p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

IDENTIFIKASI KERENTANAN KEAMANAN PADA *WEBSITE* FAKULTAS ILMU KOMPUTER UNIVERSITAS SUBANG MENGGUNAKAN METODOLOGI OWASP

Achmad Syafaat[1]
Fakultas Ilmu Komputer, Universitas Subang[1], Badan Siber dan sandi Negara[1]

asyafaat@gmail.com[1]

Abstrak

Website (web) merupakan salah satu sarana penting dalam mengakses informasi dan layanan digital di lingkungan perguruan tinggi. Namun, dengan perkembangan teknologi, *website* menjadi target empuk bagi serangan siber yang dapat mengancam keamanan data dan privasi pengguna. Pada penelitian ini dalam melakukan identifikasi kerentanan keamanan mempergunakan metodologi OWASP. Metodologi ini digunakan karena telah dikenal secara luas sebagai pedoman terkemuka dalam mengidentifikasi, mengukur, dan mengatasi kerentanan keamanan pada aplikasi web. Dalam melakukan penelitian, pengujian dilakukan secara menyeluruh untuk mengidentifikasi potensi kerentanan keamanan yang mungkin ada dalam berbagai aspek website, termasuk kelemahan dalam manajemen sesi, enkripsi data, pengelolaan akses, dan sebagainya. Hasil dari penelitian ini diharapkan dapat memberikan gambaran yang jelas tentang kerentanan keamanan yang ada pada *website* Fakultas Ilmu Komputer Universitas Subang, serta rekomendasi untuk memperbaiki dan menguatkan sistem keamanan. Dengan mengetahui dan memahami kerentanan yang ada, diharapkan dapat dilakukan langkah-langkah pencegahan dan perlindungan yang lebih efektif dapat diambil. Hal-hal tersebut dilakukan untuk menjaga integritas dan kerahasiaan data pengguna, serta memastikan kelancaran beroperasinya layanan *website* fakultas. Pada Penelitian ini memiliki implikasi dalam konteks keamanan siber pengelolaan *website* pada perguruan tinggi, dalam upaya menjaga keamanan dan privasi pengguna di era digital yang semakin kompleks dan rentan terhadap serangan siber. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi penting dalam upaya meningkatkan keamanan *website* Fakultas Ilmu Komputer Universitas.

Kata Kunci: *Siber, OWASP, Kerentanan, Keamanan,Website*

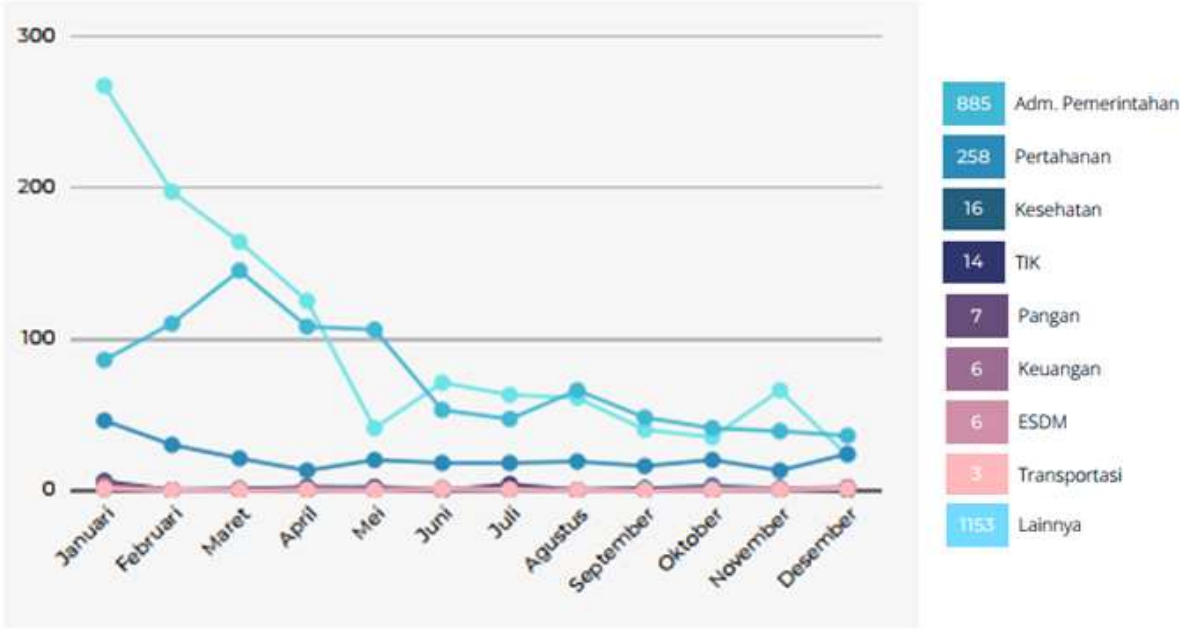
Pendahuluan,

Website (*web*) telah menjadi salah satu sarana penting dalam menyediakan informasi dan layanan bagi masyarakat umum. Selain itu penggunaan website memberikan kemudahan dalam memperbaharui informasi yang ditampilkannya. Akan tetapi di samping kemudahan yang ditawarkan, penggunaan *website* memiliki risiko ancaman yang tinggi jika dalam pengembangannya tidak memperhatikan siklus pengembangan yang memperhatikan aspek keamanan.

Berdasarkan Laporan tahunan yang dikeluarkan oleh Id-SIRTII/CC dan Badan Siber dan Sandi Negara melalui Lanskap Keamanan Siber Indonesia 2022, total trafik anomali di Indonesia selama tahun 2022 sebanyak 976.429.996 anomali yang terdeteksi. Adapun kasus *web defacement* yang terjadi di Indonesia dalam tahun 2021 sebanyak 5.940 kasus dan tahun

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

2022 sebanyak 2.348 kasus (Direktorat_Operasi_Keamanan_Siber, 2022). Para penyerang melakukan berbagai cara untuk menyusup dan berbagai aktivitas untuk mencari celah terhadap ribuan *website* (Murniati, Munadi, & Arif, 2018). *Web defacement* merupakan suatu serangan yang ditujukan untuk eksploitasi situs web atau server web yang rentan dengan memanfaatkan kerentanan dari sistem website yang dibangun sehingga penyerang dapat masuk, memodifikasi, menghapus ataupun merusak konten halaman *web* yang telah diretas.



