Cyberspace: Jurnal Pendidikan Teknologi informasi
Volume 9, Nomor 1, Maret 2025, hal. 17 - 26
ISSN 2598-2079 (print) | ISSN 2597-9671 (online)

IMPLEMENTASI PENETRATION TESTING PADA SISTEM INFORMASI TRIBRATA POLRES PIDIE MENGGUNAKAN METODE OWASP

[1]Fujatullah Narezki, [2]Desita Ria Yusian TB
[1,2]Informatika, Fakultas Sains dan Teknologi, Universitas Ubudiyah Indonesia,
Jl. Alue Naga, Tibang, Banda Aceh 23114, Indonesia
Email: fuja@uui.ac.id

Abstract

One factor that must be taken into account is information system security, which is comprised of three components confidentiality, integrity, and availability. One area that requires attention is information system security. Since there are three components to information security—confidentiality, integrity, and availability—an information system must be assessed through penetration testing in order to preserve information security. Enhancing the site's information security is the goal of this penetration test. The Pidie Police Tribrata is a system created in this regard by the Pidie Police, the Aceh Regional Police's readiness unit situated in the Pidie Regency information region. However, penetration testing must be done on the Web application in order to assess the information system's security for the site's security. The Open Web Applications Security Project (OWASP) approach is used for penetration testing on the Pidie Police Tribrata information system. From the results of the penetration testing, several vulnerabilities in the web application were found and these were used as reports to improve the security system in the information system.

Keywords: *Penetration Testing, OWASP, Information Systems.*

Abstrak

Keamanan sistem informasi merupakan aspek yang perlu diperhatikan. Keamanan informasi terdiri dari 3 aspek yaitu Kerahasiaan, Integritas, Ketersediaan maka dari itu untuk menjaga keamanan informasi tersebut perlu dilakukannya evaluasi dari suatu sistem informasi berupa pengujian penetrasi. Pengujian penetrasi ini bertujuan untuk meningkatkan keamanan sitem informasi. Barkaitan dengan hal tersebut polres pidie yang merupakan satuan Kepolisian Polda Aceh yang berada di wilayah Kabupaten Pidie telah merancang sebuah sistem informasi yakni Tribrata Polres Pidie . Namun keamanan dari Sistem Informasi tersebut perlu diuji untuk mengevaluasi sistem keamananya, maka dari itu perlu dilakukan pengujian penetrasi pada Aplikasi Web tersebut. Pengujian penetrasi pada sistem informasi tribrata Polres Pidie ini menggunakan metode *Open Web Aplications SeScurity Project* (OWASP). Dari hasil pengujian penetrasi tersebut berhasil ditemukannya beberapa kerentanan pada aplikasi web tersebut dan dijadikan pelaporan untuk meningkatkan sistem keamanan pada sistem informasi tersebut.

Kata Kunci: Pegujian Penetrasi, OWASP, Sistem Informasi.

1. Pendahuluan

Di era globalisasi saat ini, ketergantungan manusia terhadap fasilitas internet semakin meningkat [1]. Dunia teknologi informasi telah berkembang pesat di setiap sektor lapangan kerja, baik pendidikan, perkantoran, hingga industri. Pesatnya perkembangan teknologi informasi menyebabkan peningkatan informasi digital yang didukung oleh infrastruktur jaringan internet yang sangat cepat. Namun kelebihan teknologi informasi juga mempunyai kelemahan, seperti ancaman terhadap keamanan suatu sistem informasi yang dapat berujung pada kejahatan siber (*cybercrime*) [2].

Untuk memberantas cybercrime yang diartikan sebagai tindakan ilegal yang dapat mengakibatkan kerugian dan disebabkan oleh pencurian data, penipuan kode, peniruan tampilan website lain, penyebaran informasi pribadi, dan lain-lain, suatu sistem informasi perlu memperhatikan sistem keamanannya [3]. Tiga komponen keamanan informasi adalah ketersediaan, integritas, dan kerahasiaan. Pengujian berupa pengukuran penetrasi diperlukan untuk mengetahui tingkat keamanan suatu sistem informasi. Pengujian penetrasi dapat dilakukan dengan beberapa cara. Penetrasi dapat digunakan untuk mengamankan sistem informasi, mengidentifikasi area yang mungkin rentan, dan memberikan rekomendasi untuk meningkatkan keamanan sistem informasi [4].

