gandalf	200	1119			96784	

Gambar 12 Hasil A07:2021

8. A08: *Software and Data Integrity Failures*

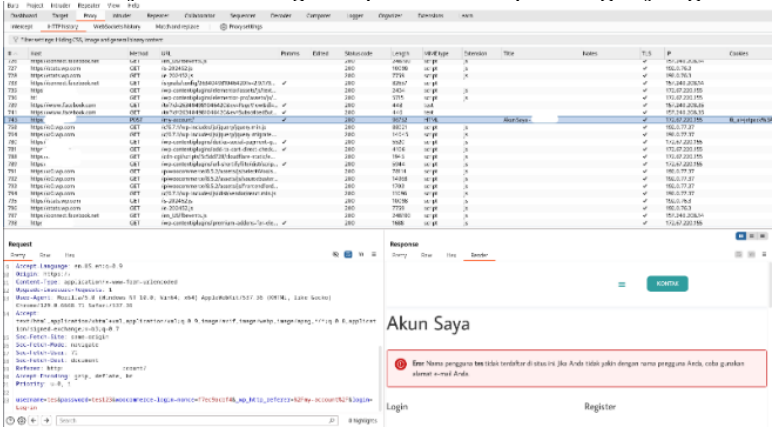
Dari hasil *scanning* menggunakan OWASP ZAP, ditemukan kerentanan *Cross-Domain JavaScript Source File Inclusion*, yang berarti halaman web mengunakan *file JavaScript* dari domain pihak ketiga atau dari skrip eksternal.



Gambar 13 Hasil A08:2021

9. A09: *Security Logging and Monitoring Failures*

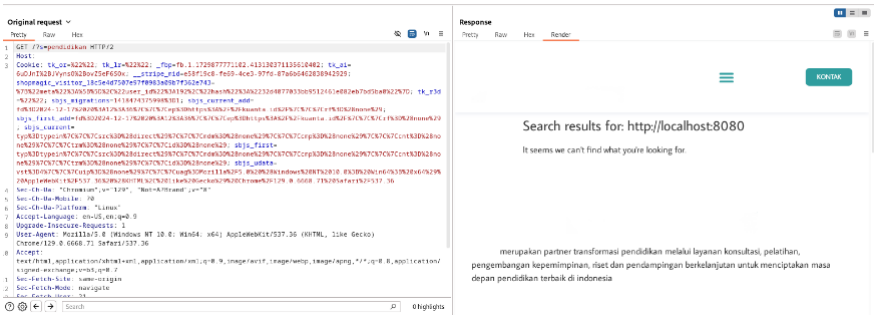
Pengujian ini dengan menggunakan alat Burpsuite untuk mengamati *response endpoint login* pada percobaan login dengan kredensial tidak sah, hasilnya server selalu merespon dengan status kode 200 OK, tidak dengan status kode yang lebih spesifik seperti 401 *unauthorized*, diketahui juga tidak adanya *rate limiting* dan pemantauan pada login yang tidak sah.



Gambar 14 Hasil A09:2021

10. A10: *Server-Side Request Forgery (SSRF)*

Pengujian ini dengan menggunakan alat Burpsuite untuk memodifikasi url pada *endpoint search bar* untuk diarahkan ke *resource* internal seperti “localhost:8080”. Hasil pengujiannya menunjukkan bahwa server tetap menerima input, namun hanya menampilkan pesan halaman yang dicari tidak ada.



Gambar 15 Hasil A10:2021

3.3 Reporting

Penyusunan laporan detail hasil pengujian serta rekomendasi perbaikan dapat dilihat pada tabel 4 sebagai berikut.

Tabel 4 Pelaporan

ID	Kategori	Temuan	Rekomendasi Perbaikan
A01:2021	*Broken Access Control*	Ditemukan *Broken Input Validation*.	Menetapkan nilai rentang maksimal pada input kuantitas.
A02:2021	*Cryptographic Failures*	Tidak ada.	-
A03:2021	*Injection*	Tidak ada.	-

ID	Kategori	Temuan	Rekomendasi Perbaikan
A04:2021	*Insecure Design*	Ditemukan desain login yang kurang baik, sehingga pesan *error* mengungkapkan validitas *username*.	Menetapkan desain yang lebih aman seperti pesan yang menyembunyikan detail validitas *username.*
A05:2021	*Security Misconfiguration*	Ditemukan ketiadaan beberapa *security headers*.	Audit keamanan secara berkala, serta menambahkan *security headers* penting, terutama yang dapat memitigasi percobaan eksploitasi.
A06:2021	*Vulnerable and Outdated Components*	Ditemukan beberapa komponen yang sudah usang.	Melakukan pemantauan terhadap komponen yang digunakan oleh sistem, serta pembaruan secara berkala pada versi sesuai versi terbaru
A07:2021	*Identification and Authentication Failures*	Ditemukan tidak adanya mekanisme *rate limiting.*	Menetapkan mekanisme *rate limiting* dalam percobaan login berulang kali.
A08:2021	*Software and Data Integrity Failures*	Ditemukan adanya penggunaan file JavaSript dari pihak ketiga.	Memastikan file JavaScript yang digunakan berasal dari sumber yang resmi dan aman
A09:2021	*Security Logging and monitoring*	Ditemukan tidak adanya pemantauan dalam aktivitas login yang tidak sah.	Menggunakan status kode yang sesuai seperti 401 *unauthorized*, log setiap aktivitas user seperti percobaan login dengan informasi seperti IP, waktu dan *user agent.*
A10:2021	*Server-Side Request Forgery*	Tidak ada.	-

