Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing Dan OWASP TOP 10

(Studi Kasus : Pengadilan Negeri Purwokerto)

1st Dhiyaa Luthfwiedy Pratama
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto
dhiyapratama@student.telkomuniversity.ac.id

2nd Trihastuti Yuniati
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto
trihastuti@telkomuniversity.ac.id

3rd Gunawan Wibisono
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto
gunawanw@telkomuniversity.ac.id

***Abstrak* — Keamanan siber menjadi aspek krusial dalam era digital, khususnya bagi instansi pemerintah yang memiliki tanggung jawab dalam menyediakan informasi publik secara transparan dan aman. Pengadilan Negeri Purwokerto sebagai lembaga peradilan turut mengelola website resmi sebagai media penyampaian informasi hukum kepada masyarakat. Namun, situs web institusional rentan terhadap serangan siber akibat kelemahan konfigurasi, penggunaan komponen usang, dan celah pada aplikasi web. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada website Pengadilan Negeri Purwokerto dan merumuskan strategi mitigasi berdasarkan pendekatan OWASP Top Ten. Metode yang digunakan adalah penetration testing dengan memanfaatkan sejumlah alat uji seperti OWASP ZAP, Burp Suite, Xray, dan Sqlmap dalam lingkungan pengujian Kali Linux. Hasil pengujian mengidentifikasi beberapa kerentanan signifikan, antara lain Broken Access Control, Cryptographic Failures, Injection, Vulnerable and Outdated Components, serta Identification and Authentication Failures. Temuan tersebut mengindikasikan kelemahan dalam pengelolaan kontrol akses, implementasi enkripsi, validasi input, dan pembaruan sistem. Berdasarkan hasil tersebut, penelitian ini menyusun rekomendasi teknis dan prosedural sebagai langkah mitigasi untuk meningkatkan ketahanan sistem terhadap serangan siber. Diharapkan, hasil penelitian ini dapat menjadi rujukan strategis bagi institusi pemerintah lainnya dalam memperkuat keamanan sistem informasi mereka.**

Kata kunci— Keamanan Siber, OWASP TOP TEN, Analisis Kerentanan, Pengadilan Negeri Purwokerto, Kerentanan Aplikasi Web.

I. PENDAHULUAN

Perkembangan teknologi di era modern telah membawa dampak besar dalam berbagai aspek kehidupan manusia. Tuntutan terhadap kehidupan yang efisien, praktis, dan aman terus meningkat seiring dengan kemajuan teknologi digital. Salah satu indikator yang mencerminkan transformasi digital tersebut adalah peningkatan jumlah pengguna internet. Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024, penetrasi internet di Indonesia telah mencapai 79,5% atau sekitar 221.563.479 jiwa dari total populasi sebesar 278.696.200 jiwa pada tahun 2023 [1]. Hal ini menunjukkan bahwa internet telah menjadi bagian integral dari kehidupan masyarakat dan mendukung berbagai layanan digital, salah satunya adalah website.

Website merupakan media informasi yang paling umum digunakan dalam dunia digital untuk menyampaikan layanan, komunikasi, dan informasi kepada publik. Namun, di balik manfaatnya, website juga menjadi sasaran berbagai ancaman siber, seperti *web defacement*, yang memanfaatkan celah keamanan pada sistem atau aplikasi web. Data dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023 mencatat bahwa terdapat 189 kasus *web defacement* yang terjadi di Indonesia [2]. Fenomena ini mencerminkan lemahnya ketahanan siber, khususnya pada sistem informasi berbasis web di berbagai sektor, termasuk instansi pemerintah.

Keamanan siber kini menjadi isu strategis bagi lembaga pemerintahan, termasuk Pengadilan Negeri Purwokerto yang mengelola situs resmi www.pn-purwokerto.go.id sebagai sarana penyampaian layanan publik, publikasi informasi hukum, serta komunikasi dengan masyarakat. Ancaman terhadap aplikasi web seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, *Broken Authentication*, dan lainnya dapat menyebabkan kebocoran data sensitif, gangguan layanan, hingga rusaknya reputasi lembaga. Oleh karena itu, perlindungan terhadap aset digital seperti website institusional menjadi sangat penting untuk menjamin integritas, kerahasiaan, dan ketersediaan informasi.

