Populer: Jurnal Penelitian Mahasiswa
Volume 3, Nomor 4, Tahun 2024
e-ISSN: 2963-5306- p-ISSN: 2962-116X, Hal 255-264
DOI: https://doi.org/10.58192/populer.v3i4.2805
Available Online at: https://journal.unimar-amni.ac.id/index.php/Populer

Evaluasi Keamanan Website dengan Menggunakan Metode NIST SP 800-115

Finka Mambo[1*], Dwi Yuniarto[2], David Setiadi[3]
[1,2,3]Program Studi Informatika, Fakultas Teknologi Informasi Universitas Sebelas April, Indonesia

Alamat: Jl. Angkrek Situ No.19, Situ, Kec. Sumedang Utara, Kabupaten Sumedang, Jawa Barat 45323
**Korespondensi penulis: finma1216@gmail.com*

Abstract*. The development of technology is increasing along with the passage of time where all users have to learn the growing technology. With the increasing development of the threat in internet users will increasingly be cyber attacks by stealing data or personal information through the website. It is necessary to conduct security vulnerability testing on the website to reduce the threat of cyber attacks by providing solutions that can be used as a measurement tool for the level of danger to improve the existing security on the website. The purpose of the study is to find out what vulnerabilities exist on the website of the Faculty of Information Technology at Sebelas April University and analyze the impact that occurs if the threat exists on the website and provide solutions to the method used by NIST SP 800-115 which consists of 4 stages, namely planning, discovery, attack, reporting. Based on the results of the scanning carried out to get 11 vulnerabilities and from the test results have not found vulnerabilities so it is still safe because it has not got vulnerabilities on the website. This researcher advises to conduct retesting as well as exploration of other methods to find vulnerabilities.*

Keywords*: Website, Security, Data, NIST SP 800-115.*

Abstrak. Perkembangan teknologi yang semakin meningkat seiring dengan berjalanya waktu dimana semua pengguna harus mempelajari teknologi yang semakin berkembang. Dengan perkembangan yang semakin meningkat maka ancaman dalam pengguna internet akan semakin meningkat akan serangan siber dengan mencuri data atau informasi peribadi melalui website. Maka perlu dilakukan pengujian kerentanan keamanan pada website untuk mengurangi ancaman dari serangan siber dengan memberikan solusi yang dapat digunakan sebagai alat pengukuran akan tingkatan bahaya untuk memperbaiki keamanan yang ada pada website. Tujuan penelitian mencari apa saja kerentanan yang ada pada website Fakultas Teknologi Informasi pada Universitas Sebelas April dan menganalisis dampak yang terjadi jika ancaman tersebut ada pada website dan memberikan solusi dengan metode yang digunakan NIST SP 800-115 yang terdiri dari 4 tahapan yaitu *planning, discovery, attack, reporting*. Berdasarkan hasil *scanning* yang dilakukan mendapatkan 11 kerentanan serta dari hasil pengujian belum ditemukan kerentanan sehingga masih dibilang aman karena belum mendapatkan kerentanan pada website tersebut. Penelitian ini memberi saran untuk melakukan pengujian ulang serta eksplorasi metode lain untuk menemukan kerentanan.

Kata Kunci: Website, Keamanan, Data, NIST SP 800-115.

1. LATAR BELAKANG

Perkembangan teknologi yang semakin meningkat seiring dengan berjalanya waktu dimana semua pengguna harus mempelajari teknologi yang terus berkembang. Hampir semua kegiatan atau bahkan aktivitas sehari-hari menggunakan internet sebagai penunjang keperluan. Seperti kegiatan yang ada di dalam rumah, kantor, hingga sekolah bahkan di kegiatan bertransaksi atau bahkan sekedar mencari data informasi sekarang dengan menggunakan internet. Website merupakan hal yang penting dalam melakukan kegiatan dimana komponen

