JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 7 No 3 – December 2024 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Identifikasi Celah Kerentanan Keamanan Pada Website Dengan Metode Pengujian Penetrasi OWASP ZAP

Devani Laras Sati[1], Devina Laras Sita[2] , Khairunnisak Nur Isnaini[3]

[1,2,3]Departemen Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto
Jl. Letjend Pol. Soemarto No. 126, Purwokerto, Indonesia

e-mail: devanilarassati@gmail.com[1], devinalarassita2001@gmail.com[2],
nisak@amikompurwokerto.ac.id[3]
Kontak WA: 08986660369[3]

Received : June, 2024	Accepted : November, 2024	Published : December, 2024

Abstract

Resepedia is a website that presents a variety of food recipes and culinary articles. In addition, resepedia also stores user data including sensitive information such as names, emails, and passwords. The existence of this information carries a potential security risk, which can cause potential leakage of user data that can make misuse of data or information. Therefore, this study uses OWASP Zed Attack Proxy (OWASP ZAP) to identify security holes and evaluate potential risks on the Resepedia website. The results identified 16 types of potential threats, with 3 categories having a Medium threat level, 6 categories having a Low threat level, and 7 categories being Informative. Thus, the level of information security on the Resepedia website is considered to be at the Medium level. This research proves that OWASP ZAP can be used to identify information security vulnerabilities based on the results obtained. This research is expected to provide an in-depth understanding, comprehensive security risk analysis, and become the foundation for further research related to security analysis on the website.

Keywords: *security vulnerabilities, vulnerability, information security, OWASP ZP, security*

Abstrak

Resepedia merupakan website yang menyajikan beragam resep makanan dan artikel kuliner. Selain itu, resepedia juga menyimpan data pengguna termasuk informasi sensitif seperti nama, email, dan password. Keberadaan informasi ini membawa potensi risiko keamanan yaitu dapat menyebabkan terjadinya potensi kebocoran data pengguna yang dapat membuat penyalahgunaan data atau informasi. Oleh karena itu, penelitian ini menggunakan OWASP Zed Attack Proxy (OWASP ZAP) untuk mengidentifikasi celah keamanan dan mengevaluasi potensi risiko pada website Resepedia. Hasil penelitian mengidentifikasi 16 jenis potensi ancaman, dengan 3 kategori memiliki tingkat ancaman Medium, 6 kategori memiliki tingkat ancaman Low, dan 7 kategori bersifat Informatif. Dengan demikian, tingkat keamanan informasi pada website Resepedia dinilai berada pada tingkat Medium. Penelitian ini membuktikan bahwa OWASP ZAP dapat digunakan untuk mengidentifikasi celah kerentanan keamanan informasi berdasarkan hasil yang diperoleh. Penelitian ini diharapkan dapat memberikan pemahaman mendalam, analisis risiko keamanan yang komprehensif dan menjadi landasan bagi penelitian selanjutnya terkait analisis keamanan pada website.

Kata Kunci: *celah kerentanan keamanan, kerentanan, keamanan informasi, OWASP ZP, keamanan*

1. PENDAHULUAN

Menurut data dari Pengelola Nama Domain Internet Indonesia (PANDI), hingga bulan September 2023, jumlah pengguna domain tercatat mencapai 794.978 pengguna. [1]. Hal ini menunjukkan bahwa masyarakat semakin menyadari pentingnya keberadaan website di era digital, di mana website memiliki fungsi yang sangat penting untuk membangun sarana daring [2].

Menurut databoks, survei yang dilakukan oleh Bank DBS terhadap konsumen di Indonesia menunjukkan bahwa 69% responden memilih untuk memasak di rumah setelah penyebaran Covid-19 di dalam negeri. Persentase ini meningkat dibandingkan dengan sebelum pandemi, di mana hanya 42% yang memilih untuk memasak di rumah. [3]. Untuk memenuhi kebutuhan masyarakat dalam memasak, sebuah website yang menyajikan berbagai resep makanan telah dibuat. Dengan adanya website ini, masyarakat dapat mengakses beragam resep dan langsung mempraktikkannya di rumah. Selain itu, pengguna juga memiliki kesempatan untuk membagikan resep makanan yang mereka buat melalui platform tersebut.