Gambar 1 Sektor Terdampak *Web Defacement*

Pada Lanskap Keamanan Siber Indonesia 2022, diinformasikan bahwa kasus *web defacement* pada *homepage* sebanyak 356 kasus dan pada *hidden page* sebanyak 1992 kasus (Direktorat_Operasi_Keamanan_Siber, 2022). Di kasus *web defacement* pada *homepage*, lokasi *defacement* terletak di halaman utama *website* yang menyebabkan ketika pengguna mengakses *website* maka akan menampilkan halaman yang di *defacement* tersebut. Sedangkan pada kasus *web defacement* yang *hidden page*, mengindikasikan bahwa *defacement* dilakukan pada lokasi tertentu selain halaman utamanya juga di *defacement*. Oleh karena itu, ketika pengguna mengakses *website* yang telah di *defacement* belum langsung menyadari dan menemukan halaman yang telah di *defacement*.

Seiring dengan perkembangan teknologi dan ketergantungan pada platform *online*, keamanan *website* menjadi hal yang semakin krusial. Adanya kemungkinan ancaman dan risiko terkait keamanan siber mengharuskan pengelola *website* dapat mengidentifikasi serta mengelola kerentanan yang mungkin ada pada *website* tersebut karena jika terjadi insiden dapat merusak reputasi institusi. Oleh sebab itu, upaya dalam menjaga integritas, kerahasiaan, serta ketersediaan informasi sangat penting dan harus menjadi prioritas institusi. Demikian halnya aspek keamanan pada *website* Fakultas Ilmu Komputer Universitas Subang dalam menyediakan informasi dan layanan bagi mahasiswa, dosen serta masyarakat umum.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Pada penelitian ini bertujuan untuk melakukan identifikasi kerentanan keamanan pada *website* Fakultas Ilmu Komputer Universitas Subang, dengan harapan temuan yang didapatkan dijadikan bahan evaluasi dan rekomendasi perbaikan terhadap celah keamanan yang ada. Identifikasi kerentanan keamanan yang dilakukan mempergunakan metodologi OWASP (*Open Worldwide Application Security Project*) dengan OWASP *Top* 10 dan analisis risiko yang timbul karena kerentanan dengan OWASP *Web Security Testing Guide* (WSTG). Metodologi ini digunakan karena telah diakui dan secara luas sebagai panduan terkemuka dalam mengidentifikasi kerentanan keamanan pada aplikasi *website*.

Kajian Teori,

Aspek Keamanan Website

Website sebagai suatu layanan pada perguruan tinggi/universitas perlu ditunjang aspek-aspek keamanan, agar informasi yang disampaikan terjamin integritasnya. Beberapa hal aspek keamanan sangat penting adalah:

a. Perlindungan Data Pribadi. Perguruan tinggi menyimpan sejumlah besar data pribadi mahasiswa, dosen, dan staf, termasuk informasi identitas, alamat, dan data akademik. Keamanan yang kuat diperlukan untuk melindungi data yang dimiliki dari akses tidak sah dan pelanggaran data;
b. Kepatuhan terhadap Regulasi. Institusi pendidikan sering harus mematuhi standar keamanan data dan privasi tertentu agar pengamanan sistem sesuai standar yang ditentukan;
c. Perlindungan Properti Intelektual. Universitas dan perguruan tinggi sering terlibat dalam penelitian yang menghasilkan properti intelektual yang berharga. Keamanan yang efektif diperlukan untuk melindungi hasil penelitian dari pencurian atau penyalahgunaan;
d. Keamanan Infrastruktur IT. Dengan meningkatnya digitalisasi, banyak aspek operasional perguruan tinggi bergantung pada infrastruktur IT. Gangguan akibat serangan siber bisa menghambat operasional pendidikan, administrasi, maupun penelitian;
e. Perlindungan terhadap Serangan Siber. Institusi pendidikan sering menjadi target serangan siber seperti *ransomware*, *phishing*, serangan DDoS, *defacement*, penyusupan konten judi *online*, dan sebagainya. Keamanan yang kuat membantu mencegah gangguan dan kerugian finansial akibat serangan ini;
f. Pendidikan dan Kesadaran Keamanan Siber kepada Dosen, Mahasiswa dan Staf. Pendidikan tentang keamanan siber penting, karena mereka sering menjadi target *phishing* dan penipuan *online*. Universitas maupun fakultas harus menyediakan sumber daya dan pelatihan untuk meningkatkan kesadaran keamanan siber;
g. Jaminan Kepercayaan Stakeholder. Keamanan yang baik menunjukkan kepada mahasiswa, staf, dan pihak lain yang bekerja sama dengan universitas maupun fakultas bahwa institusi serius dalam melindungi informasi dan operasionalnya. Ini membangun kepercayaan dan kredibilitas;
h. Akses Aman ke Sumber Daya *Online*. Keamanan website memastikan bahwa akses ke sumber daya online aman dan terjaga;
i. Mencegah Kehilangan Finansial. Serangan siber bisa menyebabkan kerugian finansial yang signifikan, baik langsung maupun tidak langsung, melalui kerusakan secata teknis, turunnya reputasi, dampak hokum yang timbul, dan biaya pemulihan;

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

j. Adaptasi dengan Ancaman yang Berkembang. Lingkungan siber terus berkembang dengan ancaman baru yang muncul secara berkala. Institusi pendidikan harus beradaptasi dengan ancaman yang ada untuk melindungi aset dan reputasi.

Pengamanan *website* dapat merujuk pada aspek merupakan fondasi dasar untuk melindungi informasi dan sistem informasi. Ada tiga komponen utama keamanan informasi (ISO/IEC, 2022):

a. *Confidentiality* (Kerahasiaan). Mengacu pada perlindungan data dan informasi agar tidak diakses oleh individu yang tidak berwenang. Pada sudut pandang di *website*, aspek ini melibatkan penggunaan teknologi seperti enkripsi, otentikasi pengguna, dan kontrol akses untuk memastikan hanya pengguna yang berwenang yang dapat mengakses informasi sensitif;
b. *Integrity* (Integritas). Berkaitan dengan menjaga keakuratan dan kelengkapan data. Pada aspek memastikan bahwa data yang disimpan atau dikirim melalui *website* tidak diubah secara tidak sah oleh pihak ketiga. Hal ini bisa dicapai melalui *checksum*, *digital signatures*, dan mekanisme audit untuk memantau perubahan data;
c. *Availability* (Ketersediaan). Mengacu pada bagaimana menjamin bahwa data dan sumber daya di sistem tersedia bagi pengguna yang berwenang saat dibutuhkan. Dalam pengamanan *website*, hal ini melibatkan penggunaan redundansi server, *load balancing*, dan teknologi lainnya untuk memastikan *website* tetap *online* dan berfungsi, bahkan selama serangan atau kegagalan sistem. Hal tersebut termasuk didalamnya untuk perlindungan terhadap serangan DoS (*Denial of Service)* dan DDoS (*Distributed Denial of Service*).

