Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025
http://doi.org/10.33395/remik.v9i2.14561
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Analisis Keamanan Sistem Informasi Menggunakan Metode Vulnerability Assesment pada Aplikasi Web Karangasem.go.id

[1]I Made Adi Surya Permana, [2] I Gede Putu Krisna Juliharta, [3]I Gede Juliana Eka Putra
[1, 2, 3]Universitas Primakara
Denpasar, Indonesia

[1]suryade61@gmail.com, [2]krisna@primakara.ac.id, [3]gedejep@primakara.ac.id

*Penulis Korespondensi
Diajukan : 11/02/2025
Diterima : 20/03/2025
Dipublikasi : 03/04/2025

ABSTRAK
Keamanan sistem informasi di era digital, khususnya pada aplikasi web, menjadi sangat penting mengingat seringnya serangan siber. Penelitian ini bertujuan menganalisis keamanan sistem informasi Website Pemerintah Kabupaten Karangasem melalui metode Vulnerability Assessment. Metode ini dipilih karena efektif mengidentifikasi celah keamanan secara proaktif. Hasil Vulnerability Assessment menunjukkan berbagai potensi celah keamanan pada website tersebut, memberikan pemahaman mendalam tentang kelemahan sistem. Celah tersebut meliputi kerentanan teknis pada perangkat lunak, masalah konfigurasi server, seperti cross-site scripting (XSS), SQL injection, dan path traversal, serta kelemahan otentikasi dan otorisasi. Penelitian ini diharapkan menjadi dasar bagi Pemerintah Kabupaten Karangasem untuk meningkatkan keamanan sistem informasi aplikasi web mereka. Rekomendasi perbaikan difokuskan pada penambalan kerentanan, penguatan otentikasi dan otorisasi, serta implementasi firewall dan sistem deteksi intrusi. Pelatihan keamanan siber bagi staf pengelola website juga penting.Melalui metode Vulnerability Assessment, penelitian ini memberikan pemahaman mendalam tentang keamanan sistem informasi Website Pemerintah Kabupaten Karangasem. Pentingnya melakukan Vulnerability Assessment secara berkala sebagai bagian dari strategi keamanan informasi yang komprehensif juga ditekankan. Dengan demikian, Pemerintah Kabupaten Karangasem dapat meningkatkan ketahanan sistem informasinya terhadap serangan siber. Hasil penelitian ini diharapkan menjadi acuan bagi pemerintah daerah lain dalam meningkatkan keamanan sistem informasi. Selain itu, penelitian ini juga menggarisbawahi pentingnya pemantauan berkelanjutan dan pembaruan sistem secara teratur untuk memastikan keamanan yang optimal.

Kata Kunci: Aplikasi Web, Keamanan Sistem Informasi, Pemerintahan Kabupaten Karangasem, *Vulnerability Assesment*

I. PENDAHULUAN
Sistem informasi merupakan bagian penting dari berbagai proses bisnis dan kegiatan dalam kehidupan saat ini di era digital yang semakin maju. Tidak jarang sistem informasi tersebut menyimpan banyak data penggunanya bahkan data yang bersifat pribadi seperti nomor telepon, *mobile banking* dan lainnya (Ericka & Prakasa, 2020). Sistem informasi berbasis aplikasi web dapat mengelola komunikasi, transaksi bisnis, dan data sensitif. Namun, keberadaan aplikasi web juga meningkatkan potens serangan keamanan yang cukup serius. Karena aplikasi web mudah diakses oleh pengguna di seluruh dunia, serangan keamanan aplikasi web seringkali menjadi sasaran utama.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i2.14561 p-ISSN : 2541-1332