Terdapat banyak website yang menyajikan resep makanan, salah satunya adalah Resepedia, yang dapat diakses melalui tautan berikut:
[https://resepedia.id/] (https://resepedia.id/).
Resepedia adalah platform yang menyediakan berbagai resep masakan dan artikel mengenai kuliner. Di website ini, pengguna dapat menemukan berbagai resep makanan serta membagikan resep kreasi mereka kepada pengguna lain.

Selain berisi berbagai macam resep makanan, website Resepedia juga memuat informasi data pengguna website. Informasi tersebut mengenai nama, email, dan password [4]. Banyak risiko yang dapat muncul jika website Resepedia tidak menerapkan dasar keamanan yang memadai. Bahaya dari pihak-pihak tidak bertanggung jawab dapat menggunakan kerentanan keamanan tersebut, yang pada akhirnya dapat merugikan baik pengguna Resepedia maupun pengembang website itu sendiri [5]. Dengan menerapkan dasar keamanan yang baik, kepercayaan publik dalam menyimpan informasi akan meningkat. Hal ini juga berdampak positif pada reputasi website, serta mengurangi kekhawatiran pengguna terkait penyalahgunaan data pribadi [6]. Oleh karena itu, diperlukan adanya keamanan informasi.

Dalam konteks keamanan informasi secara umum, beberapa jenis risiko yang perlu diidentifikasi. Secara umum, hal-hal yang memicu risiko mungkin dihadapi oleh sebuah website meliputi masalah seperti malware, virus, dan serangan SQL Injection [7]. Agar menanggulangi serangan siber dan risiko kemananan, penting untuk melakukan penilaian risiko pada keamanan informasi yang dapat mengganggu atau merugikan perusahaan atau komunitas. Evaluasi risiko memiliki fungsi sebagai panduan untuk melakukan mitigasi atau pemulihan serta untuk mencegah aktivitas yang tidak diinginkan [8].

Penilaian risiko kerentanan pada sebuah aplikasi website bias dilakukan dengan berbagai cara, salah satunya adalah menggunakan OWASP [9]. OWASP Zed Attack Proxy (OWASP Zap) yaitu alat yang digunakan untuk mengidentifikasi bermacam celah keamanan dalam website selama fase pengingkatan dan evaluasi aplikasi tersebut [10]. OWASP adalah sebuah organisasi nirlaba yang berstatus 501(c) yang berfokus pada penelitian komunitas dan mengkategorikan risiko-risiko dalam keamanan informasi [20]. Keanggotaan OWASP terdiri dari ilmuwan, peneliti, dan profesional dari sektor swasta yang menerbitkan laporan, artikel, alat, dan dokumen yang bersifat sumber terbuka [11]. Pemilihan kerangka kerja OWASP pada observasi ini didasarkan pada argumen yang diajukan oleh para ahli keamanan. Keputusan ini dipengaruhi oleh ketersediaan perangkat lunak sumber terbuka dan perbandingannya dengan alat-alat di pasar yang dianggap masih terlalu mahal [12].

Pentingnya faktor keamanan informasi pada pembuatan website Resepedia, maka penelitian ini bertujuan menggunakan OWASP ZAP untuk menemukan celah keamanan dan mengidentifikasi resiko-resiko keamanan website. Terbukti ditemukan 16 jenis peluang ancaman, dengan 3 kategori mempunyai

urutan ancaman Medium, 6 kategori lainnya mempunyai urutan bahaya Low dan 7 Informational. Oleh karena itu, dapat disimpulkan bahwa, urutan keamananan web Resepedia ada di level menengah.

Tujuan penelitian ini mengidentifikasi kerentanan website hingga menerapkan evaluasi risiko keamanan informasi agar website Resepedia aman dari bermacam ancaman dikemudian hari [20]. Di samping itu, hasil observasi ini juga bisa menjadi landasan bagi peneliti selanjutnya dengan topik analisis keamanan pada website.

2. PENELITIAN TERKAIT

Penelitian mengenai keamanan website yang juga mengggunakan metode OWASP dilakukan pada website Jago Masak. Dari hasil penelitian ini, dapat diidentifikasi kelemahan pada website Jago Masak yang dapat digunakan untuk meningkatkan keamanan situs tersebu [13].

