Journal Computer Science & Information System
Volume 5 No 1 (2025) – Maret
e-ISSN: 2776-9690
DOI: http://dx.doi.org/10.53514/jco.v5i1.613

Analisa Sistem Keamanan Web Menggunakan OWASP Zed Attack Proxy (ZAP)

Hendri Alamsyah [*1], Tomy Roynaldi [1], Toibah Umi Kalsum [1]

[1] *Universitas Dehasen*

INFORMASI ARTIKEL

Kata Kunci:
Keamanan Web,
OWASP ZAP,
CMS WordPress,
CMS Drupal

ABSTRAK

Keamanan web sangat penting untuk menjaga integritas dan kerahasiaan data. Penelitian ini menganalisis keamanan dua situs web berbasis CMS WordPress dan Drupal. Pengujian menggunakan OWASP Zed Attack Proxy (ZAP) dengan Authentication Testing, Authorization Testing, dan Session Management Testing. Hasil pengujian menunjukkan bahwa CMS WordPress memiliki celah SQL Injection berisiko tinggi pada http://192.168.10.250/wp-comments-post.php dan 12 celah otorisasi berisiko sedang yang mengarah ke direktori penyimpanan web. Sebaliknya, CMS Drupal tidak ditemukan celah keamanan pada ketiga aspek pengujian. Kesimpulannya, CMS WordPress lebih rentan dibandingkan CMS Drupal, terutama dalam autentikasi dan otorisasi. Oleh karena itu, perlu mitigasi seperti kebijakan keamanan yang lebih ketat, pembaruan sistem berkala, serta penguatan metode autentikasi dan otorisasi untuk mengurangi risiko serangan.

1. PENDAHULUAN

Penggunaan website yang menawarkan kemudahan akses ini banyak orang maupun instansi bahkan organisasi membangun sebuah sistem web server sebagai media untuk menerapkan website. Sebab, penggunaan media informasi seperti website ini dapat meningkatkan mutu dan kualitas suatu instansi ataupun organisasi. Akan tetapi, banyak juga yang belum memperhatikan apakah web server yang dibangun sudah aman atau belum terhadap gangguan ataupun serangan dari pihak lain. Gangguan yang sering terjadi diataranya berupa serangan Malicious Code atau Malware, Vulnerability, dan lain sebagainya.

Dengan melakukan selftest ini, akan diketahui tingkat kerentanan terhadap sebuah website yang ada di web server tersebut. Salah satu metode selftest yang sering digunakan adalah penetration test. Penetration test (pentest) merupakan metode yang efektif untuk menguji kerentanan sistem. Dengan demikian penetration test adalah proses mencoba untuk mendapatkan akses ke dalam sebuah sistem tanpa ada pengetahuan tentang username, password dan akses lainnya. Pengujian terhadap aplikasi web dengan metode penetration testing merupakan metode yang komprehensif mengidentifikasi kerentanan sistem.

Salah satu alat yang banyak digunakan untuk mengidentifikasi dan menganalisis kerentanan pada aplikasi web adalah OWASP Zed Attack Proxy (ZAP). ZAP merupakan alat pengujian penetrasi open-source yang dikembangkan oleh Open Web Application Security Project (OWASP) dan dirancang untuk membantu profesional keamanan dalam menemukan celah keamanan pada aplikasi web(Hasibuan et al., 2023).

Penggunaan ZAP telah terbukti efektif dalam mengidentifikasi berbagai kerentanan keamanan. Misalnya, sebuah penelitian menunjukkan bahwa ZAP dapat mengidentifikasi kerentanan seperti SQL Injection dan kelemahan autentikasi pada aplikasi web (Firman Ashari et al., 2023).

Author's email: hendri.alamsyah@unived.ac.id
**) Corresponding author*

Dengan kemampuan dan fitur yang dimilikinya, OWASP ZAP menjadi alat yang esensial bagi para profesional keamanan untuk memastikan bahwa aplikasi web yang dikembangkan atau digunakan bebas dari kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

2. TEORI DAN PENELITIAN RELEVAN

1) Sistem Keamanan

Sistem keamanan adalah serangkaian kebijakan, prosedur, dan tindakan teknis yang dirancang untuk melindungi aset informasi dari berbagai ancaman, termasuk akses yang tidak sah, gangguan, atau perusakan. Tujuan utama dari sistem keamanan mencakup:

1. Kerahasiaan (Confidentiality): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
2. Integritas (Integrity): Memastikan bahwa informasi tetap akurat dan tidak mengalami perubahan atau manipulasi oleh pihak yang tidak berwenang.
3. Ketersediaan (Availability): Menjamin bahwa informasi dan sistem terkait tersedia untuk digunakan oleh pihak yang berwenang saat diperlukan.