Received November 15, 2024; Revised Desember 02, 2024; Accepted Desember 20, 2024; Published Desember 23, 2024

yang terdapat di dalamnya berupa teks, gambar, serta suara yang membuat menarik perhatian para pengguna untuk menggunakannya (Mitra Purba et al., 2022). Dengan perkembangan yang semakin meningkat maka ancaman dalam pengguna internet akan semakin meningkat dari serangan siber dengan mencuri data atau informasi peribadi melalui website. Informasi yang ada di website juga harus dapat di akses oleh penanggung jawab yang menjamin akan kerahasian data serta keamanan (Ary et al., n.d.). Maka perlu dilakukan uji kerentanan keamanan pada website untuk mengurangi ancaman dari serangan siber dengan memberikan solusi yang dapat digunakan sebagai alat pengukuran akan tingkatan bahaya untuk memperbaiki keamanan yang ada pada website (Thurfah Afifa Rosaliah & Hananto, 2021).

Pada studi yang akan digunakan sebagai penelitian yaitu website yang ada di Fakultas Teknologi Informasi pada Universitas Sebelas April. Dimana pada website tersebut berisikan akan informasi tentang kegiatan yang ada di fakultas serta akan segala sistem yang ada. Permasalahan yang sering banyak muncul pada perguruan tinggi yaitu kurangnya perhatian akan perawatan dari segi keamanan. Jenis serangan yang akan muncul jika sistem informasi tidak memiliki keamanan yang kuat yaitu, SQL *injection, XSS, ransomware, phishing* (Sulaeman & Takwim, n.d.).

Hasil penelitian ini akan berfokus pada pengujian keamanan yang akan dilakukan pada Fakultas Teknologi Informasi (fti.unsap.ac.id). Dengan melakukan penetration testing yang digunakan untuk menemukan kerentanan pada jaringan atau sistem dengan hasil yang menjelaskan rekomendasi perbaikan (Elanda & Lintang Buana, 2021). Tujuan penelitian ini untuk mencari kerentanan yang ada di dalam website dan melakukan analisis apa saja dampak yang ada jika ancaman tersebut ada di dalam website dengan metode yang digunakan NIST SP 800-115 yang terbagi menjadi 4 tipe dalam melakukan pengujian terdiri dari *planning, discovery, attack, reporting*.

2. KAJIAN TEORITIS

Website atau web merupakan halaman yang dihubungkan pada sebuah nama domain melalui internet yang akan diakses dari segala pengguna yang ada di dunia secara luas pada beranda browser dengan nama yang unik disebut URL di situs web. Ciri yang umum dan mendasar dari sebuah website dengan mendapatkan informasi atau data yang bersifat sama. Serta website juga sering digunakan oleh pengguna dalam melakukan aktivitas sehari-hari dengan memberikan kemudahan. Namun dari semua kemudahan yang diberikan sering digunakan untuk melakukan kejahatan dengan mencuri data pengguna yang ada pada website. Yang berdampak negatif baik dari segi pengguna hingga organisasi maupun perusahaan dengan

meletakkan virus didalam website untuk mempermudah melakukan kejahatan (Thurfah Afifa Rosaliah & Hananto, 2021).

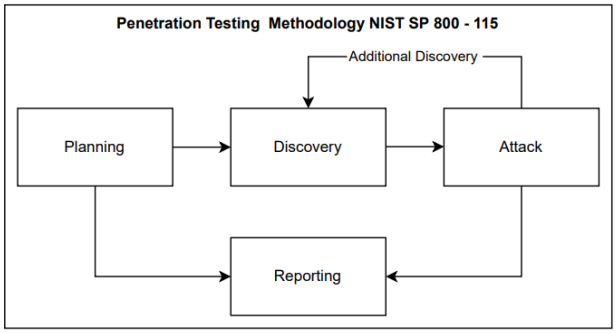
Keamanan data didalam website sangatlah penting untuk dilakukan untuk menghindari kejahatan dengan perkembangan yang semakin meningkat dengan cara penetration testing menggunakan metode untuk melakukan pengujian atau simulasi penyerangan di website untuk menemukan celah keamanan yang dapat dilakukan dengan menggunakan tools yang ada pada perangkat lunak maupun dilakukan manual (Purnomo & Chusyairi, 2024).