Website (web).

Website adalah kumpulan halaman web, yang menyediakan informasi visual, pendengaran dan tekstual, yang merupakan kartu kunjungan bisnis yang menyajikan organisasi atau layanan atau produk. (Isooraite, 2020) (Dewa Gede Govindha Dharmawangsa, Made Arya Sasmita, & Putu Agus Eka Pratama, 2023). *Website* sebagai layanan yang menyajikan informasi dengan konsep *hyperlink* (tautan), sehingga mempermudah pengguna internet. *Website* dapat memberikan *highlight* konten yang disajikan dalam sebuah dokumen untuk ditautkan ke media lain. *Website* dapat menghubungkan dari berbagai lokasi dalam sebuah dokumen atau gambar ke berbagai lokasi di dokumen lain. Dengan sebuah *browser*, tautan dapat di hubungkan ke tujuannya dengan mengklik tautan tersebut. (Susilo, Kurniati, & Kasmawi, 2018)

CVE

Common Vulnerability Exposure (CVE). merupakan daftar kerentanan aset keamanan informasi berlaku secara global yang terdiri dari nomor identifikasi, deskripsi, dampak untuk memudahkan dalam berbagi informasi antar organisasi. (Direktorat_Operasi_Keamanan_Siber, 2022). Saat ini dalam katalog kerentanan keamanan siber yang diungkapkan kepada publik terdapat 222.208 CVE Records yang dapat diakses (The_MITRE_Corporation, 2024)

Metode *Black Box*

Metode pengujian yang dilakukan untuk mengamati hasil *input* dan *output* dari sistem tanpa mengetahui struktur dari sistem yang ada (Bimandaru, Alamsyah, & Nugroho, 2023). Jenis pengujian ini mirip dengan situasi serangan dari luar dan kadang-kadang

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

dikenal sebagai tes/pengujian eksternal. Penguji penetrasi akan menjalankan tes dari lokasi yang jauh selain itu informasi yang di dapat sangat terbatas (Hasibuan & Marwan Elhanafi, 2022).

Pengujian Penetrasi Kerentanan Keamanan

Pengujian penetrasi pada website bertujuan untuk mencari celah-celah keamanan pada *website* yang nantinya dapat dikategorikan sebagai risiko kerentanan keamanan. Tahapan yang digunakan untuk melakukan *penetration testing* pada suatu *website* terdiri dari berbagai modul yang akan disesuaikan dengan standarisasi atau *framework* yang telah tersedia. (Dewa Gede Govindha Dharmawangsa, Made Arya Sasmita, & Putu Agus Eka Pratama, 2023) (Bimandaru, Alamsyah, & Nugroho, 2023)

Open Worldwide Application Security Project (OWASP)

OWASP adalah yayasan nirlaba yang bekerja untuk meningkatkan keamanan perangkat lunak. Program pada OWASP meliputi (OWASP Foundation, About the OWASP Foundation, 2024):

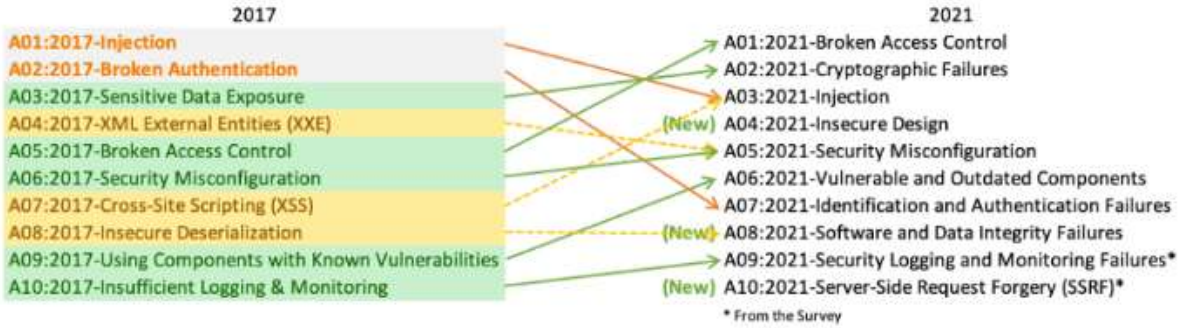
- Proyek *open source* yang dipimpin komunitas termasuk kode, dokumentasi, dan standar
- Lebih dari 250 cabang lokal di seluruh dunia
- Puluhan ribu anggota
- Konferensi pendidikan dan pelatihan terkemuka di industri

OWASP merupakan komunitas terbuka yang didedikasikan untuk memungkinkan organisasi menyusun, mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi yang dapat dipercaya. Semua proyek, alat, dokumen, forum, dan *chapters* bebas terbuka bagi siapa saja yang tertarik untuk meningkatkan keamanan aplikasi. OWASP Foundation diluncurkan pada tanggal 1 Desember 2001, dan menjadi badan amal nirlaba Amerika Serikat pada tanggal 21 April 2004. Selama dua dekade, perusahaan, yayasan, pengembang, dan relawan telah mendukung OWASP *Foundation* dan pekerjaannya. Donasi, menjadi anggota, atau menjadi pendukung saat ini. (OWASP Foundation, About the OWASP Foundation, 2024)

OWASP TOP 10

OWASP Top 10 2021 merupakan versi terbaru dari OWASP Top 10. OWASP Top 10 berisikan 10 daftar teratas celah keamanan yang secara berkala diperbaharui sesuai dengan perkembangan kerentanan, eksploitasi, dampak, dan tingkat insiden tertinggi yang terjadi dari suatu kerentanan. Sepuluh katagori yang dirumuskan menjadi acuan dan dasar banyak kalangan baik professional maupun industri dalam melakukan penilaian pengujian tingkat kerentanan, kemungkinan eksploitasi serta dampak insiden yang ditimbulkan dari kerentanan yang ditemukan. OWASP *Top* 10 versi 2017 dan konsolidasi ke versi 2021 seperti terlihat pada gambar 2.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom



Gambar 2 OWASP Top 10 dan Perubahan di Versi 2021

OWASP Top 10 merupakan dokumen kesadaran. Bagaimanapun, hal ini tidak menutup organisasi untuk menggunakannya sebagai sebuah standar *de facto* pada industri keamanan aplikasi sejak kelahirannya tahun 2003. Penggunaan OWASP Top 10 sebagai standar dalam *coding* atau pengujian merupakan batas minimal dan hanya sebuah tahap awal.