Penelitian selanjutnya mengenai penilaian risiko keamanan yang dilakukan pada website IITC menggunakan metode DREAD dan ISO 27005:2018 memperoleh nilai 11,5. Ini mengindikasikan bahwa website IITC berada pada tingkat risiko sedang, yang berarti website tersebut masih dapat digunakan, tetapi memerlukan beberapa prioritas perbaikan [14].

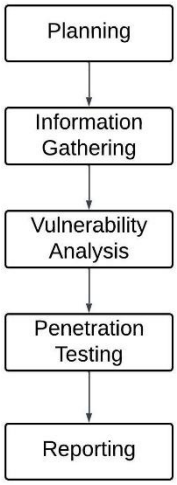
Penelitian selanjutnya mengenai penilaian risiko keamanan pada website UPN "Veteran" Yogyakarta menggunakan metode OWASP dan ISAAF. Hasilnya menunjukkan adanya beberapa kerentanan, yaitu satu kerentanan dengan tingkat tinggi, tiga dengan tingkat menengah, dan enam dengan tingkat rendah. Dari temuan tersebut, tingkat kerentanan website tersebut berada pada level menengah [15]

Penelitian lain berfokus pada analisis keamanan fisik di Universitas X menggunakan model kematangan untuk memastikan bahwa keamanan fisik yang sesuai dengan prinsip CIA (kerahasiaan, integritas, ketersediaan). Hasil penelitian ini menunjukkan bahwa Universitas X membutuhkan peningkatan keamanan fisik, seperti penambahan fasilitas prasarana berupa sistem sidik jari atau pengendalian biometrik khusus di pusat data dan ruang pengelolaan teknologi informasi [16].

Penelitian berikutnya mengenai penilaian risiko keamanan di web Universitas Singaperbangsa Karawang memakai metode OWASP menunjukkan bahwa website tersebut tidak memiliki celah keamanan yang berisiko tinggi [5].

3. METODE PENELITIAN

Pengujian penetrasi adalah langkah krusial dalam pengembangan sistem pertahanan yang berbasis komputer dan terhubung dalam suatu jaringan [13]. Pada website Resepedia, pengujian ini diperlukan untuk menilai tingkat keamanan informasi pengguna. Resepedia adalah sebuah startup yang telah diluncurkan secara global, sehingga dapat diakses oleh siapa saja. Uji coba ini dilakukan untuk mengidentifikasi berbagai kerentanan yang ada pada website Resepedia saat ini.



Gambar 1: Tahapan Penelitian

Rancangan tahapan penelitian akan diuraikan sebagai berikut:

1. Planning

Dalam fase perencanaan, kami akan merancang cakupan pengujian penetrasi mulai dari penentuan ruang hingga metode pengujian yang akan diterapkan [5].

2. Information Gathering

Tahap pengumpulan informasi melibatkan proses pengumpulan data umum yang berkaitan dengan target pengujian. Informasi yang dikumpulkan mencakup data tentang alamat IP target, registrant, dan administrator, serta informasi terkait lainnya seperti pencarian DNS dan pencarian IP [15].

3. Vulnerability Analysis

Mencari potensi kerentanan keamanan yang dapat diidentifikasi melalui metode manual maupun dengan menggunakan alat otomatis, tergantung pada perangkat yang digunakan. [5]. Pada tahap ini kami menggunakan tools OWASP ZP.

4. Penetration Testing

Tahap yang dilakukan yaitu uji coba serangan dari penentuan target. Selain itu memilih alat yang tepat untuk analisis. Umumnya, tahap ini melibatkan serangan aplikasi web, seperti cross-site scripting dan SQL Injection [19], untuk menemukan kerentanan yang ada pada target.

5. Reporting

Pada tahap akhir yaitu menyusun laporan berdasarkan parameter keamanan dari OWASP Top 10-2021 [5].