Ada banyak ancaman yang untuk dilakukan secara umum pada website seperti melakukan serangan SQL injection, cross-site scripting (XSS), dan distributed denial-of-service (DDoS). Dimana para pengembang website harus menerapkan keamanan terbaik untuk memvalidasi input, penggunaan enkripsi, serta melakukan pembaruan pada perangkat lunak secara rutin (Silaban & Wijaya, n.d.).

Ada beberapa penelitian menggunakan metode untuk melakukan tahapan pengujian seperti OWASP sebagai acuan untuk rekomandasi untuk setiap temuan pada kerentanan atau ancaman yang ada di dalam website dengan yang disusun berdasarkan level kerentanan (Darojat et al., 2022). Bahkan untuk hasil dari penelitian ini akan rekomendasikan perbaikan untuk menjaga keamanan di website dengan menggunakan metode NIST SP 800 – 115 (Raazi et al., 2024).

3. METODE PENELITIAN

Penelitian menggunakan penetration testing serta yang mengacu pada kerangka kerja *National Institute Of Standards and Technology* (NIST) dengan kode NIST SP 800-115 dengan 4 tahapan yang ada pada gambar 1.



Sumber: (Raazi et al., 2024)

Gambar 1. Tahap Penelitian

Penjelasan dari setiap tahapan yang ada pada metode NIST SP 800-115 sebagai berikut.

a. *Planning*, merupakan tahapan awal dalam melakukan pengujian serta sebagai persetujuan kepada pihak yang mengelola sistem. Serta melakukan penjelasan mengenai ruang lingkup dalam penelitian dengan melakukan *scanning* dengan menggunakan metode NIST SP 800-115 yang telah dijelaskan pada pendahuluan (Darojat et al., 2022).
b. *Discovery*, merupakan tahapan yang di bagi menjadi 2 tipe yaitu, tipe yang pertama ada *informasi gathering* yang berisikan informasi seputar website yang akan diuji bisa berupa alamat IP, teknologi yang digunakan, sistem dengan melakukan *scanning*. Lalu pada tipe kedua ada *vulnerability scanning* tahapan yang dilakukan pemindaian kerentanan pada website yang dapat digunakan sebagai tahap analisis selanjutnya (Purnomo & Chusyairi, 2024).
c. *Attack*, merupakan tahapan untuk melakukan analisis dari pemindaian yang telah dilakukan dengan melakukan penyerangan terhadap website dengan menggunakan tool yang ada di kali linux maupun yang ada di windows.
d. *Reporting*, merupakan hasil dari setiap tahapan yang telah dilakukan dari segi pengujian dan penilaian keamanan pada website.

4. HASIL DAN PEMBAHASAN

Tahapan simulasi yang dilakukan kegiatan uji coba pada Universitas Sebelas April (unsap.ac.id) dengan tahapan metode seperti pada Gambar 1.

Planning

Tahapan pertama yang dilakukan diskusi pada pengelola website untuk melakukan simulasi pengujian atau penyerangan dilakukan setelah mendapatkan persetujuan untuk melakukan uji penetrasi pada website fti.unsap.ac.id sebagai objek penelitian (Anelia et al., 2023).

Discovery

Tahapan selanjutnya mengumpulkan informasi yang ada pada website dengan subdomain fti.unsap.ac.id. Terdapat dua tahapan dalam melakukan discovery berupa *informasi gathering* serta *vulnerability scanning* (Silaban & Wijaya, n.d.).

a. *informasi gathering*

Tahapan yang pertama dilakukan untuk mencari informasi pada domain website yang akan dilakukan pengujian kerentanan. *tools* yang digunakan dalam *informasi gathering* berupa Network Mapper (NMAP) domain yang dapat digunakan pada platform Kali Linux. Berikut merupakan tabel 1 hasil yang telah didapatkan dengan menggunakan NMAP pada subdomain fti.unsap.ac.id.

