STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 4 No. 1, Februari 2025, 8 - 15
e-ISSN: 2828-5344 | DOI: 10.55123

# Analisis Website E-learning Bina Darma Menggunakan Metode Web Application Security Project Zap (Owasp Zap)

**[1)]Mgs M Nur Arromadhani, [2)]Tamsir Ariyadi, [3)]A fahlevi Hadist, [4)]M Dimas Putra**

[1,2,3,4)](Teknik Komputer, Vokasi, Universitas Bina Darma)

[1,2,3,4)] arromadhani10@gmail.com, tamsirariyadi@binadarma.ac.id, ahmadfahlevi17012003@gmail.com, muhammaddimas090704@gmail.com

**INFO ARTIKEL**

**Riwayat Artikel :**
Diterima : 30 Desember 2024
Disetujui : 20 Januari 2025

**Kata Kunci :**
keamanan *website*, *E-learning*, Owaspzap, Analisis Kerentanan

**ABSTRAK**

Analisis perlindungan situs web *e-laearning* sangat krusial untuk menjaga informasi pengguna dan data akademik dari ancaman digital. Penelitian ini memiliki tujuan untuk mengevaluasi keamanan situs e-learning di Universitas Bina Darma dengan menggunakan metode *OWASP ZAP (Zed Attack Proxy*), yang merupakan alat untuk menguji keamanan aplikasi web dengan fokus pada menemukan kerentanan umum seperti injeksi *SQL, XSS (Cross-Site Scripting),* dan kesalahan dalam pengaturan keamanan. Temuan dari analisis tersebut mengungkapkan beberapa celah yang bisa dimanfaatkan, dan selanjutnya diberikan rekomendasi perbaikan untuk memperkuat keamanan sistem. Diharapkan hasil penelitian ini dapat menjadi referensi bagi pengembang dalam mengelola keamanan aplikasi web dengan pendekatan yang lebih proaktif dan teratur. Dengan kombinasi pendekatan teknologi dan manusia, keamanan sistem *e-learning* dapat lebih terjamin di masa depan

***ARTICLE INFO***

***Article History :***
*Received : Dec 30, 2024*
*Accepted : Jan 20, 2025*

***Keywords****:*
*Web Security, E-learning, Owaspzap, Vulnerability Analysis.*

***ABSTRACT***

*The analysis of e-learning website protection is crucial to safeguard user information and academic data from digital threats. This research aims to evaluate the security of the e-learning website at Universitas Bina Darma using the OWASP ZAP (Zed Attack Proxy) method, a tool designed to test web application security by focusing on identifying common vulnerabilities such as SQL injection, XSS (Cross-Site Scripting), and misconfigurations in security settings. The findings from this analysis reveal several exploitable gaps, followed by recommendations for improvements to enhance system security. It is hoped that the results of this study can serve as a reference for developers in managing web application security with a more proactive and systematic approach. With a combination of technological and human approaches, the security of e-learning systems can be more guaranteed in the future*

## 1. PENDAHULUAN

Kemajuan teknologi informasi telah menimbulkan dampak besar di bidang pendidikan, salah satunya adalah munculnya platform pembelajaran online. Universitas Bina Darma, sebagai salah satu institusi pendidikan tinggi, memanfaatkan website *e-learning* untuk mendukung kegiatan pembelajaran daring. Namun, seiring meningkatnya penggunaan teknologi ini, ancaman terhadap keamanan siber juga semakin kompleks. Data pengguna, materi pembelajaran, dan informasi akademik lainnya menjadi target yang rentan terhadap serangan siber jika keamanan sistem tidak dikelola dengan baik (Al'am'yubi and Wijayanto, 2023).

*OWASP ZAP* (*Open Web Application Security Project Zed Attack Proxy)* adalah salah satu alat keamanan web yang dirancang untuk mendeteksi berbagai jenis kerentanan pada aplikasi web. Alat ini mampu menganalisis kelemahan seperti *injeksi SQL, Cross-Site Scripting (XSS),* dan konfigurasi keamanan yang kurang tepat. Dengan menggunakan *OWASP ZAP*, pengembang dapat mengidentifikasi celah keamanan pada website dan memberikan langkah perbaikan yang sesuai sebelum kerentanan tersebut dieksploitasi oleh pihak yang tidak bertanggung jawab (Ariyadi *et al.*, 2023).