Salah satu pendekatan yang dapat digunakan dalam mengidentifikasi dan menangani kerentanan keamanan aplikasi web adalah melalui panduan *OWASP Top Ten*. *Open Web Application Security Project (OWASP)* merupakan organisasi nirlaba yang menyediakan informasi dan panduan tentang keamanan aplikasi web. Inisiatif utamanya, *OWASP Top Ten*, memuat daftar sepuluh ancaman keamanan aplikasi web paling kritis yang harus menjadi perhatian utama bagi pengembang dan administrator sistem [3]. Panduan ini membantu dalam mendeteksi, menganalisis, dan mengimplementasikan langkah mitigasi yang efektif terhadap ancaman-ancaman tersebut.

Dalam konteks website Pengadilan Negeri Purwokerto, penerapan pendekatan *OWASP Top Ten* sangat relevan mengingat perannya sebagai portal publik yang mengelola berbagai data penting, mulai dari informasi layanan hingga data operasional internal. Keberadaan kerentanan tanpa penanganan yang memadai dapat berdampak signifikan terhadap keamanan informasi dan kepercayaan publik. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada website Pengadilan Negeri Purwokerto berdasarkan kerangka kerja *OWASP Top Ten*, serta menyusun langkah-langkah mitigasi yang tepat untuk meningkatkan ketahanan sistem terhadap serangan siber.

Melalui pengujian menggunakan metode *penetration testing* dan alat bantu seperti OWASP ZAP, Burp Suite, Xray, dan Sqlmap, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif mengenai kondisi keamanan website Pengadilan Negeri Purwokerto. Hasil dari penelitian ini juga dapat menjadi referensi bagi instansi pemerintah lainnya dalam mengelola dan meningkatkan keamanan sistem informasi berbasis web secara berkelanjutan.

II. KAJIAN TEORI

A. Analisis Keamanan Web

Analisis merupakan suatu proses sistematis dalam memecah suatu objek atau sistem ke dalam elemen-elemen yang lebih kecil guna memahami struktur, karakteristik, dan potensi kelemahannya. Dalam konteks keamanan website, analisis berfungsi untuk mengidentifikasi risiko dan celah keamanan yang dapat dimanfaatkan oleh pihak tidak berwenang. Aspek keamanan menjadi hal krusial dalam pengembangan website, karena kelalaian pada aspek ini berisiko menyebabkan kebocoran data, modifikasi tampilan situs (defacement), maupun gangguan layanan digital.

B. Website

Website adalah kumpulan halaman informasi digital yang terhubung dalam satu domain dan dapat diakses melalui jaringan internet. Setiap halaman ditulis dalam format HTML dan dapat dibuka melalui protokol HTTP maupun HTTPS menggunakan perangkat lunak peramban (browser) seperti Google Chrome, Mozilla Firefox, Opera, atau Microsoft Edge[4]. Website menjadi media komunikasi penting bagi organisasi dan lembaga pemerintah dalam menyediakan informasi kepada publik secara cepat dan luas.

C. Kali Linux

Kali Linux adalah sistem operasi berbasis Debian yang dirancang khusus untuk kegiatan keamanan informasi seperti penetration testing dan ethical hacking. Sistem ini dilengkapi dengan beragam alat analisis yang mempermudah pengguna dalam melakukan identifikasi, pemetaan, dan eksploitasi terhadap kerentanan sistem. Kali Linux dikembangkan oleh *Offensive Security* dan menjadi standar dalam pengujian keamanan[5].

D. Penetration Testing

Penetration testing atau uji penetrasi merupakan metode pengujian keamanan dengan mensimulasikan serangan terhadap sistem untuk mengidentifikasi dan mengukur tingkat kerentanannya[6]. Proses ini mencakup beberapa tahapan, mulai dari perencanaan, pengumpulan informasi, identifikasi kerentanan, eksploitasi, hingga pelaporan. Uji penetrasi memberikan data nyata tentang risiko keamanan dan membantu organisasi dalam menyusun strategi mitigasi yang efektif dan efisien.