Tabel 1. Hasil Scanning Network Mapper (NMAP)

Port	Protokol	Status	Layanan	Versi
32	TCP	Closed	unknown	
80	TCP	Open	http	Cloudflare http proxy
443	TCP	Open	ssl/http	Cloudflare http proxy
787	TCP	Closed	osc	
1029	TCP	Closed	ms-lsa	
2222	TCP	Closed	EtherNetIP-1	
2604	TCP	Closed	ospfd	
2869	TCP	Closed	icslap	
2875	TCP	Closed	dxmessagebase2	
3324	TCP	Closed	active-net	
3918	TCP	Closed	pktcablemmcops	
4446	TCP	Closed	n1-fwp	
5960	TCP	Closed	unknown	
7070	TCP	Closed	realserver	
7200	TCP	Closed	fodms	
8080	TCP	Open	http	Cloudflare http proxy
8081	TCP	Closed	blackice-icecap	
8086	TCP	Closed	d-s-n	
8088	TCP	Closed	radan-http	
8443	TCP	Open	ssl/http	Cloudflare http proxy
9000	TCP	Closed	cslistener	
10616	TCP	Closed	unknown	
16993	TCP	Closed	amt-soap-https	
20221	TCP	Closed	unknown	
24800	TCP	Closed	unknown	
61900	TCP	Closed	unknown	

b. *vulnerability scanning*

Tahapan selanjutnya dari discovery yaitu *vulnerability scanning* atau merupakan analisis kerentanan. Dengan menggunakan *tools* OWASP ZAP untuk melakukan analisis kerentanan berikut merupakan hasil yang bisa dilihat pada tabel 2.

Tabel 2. Hasil Scanning OWASP ZAP

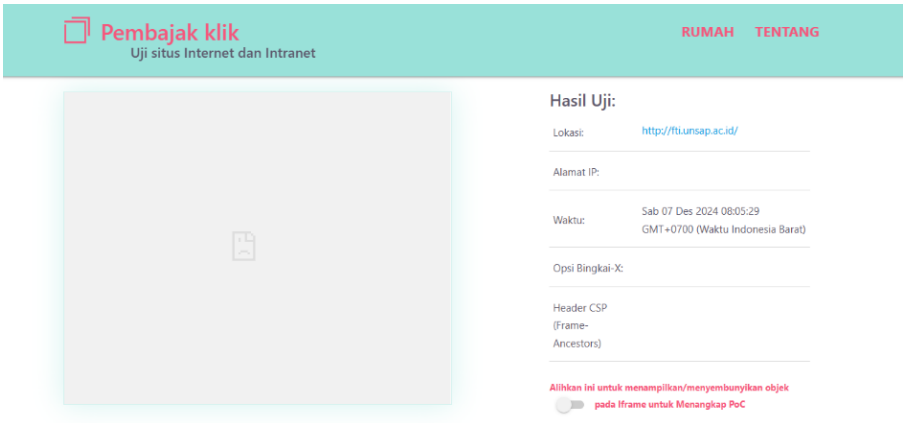
Name	Risk Level
CSP: Wildcard Directive	Medium
CSP: script-src unsafe-inline	Medium
CSP: style-src unsafe-inline	Medium
Content Security Policy (CSP) Header Not Se	Medium
Cross-Domain Misconfiguration	Medium
Missing Anti-clickjacking Header	Medium
Strict-Transport-Security Header Not Set	LOW
Timestamp Disclosure - Unix	LOW
X-Content-Type-Options Header Missing	LOW
Information Disclosure - Suspicious Comments	Informational
Modern Web Application	Informational

Attack

Tahapan selanjutnya attack merupakan simulasi untuk yang ada dalam metode NIST SP 800 – 115 dengan melakukan penetrasi kepada website yang digunakan sebagai bahan yang akan diuji untuk melihat kerentanan yang telah ditemukan di tahap sebelumnya yaitu *discovery* untuk melakukan eksploitasi.