Penelitian ini bertujuan untuk menganalisis tingkat keamanan website e-learning Universitas Bina Darma dengan menggunakan *OWASP ZAP*. Hasil dari analisis ini diharapkan mampu memberikan pemahaman yang lebih dalam mengenai kemungkinan kelemahan yang ada, serta menyajikan saran yang dapat diterapkan untuk memperkuat perlindungan sistem. Oleh karena itu, studi ini diharapkan bisa berperan dalam menjaga keutuhan dan kehandalan situs e-learning sebagai alat pendukung pendidikan masa kini (Burhani and Priyawati, 2024).

## 2. TINJAUAN PUSTAKA

### 2.1 Analisis

Analisis adalah suatu proses sistematis yang dilakukan untuk memahami, menguraikan, dan mengevaluasi suatu fenomena, data, masalah, atau objek tertentu dengan cara memisahkan komponen-komponen penyusunnya menjadi bagian-bagian yang lebih kecil. Tujuan utama dari analisis adalah untuk mendapatkan pemahaman yang lebih mendalam, mengidentifikasi pola-pola, menemukan hubungan antara elemen-elemen yang ada, serta menghasilkan kesimpulan atau rekomendasi berdasarkan hasil pemeriksaan tersebut. Dalam berbagai bidang, analisis memiliki penerapan yang luas. Misalnya, dalam dunia bisnis, analisis dilakukan untuk mengevaluasi kinerja perusahaan, memprediksi tren pasar, atau menyusun strategi berdasarkan data yang tersedia. Dalam ilmu pengetahuan, analisis digunakan untuk memahami struktur, fungsi, atau hubungan antar elemen tertentu, seperti analisis kimia yang mempelajari komposisi suatu bahan. Sementara itu, dalam ilmu sosial, analisis sering digunakan untuk memahami pola-pola perilaku manusia, hubungan sosial, atau dinamika masyarakat. Proses analisis biasanya melibatkan beberapa langkah utama, seperti pengumpulan data, pengorganisasian informasi, identifikasi elemen penting, serta interpretasi hasil untuk menghasilkan kesimpulan yang relevan. Pendekatan yang digunakan dapat bersifat kualitatif, yang berfokus pada pemahaman mendalam, atau kuantitatif, yang menggunakan angka dan statistik untuk mendapatkan hasil yang objektif. Dengan analisis, seseorang dapat memecahkan masalah, memahami akar penyebab suatu fenomena, dan membuat keputusan yang lebih baik berdasarkan fakta atau data yang teruji. Analisis bukan hanya alat untuk memahami sesuatu, tetapi juga menjadi dasar untuk pengambilan tindakan yang efektif dan terarah.

termasuk (Delone, Pambudi and Karyono, 2024).

2.2 Website E-Learning Universitas Bina Darma

Website e-learning Universitas Bina Darma dirancang sebagai platform pembelajaran daring untuk mendukung kegiatan akademik mahasiswa dan dosen. Dengan meningkatnya aktivitas pada platform ini, keamanan menjadi isu yang sangat penting. Berdasarkan penelitian sebelumnya, penerapan OWASP ZAP dapat membantu mengidentifikasi kerentanan yang berpotensi mengancam data pengguna dan keberlanjutan operasional sistem. Melalui pengujian keamanan yang terstruktur, Universitas Bina Darma dapat meningkatkan kualitas layanan e-learning sekaligus melindungi data pengguna dari ancaman siber. (Dwi Cahyani *et al.*, 2022).

2.3 Relevansi *OWASP ZAP* untuk Sistem *E-Learning*

Dalam lingkungan pendidikan, sistem e-learning menjadi komponen penting untuk mendukung proses pembelajaran jarak jauh. Sistem ini sering kali melibatkan data sensitif, seperti informasi pribadi mahasiswa, nilai akademik, dan materi pembelajaran eksklusif. Oleh karena itu, keamanan menjadi prioritas utama. Syahputra dan Pratama (2021) mengungkapkan bahwa sistem e-learning rentan terhadap serangan seperti *Cross-Site Scripting* (XSS) dan Broken Authentication, terutama jika sistem tersebut tidak dirancang dengan standar keamanan yang memadai. Santoso dan Wijaya (2023) memaparkan studi kasus tentang pengujian keamanan pada sistem e-learning menggunakan OWASP ZAP. Penelitian tersebut berhasil mendeteksi kerentanan seperti *Cross-Site Request Forgery (CSRF)* dan kebocoran informasi melalui pengaturan konfigurasi yang salah. Hasil ini menunjukkan bahwa *OWASP ZAP* adalah alat yang efektif untuk mengevaluasi keamanan sistem e-learning dan memberikan wawasan untuk perbaikan (Fathurrahmad and Ester, 2020).