Implementasi pengujian penetrasi biasanya dilakukan pada sistem informasi yang relatif baru [5]. Oleh karena itu, Polres Pidie yang merupakan bagian dari Kepolisian Daerah Aceh yang membawahi Kabupaten Pidie membuat sistem informasi Polres Tribrata Pidie yang berfungsi untuk menyebarkan informasi mengenai kepolisian dan masyarakat setempat. Di bawah arahan Kepolisian Negara Republik Indonesia, Polres Pidie merupakan organisasi pemerintah yang mempunyai andil besar dalam menjaga keutuhan negara, khususnya di Kabupaten Pidie Provinsi Aceh.

Oleh karena itu pada penelitian ini peneliti melakukan pengujian penetrasi pada suatu sistem informasi yaitu Sistem Informasi Tribrata Polres Pidie untuk mengirimkan sistem keamanan pada sistem informasi ini dengan menggunakan pendekatan *Open Web Application Security Project* (OWASP).

2. Kajian Pustaka

2.1 Penetration Testing

Pengujian penetrasi, terkadang disebut sebagai pentesting, adalah metode yang memantau serangan nyata untuk menentukan kemungkinan potensi pelanggaran keamanan [6]. Untuk memastikan dampak potensial dari eksploitasi yang berhasil, penguji tidak hanya menemukan kerentanan yang dapat dieksploitasi oleh penyerang, namun mereka juga memanfaatkan kelemahan tersebut [7].

Pengujian penetrasi adalah salah satu metode untuk memperingatkan keamanan sistem komputer atau jaringan dari potensi serangan hacker. Tahap ini penting untuk menciptakan pertahanan yang kuat untuk komputer server jaringan karena tahap ini mengevaluasi implementasi dan desain sistem selain operasi. Meskipun penting, pengujian penetrasi sering kali tidak diterima oleh berbagai bisnis dan institusi. Mereka membedakan diri mereka dari penyerang dengan melakukannya secara resmi dan terjadwal [8].

2.2 OWASP

OWASP adalah grup ekosistem nirlaba untuk meningkatkan keamanan perangkat lunak dan aplikasi web. Kelompok OWASP mengembangkan aplikasi OWASP ZAP (Zed Attack Proxy) open source untuk menerapkan keamanan aplikasi web [9]. Alat ini mencakup fitur-fitur utama seperti SQL Injection, Cross Site Scripting (XSS), dan Cross Site Request Forgery (CSRF) untuk mengidentifikasi dan mengatasi kerentanan

keamanan dalam aplikasi web, dan juga memungkinkan pengguna untuk melakukan eksplorasi sistem dan fuzzing manual [10]. Antarmuka pengguna grafis (GUI) memudahkan pengembang dan peneliti keamanan untuk menggunakannya, dan dapat berinteraksi dengan prosedur pengujian keamanan kontinental dengan mendukung otomatisasi melalui baris perintah[11].

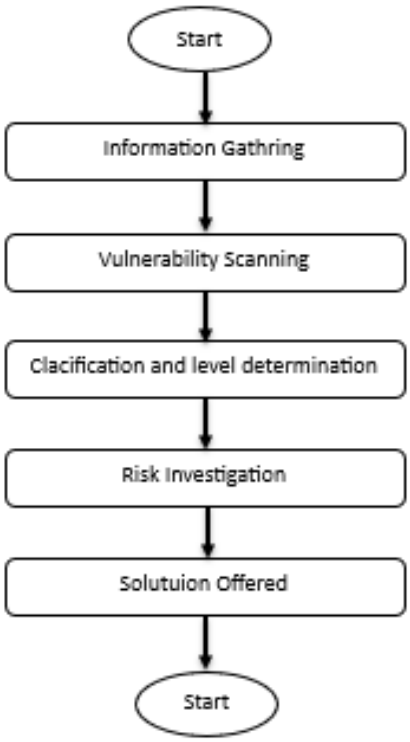
3. Metode Penelitian

3.1 Sistem Operasi

TABLE 1. *SPESIFIKASI HADWARE*

Komponen	
Processor	Intel® Core ™ i7-4790 CPU @ 3.60GHz (8CPUs), ~3.6GHz
Random Acces memory (RAM)	8 GB
Storage Memory	512 GB
Operating System (OS)	Windows 10 Home Single Languange 64-bit (10.0, Build 19045)

3.2 Rancangan Penelitian



Gambar 1. *Flowchart* Metode OWASP

Berikut merupakan pejelasan dari tahapan dari metode Owasp:

1. Start
2. *Information Gathering*
   Information Gathering adalah megumpulkan segala informasi dai sistem informasi dengan menggunakan teknik Black Box.