Dengan menerapkan sistem keamanan yang tepat, organisasi dapat memastikan bahwa data mereka tetap aman dan terlindungi dari ancaman keamanan yang muncul. Hal ini melibatkan pengaturan hak akses untuk pengguna dalam basis data, sehingga hanya pengguna yang berwenang yang dapat mengakses data yang disimpan. Selain itu, enkripsi data adalah proses untuk mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang sesuai. Backup dan recovery, di sisi lain, melibatkan proses untuk membuat salinan cadangan data dan memulihkan data yang hilang atau rusak. Terakhir, pengawasan dan monitoring dilakukan untuk memastikan bahwa semua akses ke basis data dicatat dan dipantau untuk mendeteksi potensi ancaman keamanan (Ujung et al., 2023).

2) Kemanan Aplikasi WEB

Keamanan aplikasi web adalah praktik yang berfokus pada perlindungan aplikasi berbasis web dari berbagai ancaman dan serangan siber yang dapat merusak data serta membahayakan pengguna. Tujuan utamanya adalah memastikan integritas, kerahasiaan, dan ketersediaan data dalam lingkungan digital. Seiring dengan kemajuan teknologi, ancaman serangan siber yang semakin canggih menjadikan keamanan aplikasi web sebagai aspek yang sangat krusial (Fatihah & Dinarto, 2024).

3) Firewall

Firewall merupakan sistem keamanan yang dibuat untuk mengamankan sebuah jaringan maupun sistem informasi, sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan maupun pencegahan sehingga aliran data dapat dikendalikan untuk mencegah bahaya atau ancaman yang datang dari jaringan publik (Alamsyah et al., 2018).

4) Website

Website adalah kumpulan halaman yang berisi informasi data digital, seperti teks, gambar, animasi, suara, dan video, yang disediakan melalui koneksi internet sehingga dapat diakses oleh pengguna di seluruh dunia. Halaman-halaman ini dibuat menggunakan bahasa standar seperti HTML dan diterjemahkan oleh web browser untuk ditampilkan dalam bentuk yang dapat dibaca (Permata Sari & Suhendi, 2020).

5) Owasp ZAP

Zed Attack Proxy (ZAP) merupakan aplikasi yang digunakan untuk pengujian penetrasi (pentest) guna mengidentifikasi kerentanan dalam aplikasi web dengan cara yang sederhana.

ZAP menyediakan pemindaian otomatis serta memungkinkan pengguna untuk menemukan kerentanan secara manual menggunakan berbagai alat yang tersedia. Ketika digunakan sebagai server proxy, ZAP memungkinkan manipulasi terhadap semua lalu lintas yang melaluinya, termasuk lalu lintas yang terenkripsi dengan HTTPS. Selain itu, aplikasi ini juga dapat berjalan dalam mode daemon dan dikendalikan melalui REST API. Pada 30 Mei 2015, ZAP dimasukkan ke dalam Radar Teknologi ThoughtWorks pada kategori percobaan. Awalnya, ZAP merupakan hasil pengembangan dari Paros, sebuah proxy untuk pengujian keamanan web. Menurut Simon Bennetts, pemimpin proyek ZAP, pada tahun 2014 hanya sekitar 20% dari kode sumber ZAP yang masih berasal dari Paros (Kusuma A, 2022).

6) Content Management System (CMS)

CMS adalah sebuah aplikasi website yang bersifat generik dalam arti telah memiliki sejumlah fitur yang dapat diaktifkan dan dimanipulasi sesuai kebutuhan pengguna dan dapat digunakan dengan mudah tanpa pemrograman (Dharmawan & Gata, 2020).