Serangan seperti SOL *injection*, *cross-site scripting* (XSS), dan serangan terhadap sesi pengguna adalah contoh potensi ancaman terhadap aplikasi web (Aryapranata, 2020). Serangan ini dapat mencuri data sensitif, menyalahgunakan informasi, dạn merusak sistem. Hal ini bisa dicegah dengan melakukàn pengamanan dengan cara menemukan celah keamanan di sebuah sistem informasi aplikasi web.*Vulnerability asessment* merupakan proses indentifikasi, evaluasi dan pemahaman potensi kerentanan atau kelemahan yang terdapat di dalam sistem komputer, jaringan, atau perangkat lunak. Tujuan dari vulnerability assessment adalah untuk mengidentifikasi area yang memiliki kerentananan terhadap serangan dan risiko keamanan, sehingga tindakan pencegahan dan perbaikan dapat diambil untuk mengurangi risiko keamanan. Ini melibatkan pemindaian sistem, pengujian kelemahan dan analisis untuk mengidentifikasi potensi resiko keamanan pada aplikasi web yang di uji. Keamanan sistem informasi sangat penting untuk dijaga dari berbagai ancaman, baik yang berasal dari dalam maupun luar sistem. Ancaman-ancaman ini dapat mengganggu stabilitas sistem dan berasal dari berbagai sumber, seperti individu, kelompok, organisasi, atau bahkan mekanisme tertentu. Jika tidak ditangani dengan baik, ancaman ini dapat menyebabkan kerusakan dan gangguan pada informasi yang disimpan dalam sistem. Oleh karena itu, penting untuk memahami dan memprediksi potensi ancaman sebelum terjadi serangan. Dengan prediksi ancaman yang akurat, langkah-langkah pencegahan yang tepat dapat diambil untuk meminimalkan risiko ketidakstabilan sistem akibat serangan (Harahap & Zufria, 2024).

Pada penelitian ini cara yang digunakan dalam melakukan analisis keamanan sistem informasi adalah vulnerability scanning. *Vulnerability scanning* merupakan propses yang digunakan untuk mengindentifikasi kerentanan atau kelemahan dalam sebuah sistem komputer, jaringan atau perangkat lunak yang melibatkan penggunaan perangkat lunak pemindaian dan pengujian terhadap potensi masalah keamanan seperti kesalahan konfigurasi, perangkat lunak yang belum diperbaharui dan kerentanan lainnya. Hasil pemindaian ini digunakan untuk membantu mengambil langkah-langkah pencegahan atau perbaikan yang dapat mengurangi resiko tersebut. Kabupaten Karangasem merupakan kabupaten yang terletak di bagian timur pulau bali. K abupaten karangasem memiliki website yang berisikan banyak informasi seperti Profil, Pemerintahan, Bank Data, Informasi, Berita Terkini dan Artikel. Permasalahan yang ditemukan pada website pemerintahan kabupaten karangasem adalah sempat terjadi hacking yang membuat situs website ini diretas dan diambil alih oleh hacker. Solusi dari permasalahan di atas adalah dengan melakukan analisis celah keamanan pada website pemerintahan kabupaten karangasem. Pada penelitian ini penulis akan melakukan analisis keamanan web pemerintahan karangasem dengan menggunakan metode *vulnerability assesment*.

II. STUDI LITERATUR

Penelitian Terdahulu

Penelitian dari Muhammad Aziz pada tahun 2021 yang berjudul "*Vulnerability Assesment* Untuk Mencari Celah Keamanan Web Aplikasi *E-Learning* Pada Universitas XYZ". Dengan kesimpulan yaitu, dalam melakukan evaluasi keamanan terkait kerentanan Web Aplikasi *E-Learning* Pada Universitas XYZ dapat menggunakan *tool nessus*, hal ini dibuktikan dengan hasil *vulnerability scanning* menggunakan *tool nessus* yang dapat memberikan daftar kerentanan, penjelasan di setiap kerentanan, dampak dari kerentanan, serta rekomendasi untuk mengatasi kerentanan yang telah ditemukan (Aziz, 2021).

Penelitian berikutnya dari Alfin Syarifuddin Syahab, dkk pada tahun 2023 dengan judul artikel yaitu "Penggunaan *Wireshark* dan *Nessus* Untuk Analisis SSL/TLS Pada Keamanan Data Pengguna Website". Dengan Kesimpulan sebagai berikut Website BMKG daerah X telah menerapkan enkripsi data yang kuat menggunakan TLS 1.2 dan SHA256. Namun, pemindaian kerentanan menemukan tiga potensi celah keamanan terkait SSL/TLS yang perlu segera ditangani untuk meningkatkan keamanan website secara keseluruhan (Syahab et al., 2023).

Penelitian dari Alif Muhammad Akmal, dkk pada tahun 2023 dengan judul artikel yaitu "Analisis Keamanan *Website* Universitas Singaperbangsa Karawang Menggunakan Metode *Vulnerability Assesment*". Dengan kesimpulan sebagai berikut pengujian pada aplikasi Web perpus Unsika menggunakan *tools nmap* menemukan kebocoran informasi yang sensitif kaarena sistem kontrolnya yang dapat mengakses sistem informasi tanpa adanya proses autorisasi (Akmal A,

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i2.14561 p-ISSN : 2541-1332

2023).