2.4 Web

Web adalah sistem informasi berbasis internet yang memungkinkan pengguna untuk mengakses, berbagi, dan bertukar informasi dalam bentuk halaman-halaman yang saling terhubung melalui hyperlink. Web merupakan bagian dari internet yang paling dikenal oleh masyarakat karena menyajikan informasi dalam bentuk teks, gambar, video, dan berbagai format multimedia lainnya yang dapat diakses melalui perangkat seperti komputer, tablet, atau ponsel pintar menggunakan aplikasi yang disebut peramban (browser), seperti Google Chrome, Mozilla Firefox, atau Safari. (Febriani *et al.*, 2024).

## 3. METODE

Penelitian ini menggunakan metode deskriptif dengan pendekatan studi kasus pada website e-learning Universitas Bina Darma. Proses analisis dilakukan dengan menggunakan alat keamanan aplikasi web OWASP ZAP (Zed Attack Proxy) untuk mengidentifikasi dan mengevaluasi potensi kerentanan yang ada pada sistem. Tahapan penelitian meliputi:

1. Pengumpulan Data

   Data dikumpulkan dengan cara mengakses sistem e-learning Universitas Bina Darma melalui metode black-box testing. Data yang diperoleh meliputi informasi mengenai struktur aplikasi, parameter input, dan jenis teknologi yang digunakan pada sistem e-learning (Jakobsson and Häggström, 2022).

2. Konfigurasi OWASP ZAP

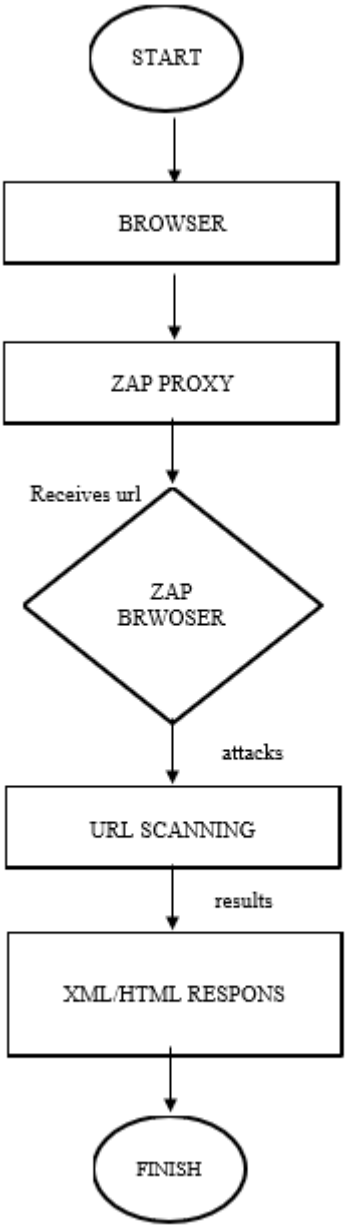
   OWASP ZAP diatur sebagai proxy server untuk menganalisis lalu lintas HTTP dan HTTPS antara klien dan server. Konfigurasi mencakup penyesuaian pengaturan target website,

parameter scanning, dan tingkat sensitivitas deteksi kerentanan (Hasibuan and Handoko, 2023).

3. Pemindaian Otomatis dan Manual
   Pemindaian Otomatis: OWASP ZAP melakukan proses pemindaian otomatis terhadap sistem untuk mendeteksi kerentanan yang sesuai dengan OWASP Top 10, seperti *Cross-Site Scripting (XSS), SQL Injection, dan Broken Authentication* (Putra *et al.*, 2024).

4. Pemindaian Manual
   Pengujian manual dilakukan untuk memastikan validitas hasil pemindaian otomatis dan mengeksplorasi area aplikasi yang memerlukan analisis lebih lanjut (Rahman *et al.*, 2024).