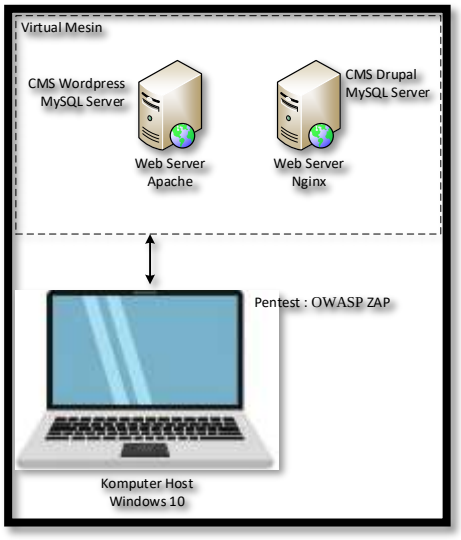
7) SQL Injection

SQL Injection adalah teknik serangan yang mengeksploitasi kerentanan dalam aplikasi yang berinteraksi dengan basis data SQL, di mana penyerang menyisipkan pernyataan SQL berbahaya melalui input pengguna yang tidak divalidasi dengan baik. Serangan ini memungkinkan akses tidak sah ke data, modifikasi, atau bahkan penghapusan data dalam basis data (Perdana Putranto et al., 2022).

3. METODE PENELITIAN

1) Blok diagram Global

Dalam penelitian ini diagram blok global yang di terapkan ini adalah menghubungkan antara komputer web server apache dengan *content management system* (CMS) wordpreess dan web server nginx dengan CMS Drupal. Kedua komputer server tersebut dibuat pada mesin virtual menggunakan virtualbox. Untuk komputer *host* digunakan untuk melakukan penetrasi ke masing-masing server, sehingga akan diketahui celah dari keamanan masing-masing server.



Gambar 1 Diagram Blok Global

2) Prinsip kerja Sistem

Prinsip kerja dalam penelitian ini adalah melakukan analisa terhadap sistem keamanan web server atau khususnya terhadap aplikasi web adalah dengan melakukan penetration test

(pentest), dimana penetration test (pentest) ini merupakan sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah sistem dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan (attack). Hasil dari pentest ini sangat penting sebagai feedback bagi pengelola sistem untuk memperbaiki tingkat keamanan dari sistem yang sudah dilakukan analisa dengan metode pentest. Laporan hasil pentest akan memberikan masukan terhadap kondisi vulnerabilitas sistem sehingga memudahkan dalam melakukan evaluasi dari sistem keamanan pada aplikasi web yang sedang berjalan.

3) Tahapan Kerja Penelitian

Rencana kerja dari analisa sistem keamanan pada web server menggunakan Owasp ZAP adalah sebagai berikut.

Gambar 2 Rancangan Kerja Sistem

Keterangan :

1 Study Literatur merupakan tahan untuk memperlajari apa saja yang diperlukan dalam penelitian ini.
2 Persiapan Alat dan Bahan Mempesiapkan peralatan yang dibutuhakn
3 Instalasi dan Konfigurasi Web Server : Proses yang dilakukan pada tahapan ini adalah melakukan instalasi dan konfigurasi terhadap web server.
4 Instalasi dan Konfigurasi OWASP ZAP : Tahapan ini dilakukan untuk mempersiapkan aplikasi yang akan digunakan untuk melakukan analisa terhadap sistem keamanan aplikasi web.
5 Pengujian dan Analisa: Tahapan ini dilakukan untuk menguji sistem keamanan pada aplikasi web di dalam web server. Apakah berjalan dengan baik ataupun sebaliknya.
6 Hasil Pengujian dan Analisa: Tahapan ini adalah tahapan yang dilakukan untuk menyimpulkan hasil dari pengujian yang dilakukan.
7 Kesimpulan: Pada tahapan ini adalah tahapan untuk menyimpulkan hasil dari penelitian yang telah dilakukan.