4. HASIL DAN PEMBAHASAN

Open W*eb Aplication Security Project* atau *OWASP* adalah suatu komunitas internasional non-profit yang focus pada bidang keamanan website. OWASP memberikan pengujian gratis pada keamanan website, sehingga mempermudah developer website dalam memastikan keamanan websitenya [18]. Pengujian tersebut yaitu *OWASP ZAP* yang terdiri dari beberapa tahapan yang meliputi *planning, information gathering, vulnerability analysis, penetration testing, dan reporting* [21]. Hasil dari pengujian ini akan dijelaskan pada tahap reporting, dimana hasil tersebut didapatkan Ketika *penetration testing.*

4.1 Planning

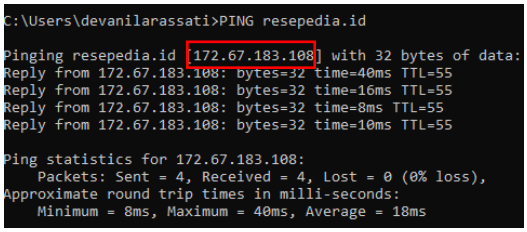
Perencanaan merupakan tahapan awal yang sangat penting dalam pelaksanaan penetration testing [5]. Menetapkan objek dan ruang lingkup pengujian adalah bagian integral dari proses perencanaan tersebut. Dalam konteks ini, objek pengujian yang akan ditetapkan adalah situs web Resepedia dengan nama domain respedia.id.

Gambar 2: Web Resepedia

Pada Gambar 2 merupakan tampilan utama halaman website resepedia yang menyajikan berbagai resep masakan.

4.2 Information Gathering

Pada langkah ini dilakukan pencarian informasi pada website yang akan diobservasi yaitu Resepedia. Berikut adalah hasil pencarian informasi IP Address dengan command prompt pada Gambar 3.

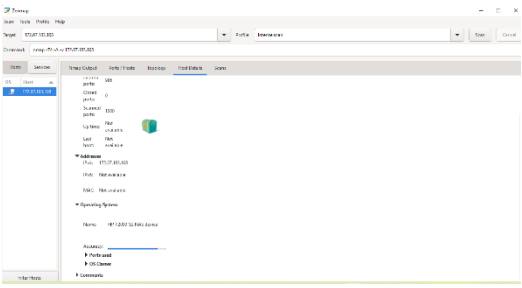


Gambar 3: IP Address Web Resepedia

IP Address yang sudah diketahui, kemudian digunakan untuk mencari informasi Domain, nama domain, port, status, system operasi yang digunakan, dan waktu pemakaian domain. Pada Gambar 4 adalah hasil pencarian informasi terhadap website yang akan diteliti yaitu Resepedia. Berikut adalah hasil pencarian memakai aplikasi Whois Domain yang tampak pada Gambar 4. Informasi yang didapatkan yaitu nama domain id, domain name, dan jangka waktu pemakaian domain.

Gambar 4: Informasi Domain Web Resepedia

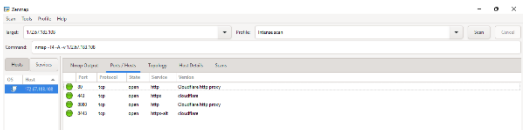
Tahap berikutnya akan dilakukan OS fingerprint untuk mengenali jenis sistem operasi yang dipakai di server Resepedia. Pengujian OS fingerprint akan digunakan tool zenmap [17]. Sehingga diperoleh hasil HP 2000 G3 Nas Device dengan tingkat akurasi 90% yang tampak pada Gambar 5.



Gambar 5: Sistem Operasi Yang Dipakai Web Resepedia

Dari Gambar 5 diperoleh beberapa informasi mengenai website resepedia yaitu windows server.

Lalu, selanjutnya mencari port yang digunakan pada web resepedia. Pencarian informasi port menggunakan tool zenmap. Hasil pencarian didapatkan port yang digunakan yaitu 80, 443, 8080, 8443. Terlihat pada Gambar 6.



Gambar 6: Port Web Resepedia

Setelah dilakukan pengumpulan informasi pada web Resepedia, didapatkan beberapa informasi web Resepedia yang dapat terlihat di Tabel 1.