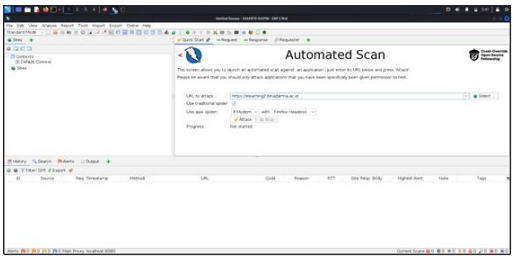
5. Identifikasi dan Analisis Kerentanan
   Hasil pemindaian OWASP ZAP berupa daftar kerentanan yang ditemukan, lengkap dengan deskripsi, tingkat keparahan, dan saran mitigasi. Data ini dianalisis untuk menentukan jenis dan tingkat risiko dari setiap kerentanan yang ditemukan (Rizkyudin, Pradhana and Fitriani, 2022).




## 4. HASIL DAN PEMBAHASAN

*Web e-learning* Universitas Bina Darma adalah platform penting untuk mendukung pembelajaran daring. Mengingat data sensitif yang dikelola, analisis keamanan menjadi prioritas. *OWASP ZAP* digunakan untuk mengidentifikasi kerentanan dalam aplikasi web ini (Victor Ilyas Sugara and I Wayan Sriyasa, 2024).

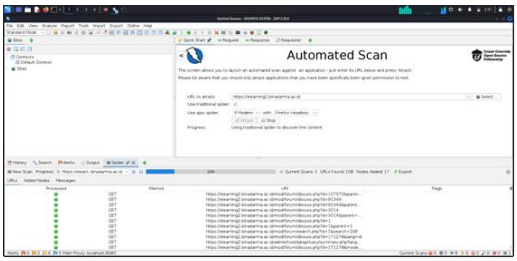
1. Analisa Web Menggunakan Owaspzap




Gambar 1 Owaspzap 1

Disini masukkan web yang akan di analisis disini kami memasukkan web elearning binadarma

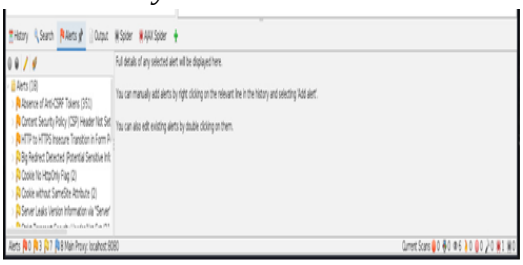
2. Lakukan scan dengan klik attack untuk mengetahui kerentanan web.




Gambar 2 Owaspzap 2

Hasil dari uji coba Automated Scan

3. Kenudian cek alerets untuk mengetahui keamanan *system.*



Gambar 3 Owaspzap 3

Disini terlihat bermacam warna bendera yang menandakan keamanan *system* dari *elearning*

Keterangan Warna XML/HTML Respons

| | |
|---|---|
| Merah | critical yaitu menunjukan kerentanan yang sangat serius yang berpotensi mengekspos data sensitif. |
| oranye | Menunjukkan masalah keamanan yang cukup serius yang dapat menyebabkan akses tidak sah ataupun kebocoran data |
| kuning | Menunjukkan kerentanan yang kurang berbahaya tetapi masih memerlukan perbaikan. |
| hijau | Yang menunjukkan bahwa jaringan tersebut mempunyai Tingkat keamanan yang bagus. |

## 5. PENUTUP

### 5.1 Kesimpulan

Penelitian ini bertujuan untuk menganalisis keamanan *website e-learning* Universitas Bina Darma menggunakan metode *Web Application Security Project ZAP* (OWASP ZAP). Berdasarkan hasil analisis, dapat disimpulkan bahwa *OWASP ZAP* merupakan alat yang efektif dalam mengidentifikasi kerentanan pada aplikasi berbasis *web*, termasuk sistem *e-learning*. Dengan fitur seperti pemindaian otomatis, analisis manual, dan deteksi berbasis OWASP Top 10, OWASP ZAP mampu memberikan gambaran menyeluruh tentang potensi ancaman keamanan yang dihadapi oleh *website e-learning* (Supriadi *et al.*, 2024).