4) Perancangan Pengujian

Pengujian ini dilakukan dengan metode blackbox, yaitu sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional dalam sistem saat dioperasikan ,apakah input diterima dengan benar dan output yang dihasilkan telah sesuai dengan yang diharapkan, sehingga dapat membuktikan kebenarannya. Adapun jenis pengujian dan analisa yang dilakukan dapat dilihat pada tabel sebagai berikut:

Tabel 1 Pengujian dan Analisa

No	**Pengujian**	**Pengujian**		**Keterangan**
		Web Server Apache dengan CMS Wordpress	*Web Server* Nginx dengan CMS Drupal	

1.	*Authentication Testing* (Pengujian Autentikasi)
2.	*Authorization Testing* (Pengujian Otorisasi)
3.	*Session Management Testing* (Pengujian Manajemen Sesi)

4. HASIL DANPEMBAHASAN

Dalam penelitian yang penulis lakukan ini, penelitian terfokus pada perbandingan sistem kemanan dua website dengan *Content Management System* (CMS) berbeda serta menggunakan web *server* yang berbeda pula, yang mana dalam penelitian ini penulis menggunakan CMS Wordpress dengan web *server* Apache dan CMS Drupal dengan web *server* Nginx.

Adapun hasil dari implementasi aplikasi web dengan CMS wordpress dan drupal dapat dilihat seperti dibawah ini :

Gambar 3 Web dengan CMS Wordpress

Pada gambar 4.1 diatas, terlihat sebuah website dengan CMS wordpress yang sudah penulis terapkan di web server apache yang dapat diakses secara lokal dengan menggunakan alamat http://192.168.10.250. Untuk hasil aplikasi web dengan CMS drupal adalah sebagai berikut.

Gambar 4 Web dengan CMS Drupal

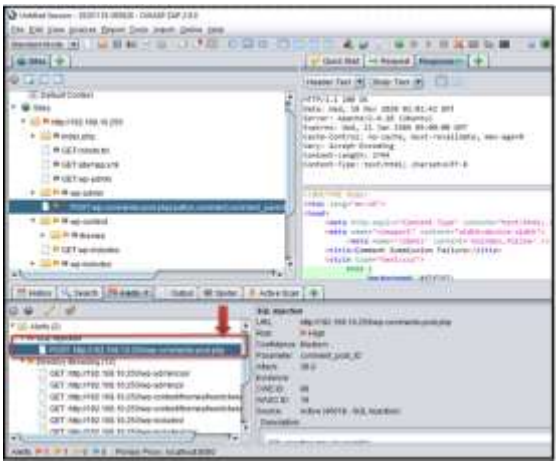
Pada gambar 4.2 diatas, terlihat sebuah website dengan CMS Drupal dengan web server nginx dan database MySQL yang dapat diakses secara lokal menggunakan alamat http://192.168.10.201 yang berada satu jaringan dengan aplikasi web CMS Wordpress.

1) Autentication Testing (Pengujian Autentikasi)

Pengujian ini dilakukan untuk melihat pengujian autentifikasi terhadap web yang penulis gunakan dalam penelitian ini, adapun hasilnya adalah sebagai berikut.

a. CMS Wordpress

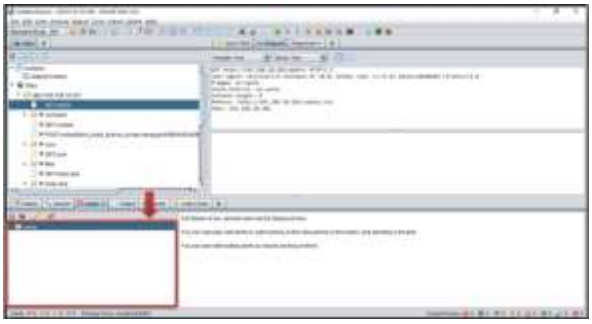
Adapun hasil yang penulis temukan pada saat melakukan analisis sistem keamanan web menggunakan CMS wordpress dengan web server apache ditemukan satu Authentication Testing berupa SQL Injection pada alamat http://192.168.10.250/wp-comments-post.php yang memiliki resiko high (tinggi) seperti yang terlihat pada Gambar 4.3 dbawah.



Gambar 5 Hasil Analisis Autentikasi CMS Wordpress

b. CMS Drupal

Adapun hasil dari analisis yang penulis lakukan pada web dengan CMS drupal, tidak ditemukannya celah Authentication Testing seperti yang terlihat pada Gambar 4.4 dibawah.