3. *Vulnerability Scanning*
   Vulnerability Scanning adalah Melakukan analisis mendalam pada data OWASP untuk mengidentifikasi celah keamanan yang mungkin ada dalam aplikasi web.
4. *Clacification and level determination*
   Clacification and level determination adalah mengelompokkan dan mengurutkan kerentanan berdasarkan tingkat bahayanya.
5. *Risk Investigation*
   Risk Investigation adalah menjelaskan kerentanan yang ditemukan.
6. *Solution Offered*.
   Solution Offered yaitu membuat laporan berupa Solusi untuk perbaikan pada sistem.
7. Selesai[12]

Berikut Komponen yang digunakan pada metode OWASP.

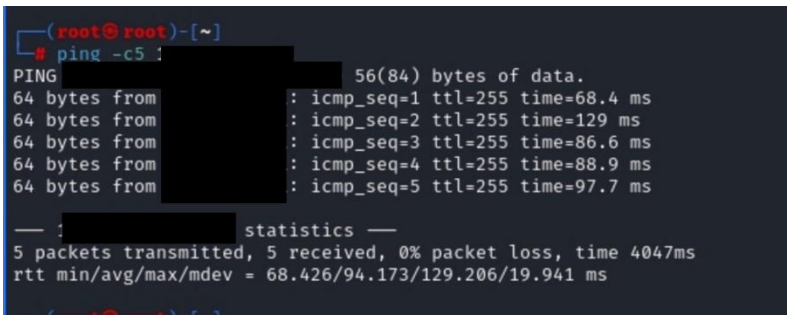
TABLE 2. *SPESIFIKASI SOFTWARE* METODE OWASP

Komponen	Komponen	Versi
OS	Kali Linux	2023.1
Information Gathering	Ping	-
	Whois	5.5.23
	SSLScan	1.0.2
Vulnerability Scanning	Nmap	7.94
	Zap	2.4.0
Reporting	Microsoft Word	2018

4. Hasil dan Pembahasan

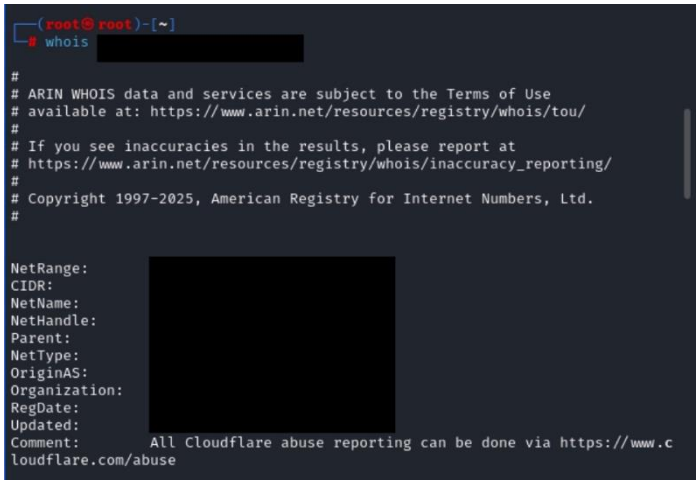
4.1. *Information Gathring*

Pengumpulan data adalah dengan mengekstraksi informasi dari sampel penelitian dengan menggunakan teknik Black box. Langkah pertama adalah melihat kecepatan sistem informasi dalam merespon data pada sistem, dalam hal ini jalankan perintah ping -c5 Ip Address.



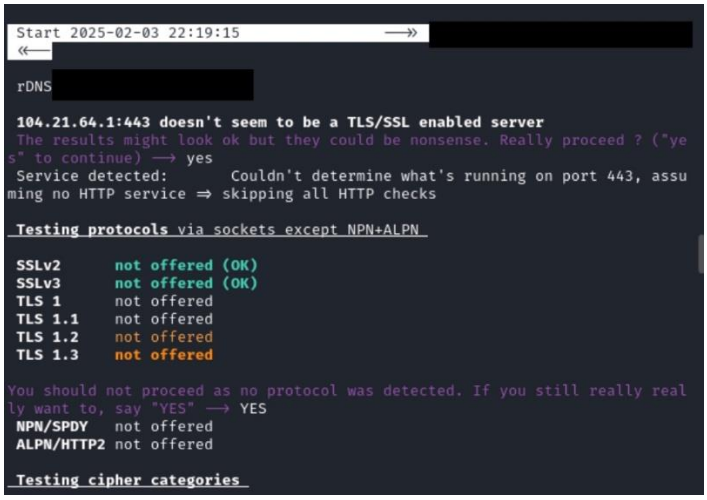
Gambar 2. Respon Pengiriman paket data

Dari hasil uji tersebut menujukan bahwa kecepatan pengiriman data pada sistem informasi tersebut masih lumayan bagus. Time yang bagus menujukan waktu dibawah 100ms. Kemudian, jalankan perintah whois “IP Address” untuk melihat informasi sistem yang lebih spesifik, seperti pada gambar dibawah.