Pada proses analisis, beberapa kerentanan ditemukan, seperti potensi *Cross-Site Scripting (XSS), Security Misconfiguration, dan Broken Authentication.* Kerentanan ini menunjukkan bahwa sistem *e-learning* Universitas Bina Darma memerlukan penguatan dalam beberapa aspek, terutama pada pengelolaan input pengguna, pengaturan keamanan *server*, dan perlindungan data sensitif. Tingkat keparahan dari kerentanan yang ditemukan bervariasi, mulai dari rendah hingga tinggi, dengan beberapa di antaranya berpotensi untuk dieksploitasi oleh pihak yang tidak bertanggung jawab (Zaidan *et al.*, 2023).

Selain itu, validasi hasil pemindaian menunjukkan adanya sejumlah *false positives*, yang menegaskan pentingnya verifikasi manual dalam proses pengujian keamanan. Meskipun OWASP ZAP telah memberikan hasil yang signifikan, validasi manual ini menjadi langkah tambahan yang penting untuk memastikan

akurasi dan relevansi dari laporan kerentanan yang dihasilkan.

Berdasarkan hasil penelitian ini, ditemukan bahwa beberapa langkah mitigasi perlu segera diambil untuk meningkatkan keamanan sistem e-learning Universitas Bina Darma. Langkah-langkah tersebut meliputi penerapan input validation yang lebih ketat untuk mencegah serangan berbasis injection, pengaturan ulang konfigurasi server untuk mengurangi risiko *information leakage*, dan implementasi kebijakan autentikasi serta manajemen sesi yang lebih aman.

Kesimpulannya, analisis dengan *OWASP ZAP* memberikan manfaat besar dalam membantu institusi pendidikan seperti Universitas Bina Darma untuk meningkatkan keamanan sistem informasi mereka. Dengan pemahaman yang lebih baik tentang potensi kerentanan, pengelola sistem dapat mengambil langkah proaktif untuk melindungi data pengguna dan menjaga integritas sistem. Namun, penelitian ini juga menggarisbawahi pentingnya pendekatan yang berkelanjutan, di mana pengujian keamanan perlu dilakukan secara berkala untuk memastikan bahwa sistem tetap terlindungi dari ancaman baru yang terus berkembang.

Sebagai rekomendasi tambahan, institusi disarankan untuk tidak hanya mengandalkan alat otomatis seperti OWASP ZAP, tetapi juga melibatkan tim keamanan untuk melakukan pengujian manual, serta menerapkan pelatihan keamanan bagi pengembang dan administrator sistem. Dengan kombinasi pendekatan teknologi dan manusia, keamanan sistem e-learning dapat lebih terjamin di masa depan.

### 5.2. Saran

Berdasarkan hasil analisis yang dilakukan terhadap *website e-learning* Universitas Bina Darma menggunakan metode OWASP ZAP, berikut adalah beberapa saran yang dapat diterapkan untuk meningkatkan keamanan sistem:

1. Peningkatan Validasi Input
   Diterapkan mekanisme validasi input yang lebih ketat untuk mencegah serangan seperti *SQL Injection* dan *Cross-Site Scripting (XSS)*. Semua input pengguna harus diperiksa dan disanitasi sebelum diproses oleh server, khususnya pada parameter input di formulir dan URL.
2. Penguatan Kebijakan Autentikasi dan Manajemen Sesi
   Terapkan autentikasi berbasis multifaktor (MFA) untuk meningkatkan keamanan akses pengguna.Gunakan token sesi yang kompleks dan tidak dapat ditebak. Pastikan token sesi diperbarui secara berkala dan berakhir setelah periode tidak aktif tertentu (timeout session). Implementasikan logout otomatis setelah periode tidak aktif sebagai langkah perlindungan tambahan.
3. Konfigurasi Keamanan Server yang Lebih Baik
   Pastikan server web menggunakan konfigurasi yang aman, seperti menonaktifkan header yang dapat membocorkan informasi sensitif (contoh: *Server Header*). Terapkan kebijakan Content *Security Policy (CSP)* untuk melindungi aplikasi dari serangan berbasis skrip seperti XSS. Perbarui semua perangkat lunak, *framework*, dan pustaka yang digunakan ke versi terbaru yang bebas dari kerentanan.
4. Peningkatan Keamanan Data Sensitif
   Enkripsi semua data sensitif, baik saat disimpan (*at rest*) maupun saat ditransmisikan (in transit). Gunakan protokol HTTPS dengan sertifikat SSL/TLS yang valid. Hindari penyimpanan data sensitif seperti kata sandi dalam bentuk teks biasa. Kata sandi harus di-hash menggunakan algoritma yang kuat seperti bcrypt atau Argon2.
5. Pengujian Keamanan Berkala
   Lakukan pengujian keamanan secara berkala menggunakan OWASP ZAP dan alat keamanan lainnya, seperti Burp Suite atau Nikto. Hal ini penting untuk memastikan bahwa sistem tetap

terlindungi dari ancaman baru yang terus berkembang.