Penelitian dari Arief Budiman, dkk Pada tahun 2021 yang berjudul "Analisis Celah Keamanan Aplikasi Web *E-Learning* Universitas ABC Dengan *Vulnerability Assesment*". Dengan Kesimpulan sebagai berikut Sistem *E-Learning* Universitas ABC diharsukan melakukan perbaikan dan evaluasi sistem mereka, karena sesuai dengan hasil penelitian yang menunjukkan *Overall* (keseluruhan) Risk Level Web Aplikasinya berada pada level *High* (Budiman et al., 2021).

Penelitian berikutnya yaitu dari Muhammad Abdul Muin dkk pada tahun 2020, dengan judul "*Campus Website Security Vulnerability Analysis Using Nessus*". Memliki Kesimpulan sebagai berikut menganalisis keamanan sistem dengan tools Nessus dan ditemukan terdapat di 3 web yang di uji terdapat kebocoran keamanan (Muhammad Abdul Muin et al., 2020).

III. METODE

Metode Penelitian

Dalam penelitian ini menggunakan metode vulnerability assessment terhadap aplikasi web yang digunakan. *Vulnerability Assessment* merupakan upaya untuk mencari dan menemukan kelemahan pada sistem atau jaringan komputer. Tujuannya adalah untuk mengantisipasi potensi serangan dengan mengidentifikasi kerentanan dan melakukan tindakan pencegahan yang diperlukan (Wahyudin, 2024).

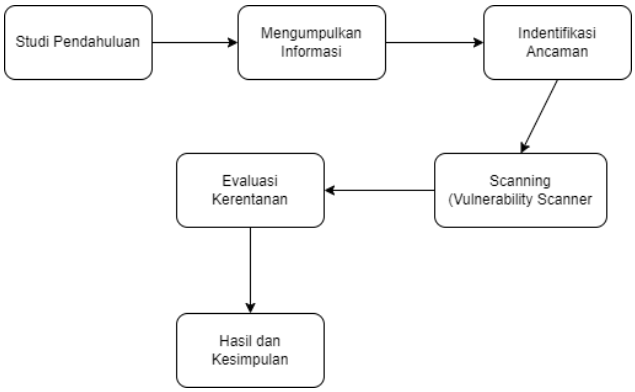
Jenis Data

Dari penelitian ini ada beberapa macam data yang digunakan oleh penulis dalam menyelesaikan perumusan masalah pada penulisan ini adalah menggunakan data kuantitatif dan kualitatif.

Sumber Data

Dalam penelitian ini menggunakan sumber data yaitu data primer dan data sekunder. Data primer diperoleh dari hasil wawancara dan observasi secara langsung ke lapangan. Sedangkan data sekunder dirujuk pada hasil pustaka yang dilakukan oleh penulis.

Alur Penelitian



Gambar 1 Alur Penelitian

IV HASIL DAN PEMBAHASAN

Mencari IP *Address*

Tahap selanjutnya adalah melakukan konfigurasi IP yang aktif dengan *Angry* IP *Scanner* sesuai dengan kebutuhan dan tujuan yang ingin dicapai. IP Address dari aplikasi web karangasemkab.go.id adalah

Lookup Hostname: karangasemkab.go.id
Lookup IPv4 Address: 103.160.161.69

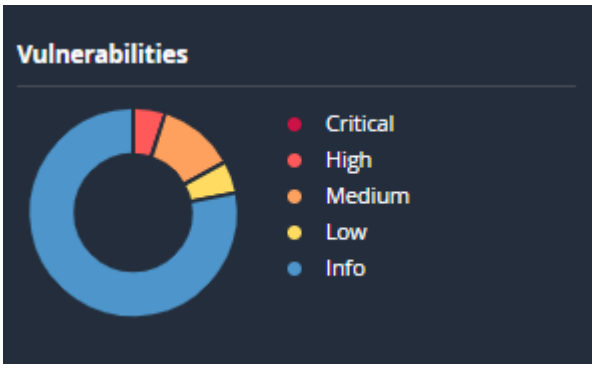
Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025
http://doi.org/10.33395/remik.v9i2.14561
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Pelaksanaan *Scan*