E. OWASP dan OWASP Top Ten

OWASP (Open Web Application Security Project) adalah organisasi nirlaba global yang fokus pada peningkatan keamanan perangkat lunak. Salah satu kontribusi utamanya adalah OWASP Top Ten[7].Panduan yang merangkum sepuluh risiko keamanan aplikasi web paling kritis, di antaranya Broken Access Control, Injection, Cryptographic Failures, hingga Security Misconfiguration. Daftar ini digunakan sebagai standar oleh para pengembang, auditor, dan pengelola sistem untuk mengenali dan mengurangi risiko pada aplikasi berbasis web.

F. Eksploitasi

Eksploitasi merujuk pada upaya pemanfaatan kelemahan dalam sistem komputer, jaringan, atau aplikasi untuk memperoleh akses yang tidak sah. Serangan eksploitasi dapat dilakukan dari jarak jauh (remote), secara lokal oleh pengguna internal (local exploit), atau melalui interaksi pengguna seperti client-side exploit. Eksploitasi sering menjadi tahapan lanjutan dalam uji penetrasi untuk mengukur dampak dari kerentanan yang ditemukan[8].

G. SQL Injection

SQL Injection adalah teknik serangan siber yang mengeksploitasi input pengguna yang tidak tervalidasi dengan benar pada aplikasi yang terhubung dengan basis data. Penyerang dapat menyisipkan perintah SQL berbahaya ke dalam formulir input seperti login, pencarian, atau URL, yang kemudian dijalankan oleh sistem[9]. Akibatnya, penyerang dapat mengakses, mengubah, atau menghapus data sensitif tanpa otorisasi.

H. OWASP ZAP (Zed Attack Proxy)

OWASP ZAP adalah alat uji keamanan aplikasi web yang dikembangkan oleh OWASP dan bersifat open-source. Tool ini digunakan secara luas untuk mendeteksi kerentanan seperti SQL Injection, XSS, dan kelemahan konfigurasi sistem[10]. ZAP menawarkan pemindaian otomatis maupun pengujian manual, serta menyediakan fitur pelaporan yang komprehensif untuk dokumentasi hasil uji keamanan[11].

III. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode penetration testing, yang bertujuan untuk mengevaluasi dan mengidentifikasi celah keamanan pada website resmi Pengadilan Negeri Purwokerto. Fokus utama dari penelitian ini adalah melakukan pengujian terhadap sistem keamanan aplikasi web dengan menerapkan teknik *penetration testing*, yang dikombinasikan dengan kerangka kerja OWASP Top 10 sebagai acuan klasifikasi dan analisis risiko.

Prosedur penelitian dilakukan secara bertahap. Langkah awal dimulai dari proses perencanaan (*planning*), yakni penentuan ruang lingkup pengujian, batasan teknis, serta

penyusunan dokumentasi izin dari pihak terkait. Selanjutnya dilakukan pengumpulan informasi (*information gathering*) dengan cara memetakan domain, IP address, server, jenis framework, serta struktur sistem dari website target. Setelah informasi dasar diperoleh, proses dilanjutkan dengan identifikasi kerentanan (*vulnerability assessment*) yang dilakukan menggunakan berbagai alat bantu keamanan, antara lain OWASP ZAP, Burp Suite, Xray, dan SQLMap. Setiap kerentanan yang ditemukan kemudian diuji lebih lanjut pada tahap eksploitasi (*exploitation*) untuk mengetahui dampak dan potensi ancaman nyata terhadap sistem. Tahap akhir adalah pelaporan (*reporting*), yaitu dokumentasi temuan keamanan berikut rekomendasi mitigasi teknis dan prosedural.

Objek penelitian berupa website Pengadilan Negeri Purwokerto yang beralamat di www.pn-purwokerto.go.id. Sumber data utama berasal dari hasil pemindaian sistem dan log pengujian keamanan. Data dikumpulkan secara langsung melalui aktivitas pengujian berbasis *penetration testing* dan dicatat dalam bentuk dokumentasi teknis, tangkapan log, serta hasil output dari tools yang digunakan.

Data yang diperoleh dianalisis dengan mengacu pada daftar risiko *OWASP Top 10* versi 2021, yang mencakup berbagai jenis kerentanan umum seperti *Broken Access Control*, *Injection*, dan *Security Misconfiguration*. Setiap temuan dikaji berdasarkan tingkat keparahan, potensi eksploitasi, dan konsekuensi terhadap sistem.