6. Pelatihan dan Kesadaran Keamanan
   Selenggarakan pelatihan keamanan secara rutin untuk pengembang, administrator sistem, dan pengguna *platform e-learning*. Tingkatkan kesadaran pengguna tentang pentingnya menjaga kerahasiaan informasi login dan menghindari perilaku berisiko, seperti mengklik tautan mencurigakan.

## DAFTAR PUSTAKA

Al'am'yubi, M.R.S.. and Wijayanto, D.. (2023) 'Analisis Sistem Keamanan Website XYZ Menggunakan Framework OWASP ZAP', Jurnal Ilmu Komputer (JUIK), 3(1), pp. 1–5. Available at: https://journal.umgo.ac.id/index.php/juik/index.

Ariyadi, T. et al. (2023) 'Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP', Techno.Com, 22(2), pp. 418–429. Available at: https://doi.org/10.33633/tc.v22i2.7562.

Burhani, L.F. and Priyawati, D. (2024) 'Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes)', JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 9(1), pp. 307–319. Available at: https://doi.org/10.29100/jipi.v9i1.4455.

Delone, M., Pambudi, R. and Karyono, G. (2024) 'Analisis Kesuksesan Pengguna Website E-Learning Menggunakan', 4(3), pp. 948–967.

Dwi Cahyani, D. et al. (2022) 'Analisis Kerentanan Website SMP Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting dan OWASP', INSERT : Information System and Emerging Technology Journal, 2(2), pp. 106–112. Available at: https://doi.org/10.23887/insert.v2i2.42936.

Fathurrahmad and Ester (2020) 'Automatic Scanner Tools Analysis As A Website Penetration Testing', Jurnal Mantik, 4(2), pp. 1138–1144. Available at: https://iocscience.org/ejournal/index.php/mantik.

Febriani, S.A. et al. (2024) 'Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Owasp-Zap Di Universitas Islam Indragiri', Jurnal Sistem Informasi (TEKNOFILE), 2(6), pp. 409–420.

Hasibuan, A.F. and Handoko, D. (2023) 'Analisis Keretanan Website Dengan Aplikasi Owasp Zap', Jurnal Ilmu Komputer dan Sistem Informasi, 2(2), pp. 257–270. Available at: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51.

Jakobsson, A. and Häggström, I. (2022) 'Study of the techniques used by OWASP ZAP for analysis of vulnerabilities in web applications', p. 69. Available at: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1675227&dswid=-4307.

Putra, F.P.E. et al. (2024) 'Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap', Brilliance: Research of Artificial Intelligence, 4(1), pp. 348–355. Available at: https://doi.org/10.47709/brilliance.v4i1.4227.

Rahman, R. et al. (2024) 'PENGUJIAN PENETRASI JARINGAN MENGGUNAKAN OWASP ZAP DAN SQLMAP UNTUK', 1(4), pp. 9–12.

Rizkyudin, M.S., Pradhana, C. and Fitriani, I.M. (2022) 'Garuda2821816', 1(1), pp. 31–36.

Supriadi, D. et al. (2024) 'IMPLEMENTASI VULNERABILITY ASSESSMENT OWASP ( OPEN WEB APPLICATION SECURITY PROJECT ) PADA WEBSITE', 1(4), pp. 232–240.

Victor Ilyas Sugara and I Wayan Sriyasa (2024) 'Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP)', The Indonesian Journal of Computer Science, 13(2), pp. 3315–3327. Available at: https://doi.org/10.33022/ijcs.v13i2.3736.

Zaidan, M. et al. (2023) 'Website Vulnerability Analysis of AB and XY Office in East Java ARTICLE INFO ABSTRACT', Jurnal

Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), 9(2), pp. 455–492. Available at: https://doi.org/10.26555/jiteki.v9i2.26183.