Setelah mendapatkan IP *Address* dari aplikasi web karangasemkab.go.id proses selanjutnya adalah melaksanakan scan dengan Framework NIST SP 800-115 terhadap sistem atau jaringan yang dituju menggunakan tools yang sudah dipilih sebelumnya. *Framework* yang digunakan di dalam *website* ini adalah bahasa pemograman PHP serta untuk hosting dan servernya menggunakan cPanel. cPanel ini sering digunakan karena menyederhanakan banyak tugas administrasi server yang biasanya memerlukan pengetahuan teknis mendalam. Dengan antarmuka yang ramah pengguna, bahkan mereka yang tidak memiliki pengalaman dalam manajemen server dapat dengan mudah mengelola situs web mereka.

Hasil Analisis Dengan Nessus

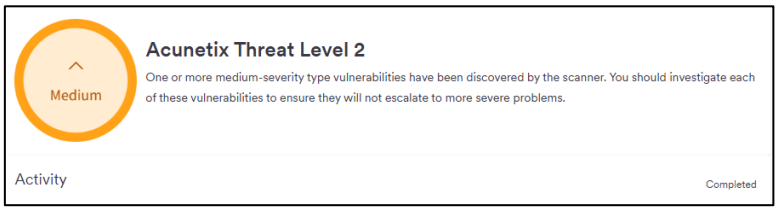
Nessus telah mengidentifikasi beberapa kerentanan dengan tingkat *High*, *Medium*, dan *Low* yang ada pada aplikasi web karangasemkab.go.id. Berikut hasil dari *scanning* yang telah dilakukan:



Gambar 2 Diagram Kerentanan

Hasil Analisis Dengan *Acunetix*

Acunetix telah menemukan beberapa kerentanan pada aplikasi web yang berjalan dalam sistem dengan tingkat resiko kategori *Medium* dan *Low*. Berikut hasil dari scanning menggunakan Acunetix :



Gambar 3 Level Kerentanan yang di dapatkan

Hasil Analisis Dengan Nmap

Nmap adalah alat yang digunakan untuk memindai *port* yang terbuka dari IP publik atau domain. Alat ini juga dapat digunakan untuk melihat versi dari *port* yang terbuka (Linggih Jaelani et al., 2023). Nmap memberikan gambaran yang komprehensif tentang topologi jaringan dan layanan yang aktif. Nmap menemukan 12 port terbuka dari 1000 port yang didapatkan. Berikut hasil yang didapatkan dari scanning menggunakan Nmap:

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025
http://doi.org/10.33395/remik.v9i2.14561
e-ISSN : 2541-1330
p-ISSN : 2541-1332

```
Scanning ipv4-69-161-160-103-as141594.karangasemkab.go.id (103.160.161.69) [1000 ports]
Discovered open port 53/tcp on 103.160.161.69
Discovered open port 995/tcp on 103.160.161.69
Discovered open port 443/tcp on 103.160.161.69
Discovered open port 143/tcp on 103.160.161.69
Discovered open port 3306/tcp on 103.160.161.69
Discovered open port 110/tcp on 103.160.161.69
Discovered open port 587/tcp on 103.160.161.69
Discovered open port 80/tcp on 103.160.161.69
Discovered open port 993/tcp on 103.160.161.69
Discovered open port 21/tcp on 103.160.161.69
Discovered open port 23/tcp on 103.160.161.69
Discovered open port 23/tcp on 103.160.161.69
Discovered open port 993/tcp on 103.160.161.69
Discovered open port 21/tcp on 103.160.161.69
Discovered open port 80/tcp on 103.160.161.69
Discovered open port 465/tcp on 103.160.161.69
Discovered open port 465/tcp on 103.160.161.69
Discovered open port 465/tcp on 103.160.161.69
Completed SYN Stealth Scan at 23:17, 18.01s elapsed (1000 total ports)
```