Tabel 1: Hasil Pengumpulan Informasi

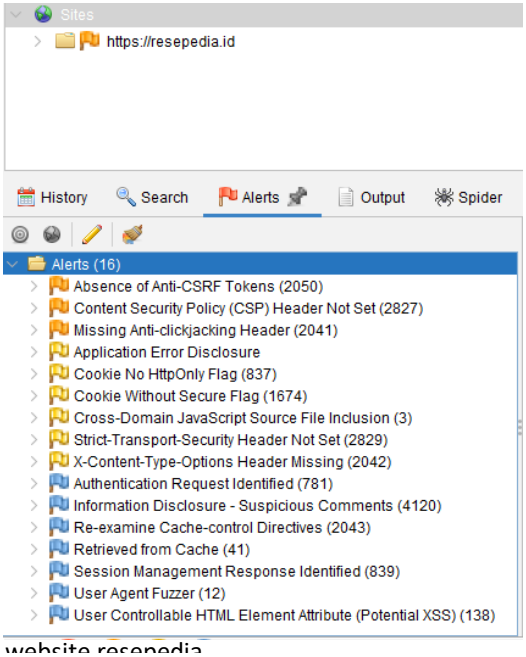
Hasil Pengumpulan Informasi Web Resepedia

Domain ID	PANDI D02130156
Domain Name	Resepedia.id
Create On	20 April 2020
Expiration Date	20 April 2025
Status	ClientTransferProhibited
IP Address	172.67.183.108
Port	80, 443, 8080, 8443
Sistem Operasi	HP 2000 G3 Nas Device

Tabel 1 berisi kumpulan informasi mengenai website resepedia yang terdiri dari domain, waktu masa pemakaian domain, ip address dan port dari website resepedia.

4.3 Vulnerability Analysis

Tahap ke tiga melakukan proses vulnerability analysis pada domain resepedia.id. Pada proses ini bertujuan untuk menemukan kelemahan yang ada dalam system menggunakan tools OWASP ZAP. Hasil analysis dapat dilihat pada Gambar 7.



Gambar 7: Vulnerability Analysis dengan Tool OWASP

4.4 Penetration Testing

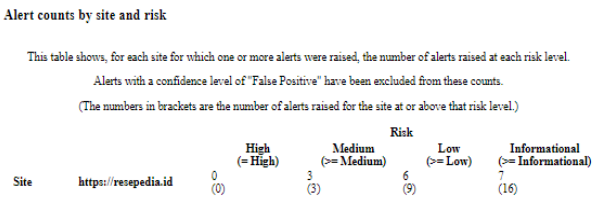
Dari evaluasi vulnerability analysis memberikan informasi kerentanan keamanan pada website resepedia.id. Berdasarkan dari hasil kerentanan diperoleh, celah keamanan seperti berikut.

1. Absence of Anti-CSRF Tokens
2. Missing Anti-clickjacking Header
3. Absence of Content Security Policy (CSP) Header
4. Application Error Disclosure
5. Cookie No HttpOnly Flag
6. Cookie Without Secure Flag
7. Cross-Domain JavaScript Source File Inclusion
8. Strict-Transport-Security Header Not Set, dll.

4.5 Reporting

Berikutnya dari hasil scanning memakai alat otomatisasi OWASP Zap yang dikembangkan

menunjukkan terdapat 16 kategori peluang ancaman dengan 3 kategori memiliki tingkat ancaman Medium, 6 kategori lainya memiliki tingkat ancaman rendah dan 7 Informational yang tampak di Gambar 8.



Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.
Alerts with a confidence level of "False Positive" have been excluded from these counts.
(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://resepedia.id	0 (0)	3 (3)	6 (9)	7 (16)

Gambar 8. Hasil Scanning OWASP ZAP

Dari hasil pengujian dengan tools OWASP ZAP didapatkan informasi berbagai jenis celah keamanan pada web resepedia.id dengan tingkatannya banyaknya celah-celah keamanan dapat dilihat pada Tabel 2.