Gambar 3. Hasil *Whois* Pada *IP Address.*

Langkah selanjutnya yaitu mencari informasi mengenai standar keamanan suatu sistem informasi berupa SSL/ TLS dari sistem informasi tersebut.

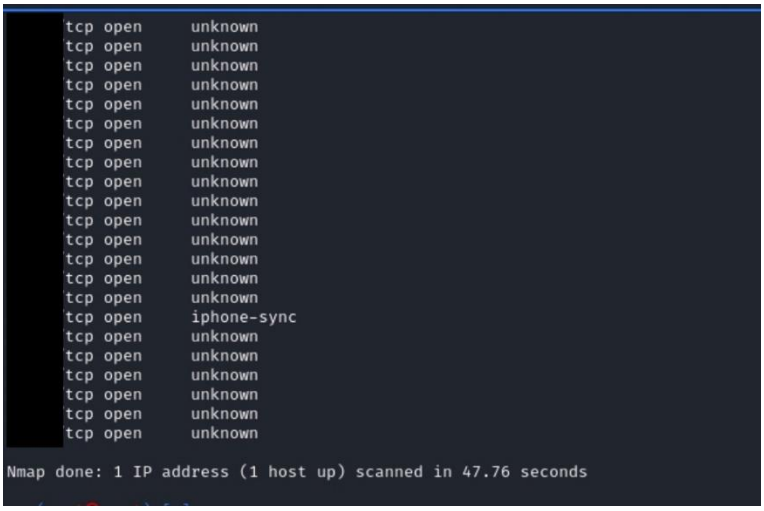


Gambar 4. Hasil *Testssl* Pada *IP Addres.*

Dari hasil perintah pengujian SSL dan TLS sistem informasi menyatakan bahwa SSL dan TLS sistem telah kedaluwarsa, dan tidak ada pemberitahuan yang diberikan dalam hasil pengujian.

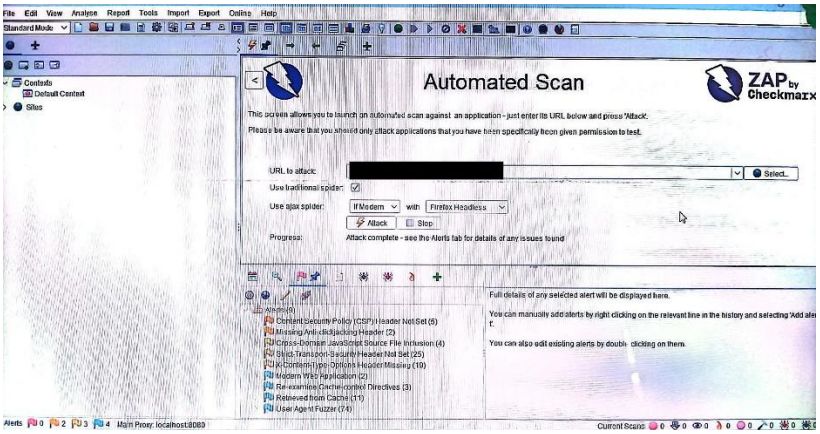
4.2. *Vulnerability Scanning*

Program ini sekarang sedang dipindai menggunakan nmap. Di sini, port terbuka aplikasi web dilihat menggunakan perintah nmap -sT "IP Address", seperti yang terlihat pada gambar di bawah.



Gambar 5. Hasil *nmap* Pada *IP Addres.*

Banyak port di server terbuka, menurut temuan pemindaian alat nmap. Menggunakan framework Zap untuk melakukan pemindaian adalah tahap selanjutnya, seperti terlihat pada gambar di bawah.



Gambar 6. Proses *Scanning* menggunakan Zap.

Aplikasi online memiliki beberapa kerentanan, seperti yang ditunjukkan oleh temuan pemindaian kerangka kerja OWASP Zap, yang mengungkapkan beberapa tingkatan kerentanan. Hasil pemindaian dengan framework OWASP Zap adalah sebagai berikut.