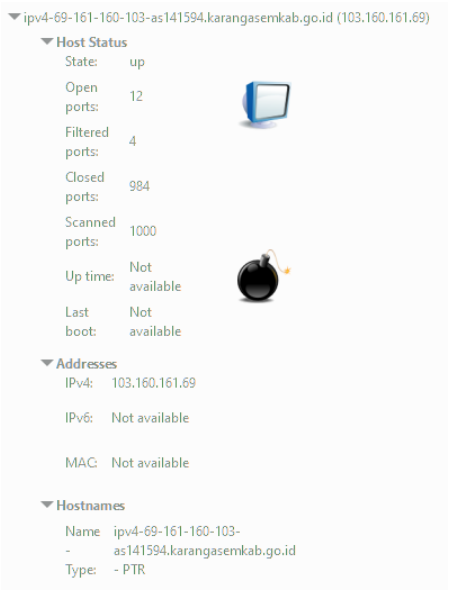
Gambar 4 Proses *Scanning* Dengan Nmap

Selanjutnya setelah proses *scanning* selesai, Nmap menemukan 12 port yang terbuka berikut hasil dan keterangan dari port yang didapatkan:

Port	Protocol	State	Service	Version
21	tcp	open	ftp	Pure-FTPd
23	tcp	open	telnet	
25	tcp	filtered	smtp	
53	tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
139	tcp	filtered	netbios-ssn	
143	tcp	open	imap	Dovecot imapd
443	tcp	open	http	Apache httpd
445	tcp	filtered	microsoft-ds	
465	tcp	open	smtp	Exim smtpd 4.96.2
587	tcp	open	submission	
993	tcp	open	imap	Dovecot imapd
995	tcp	open	pop3	Dovecot pop3d
3306	tcp	open	mysql	MySQL 5.7.39
5678	tcp	filtered	rrac	

Gambar 5 Hasil *Scanning* dengan Nmap

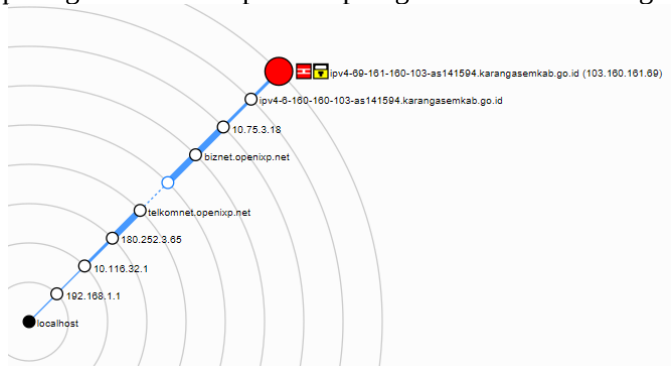
Berikutnya pada gambar 6 merupakan *Host* Detail dari IP *Address* yang sudah di *scanning*:



Gambar 6 *Host Details*

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 2, April 2025
http://doi.org/10.33395/remik.v9i2.14561
e-ISSN : 2541-1330
p-ISSN : 2541-1332

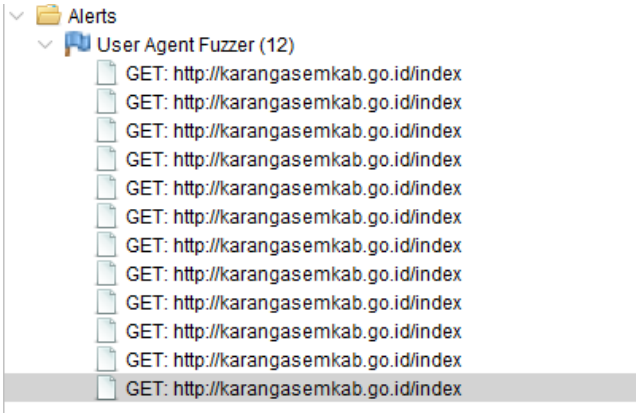
Selanjutnya pada gambar 7 merupakan topologi dari *website* karangasemkab.go.id



Gambar 7 Topologi Jaringan website karangasem.kab.id

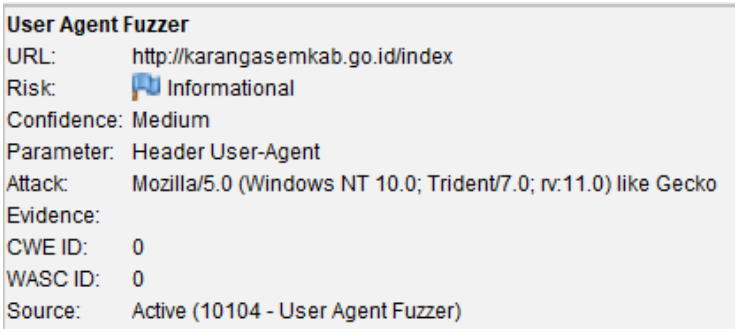
Hasil Analisis dengan ZAP (Zed Attack Proxy)

ZAP telah melakukan serangkaian *scanning* dan menemukan celah yang dikategorikan informational dengan parameter *Head User-Agent* dengan keterangan "*Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response*." Berikut hasil scanning dari ZAP:



Gambar 8 Alert yang didapatkan

Selanjutnya pada gambar 4.4 menunjukan deskrispi dari hasil kerentanan yang didapatkan oleh ZAP (Zed Attack Proxy).