Tabel 2: Kategori Ancaman Hasil Scanning OWASP ZAP
[Sumber: Report OWASP ZAP]

Tingkat Ancaman	Jenis Ancaman	Jumlah
MEDIUM	Absence of Anti-CSRF Tokens	1753
MEDIUM	Content Security Policy (CSP) Header Not Set	2345
MEDIUM	Missing Anti-clickjacking Header	1743
LOW	Application Error Disclosure	1
LOW	Cookie No HttpOnly Flag	607
LOW	Cookie Without Secure Flag	1214
LOW	Cross-Domain JavaScript Source File Inclusion	3
LOW	Strict-Transport-Security Header Not Set	2348
LOW	X-Content-Type-Options Header Missing	1745
INFORMATIONAL	Authentication Request Identified	597
INFORMATIONAL	Information Disclosure - Suspicious Comments	3526
INFORMATIONAL	Re-examine Cache-control Directives	1745
INFORMATIONAL	Retrieved from Cache	40
INFORMATIONAL	Session Management Response Identified	608
INFORMATIONAL	User Agent Fuzzer	12
INFORMATIONAL	User Controllable HTML Element Attribute (Potential XSS)	75

Berdasarkan hasil pengujian OWASP didapatkan 3 celah keamanan berada pada level medium sehingga diperlukan solusi untuk mengatasi celah keamanannya yang dapat dilihat pada Tabel 3.

Tabel 3: Rekomendasi Mengatasi Jenis Ancaman

Jenis Ancaman	Solusi
Absence of Anti-CSRF Tokens	Gunakan token khusus untuk memastikan bahwa permintaan yang datang ke server berasal dari pengguna yang sah. Token ini seperti kunci yang harus dimiliki oleh pengguna untuk mengirim permintaan.
Content Security Policy (CSP) Header Not Set	Terapkan header CSP pada server web Anda. CSP memungkinkan untuk mengendalikan sumber daya yang dapat dimuat oleh browser dari halaman web Anda. Anda dapat mengatur aturan untuk memblokir sumber daya yang tidak diizinkan, mengurangi risiko injeksi skrip, dan perlindungan lainnya.
Missing Anti-clickjacking Header	Aktifkan header HTTP yang disebut "X-Frame-Options" dan atur nilainya ke "DENY" atau "SAMEORIGIN". Ini akan mencegah halaman web dimuat dalam bingkai (frame) yang disediakan oleh domain lain, yang dapat digunakan dalam serangan clickjacking.

Dari Tabel 3 dapat dilihat untuk solusi dari setiap ancaman pada website berbeda-beda, tergantung jenis ancamannya [18].

5. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan pada website resepedia.id menggunakan OWASP ZAP untuk menemukan celah keamanan dan mengidentifikasi resiko-resiko keamanan website, diperoleh Hasil scanning menggunakan alat OWASP ZAP menunjukkan terdapat 16 kategori peluang ancaman dengan 3 kategori memiliki tingkat ancaman Medium, 6 kategori lainya memiliki tingkat ancaman rendah dan 7 Informational yang tampak. Berdasarkan informasi yang sudah didapatkan, melakukan penetrasi testing dengan menggunakan OWASP ZAP terbukti cukup optimal karena dapat mengetahui celah-celah keamanan yang ada pada website seperti clickjacking. Saran perbaikan yang diberikan diharapkan mampu memberikan gambaran mengenai prioritas perbaikan yang bisa digunakan pada website Resepedia.

Penelitian berikutnya dapat dilakukan diantaranya yang pertama dengan mengkaji lebih dalam risiko keamanan informasi berdasarkan aset-aset informasi yang ada didalam sebuah website. Kedua, pengenalan risiko dapat dilakukan dengan memakai alat selain OWASP ZP seperti OpenVAS, Nessus, dan lainnya.

DAFTAR PUSTAKA

[1] Pandi. “Laporan Statistik”. Internet: https://pandi.id/laporan-statistik, Oktober, 2023 [Nov. 2 2023].[2] F. Kurniawan, "Pengguna website di Indonesia naik 61,6% sepanjang 2020." Internet: https://tekno.sindonews.com, 25 Maret 2021 [Jan. 1, 2024] Fikri Kurniawan, “Pengguna Website di Indonesia Naik 61,6% Sepanjang 2020,” tekno.sindonews.com.