TABLE 3. HASIL PROSES SCANNING BERDASARKAN *LEVEL*

Risk Level	Number of Allert
High	0
Medium	2
Low	3
Informational	4

TABLE 4. PENJELASAN *SCANNING* MENGGUNAKAN *FRAMEWORK* ZAP.

NO	*Allert*	*Description*	*Level*	*Solution*
1	*Content Security Policy (CSP) Header Not Set*	Kebijakan Keamanan Konten (CSP), yang merupakan lapisan pertahanan tambahan, membantu mengidentifikasi dan menggagalkan beberapa jenis serangan, termasuk injeksi data dan Cross Site Scripting (XSS). Serangan ini dapat digunakan untuk segala hal, mulai dari pencurian data hingga perusakan situs atau penyebaran virus.	*Medium*	Verifikasi penyeimbang beban, server web, server aplikasi, dll. sebelum menerapkan header Kebijakan Keamanan Konten.
2	*Missing Anti-clickjacking Header*	'ClickJacking' tidak bisa dijelaskan dengan realisme. Dalam kebijakan ini, kebijakan 'frame-ancestor' atau X-Frame-Options Content harus digunakan..	*Medium*	Header HTTP X-Frame-Options dan Content-Security-Policy didukung oleh browser web kontemporer. Pastikan salah satunya dipilih pada setiap halaman yang ditampilkan situs web atau aplikasi Anda. bermaksud untuk melaksanakan Petunjuk "nenek moyang" Kebijakan Keamanan Konten.
3	*Cross-Domain JavaScript Source File Inclusion*	Halaman tersebut berisi satu atau lebih file skrip dari domain pihak ketiga.	*Low*	Verifikasi bahwa hanya sumber terpercaya yang digunakan untuk memuat file sumber JavaScript, dan pengguna akhir aplikasi tidak memiliki kendali atas sumber tersebut.
4	*Strict-Transport-Security Header Not Set*	Agen pengguna yang patuh, termasuk browser web, hanya boleh berkomunikasi dengan server web yang menggunakan HTTP Strict Transport Security (HSTS) melalui koneksi HTTPS yang aman, atau HTTP berlapis TLS/SSL.	*Low*	Pastikan web server, server application, beban penyeimbang, etc. You are committed to implementing Keamanan Transportasi Ketat.
5	*X-Content-Type-Options Header*	Header Anti-MIME-Sniffing X-Content-Type-Options tidak mengaktifkan opsi "nosniff". Hal	*Low*	Verifikasi bahwa aplikasi web atau server menyisipkan

	Missing	ini memungkinkan versi Chrome dan Internet Explorer yang lebih lama untuk melakukan MIME mengendus isi respons, yang dapat menyebabkan isi respons diubah dan ditampilkan sebagai jenis konten yang berbeda dari yang ditentukan.		header X-Content-Type-Options ke 'nosniff' untuk setiap halaman web dan memuat header Tipe Konten dengan benar.
6	*Modern Web Application*	Tampaknya menjadi aplikasi online kekinian. Jika Anda memerlukannya untuk menjelajah secara otomatis, Ajax Spider bisa lebih efektif daripada yang default.	*Informational*	Karena ini hanyalah peringatan informasional, tidak ada yang perlu diubah.
7	*Re-examine Cache-control Directives*	Karena header kontrol cache tidak ada atau tidak ada, browser atau proksi mungkin dapat menyimpan konten dalam cache.	*Informational*	Pastikan header HTTP kontrol cache diatur ke "tidak ada cache, tidak ada penyimpanan, harus divalidasi ulang" untuk konten yang aman.
8	*Retrieved from Cache*	Content is loaded from the shared cache. If the response data is user-specific, sensitive, or personal, sensitive information can be revealed. This can occasionally even grant a user total control over another user's session, depending on the cache settings of the components used in their environment.	*Informational*	Verifikasi bahwa tidak ada informasi pribadi, sensitif, atau khusus pengguna yang disertakan dalam respons. Jika demikian, pertimbangkan untuk membatasi atau memblokir konten agar tidak di-cache dan diambil oleh pengguna lain dengan menggunakan header respons HTTP.
9	*User Agent Fuzzer*	Look for changes in answers based on unclear User Agents (such as mobile websites or search engine crawlers).	*Informational*	Manfaatkan Validasi Agen Pengguna, Analisis Log Server, dan Monitor Header HTTP.