a. *Clickjacking*

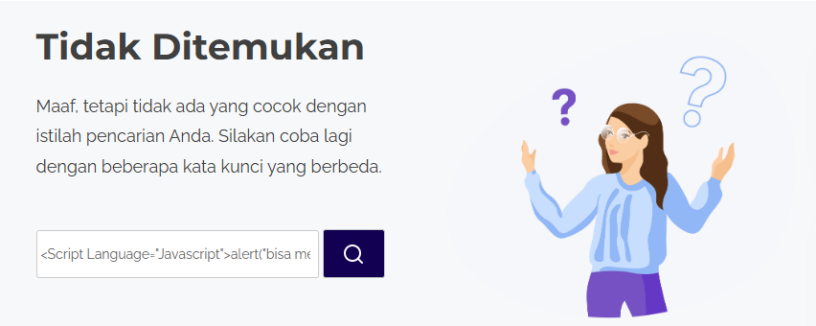
Merupakan tahapan melakukan simulasi akan penyerangan *Clickjacking* dengan menggunakan clickjacker.io**.** Pada hasil temuan yang ada pada gambar 2 dimana pada hasil melakukan penyerangan yang dilakukan pada website perguruan tinggi tidak ada kerentan terhadap serangan *Clickjacking* dimana terdapat sistem keamanan yang menghalang untuk melakukan penyerangan *Clickjacking*.



Gambar 2. Hasil melakukan *Clickjacking*

b. XSS

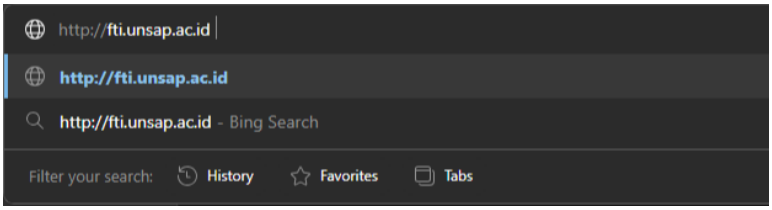
Tahap berikutnya, melakukan uji coba simulasi serangan *Cross Site Scripting* (XSS) pada website yang diuji yang dapat dilihat pada gambar 4 dan gambar 5 dengan memasukkan perintah untuk memunculkan pop up menggunakan script yang dapat dilihat bahwa simulasi untuk melakukan kerentanan yang diuji tidak mengalami error.



Gambar 3. Uji Coba melakukan *Cross Site Scripting* (XSS)

c. HSTS Missing

Tahapan pengujian selanjutnya *HTTP Strict Transport Security* (HSTS) merupakan mekanisme keamanan website dengan ijin akses koneksi aman saja. Dengan melakukan uji coba ke dalam situs dengan menggunakan http dengan hasil yang dapat dilihat pada gambar 6 tidak dapat langsung diakses tanpa HTTPS dan segera mengarahkan ulang langsung untuk menggunakan HTTPS.



Gambar 4. Hasil melakukan HSTS Missing

Reporting

Tahapan terakhir melakukan reporting dari metode NIST 800 – 115 yang digunakan. Dimana telah mengumpulkan hasil yang telah dilakukan dari hasil temuan akan informasi, kelemahan website, hingga melakukan simulasi penyerangan. Berikut hasil reporting pada table 3.

Tabel 3. Hasil Tabel Kerentanan

No	Nama Kerentanan	Dampak	Status Valid	Rekomendasi
1	*Clickjacking*	Dampak dari serangan *clickjacking* yang digunakan dalam penipuan user interface yang dimanfaatkan untuk mengambil data pengguna tanpa disadari (Firly, 2023).	Tidak Valid	Mencegah dari serangan *clickjacking* dengan menggunakan SAMEORIGIN, DENY, Set header 'X-Frame-Options', dan ALLOW-FROM, Set header 'X-Frame-Options'.
2	XSS	Dampak dari serangan XSS berupa gangguan untuk mengambil data melalui script melalui halaman situs yang ada di website (Chandra et al., 2024).	Tidak Valid	Mencegah dari serangan XSS yaitu Periksa Keamanan Situs secara berkala, Mengadopsi Crossing Boundaries Policy kebijakan yang membatasi bagaimana data dari satu konteks, serta Menambahkan SDL (Security Development Lifecycle)
3	HSTS Missing	Dampak dari seranagan ini dimana data yang akan dikirim dapat dilihat penyerang yang berdampak pada serangan Man-in-The-Middle (Maherza et al., 2023).	Tidak Valid	Mencegah dari serangan HSTS yaitu melakukan Missing HTTP sering disalurkan melalui SSL atau TLS sebagai perlindungan dimana HTTPS terenkripsi.