[3] A. Lidwina, "Masyarakat lebih sering memasak di rumah sejak pandemi Covid-19." Internet: https://databoks.katadata.co.id, 15 Juli 2020 [Jan. 2, 2024]. Andrea Lidwina,

"Masyarakat Lebih Sering Memasak di Rumah sejak Pandemi Covid-19," databoks.katadata.co.id.[4] D. Irawan, "Mencuri informasi penting dengan mengambil alih akun Facebook dengan metode phising," *JIKI (Jurnal Ilmu Komputer & Informatika),* vol. 1, no. 1, pp. 43-46, 2020. D. Irawan and S. Kom, "MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING," 2020.

[5] M. R. Ramdani, N. Heryana, and A. S. Y. Irawan, "Penetration testing pada website Universitas Singaperbangsa Karawang menggunakan Open Web Application Security Project (OWASP)," *Jurnal Pendidikan dan Konseling (JPDK),* vol. 4, no. 4, pp. 5522-5529, 2022. J. Pendidikan and D. Konseling, "Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)."

[6] M. D. K. Perdani, Widyawan, dan P. I. Santosa, "Blockchain untuk keamanan transaksi elektronik perusahaan financial technology (studi kasus pada PT XYZ)," *Semnasteknomedia Online*, vol. 6, no. 1, pp. 1-14, 2018. M. Dolorosa Kusuma Perdani and P. Insap Santosa, "BLOCKCHAIN UNTUK KEAMANAN TRANSAKSI ELEKTRONIK PERUSAHAAN FINANCIAL TECHNOLOGY (STUDI KASUS PADA PT XYZ)," UNIVERSITAS AMIKOM Yogyakarta, 2018.

[7] T. Adianto, Y. Ali, dan E. Saptono, "Penilaian risiko serangan siber pada sistem manajemen keamanan informasi PT. UAV," *Manajemen Pertahanan: Jurnal Pemikiran dan Penelitian Manajemen Pertahanan*, vol. 6, no. 1, 2020. T. Adianto, Y. Ali, E. Saptono, : Penilaian, R. Serangan, and S. Pada…, "RISK ASSESSMENT OF CYBER ATTACKS ON INFORMATION SECURITY MANAGEMENT SYSTEM OF PT. UAV." [Online]. Available: https://jatim.sindonews.com/read/8917/1/bssn-sebut-ada-10-sektor-yang-rentan-serangan-siber-

[8] Jonny, J., and Darujati, C., "Penilaian risiko data sistem informasi manajemen puskesmas dan aset menggunakan ISO 27005," *Sistemasi: Jurnal Sistem Informasi,* vol. 10, no. 1, pp. 13-25, 2021. J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset Menggunakan ISO 27005," SISTEMASI, vol. 10, no. 1, p. 1, Jan. 2021, doi: 10.32520/stmsi.v10i1.995.

[9] Listartha, I. M. E., Mitha, I. M. A. P., Arta, M. W. A., dan Arimika, I. K. W. Y., "Analisis kerentanan website SMA Negeri 2 Amlapura menggunakan metode OWASP (Open Web Application Security Project)," *Jurnal Sistem Informasi dan Sistem Komputer*, vol. 7, no. 1, pp. 23-27, 2022. I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, and I. Km. W. Yuda Arimika, "Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project)," SIMKOM, vol. 7, no. 1, pp. 23–27, Jan. 2022, doi: 10.51717/simkom.v7i1.63.

[10] A. C. Izumi dan I. R. Widiasari, "'SIASAT' UKSW (Universitas Kristen Satya Wacana) website security analysis using OWASP (Open Web Application Security Project)," *Jurnal Teknik Informatika (JUTIF)*, vol. 3, no. 3, 2022. A. Calvina Izumi and I. R. Widiasari, "'SIASAT' UKSW (UNIVERSITAS KRISTEN SATYA WACANA) WEBSITE SECURITY ANALYSIS USING OWASP (OPEN WEB APPLICATION SECURITY PROJECT)," Jurnal Teknik Informatika (JUTIF), vol. 3, no. 3, 2022, doi: 10.20884/1.jutif.2022.3.3.346.

[11] B. Appiah, E. Opoku-Mensah, dan Z. Qin, "SQL injection attack detection using fingerprints and pattern matching technique," in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, IEEE, Nov. 2017, pp. 583–587. B. Appiah, E. Opoku-Mensah, and Z. Qin, "SQL injection attack detection using fingerprints and pattern matching technique," in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), IEEE, Nov. 2017, pp. 583–587. doi: 10.1109/ICSESS.2017.8342983.