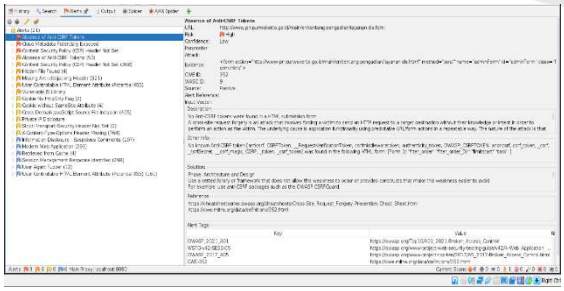
IV. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan website Pengadilan Negeri Purwokerto dengan pendekatan penetration testing berdasarkan referensi standar OWASP Top Ten 2021.

Pengujian dilakukan dalam lingkungan simulasi menggunakan beberapa endpoint yang teridentifikasi selama proses *information gathering* dan *vulnerability scanning*. Melalui SQLMap, ditemukan bahwa sistem tidak mengimplementasikan validasi input atau *parameterized queries* dengan baik, yang mengakibatkan terbukanya peluang bagi penyerang untuk mengeksekusi kueri injeksi dan mengakses informasi sensitif seperti struktur tabel dan isi data.

A. Penetration Testing

Pada tahap penetration test ini dilakukan pengujian menggunakan metode OWASP Top Ten terhadap celah keamanan atau kerentanan web. ut hasil scanning menggunakan tools OWASP ZAP versi 2.15.0



GAMBAR 1.
PENGUJIAN MENGGUNAKAN OWASP ZAP

B. Eksploitasi

Eksploitasi mengacu pada penggunaan kerentanan yang ditemukan dalam perangkat lunak untuk mendapatkan akses tidak sah atau menyebabkan kerusakan pada sistem.

1. A1 Cryptographic Failures

Cryptographic Failures, sebelumnya dikenal dalam OWASP Top 10 sebagai Sensitive Data Exposure, adalah jenis kerentanan yang muncul ketika data sensitif tidak dilindungi dengan benar oleh mekanisme kriptografi, baik saat disimpan (at-rest) maupun saat ditransmisikan (in-transit). Kerentanan ini termasuk dalam kategori A02 pada OWASP Top 10 tahun 2021, dan merupakan salah satu celah keamanan paling berisiko karena dapat menyebabkan kebocoran data pribadi, informasi akun, atau kredensial pengguna.

Pada pengujian yang dilakukan terhadap sistem <nama sistem/web target>, ditemukan bahwa data sensitif berupa username dan password dikirimkan melalui cookie HTTP dalam bentuk plaintext, tanpa adanya perlindungan kriptografi seperti enkripsi, serta tanpa penggunaan atribut keamanan cookie seperti HttpOnly, Secure, atau SameSite.

GAMBAR 2.
PENGUJIAN MENGGUNAKAN BURPSUITE

Kondisi ini sangat rentan terhadap serangan seperti packet sniffing atau man-in-the-middle attack, terutama jika pengguna mengakses sistem melalui jaringan yang tidak aman (misalnya Wi-Fi publik). Selain itu, tanpa atribut HttpOnly, skrip JavaScript yang berjalan di browser dapat membaca isi cookie, sehingga membuka kemungkinan serangan Cross-Site Scripting (XSS) yang digunakan untuk mencuri informasi login.

2. A3 Injection (Sql Injection)

SQL Injection adalah serangan di mana penyerang dapat menyisipkan perintah SQL berbahaya melalui input pengguna untuk mengakses atau memodifikasi data dalam basis data. Injeksi: Sqlmap adalah alat sumber terbuka yang sangat efektif dalam mendeteksi dan mengeksploitasi kerentanan injeksi SQL dalam aplikasi web [22]. Tujuan dari pengujian ini adalah untuk mengidentifikasi potensi kelemahan dalam data masukan yang dapat dieksploitasi oleh penyerang untuk memasukkan dan menjalankan perintah SQL berbahaya. Dengan Sqlmap, kami melakukan serangkaian pengujian untuk memastikan bahwa sistem database tereksploitasi