Dari hasil *Scanning* menggunakna *framework* Zap tersebut ditemukan beberapa faktor dan sebagian besar kerentanan yang ditemukan disebabkan karena server yang sudah melewati masa tenggang dan faktor lainnya seperti kesalahan dalam proses pemrograman yang berdampak pada keamanan website tersebut, hal ini bisa terjadi karena kurangnya kesadaran tentang keamanan selama fase desain.

5. Kesimpulan

Dari hasil pengujian pada Penetration Testing pada sistem informasi Tribrata Polres Pidie terdapat beberapa kerentanan-kerentanan yang ditemukan seperti:

1. Header CSP tidak dikonfigurasi sehingga berbahaya terhadap serangan XSS dan pencurian data, sebaiknya dilakukan konfigurasi untuk meminimalisir dan memproteksi serangan XSS dan pencurian data.
2. Transport Security berupa TLS/SSL tidak dikofigurasi sehingga membahayakan sistem keamanan pada sistem informasi tersebut
3. Terdapat beberapa script yang dapat membahayakan pada sistem informasi tersebut yang memungkinkan menjadi salah satu kerentanana, sebaiknya menghapus beberapa script yang tidak terlalu diperlukan
4. Banyak open port yang ditemukan pada saat dilakukannya scanning sehingga membahayakan sistem informasi tersebut, sebaiknya segera menutup port-port yang terbuka.
5. Header X Type Options tidak di konfigurasi sehingga dapat membahayakan apaila terjadi MIME sniffing, sebaikya konfigurasi Header X Type Options agar Sistem Informais tersebut lebih aman.

Sebaiknya segera dilakukan perbaikan sistem keamanan untuk meningtakan sistem keamanan pada sistem informasi tersebut agar data-data pada sistem informasi tersebut lebih aman dan lebih terproteksi dari pihak-pihak yang tidak bertanggng jawab.

Referensi

[1] Firda, S. Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," *Pros. SEMNAS INOTEK (Seminar Nas. Inov. Teknol.*, vol. 7, no. 1, pp. 52–59, 2023, [Online]. Available: https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/3411

[2] T. Rahmadi, Khairil, and R. Supardi, "Website Security Analysis Using Penetration Testing Method," *GATOTKACA J. (Teknik Sipil, Inform. Mesin dan Arsitektur)*, vol. 2, no. 2, pp. 147–152, 2021.

[3] W. Ma, M. T. S. Husnul, and K. Kuningan, "1262-Article Text-3020-1-10-20230116," vol. 8, no. 3, pp. 138–145, 2022.

[4] S. Serangan, "Ancaman dan Solusi Serangan Siber di Indonesia," vol. 1, no. 2, pp. 85–92, 2021.

[5] S. R. Yulistina, T. Nurmala, R. M. A. T. Supriawan, S. H. I. Juni, and A. Saifudin, "Penerapan Teknik Boundary Value Analysis untuk Pengujian Aplikasi Penjualan Menggunakan Metode Black Box Testing," *J. Inform. Univ. Pamulang*, vol. 5, no. 2, p. 129, 2020, doi: 10.32493/informatika.v5i2.5366.

[6] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[7] F. T. Wahyuni, G. P. Utama, I. Imelda, and P. Painem, "Analisis vulnerability dan risk assesment terhadap website pt . dapur cokelat indonesia menggunakan metode penetration testing vulnerability analysis and risk assesment againts website pt . dapur cokelat indonesia using penetration testing," vol. 3, no. September, pp. 1134–1143, 2024.

[8] F. Septian, M. H. Arfian, J. S. Asri, and B. Tjahjono, "Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus : Universitas Esa Unggul)," vol. 4, pp. 3629–3647, 2024.

[9] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[10] M. R. Ramdani, N. Heryana, and Y. S. A. Irawan, "Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)," *J. Pendidik. dan Konseling*, vol. 4, no. 3, pp. 5522–5529, 2022, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/6353

[11] Sunardi, I. Riadi, and P. A. Raharja, "Vulnerability analysis of E-voting application using open web application security project (OWASP) framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 135–143, 2019, doi: 10.14569/IJACSA.2019.0101118.

[12] Syahril Handaya, Raihan Islamadina, "Implementasi Penetration Testing Pada Aplikasi Web Sistem Evaluasi Data Bidang Tik Polda Aceh Menggunakan Metode Owasp Dan Nist SP 800-115", 2025.