Gambar 9 Deskripsi dari kerentanan yang didapatkan

V. KESIMPULAN

Menyoroti pentingnya sistem informasi dalam kehidupan sehari-hari, terutama di era digital saat ini. Sistem informasi, terutama yang berbasis aplikasi web, menyimpan banyak data sensitif yang rentan terhadap serangan keamanan. Untuk mengatasi ancaman ini, diperlukan langkah-langkah keamanan yang tepat, seperti vulnerability assessment untuk menemukan dan memperbaiki celah keamanan.

Metode *vulnerability assessment* yang digunakan dalam penelitian ini telah terbukti efektif dalam mengidentifikasi kelemahan dan potensi risiko keamanan pada aplikasi web. Pemindaian kerentanan ini melibatkan identifikasi, evaluasi, dan analisis sistem untuk menemukan kerentanan seperti kesalahan konfigurasi dan perangkat lunak yang belum diperbarui. Hasil dari pemindaian ini membantu dalam mengambil langkah-langkah pencegahan dan perbaikan untuk mengurangi risiko serangan keamanan.

Penelitian ini dilakukan pada website pemerintah Kabupaten Karangasem yang pernah mengalami serangan peretasan. Dengan melakukan *vulnerability assessment*, penelitian ini berhasil mengidentifikasi celah keamanan yang ada dan memberikan rekomendasi perbaikan. Tujuan utama dari penelitian ini adalah untuk meningkatkan keamanan aplikasi web, sehingga data sensitif dan informasi penting dapat terlindungi dengan lebih baik dari potensi serangan.

VI. REFERENSI

Akmal A, H. N. S. A. (2023). *Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment* (Vol. 4).

Aryapranata, A. (2020). Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id. *Jurnal Esensi Infokom*, *4*.

Aziz, M. (2021). VULNERABILITY ASSESMENT UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI E-LEARNING PADA UNIVERSITAS XYZ. In *JECSIT* (Vol. 1, Issue 1).

Budiman, A., Ahdan, S., & Aziz, M. (2021). ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT. In *Jurnal Komputasi* (Vol. 9, Issue 2).

Ericka, J., & Prakasa, W. (2020). Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. *Jurnal Ilmiah Teknologi Informasi Asia*, *14*(2).

Harahap, P., & Zufria, I. (2024). Analisis Keamanan Pada Website UPM SAINTEK UIN-SU Medan Menggunakan Metode Vulnerability Assesment. *FEBRUARI*, *2*(1), 10–20. https://doi.org/10.55537/cosmic

Linggih Jaelani, W., Khoirunnisa, F., Studi Teknik Informatika, P., Tinggi Teknologi Bandung, S., & Adhirajasa Reswara Sanjaya, U. (2023). *PENETRATION TESTING WEBSITE DENGAN METODE BLACK BOX TESTING UNTUK MENINGKATKAN KEAMANAN WEBSITE PADA INSTANSI (REDACTED)*. *05*.

Muhammad Abdul Muin, st, Kapti, nd, Tri Yusnanto, th, Bina Patria, S., Managenent, I., & tengah, J. (2020). Campus Website Security Vulnerability Analysis Using Nessus. In *International Journal of Computer and Information System (IJCIS) Peer Reviewed-International Journal* (Vol. 03). https://ijcis.net/index.php/ijcis/index

e-ISSN : 2541-1330
p-ISSN : 2541-1332

Syahab, A. S., Ujianto, E. I. H., & Rianto, R. (2023). PENGGUNAAN WIRESHARK DAN NESSUS UNTUK ANALISIS SSL/TLS PADA KEAMANAN DATA PENGGUNA WEBSITE. *JIKA (Jurnal Informatika)*, *7*(2), 183. https://doi.org/10.31000/jika.v7i2.7566

Wahyudin, K. H. R. D. S. (2024). Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales. *Computer Science (CO-SCIENCE)*, *4*.