Parameter pada OWASP Top 10 2021 terdiri atas (OWASP Foundation, OWASP Top Ten - 2021, 2021):

- A01:2021-Broken Access Control, pada katagori ini berkaitan Akses Kontrol menetapkan sebuah peraturan yang dimana user tidak dapat melakukan sebuah aksi diluar permission yang diberikan. Kegagalan atas hal ini dapat mengakibatkan pengeluaran informasi yang tidak diizinkan, modifikasi, atau penghancuran dari semua data atau pemberlakuan sebuah fungsi bisnis di luar limit sebuah *user*;
- A02:2021-Cryptographic Failures adalah katagori yang fokus pada kegagalan terkait dengan Kriptografi yang sering mengarah pada Pengungkapan Data Sensitif atau sistem yang telah terinfeksi oleh hacker;
- A03:2021-Injection adalah katagori yang fokus pada injeksi yang biasa terjadi pada SQL, NoSQL, perintah OS, *Object Relational Mapping* (ORM), LDAP, dan *Expression Language* (EL) atau injeksi *Object Graph Navigation Library* (OGNL). Konsepnya adalah identik di antara semua mesin penerjemah. Penelaahan kode sumber adalah metode terbaik dalam mendeteksi apakah aplikasi tersebut beresiko untuk diinjeksi. Testing otomatis terhadap semua parameter-parameter, headers, URL, cookies, JSON, SOAP, and input data XML sangat disarankan. Organisasi dapat menyertakan sumber statik (SAST) dan perangkat tes aplikasi dinamis (DAST) ke dalam CI/CD pipeline untuk mengidentifikasi pengenalan serpihan-serpihan injeksi sebelum di sebarkan ke produksi. Celah injeksi terjadi ketika data yang berbahaya milik penyerang dikirim ke interpreter sebagai bagian dari perintah atau query dapat mengelabui interpreter untuk mengeksekusi perintah yang tidak diinginkan atau mengakses data secara illegal (Yudiana, Elanda, & Lintang Buana, 2021);
- A04:2021-Insecure Design adalah kategori dengan fokus pada resiko yang terkait pada kekurangan desain. Jika kita ingin benar-benar bergerak sebagai industri, itu membutuhkan lebih banyak penggunaan pemodelan ancaman, pola dan desain yang aman, dan arsitektur referensi;
- A05:2021-Security Misconfiguration adalah katagori yang fokus pada bentuk kesalahan konfigurasi;
- A06:2021-Vulnerable and Outdated Components adalah katagori yang fokus pada.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

- A07:2021-Identification and Authentication Failures adalah katagori yang fokus pada kegagalan identifikasi..
- A08:2021-Software and Data Integrity Failures adalah kategori yang berfokus pada pembuatan asusmsi terkait pembaruan perangkat lunak, data penting, dan pipeline CI/CD tanpa memverifikasi integritas.
- A09:2021-Security Logging and Monitoring Failures adalah katagori yang fokus pada
- A10:2021-Server-Side Request Forgery, kategori ini berfokus pada.

OWASP *Web Security Testing Guide*

Web Security Testing Guide (WSTG) merupakan panduan komprehensif untuk menguji keamanan aplikasi web dan layanan web. Dibuat melalui upaya kolaboratif para profesional keamanan siber dan sukarelawan yang berdedikasi, WSTG menyediakan kerangka praktik terbaik yang digunakan oleh penguji penetrasi dan organisasi di seluruh dunia. (OWASP Foundation, OWASP Web Security Testing Guide, 2023).
OWASP Web Security Testing Guide v4.2

OWASP ZAP

OWASP Zed Attack Proxy (ZAP) atau sekarang dikenal sebagai Zed Attack Proxy (ZAP) merupakan perangkat lunak pengujian penetrasi terintegrasi yang mudah digunakan untuk menemukan kerentanan dalam aplikasi *website*. Perangkat lunak Ini dirancang untuk digunakan oleh pengguna dengan berbagai pengalaman keamanan, dikarenakan hal tersebut menjadikannya ideal untuk pengembang dan penguji fungsional yang baru dalam pengujian penetrasi.

Gambar 3. ZAP 2.14.0

ZAP menyediakan pemindai otomatis serta satu set kelengkapan yang memungkinkan untuk menemukan kerentanan keamanan secara manual (OWASP Foundation, Testing Tools Resource, 2023). Di tahun 2023, ZAP sudah tidak lagi menjadi bagian langsung dari OWASP dan menjadi bagian dari Software Security Project (SSP) di bawah Linux Foundation (Bennetts, 2023), (ZAP_Dev_Team, Zed Attack Proxy (ZAP), 2024), (The_Linux_Foundation, 2023). (Guntoro, Costaner, & Musfawati, 2020)

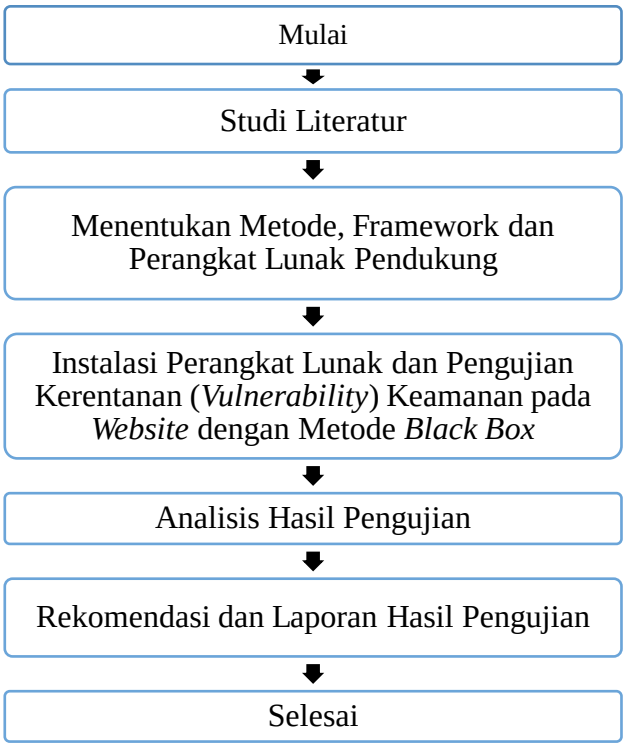
p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Metodologi

Metodologi penelitian merupakan alur atau tahapan dalam menjelaskan bagaimana penelitian dilaksanakan. Pada penelitian ini identifikasi kerentanan keamanan mempergunakan metodologi OWASP.