4. KESIMPULAN

Pengujian penetrasi pada website XYZ mengidentifikasi berbagai kerentanan yang signifikan berdasarkan panduan OWASP Top 10 – 2021, yang menunjukkan bahwa keamanan website masih memiliki celah yang dapat dieksploitasi. Temuan utama meliputi: A01: *Broken Access Control*, ditemukan kelemahan validasi input pada fitur pembelian barang, yang memerlukan penetapan nilai rentang maksimal pada input kuantitas; A02: *Cryptographic Failures*, tidak ada temuan; A03: *Injection*, tidak ada temuan; A04: *Insecure Design*, desain sistem login yang mengungkapkan validitas username, yang memerlukan perbaikan untuk menyembunyikan detail validitas username pada pesan error; A05: *Security Misconfiguration*, ditemukan ketiadaan beberapa header keamanan penting, yang memerlukan audit keamanan berkala dan penambahan security headers; A06: *Vulnerable and Outdated Components*, banyaknya komponen yang usang, yang memerlukan pembaruan dan pemantauan berkala pada komponen sistem; A07: *Identification and Authentication Failures*, ditemukan tidak adanya mekanisme *rate limiting*, yang memerlukan pengaturan rate limiting dalam percobaan login berulang; A08: *Software and Data Integrity Failures*, ditemukan penggunaan file JavaScript dari pihak ketiga yang berisiko, yang memerlukan penggunaan file JavaScript hanya dari sumber yang aman dan terpercaya; A09: *Security Logging and Monitoring Failures*, ditemukan tidak adanya pemantauan aktivitas login yang mencurigakan, yang memerlukan implementasi status kode yang tepat dan pencatatan log aktivitas user seperti IP, waktu, dan user agent; serta A10: *Server-Side Request Forgery* (SSRF), tidak ada temuan. Dengan implementasi perbaikan yang direkomendasikan, PT XYZ dapat meminimalkan risiko serangan, melindungi data sensitif, dan meningkatkan kepercayaan pelanggan terhadap layanan yang diberikan

5. DAFTAR RUJUKAN

[1] A. Bastian, H. Sujadi, and L. Abror, "Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan SQL Injection," *INFOTECH journal* , vol. 6, no. 2, pp. 65–70, Dec. 2020.

[2] D. Hendarsyah, "E-Commerce Di Era Industri 4.0 Dan Society 5.0," *IQTISHADUNA : Jurnal Ilmiah Ekonomi Kita*, vol. 8, no. 2, pp. 171–184, 2019.

[3] D. M. Al Vriano, "Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis OWASP Top 10," *Kohesi: Jurnal Sains dan Teknologi*, vol. 1, no. 6, pp. 91–100, Oct. 2023.

[4] E. Irawadi Alwi, Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *Informatics Journal*, vol. 5, no. 2, pp. 43–48, 2020, doi: https://doi.org/10.19184/isj.v5i2.18941.

[5] R. Febriana, "Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack," *Jurnal Ilmiah Wahana Pendidikan*, vol. 2022, no. 12, pp. 327–334, 2022, doi: 10.5281/zenodo.6945632.

[6] OWASP Foundation, "Welcome to the OWASP Top 10 - 2021," OWASP. Accessed: Nov. 24, 2023. [Online]. Available: https://owasp.org/Top10/

[7] A. Elanda and R. Lintang Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP TOP 10," 2021.

[8] The OWASP® Foundation, "OWASP Top Ten 2021," OWASP Top 10 2021.

[9] D. Anugrah Utama and R. Supardi, "Analisis Keamanan Website Menggunakan PTES (Penetration Testing Execution And Standart)," *Jurnal Media Infotama*, vol. 20, no. 1, pp. 106–112, 2024, [Online]. Available: http://info.cern.ch.

[10] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati*, vol. 8, no. 2, pp. 113–124, Aug. 2020, doi: https://doi.org/10.24843/JIM.2020.v08.i02.p05.

[11] A. Bimandaru, A. Alamsyah, and A. Nugroho, "Analisis Pengujian Penetrasi Pada Layanan Hosting Menggunakan Metode Black Box (Studi kasus : Blogspot, Wordpress dan Shared Hosting)," *Jurnal Foristek*, vol. 14, no. 1, Jun. 2023, doi: 10.54757/fs.v14i1.238.

[12] S. P. Salsabillah, A. Al Mita, M. Z. Irsyad, E. Malays, and S. Sakti, "Implementasi Penggunaan Kali linux dengan Teknik Ddos dalam Uji coba Keamanan Website," *Tekinfo: Jurnal Ilmiah Teknik Industri dan Informasi*, vol. 25, no. 1, pp. 98–106, 2024, doi: 10.37817/tekinfo.v25i1.

[13] A. Kothia, B. Swar, and F. Jaafar, "Knowledge Extraction and Integration for Information Gathering in Penetration Testing," in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, Jul. 2019, pp. 330–335. doi: 10.1109/QRS-C.2019.00068.

[14] M. Ahsan, D. A. Rochmah, and D. Redaksi, "Analisa Kerentanan Sistem Dengan Menerapkan Open Vulnerability Assessment System Menggunakan Greenbone Vulnerability Management (GVM) INFORMASI ARTIKEL ABSTRACT," *INFORMATIKA DAN TEKNOLOGI (INTECH)* , vol. 3, no. 2, pp. 23–29, 2022.

[15] A. Fatihah and P. Dinarto, "Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ," *INNOVATIVE: Journal Of Social Science Research*, vol. 4, pp. 4536–4549, 2024.