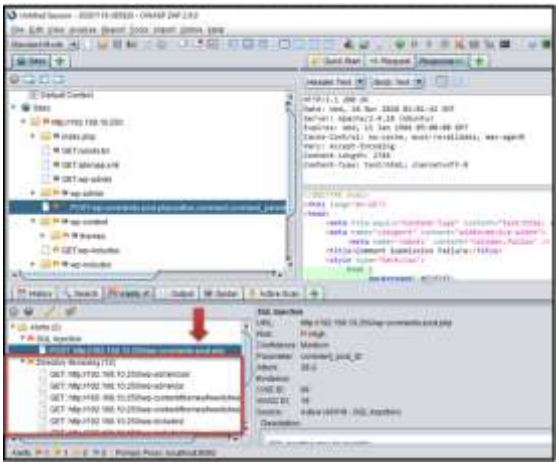
Gambar 6 Hasil Analisis CMS Drupal

2) Authorization Testing (Pengujian Otentikasi)

Pengujian ini dilakukan untuk melihat pengujian otorisasi terhadap web yang penulis gunakan dalam penelitian ini, adapun hasilnya adalah sebagai berikut.

a. CMS Wordpress

Adapun hasil dari analisis terhadap sistem keamanan web berdasarkan Authorization Testing pada aplikasi web dengan CMS worpdpress, ditemukan 12 otorisasi yang beresiko medium yang mengarah langsung ke direktori penyimpanan web seperti yang terlihat pada Gambar 4.5 berikut.



Gambar 7 Hasil Analisis Otorisasi CMS Wordpress

b. CMS Drupal

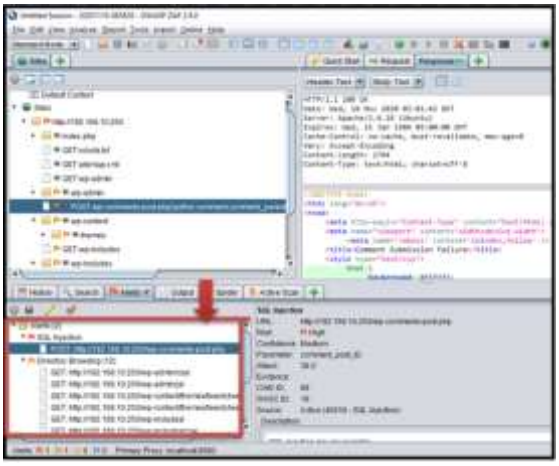
Adapun hasil dari analisis yang penulis lakukan pada web dengan CMS drupal, tidak ditemukannya celah Authorization Testing seperti yang terlihat pada Gambar 4.4 datas.

3) Session Management Testing (Pengujian Manajemen Sesi)

Pengujian ini dilakukan untuk melihat pengujian manajemen sesi terhadap web yang penulis gunakan dalam penelitian ini, adapun hasilnya adalah sebagai berikut.

a. CMS Wordpress

Adapun hasil dari analisis yang penulis lakukan pada web dengan CMS wordpress, tidak ditemukannya celah Session Management Testing seperti yang terlihat pada gambar berikut.



Gambar 8 Hasil Analisa CMS Wordpress

b. CMS Dupal

Adapun hasil dari analisis yang penulis lakukan pada web dengan CMS drupal, tidak ditemukannya celah Session Management Testing seperti yang terlihat pada Gambar 4.4 diatas

A. Hasil Pengujian

Tabel 2 Hasil Pengujian dan Analisa

No	Pengujian	Hasil Pengujian		Keterangan
		***Web Server* Apache dengan CMS Wordpress**	***Web Server* Nginx dengan CMS Drupal**	

1	*Authentication Testing* (Pengujian Autentikasi)	Ditemukan celah *Authentication* berupa *SQL injection* yang beresiko tinggi dan dapat diatasi dengan mengubah nama pengguna *database* yang tidak sama dengan user *web server* sehingga saat dilakukan pungujian yang kedua tidak ditemukan lagi celah keamanan *SQL injection*	Tidak ditemukan celah *Authentication* (Autentikasi)	CMS drupal lebih baik kemanannya dari segi *Authentication* (Autentikasi)
2.	*Authorization Testing* (Pengujian Otorisasi)	Ditemukan celah *Authorization* berupa 12 *directory traversal* yang beresiko medium dan dapat diatasi dengan mengubah nama pengguna *database* yang tidak sama dengan user *web server* sehingga saat dilakukan pengujian sistem keamanan yang kedua celah terhadap *directory traversal* menjadi berkurang yaitu 2 celah saja.	Tidak ditemukan celah *Authorization* (Otorisasi)	Tidak ditemukan celah *Authorization* (Otorisasi)
3.	*Session Management Testing* (Pengujian Manajemen Sesi)	Tidak ditemukan celah *Session Management* (Sesi Manajemen)	Tidak ditemukan celah *Session Management* (Sesi Manajemen)	Tidak ada celah *Session Management* baik pada CMS wordpress maupun CMS drupal