Alur Penelitian

Secara umum pada penelitian ini memiliki lima tahapan, dalam melakukan identifikasi kerentanan keamanan website. Tahapan dalam penelitian berkaitan dengan identifikasi kerentanan pertama dimulai dari Studi Literatur, kedua Menentukan Metode, Framework dan Perangkat Lunak Pendukung, ketiga Instalasi Perangkat Lunak dan Pengujian Kerentanan (*Vulnerability*) Keamanan pada *Website*, keempat Analisis Hasil Pengujian, kelima Rekomendasi dan Laporan Hasil Pengujian. Alur penelitian ditunjukkan seperti pada Gambar 2.



Gambar 4 Alur Penelitian

Studi Literatur

Pada suatu penelitian, tidak jarang penelitian tersebut melihat penelitian terdahulu sebagai referensi dalam melaksanakan dan pengembangan penelitiannya. Hal tersebut merupakan bagian dari studi literatur yang dilakukan untuk memperkaya teori dan kajian penelitian yang sedang berlangsung. Pada penelitain terdahulu dapat dijadikan bahan pembanding maupun memperkaya kajian pada penelitian yang dilaksanakan oleh penulis. Adapun pun penelitian-penelitian yang menjadi bahan studi literature seperti pada tabel 1.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Tabel 1 Penelitian Terdahulu

No	Jurnal/Prosiding	Judul	Sititasi
1	Jurnal Ilmiah Teknologi dan Komputer	*Penetration Testing* Berbasis *OWASP Testing Guide`*	(Dewa Gede Govindha Dharmawangsa, Made Arya Sasmita, & Putu Agus Eka Pratama, 2023)
2	*International Journal of Engineering and Computer Science Applications* (IJECSA)	*Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas*	(Saktiansyah & Muharrom, 2023)
3	Jurnal FORISTEK	Analisis Pengujian Penetrasi Pada Layanan *Hosting* Menggunakan Metode *Black Box* (Studi kasus : *Blogspot, Wordpress* dan *Shared Hosting)*	(Bimandaru, Alamsyah, & Nugroho, 2023)
4	SUDO Jurnal Teknik Informatika	Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode *Black Box*	(Hasibuan & Marwan Elhanafi, 2022)
5	*2022 10th International Conference on Cyber and IT Service Management (CITSM)*	*Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP*	(Nurbojatmiko, Lathifah, & Bil Amri, 2022)
6	*Journal of Computer Engineering System and Science*	Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis *Website* Pada STMIK Rosma dengan Menggunakan OWASP Top 10	(Yudiana, Elanda, & Lintang Buana, 2021)
7	Syntax Fusion: Jurnal Nasional Indonesia	Analisis Kerentanan Keamanan *Website* Menggunakan Metode OWASP (*Open Web Application Security Project)* Pada Dinas Tenaga Kerja	(Aryanti, Nurholis, & Nashar Utamajaya, 2021)
8	*International Journal of Trend in Scientific Research and Development*	*Internet Website Analysis*	(Isooraite, 2020)
9	Jurnal Ilmiah Penelitian dan Pembelajaran Informatika	*Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)*	(Guntoro, Costaner, & Musfawati, 2020)
10	Jurnal Inovasi Teknologi dan Rekayasa	*Analysis of Web Server Security Against Structure Query Language Injection Attacks in ASEAN Senior High Schools*	(Murniati, Munadi, & Arif, 2018)
11	Jurnal Nasional Informatika dan Teknologi Jaringan	Rancang Bangun Website Toko *Online* Menggunakan Metode *Waterfall*	(Susilo, Kurniati, & Kasmawi, 2018)

Identifikasi Kerentanan

Identifikasi kerentanan keamanan *website* dalam penelitian ini mempergunakan metodologi OWASP. Penggunaan metodologi ini sebagai prosedur pengujian kerentanan keamanan secara terstruktur mengacu pada OWASP Top 10 dan *Web Security Testing Guide* v4.2. Pada perangkat lunak pendukung pengujian keamanan *website* yang sesuai untuk mengidentifikasi kerentanan, analisis kode, uji penetrasi yang sesuai dengan metodologi OWASP mempergunakan OWASP ZAP. Saat ini OWASP ZAP dikenal hanya sebagai ZAP saja dikarenakan adanya pemisahan pada tahun 2023. OWASP ZAP (Zed Attack Proxy) adalah aplikasi untuk pengujian penetrasi kerentanan oleh hacker untuk mendapatkan data dan informasi penting dari aplikasi/*website* suatu perusahaan atau organisasi. ZAP dapat memindai website secara manual dan/atau otomatis (Guntoro, Costaner, & Musfawati, 2020).

Penelitian ini mengidentifikasi tingkat kerentanan *website* Fakultas Ilmu Komputer Universitas Subang menggunakan perangkat lunak NMAP dan ZAP versi 2.14.0. Pada pelaksanaan identifikasi kerentanan keamanan website, merupakan bagian dari proses

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

pengujian dan penetrasi. Adapun katagori dalam pengujian kerentanan keamanan mempergunakan ZAP seperti pada table 2.

Tabel 2. Katagori Analyser dalam Pengujian Penestrasi

No	Analyser	No	Analyser
1	Path Traversal	25	XPath Injection
2	Remote File Inclusion	26	XML External Entity Attack
3	Heartbleed OpenSSL Vulnerability	27	Generic Padding Oracle
4	Source Code Disclosure - /WEB-INF folder	28	Cloud Metadata Potentially Exposed
5	Source Code Disclosure - CVE-2012-1823	29	Server Side Template Injection
6	Remote Code Execution - CVE-2012-1823	30	Server Side Template Injection (Blind)
7	External Redirect	31	Directory Browsing
8	Server Side Include	32	Buffer Overflow
9	Cross Site Scripting (Reflected)	33	Format String Error
10	Cross Site Scripting (Persistent) - Prime	34	CRLF Injection
11	Cross Site Scripting (Persistent) - Spider	35	Parameter Tampering
12	Cross Site Scripting (Persistent)	36	ELMAH Information Leak
13	SQL Injection	37	Trace.axd Information Leak
14	SQL Injection - MySQL	38	.htaccess Information Leak
15	SQL Injection - Hypersonic SQL	39	.env Information Leak
16	SQL Injection - Oracle	40	Hidden File Finder
17	SQL Injection - PostgreSQL	41	Spring Actuator Information Leak
18	SQL Injection - SQLite	42	XSLT Injection
19	Cross Site Scripting (DOM Based)	43	GET for POST
20	SQL Injection - MsSQL	44	User Agent Fuzzer
21	Log4Shell	45	Script Active Scan Rules
22	Spring4Shell	46	SOAP Action Spoofing
23	Server Side Code Injection	47	SOAP XML Injection
24	Remote OS Command Injection		