GAMBAR 3.
PENGUJIAN MENGGUNAKAN SQLMAP

3. A5 Security Misconfiguration

Pada gambar dapat dilihat bahwa SSLv3 statusnya disabled atau tidak diaktifkan. SSL dan penerusnya TLS adalah protokol kriptografi yang dirancang untuk memberikan keamanan komunikasi melalui Internet. Dalam konteks web, protokol ini menyediakan layanan HTTPS, namun juga digunakan oleh berbagai protokol aplikasi lainnya. SSLv1 tidak pernah dirilis secara publik, dan SSLv2 dengan cepat ditemukan memiliki kelemahan serius. SSLv3 kemudian dikembangkan dan sempat menjadi standar, sebelum akhirnya diikuti oleh TLSv1, TLSv1.1, dan TLSv1.2 yang lebih aman dan efisien. Seiring waktu, SSLv3 juga diketahui memiliki kerentanan serius, salah satunya adalah celah keamanan yang dikenal sebagai POODLE (Padding Oracle On Downgraded Legacy Encryption) yang dipublikasikan oleh Google Engineering. Meskipun terdapat tambalan sementara, solusi ini hanya efektif jika kedua sisi koneksi (klien dan server) telah ditambal. Karena SSLv3 merupakan protokol lama dan sudah tidak aman, disarankan agar semua server dan klien menonaktifkannya sepenuhnya.

GAMBAR 4. P
ENGUJIAN MENGGUNAKAN SSLSCAN

4. A6 Vulnerable and Outdatet Components

Vulnerable and Outdated Components adalah kerentanan yang muncul ketika aplikasi web menggunakan pustaka (library), framework, modul, atau komponen pihak ketiga yang sudah usang (outdated) atau memiliki kerentanan keamanan yang diketahui, namun belum diperbarui atau ditambal. Kerentanan ini sangat umum terjadi dan berdampak serius terhadap keamanan aplikasi. Berdasarkan hasil pemindaian menggunakan tools keamanan (seperti OWASP ZAP), ditemukan bahwa aplikasi menggunakan pustaka JavaScript yang rentan (Vulnerable JS Library). Meskipun fungsi aplikasi masih berjalan dengan baik, pustaka tersebut memiliki riwayat kerentanan yang terdokumentasi di basis data seperti CVE (Common Vulnerabilities and Exposures)

GAMBAR 5.
PENGUJIAN MENGGUNAKAN OWASPZAP

C. Pembahasan

Bab ini menguraikan hasil pengujian keamanan website yang dilakukan dengan pendekatan penetration testing berdasarkan standar OWASP Top 10. Dari hasil pengujian yang dilakukan, diperoleh temuan beberapa potensi kerentanan yang termasuk dalam lima dari sepuluh kategori OWASP, yaitu: Broken Access Control, Cryptographic Failures, Injection, Security Misconfiguration, dan Vulnerable and Outdated Components.

TABEL 1

Kategori Kerentanan	Status	Hasil Temuan
Broken Acces Control	Ditemukan menggunakan OWASP ZAP	Ditemukan kelemahan berupa Absence of Anti-CSRF Tokens, yang memungkinkan serangan Cross-Site Request Forgery (CSRF) karena tidak ada token verifikasi dalam form submission. Ini termasuk dalam kategori kontrol akses yang lemah karena otorisasi bisa dimanipulasi oleh pihak ketiga
Cryptographic Failures	Ditemukan menggunakan Burpsuite	Password disimpan dan dikirim melalui cookie dalam bentuk plaintext tanpa atribut Secure, HttpOnly, atau enkripsi, sesuai gambar request sebelumnya. Ini termasuk dalam A2 karena data sensitif tidak dilindungi dengan kriptografi yang sesuai.
Injection	Ditemukan menggunakan Xray yang di eksekusi menggunakan Sqlmap	Berdasarkan pengujian menggunakan SQLMap, ditemukan adanya celah SQL Injection pada parameter tertentu, yang memungkinkan penyerang mengeksekusi perintah SQL arbitrer di sisi server, membaca data database, dan bahkan memperoleh informasi struktur basis data.
Security Misconfiguration	SSLSCAN tidak ditemukan OWASP ZAP Ditemukan	- Header keamanan seperti Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, dan X-Content-Type-Options tidak diatur, mencerminkan kurangnya konfigurasi keamanan pada sisi server.