Pada Pembahasan ini dilakukan untuk membandingkan hasil penelitian yang diperoleh pada setiap metode yang digunakan peneliti ini tujuan untuk mencapai hasil penelitian tersebut.

Penelitian dilakukan oleh Verry Budiyanto, Nuniek Herawatie, Uminingsih (2023), menganalisis keamanan pada domain akprind.ac.id dengan menggunakan OWASP Zap dengan hasil yang diperoleh berdasarkan kajian pustaka serta hasil observasi. Dengan hasil penelitian terhadap domain ditemukan beberapa kerentanan yang berdampak negatif bagi pihak yaitu celah keamanan masih berhasil untuk dilakukan eksploitasi sehingga mendapatkan informasi penting yang memiliki hak akses. Lalu untuk sistem keamanan pada akprind.ac.id masih cukup aman serta peneliti memberikan rekomendasi keamanan pada domain akprind.ac.id serta dilakukan penelitian lebih mendalam menggunakan metode ISSAF (Information System Security Assessment Framework) (Herawati et al., 2023).

Penelitian yang dilakukan oleh Syarif Hidayatulloh, Desky Saptadiaji (2021), dengan melakukan tahapan penetration testing di website universitas ARS dengan OWSAP top-10 2017. Pada domain yang akan dilakukan analisis ada 5 dengan hasil memiliki 13 kerentanan dengan hasil tersebut dimana universitas ARS masih dibilang aman dengan memenuhi 3 tahapan dalam keamanan pada informasi, web server, serta pada software (Hidayatulloh & Saptadiaji, 2021).

Penelitian yang dilakukan oleh Hena Sulaeman, Ahsani Takwim (2024), melakukan penilaian keamanan aplikasi Slims Akasia dengan menggunakan metode NIST SP 800 – 115

serta OWASP sebagai nilai ukur akan kerentanan dengan hasil untuk melihat kualitas aplikasi dari serangan setelah dilakukan pengujian mendapatkan 5 kerentanan dengan tingkatan level high maka perlu dilakukan peningkatan pada keamanan dengan melakukan eksploitasi pada sistem yang akan mendatang (Sulaeman & Takwim, n.d.).

5. KESIMPULAN DAN SARAN

Berdasarkan pengujian dimana hasil temuan dalam penelitian ini di website Fakultas Teknologi Informasi (fti.unsap.ac.id), dari hasil penelitian terhadap keamanan dalam menggunakan website fti.unsap.ac.id yang menggunakan metode NIST SP 800–115 dengan 4 tipe yaitu, *planning, discovery, attack*, dan *reporting*. Hasil kerentanan yang ditemukan dengan melakukan *scanning* dengan hasil 6 kategori medium, 3 low, dan 2 informational dan belum menemukan tingkat kerentanan dengan level high. Keamanan yang ada pada website fti.unsap.ac.id masih dibilang aman karena dari hasil melakukan pengujian belum menemukan kerentanan karena sistem yang ada pada website tersebut terdapat firewall yang mampu menghalangi serangan. Saran berdasarkan hasil kesimpulan yaitu dapat dilakukan pengujian ulang baik dari pihak Fakultas Teknologi Informasi maupun dari penguji yang lain pada website supaya dapat menemukan celah keamanan yang lebih mendalam. Serta melakukan pengujian dengan menambahkan metode bebrapa metode sebagai penunujang untuk menemukan kerentanan.

6. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada pihak penerbit serta kesempatan yang telah diberikan untuk melakukan publikasikan jurnal ini. Serta ucapan terima kasih ditunjukkan juga kepada semua pihak telah memberikan dukungan pada proses penelitian hingga selesai.