Hasil dan Pembahasan,

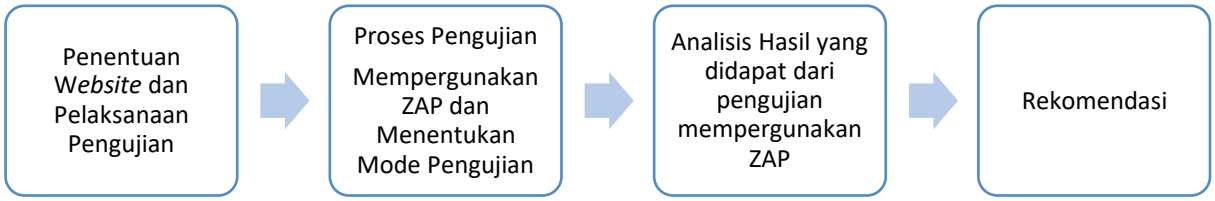
Pengujian penetrasi keamanan *website* yang dilaksanakan dalam mengetahui kerentanan pada *website* Fakultas Ilmu Komputer Universitas Subang dengan metodologi OWASP mengacu *Web Security Testing Guide* v4.2. serta mempergunakan perangkat lunak NMAP dan ZAP 2.14.0. Pada pengujian penetrasi dengan ZAP dapat dilakukan eksplorasi secara manual atau *scan* otomatis dengan beberapa mode. Mode pengujian otomatis terdiri atas empat mode yaitu:

1. *Safe Mode*. Pada mode ini tidak ada operasi yang berpotensi berbahaya yang diizinkan;
2. *Protected Mode*. Di mode pengujian ini hanya dapat melakukan tindakan (yang berpotensi) berbahaya pada URL dalam cakupannya;
3. *Standard Mode*. Pada mode ini, pengujian dijalankan tanpa membatasi apa pun;
4. *ATTACK Mode*. Pada mode ini, pengujian pada node baru yang berada dalam cakupan dipindai secara aktif segera setelah ditemukan.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Skenario Proses Pengujian

Pada skenario proses pengujian untuk identifikasi kerentanan keamanan pada *website* Fakultas Ilmu Komputer Universitas Subang seperti pada gambar 5.

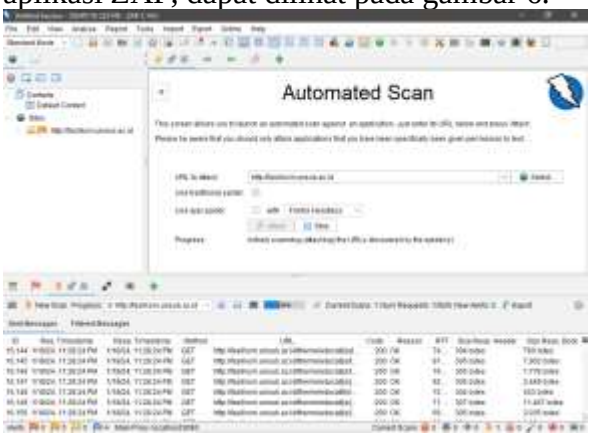


Gambar 5. Skenario Proses Pengujian

Pengujian Identifikasi Kerentanan Keamanan

- Penentuan W*ebsite* dan Pelaksanaan Pengujian
  Website: https://www.fasilkom.unsub.ac.id
  Pelaksanaan Pengujian: 18 Januari 2023

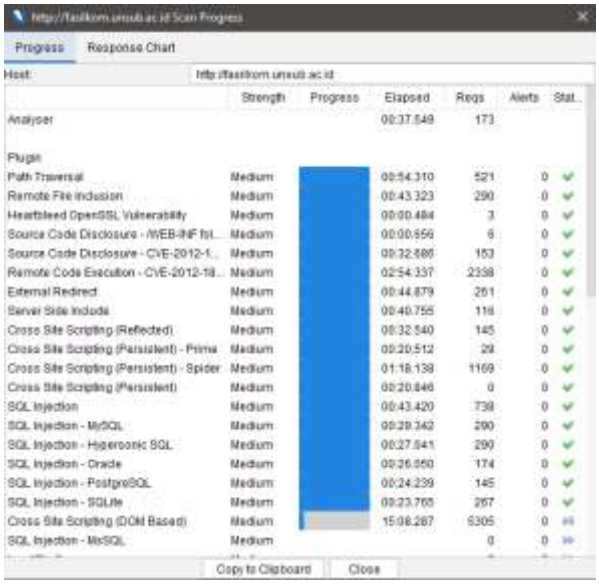
- Proses Pengujian
  Pada pengujian di penelitian ini mempergunakan aplikasi ZAP versi 2.14.0 dengan mode: *Standard Mode*
  a. Memasukan Website yang akan dilakukan pengujian kerentanan keamanan dalam aplikasi ZAP, dapat dilihat pada gambar 6.



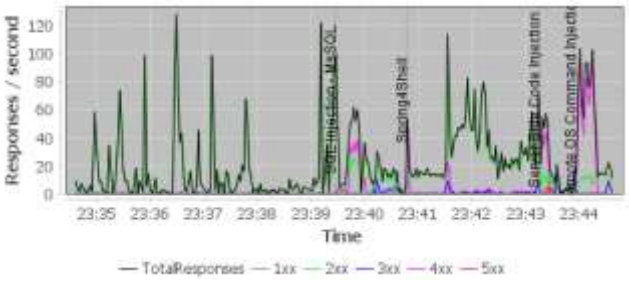
Gambar 6. Memulai Pengujian

  b. Proses Pengujian. Pada bagian ini, aplikasi melakukan pengujian sesuai dengan katagori Analyser seperti yang diuraikan di table 2, adapun prosesnya seperti pada gambar 7 dan gambar 8.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom



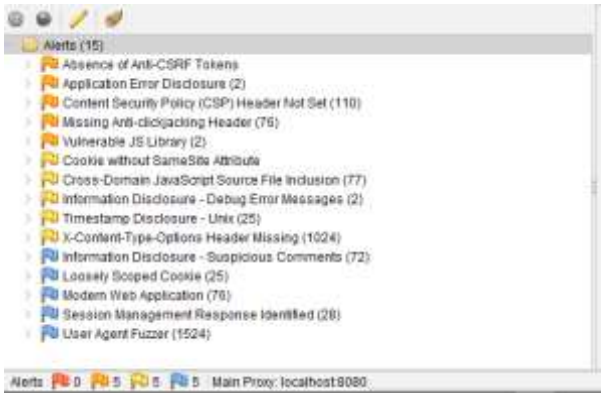
Gambar 7. Progress Pengujian



Gambar 8. Respon Chart Pengujian

- Hasil yang didapat dari pengujian. Hasil yang didapatkan dari pengujian mempergunakan aplikasi ZAP dengan *Standard Mode* diperoleh *Alret*/notifikasi katagori kerentanan sebanyak 15 notifikasi katagori kerentanan seperti pada gambar 9. Alret yang didapatkan adalah:
  a. Alret dengan risiko level *High* (Tinggi) tidak ditemukan katagori kerentanan
  b. Alret dengan risiko level *Medium* (Menengah) ditemukan sebanyak 5 notifikasi katagori kerentanan
  c. Alret dengan risiko level *Low* (Rendah) ditemukan sebanyak 5 notifikasi katagori kerentanan
  d. Alret dengan risiko level *Informational* (Informasi) ditemukan sebanyak 5 notifikasi katagori kerentanan

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom



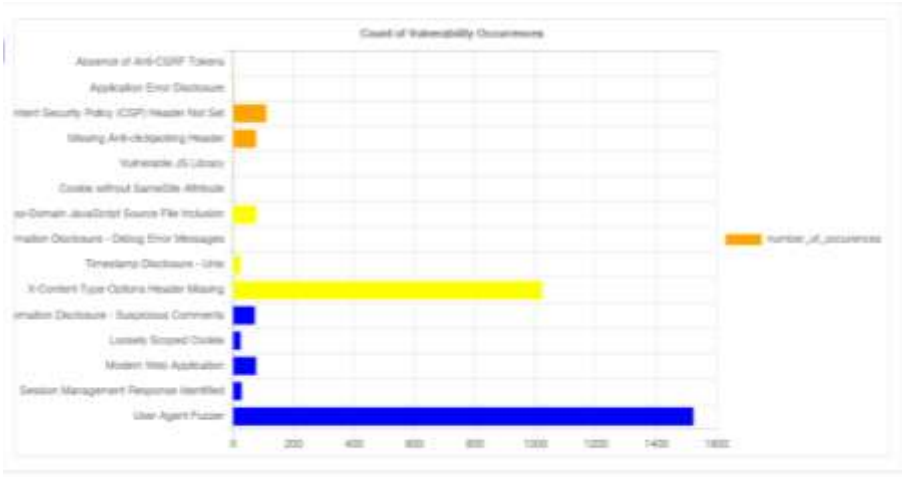
Gambar 9. Hasil Pengujian

Analisis Hasil Pengujian Kerentanan Keamanan

Grafik temuan kerentanan dapat dilihat pada gambar 19, adapun detail katagori kerentanan yang didapatkan dalam pengujian sebagai *alret*/notifikasi di *level medium, low*, dan *informational* adalah sebagai berikut:

1. *Absence of Anti-CSRF Tokens* sebanyak 1 notifikasi dengan Level Risiko Medium
2. *Application Error Disclosure* sebanyak 2 notifikasi dengan Level Risiko Medium
3. *Content Security Policy (CSP) Header Not Set* sebanyak 110 notifikasi dengan Level Risiko Medium
4. *Missing Anti-clickjacking Header* sebanyak 76 notifikasi dengan Level Risiko Medium
5. *Vulnerable JS Library* sebanyak 2 notifikasi dengan Level Risiko Medium
6. *Cookie without SameSite Attribute* sebanyak 1 notifikasi dengan Level Risiko Low
7. *Cross-Domain JavaScript Source File Inclusion* sebanyak 77 notifikasi dengan Level Risiko Low
8. *Information Disclosure - Debug Error Messages* sebanyak 2 notifikasi dengan Level Risiko Low
9. *Timestamp Disclosure - Unix* sebanyak 25 notifikasi dengan Risiko dengan Level Risiko Low
10. *X-Content-Type-Options Header Missing* sebanyak 1024 notifikasi dengan Level Risiko Low
11. *Information Disclosure - Suspicious Comments* sebanyak 72 notifikasi dengan Level Risiko Informational
12. *Loosely Scoped Cookie* sebanyak 25 notifikasi dengan Level Risiko Informational
13. *Modern Web Application* sebanyak 76 notifikasi dengan Risiko Informational
14. *Session Management Response Identified* sebanyak 28 notifikasi dengan Risiko Informational
15. *User Agent Fuzzer* sebanyak 1524 notifikasi dengan Risiko Informational

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom



Gambar 10 Tingkat Kerentanan yang Terjadi

Dalam penelitian ini yang menjadi temuan dan dilakukan identifikasi secara mendalam adalah pada temuan katagori kerentanan dengan level risiko tinggi (*high*) dan menengah (*medium*) dikarnakan memiliki dampak yang cukup signifikan. Berdasarkan hasil pengujian mempergunakan aplikasi ZAP dengan *standard mode* diidentifikasi tidak ada temuan dengan level risiko tinggi pada katagori kerentanan, akan tetapi ditemukan lima notifikasi dengan level menengah pada katagori kerentanan.

Berikut ini identifikasi dampak kerentanan (*Vulnerability Impact*) pada level katagori kerentanan menengah yang didapatkan dari hasil pengujian kerentanan keamanan:

1. *Absence of Anti-CSRF Tokens*.
   Pada kerentanan ini berdampak pada tidak ada token Anti-CSRF yang ditemukan dalam formulir pengiriman HTML, sehingga formulir kemungkinan dapat dimodifikasi;
2. *Application Error Disclosure*
   Pada kerentanan ini berdampak pada halaman yang berisi pesan kesalahan/peringatan mungkin mengungkapkan informasi sensitif seperti lokasi file yang menghasilkan pengecualian yang tidak tertangani. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut terhadap aplikasi web. Peringatan bisa menjadi *false positif* jika pesan kesalahan ditemukan di dalam halaman dokumentasi
3. *Content Security Policy* (CSP) *Header Not Set*
   Pada kerentanan ini berdampak pada Kebijakan Keamanan Konten (CSP). CSP merupakan lapisan keamanan tambahan yang membantu mendeteksi dan memitigasi jenis serangan tertentu, termasuk *Cross Site Scripting* (XSS) dan serangan injeksi data. Serangan-serangan ini digunakan untuk berbagai macam serangan mulai dari pencurian data hingga perusakan situs atau distribusi *malware*. CSP menyediakan serangkaian *header* HTTP standar yang memungkinkan pemilik situs web mendeklarasikan sumber konten yang disetujui dan boleh dimuat oleh browser di halaman tersebut seperti JavaScript, CSS, bingkai HTML, *font*, gambar, dan objek yang dapat disematkan seperti Java applet, ActiveX, file audio dan video
4. *Missing Anti-clickjacking Header*
   Kerentanan ini berdampak pada respon yang tidak mencakup kebijakan keamanan konten dengan arahan 'frame-ancestors' atau X-Frame-Options untuk melindungi dari serangan 'ClickJacking'