Vulnerable and Outdatet Components	Ditemukan Menggunakan OWASP ZAP	Terdeteksi adanya penggunaan pustaka JavaScript yang sudah usang dan mengandung kerentanan yang diketahui, namun belum diperbarui atau ditambal.

V. KESIMPULAN

Berdasarkan hasil pengujian keamanan terhadap situs www.pn-purwokerto.go.id, ditemukan beberapa indikasi kerentanan yang masuk dalam kategori OWASP Top Ten 2021, seperti Broken Acces Control, Cryptographic Failures, Injection, Security Misconfiguration, dan Vulnerable Components. Namun, dari seluruh temuan tersebut, hanya kerentanan pada kategori Injection, khususnya SQL Injection, yang berhasil dibuktikan secara teknis dan terverifikasi., yang berhasil dieksploitasi menggunakan alat otomatisasi seperti SQLMap. Serangan ini memungkinkan penyerang untuk mengakses struktur basis data, membaca tabel dan kolom sensitif, bahkan memodifikasi data jika hak akses tidak dibatasi dengan tepat. Kondisi ini mengindikasikan bahwa pengelolaan input dari pengguna tidak dilakukan dengan baik, tidak adanya implementasi parameterized queries atau input validation yang memadai, serta lemahnya segmentasi hak akses di sisi server maupun basis data. Kerentanan ini bersifat sangat kritis karena menyangkut situs milik institusi peradilan yang memproses data penting, dan kegagalan dalam melindungi integritas dan kerahasiaan data berisiko menyebabkan pelanggaran terhadap Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi serta menurunkan kepercayaan publik terhadap keamanan sistem layanan hukum digital pemerintah.

REFERENSI

[1] A. P[1] “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,” APJII. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[2] A. M. Tania, D. Setiyadi, and F. N. Khasanah, “Keamanan website menggunakan vulnerability assessment,” Informatics Educ. Prof., vol. 2, no. 2, pp. 171–180, 2018.

[3] BSSN, “Lanskap Keamanan Siber Indonesia 2023,” Badan Siber dan Sandi Negara, no. 70, 2023.

[4] Rudika Harminingtyas, “Analisis Website Layanan Sebagai Media Promosi, Media Transaksi Dan Media Informasi Dan Pengaruhnya Terhadap Brand Image Perusahaan Pada Hotel Ciputra Di Kota Semarang,” STIE SEMARANG, 2024, [Online]. Available: https://jurnal3.stiesemarang.ac.id/index.php/jurnal/article/view/120

[5] Andria, “Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux,” Gener. J., vol. 4, no. 2, pp. 69–76, 2020

[6] A. I. Rafeli, H. B. Seta, and I. W. Widi, “Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ,” Inform. J. Ilmu Komput., vol. 18, no. 2, p. 97, 2022, doi: 10.52958/iftk.v18i2.4632.

[7] Foundation OWASP®, “OWASP Top Ten,” 2021, [Online]. Available: https://owasp.org/www-project-top-ten/

[8] N. D. Anggana, “Apa itu Exploit? Penjelasan, Jenis dan Pencegahannya,” 2024, [Online]. Available: https://widyasecurity.com/2024/01/09/apa-itu-exploit-penjelasan-jenis-dan-pencegahannya/

[9] ASDF.ID, “Sniffing Adalah: Cara Kerja dan Cara Pencegahannya,” 2022, [Online]. Available: https://www.asdf.id/sniffing-adalah/

[10] D. Ending Narhudin, B. Irawan, and A. Bahtiar, “Evaluasi Keamanan Website Menggunakan Metode Owasp: Penilaian Terhadap Serangan Injeksi Sql Dan Cross-Site Scripting (Xss),” JATI (Jurnal Mhs. Tek. Inform., vol. 8, no. 1, pp. 675–680, 2024, doi: 10.36040/jati.v8i1.8700.

[11] Hackerone, “OWASP ZAP: 6 Key Capabilities and a Quick Tutorial,” 2024, [Online]. Available: https://www.hackerone.com/knowledge-center/owasp-zap-6-key-capabilities-and-quick-tutorial