[12] A. Kurniawan, "Penerapan framework OWASP dan network forensics untuk analisis, deteksi, dan pencegahan serangan injeksi di sisi host-based," *Jurnal Telematika*, vol. 14, no. 1, pp. 9-18, 2019. A. Kurniawan, “Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based,” Jurnal Telematika, vol. 14, no. 1.

[13] R. V. Aditama dan E. S. Negara, "Pemindai kerentanan terhadap website Jago Masak dengan metode pengujian penetrasi OWASP ZAP," *Jurnal Mantik*, vol. 6, no. 3, pp. 3406-3412, 2022. R. V. Aditama and E. S. Negara, “Pemindai Kerentanan Terhadap Website Jago Masak Dengan Metode Pengujian Penetrasi OWASP ZAP”.

[14] G. C. Utami, A. B. Supramaji, dan K. N. Isnaini, "Penilaian risiko keamanan informasi pada website dengan metode DREAD dan ISO 27005:2018," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 8, no. 1, pp. 47–56, Feb. 2023. Gina Cahya Utami, Aden Bahtiar Supramaji, and Khairunnisak Nur Isnaini, “Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018,” JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), vol. 8, no. 1, pp. 47–56, Feb. 2023, doi: 10.32528/justindo.v8i1.219.

[15] H. Sofyan, M. Sugiarto, dan B. M. Akbar, "Implementation of penetration testing on websites to improve security of information assets UPN 'Veteran' Yogyakarta," *Telematika: Jurnal Informatika dan Teknologi Informasi*, vol. 20, no. 2, pp. 153-162, 2023. I. Uji et al., “Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN ‘Veteran’ Yogyakarta,” Jurnal Informatika dan Teknologi Informasi, vol. 20, no. 2, pp. 153–162, 2023, doi: 10.31515/telematika.v20i2.7757.

[16] K. N. Isnaini dan S. A. Solikhatin, "Information security analysis on physical security in University X using maturity model," *Jurnal Informatika*, vol. 14, no. 2, pp. 76-84, 2020. K. N. Isnaini and S. A. Solikhatin, “Information security analysis on physical security in university x using maturity model,” Jurnal Informatika, vol. 14, no. 2, p. 76, May 2020, doi: 10.26555/jifo.v14i2.a14434.

[17] I. R. Widiasari, "'SIASAT' UKSW (Universitas Kristen Satya Wacana) website security analysis using OWASP (Open Web Application Security Project)," *Jurnal Teknik Informatika (Jutif)*, vol. 3, no. 3, pp. 763-770, 2022. A. Calvina Izumi and I. R. Widiasari, “‘SIASAT’ UKSW (UNIVERSITAS KRISTEN SATYA WACANA) WEBSITE SECURITY ANALYSIS USING OWASP (OPEN WEB APPLICATION SECURITY PROJECT),” Jurnal Teknik Informatika (JUTIF), vol. 3, no. 3, 2022, doi: 10.20884/1.jutif.2022.3.3.346.

[18] M. F. A. Ramadhan and A. S. Ilmananda, "Analisis Ancaman Keamanan pada Sistem Informasi Akademik Kampus Menggunakan Metode OWASP ZAP," *JATI*, vol. 8, no. 4, pp. 7985–7991, 2024.

[19] A. Gustiyonoo, E. I. Alwi, and S. M. Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing," *JATI*, vol. 7, no. 1, pp. 25–33, May 2024

[20] R. Rahman and D. F. Razak, "Pengujian Penetrasi Jaringan Menggunakan OWASP ZAP dan SQLMAP untuk Mengidentifikasi Kerentanan Keamanan Website," Jurnal Riset Sistem Informasi, vol. 1, no. 4, pp. 8–11, Oct. 2024.

[21] S. D. Hilda, N. Heryana, and A. A. Ridha, "Website Security Analysis Curug Village Government Using Open Web Application Security Project (OWASP)," JATI, vol. 12, no. 3S1, pp. 3941–3957, 2024.