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

5. *Vulnerable JS Library*
   Kerentanan ini berdampak pada identifikasi kerentanan di library jquery, versi 1.12.4

Penutup (Simpulan dan Saran)

Berdasarkan dari hasil pengujian untuk identifikasi kerentanan keamanan pada *website* Fakultas Ilmu Komputer Universitas Subang didapatkan sebanyak 15 notifikasi katagori kerentanan. Katagori notifikasi dari hasil pengujian identifikasi kerentanan ditemukan 5 notifikasi katagori kerentanan level risiko menengah, 5 katagori kerentanan notifikasi level rendah dan 5 katagori kerentanan notifikasi level informasi. Walaupun hanya 15 katagori notifikasi, total dari alert/notifikasi seluruh kerentanan yang ditemukan sebanyak 3045 notifikasi.

Berdasarkan hasil yang di dapat dari identifikasi kerentanan, maka rekomendasi yang disarankan dari penelitian ini Fakultas Ilmu Komputer Universitas Subang diharapkan sesegera mungkin fakultas melakukan tindakan menutup celah-celah kerentanan yang didapatkan dari hasil pengujian kerentanan. Hal ini agar *website* Fakultas Ilmu Komputer Universitas Subang dari terkena serangan siber yang dapat mengakibatkan dampak buruk bagi reputasi fakultas maupun kemungkinan dampak finansial yang mungkin timbul ataupun kemungkinan dampak lainnya.

Daftar Pustaka

Aryanti, D., Nurholis, & Nashar Utamajaya, J. (2021, Maret). Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja. *Syntax Fusion : Jurnal Nasional Indonesia, 1*(3), 15-25. Retrieved 2024

Bennetts, S. (2023, August 1). *ZAP is Joining the Software Security Project*. Retrieved 2024, from THE ZAP BLOG: https://www.zaproxy.org/blog/2023-08-01-zap-is-joining-the-software-security-project/

Bimandaru, A., Alamsyah, & Nugroho, A. (2023). Analisis Pengujian Penetrasi Pada Layanan Hosting Menggunakan Metode Black Box (Studi kasus : Blogspot, Wordpress dan Shared Hosting). *Jurnal FORISTEK, 14*(1), 1-12. doi:10.54757/fs.v14i1.238

Dewa Gede Govindha Dharmawangsa, I., Made Arya Sasmita, G., & Putu Agus Eka Pratama, I. (2023, April 1). Penetration Testing Berbasis OWASP Testing Guide. *Jurnal Ilmiah Teknologi dan Komputer, 4*(1).

Direktorat_Operasi_Keamanan_Siber. (2022). *Lanskap Keamanan Siber Indonesia 2022.* Jakarta: Badan Siber dan Sandi Negara.

Guntoro, G., Costaner, L., & Musfawati, M. (2020, Juni). Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning). *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, 5*(1), 45-55. doi:10.29100/jipi.v5i1.1565

Hasibuan, M., & Marwan Elhanafi, A. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box Studi Kasus Web Server Diva Karaoke.co.id. *SUDO Jurnal Teknik Informatika, 1*(4), 171-177. doi:10.56211/sudo.v1i4.160

ISO/IEC. (2022). International Standard ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO/IEC.

p-ISSN 2086-7395 | e-ISSN 2964-8785
http://ejournal.unsub.ac.id/index.php/Fasilkom

Isooraite, M. (2020). Internet Website Analysis. *International Journal of Trend in Scientific Research and Development, 5*(1), 9–12.

Murniati, Munadi, R., & Arif, T. Y. (2018, June). Analysis of Web Server Security Against Structure Query Language Injection Attacks in ASEAN Senior High Schools. *Jurnal Inovasi Teknologi dan Rekayasa, 3*(1), 1-7. doi:10.31572/inotera.Vol3.Iss1.2018.ID41

Nurbojatmiko, Lathifah, A., & Bil Amri, F. (2022). Security Vulnerability Analysis of the Sharia Crowdfunding Website Using OWASP-ZAP. *2022 10th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). Yogyakarta, Indonesia: IEEE. doi:10.1109/CITSM56380.2022.9935837

OWASP Foundation, I. (2021). *OWASP Top Ten - 2021*. Retrieved 2024, from OWASP: https://owasp.org/www-project-top-ten/ ; https://owasp.org/Top10/id/

OWASP Foundation, I. (2023). *OWASP Web Security Testing Guide*. Retrieved 2024, from OWASP: https://owasp.org/www-project-web-security-testing-guide/

OWASP Foundation, I. (2023). *Testing Tools Resource*. Retrieved from OWASP: https://owasp.org/www-project-web-security-testing-guide/stable/6-Appendix/A-Testing_Tools_Resource

OWASP Foundation, I. (2024). *About the OWASP Foundation*. Retrieved 2024, from OWASP: https://owasp.org/about

Saad, E., & Mitchell, R. (2020). *OWASP Web Security Testing Guide v4.2*. OWASP Foundation, Inc.

Saktiansyah, A., & Muharrom, M. (2023, September). Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas. *International Journal of Engineering and Computer Science Applications, 2*(2), 51-58. doi:10.30812/IJECSA.v2i2.3297

Susilo, M., Kurniati, R., & Kasmawi. (2018, Maret). Rancang Bangun Website Toko Online Menggunakan Metode Waterfall. *Jurnal Nasional Informatika dan Teknologi Jaringan, 2*(2), 98-105. doi:10.30743/infotekjar.v2i2.171

The_Linux_Foundation. (2023). *Welcoming ZAP to the Software Security Project*. (O. Arasaratnam, Editor) Retrieved 2024, from The Software Security Project: https://softwaresecurityproject.org/blog/welcoming-zap-to-the-software-security-project/

The_MITRE_Corporation. (2024). *CVE® Program Mission*. Retrieved from CVE: https://www.cve.org

Yudiana, Elanda, A., & Lintang Buana, R. (2021, Juli 2). Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma dengan Menggunakan OWASP Top 10. *Journal of Computer Engineering System and Science, 6*(2), 185-191. doi:10.24114/cess.v6i2.24777

ZAP_Dev_Team. (2024). *Download ZAP*. Retrieved 2024, from ZAP: https://www.zaproxy.org/download/

ZAP_Dev_Team. (2024). *Zed Attack Proxy (ZAP)*. Retrieved 2024, from https://www.zaproxy.org