Dari hasil pengujian dan analisa pada table 2, dapat dilihat bahwah web dengan CMS wordpress memiliki celah keamanan berupa Authentication SQL injection dan Authorization berupa directory traversal yang dapat diatasi dengan mengubah nama pengguna database yang tidak sama dengan user pada web server, sedangkan web dengan CMS drupal tidak ditemukan celah apapun. Secara keseluruhan berdasarkan penelitian yang penulis lakukan terhadap web dengan CMS wordpress yang diterapkan pada web server apache dengan database server MySQL dan web dengan CMS drupal yang diterapkan pada web server Nginx dengan database server MySQL yang sama – sama diinstall pada mesin virtual dengan sistem operasi linux ubuntu 16.04 menunjukkkan bahwa web dengan CMS drupal memiliki sistem keamanan lebih baik dari pada web dengan CMS wordpress.

5. KESIMPULAN

Aplikasi owasp zap dapat melakukan an alisis terhadap sistem keamanan web dengan menampilkan celah yang ada pada sebuah aplikasi web.

Web dengan CMS wordpress memiliki celah kemanan berupa Authentication Testing SQL injection dan Authorization Testing berupa directory traversal yang dapat diatasi dengan mengubah nama pengguna database yang tidak sama dengan user pada web server, sedangkan web dengan CMS drupal tidak ditemukan celah apapun.

Web dengan CMS drupal memiliki sistem keamanan lebih baik dari pada web dengan CMS wordpress.

DAFTAR RUJUKAN

Alamsyah, H., Riska, & Al Akbar, A. (2018). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System. JOINTECS (Journal of Information Technology and Computer Science) , 3(1), 17–24.

Dharmawan, R., & Gata, G. (2020). Penerapan Aplikasi Penjualan Online (E-Commerce) Menggunakan Content Management System Wordpress Pada Toko Jaksquare. Jurnal IDEALIS, 3(1), 132–138.

Fatihah, A., & Dinarto, P. (2024). Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ. INNOVATIVE: Journal Of Social Science Research, 4, 4536–4549.

Firman Ashari, I., Rizta Anugrah P, L., Andintya W, N., Denira, S. T., Teknik, J., Fisis, S., Produksi, J. T., Industri, D., Sumatera, T., & Selatan, L. (2023). Analisis Celah Keamanan Dan Mitigasi Website E-Learning Itera Menggunakan Owasp Zed Attack Proxy (Zap) Vulnerability And Mitigation Analysis Of The Itera E-Learning Website Using Owasp Zed Attack Proxy (ZAP). DINAMIKA REKAYASA, 9(1), 29–35. http://dinarek.unsoed.ac.id

Hasibuan, A. F., Tommy, & Handoko, D. (2023). Analisis Keretanan Website Dengan Aplikasi Owasp Zap. Jurnal Ilmu Komputer Dan Sistem Informasi (JIRSI), 2(2), 257–270.

Kusuma A, G. H. (2022). Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik. Jurnal Teknologi Informasi, 16(2), 178–186.

Perdana Putranto, D., Jayanta, & Hananto, B. (2022). Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack. JURNAL INFORMATIK, 18(3), 230–238.

Permata Sari, A., & Suhendi. (2020). Rancang Bangun Sistem Informasi Pengelolaan Talent Film Berbasis Aplikasi Web. Jurnal Informatika Terpadu, 6(1), 29–37. https://journal.nurulfikri.ac.id/index.php/JIT

Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. JISKA: Jurnal Sistem Informasi Dan Informatika, 1(2), 44. http://jurnal.unidha.ac.id/index.php/jteksis