DAFTAR REFERENSI

Anelia, S. S., Jayanta, J., & Hananto, B. (2023). Uji penetrasi server Universitas PQR menggunakan metode National Institute Of Standards And Technology (NIST SP 800-115). *Jurnal Ilmu Teknik Dan Komputer*, *7*(1), 34. https://doi.org/10.22441/jitkom.2023.v7i1.005

Ary, G., Sanjaya, S., Made, G., Sasmita, A., Made, D., & Arsa, S. (n.d.). Evaluasi keamanan website lembaga X melalui penetration testing menggunakan framework ISSAF.

Chandra, A. A., Turmudi Zy, A., & Nugroho, A. (2024). Penerapan teknik penetration testing terhadap cross-site scripting (XSS) dalam pengembangan website. *Rabit: Jurnal*

Teknologi Dan Sistem Informasi Univrab, *9*(2), 262–270. https://doi.org/10.36341/rabit.v9i2.4822

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability assessment website e-government dengan NIST SP 800-115 dan OWASP menggunakan web vulnerability scanner. *Jurnal Sistem Informasi Bisnis*, *12*(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44

Elanda, A., & Lintang Buana, R. (2021). Analisis kualitas keamanan sistem informasi e-office berbasis website pada STMIK Rosma dengan menggunakan OWASP Top 10 (Vol. 6, Issue 2).

Firly, A. (2023). Implementasi clickjacking dalam serangan tautan palsu untuk eksplorasi media sosial. *Jurnal TIMES*, *12*(2), 15–18. https://doi.org/10.51351/jtm.12.2.2023702

Herawati, N., Budiyanto, V., & Uminingsih. (2023). Analisis keamanan sebuah domain menggunakan Open Web Application Security Project (OWASP) Zap. *Jurnal Teknologi Technoscientia, 27–36.* https://doi.org/10.34151/technoscientia.v15i2.4013

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration testing pada website Universitas ARS menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *18*(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

Maherza, S. A., Hananto, B., Wayan, I., Pradnyana, W., Fakultas, I./, Komputer, I., Pembangunan, U., Veteran Jakarta, N., & Fatmawati, J. R. S. (2023). *Jurnal Informatika, Edisi ke-19, Nomor 1*.

Mitra Purba, P., Azrah Cipta Amandha, Riyan Hidayah Purnama, & Ali Ikhwan. (2022). Analisis keamanan website Prodi Sistem Informasi Uinsu menggunakan metode application scanning. *Jurnal Informatika Teknologi Dan Sains*, *4*(4), 325–329. https://doi.org/10.51401/jinteks.v4i4.2065

Purnomo, M. D., & Chusyairi, A. (2024). Pengujian keamanan sistem menggunakan metode penetration testing di website Diskominfostandi Kota Bekasi. *Sistematis: Jurnal Ilmiah Sistem Informasi*, *1*(1). https://doi.org/10.69533

Raazi, I. M., Malahayati, M., Basrul, B., Malia, R., & Fadhli, M. (2024). Analysis server security assessment of staffing management information system using the NIST SP 800-115 method at UIN Ar-Raniry Banda Aceh. *Circuit: Jurnal Ilmiah Pendidikan Teknik Elektro*, *8*(1), 46. https://doi.org/10.22373/crc.v8i1.20808

Silaban, R. C., & Wijaya, E. (n.d.). Analisis kerentanan website menggunakan metode NIST SP 800-115 dan OWASP di Diskominfo Kabupaten Bandung.

Sulaeman, H., & Takwim, A. (n.d.). Analisa kualitas keamanan pada aplikasi Slims Akasia dengan metode NIST SP 800-115 dan OWASP. *Seminar Nasional Corisindo*.

Thurfah Afifa Rosaliah, Y., & Hananto, B. (2021). Pengujian celah keamanan website menggunakan teknik penetration testing dan metode OWASP Top 10 pada website SIM xxx. In *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, Jakarta-Indonesia.