Evaluasi Keamanan Sistem Informasi Situs Web Lembaga XYZ dengan Menggunakan Metode OWASP Top 10 2021

1st Rizky Arya Andita
Sistem Informasi
Universitas Telkom
Surabaya, Indonesia
rizkyarya@student.telkomuniversity.ac.id

2nd Muhamad Nasrullah
Sistem Informasi
Universitas Telkom
Surabaya, Indonesia
emnasrul@telkom.university.ac.id

3rd Muhammad Ilham Alhari
Sistem Informasi
Universitas Telkom
Surabaya, Indonesia
ilhamalhari@telkomuniversity.ac.id

Abstrak* — *Lembaga XYZ memiliki 2 situs web untuk menjalankan tugasnya, situs A yang menyajikan berita kegiatan lembaga dan situs B yang menyediakan informasi lembaga serta menyimpan data pribadi pengguna (email, nomor telepon, alamat, dan dokumen KTP). Mengingat sensitivitas data dan potensi serangan siber yang dapat merusak kredibilitas, kedua situs harus dilengkapi lapisan keamanan yang kuat. Dengan menggunakan pendekatan pengujian penetrasi berdasarkan OWASP Top 10 2021, penelitian ini mengevaluasi kerentanan melalui tahapan Planning, Information Gathering, Vulnerability Scanning, Attacking, Validasi, Analisa Hasil, dan Reporting. Hasil pengujian mengidentifikasi 11 kerentanan di situs A (1 high, 6 medium, 4 low) dan 11 kerentanan di situs B (2 high, 4 medium, 5 low). Berdasarkan temuan tersebut, disusun rekomendasi perbaikan untuk mengurangi potensi serangan siber serta melindungi reputasi lembaga. Penelitian ini diharapkan dapat menjadi acuan dalam peningkatan keamanan situs web lembaga melalui pengujian penetrasi guna melindungi data dan informasi penting. Temuan penelitian ini memberikan kontribusi penting bagi pengembangan strategi keamanan siber.

***Kata kunci*— Keamanan situs web, Evaluasi Kerentanan, Uji Penetrasi, OWASP Top 10, Lembaga XYZ**

I. PENDAHULUAN

Di era kemajuan teknologi seperti saat ini, kita tidak terlepas dari penggunaan internet. Internet telah merubah berbagai aktivitas manusia menuju gaya hidup digital, memungkinkan pertukaran informasi, komunikasi global, dan akses ke sumber daya digital secara instan [1]. Fenomena ini tidak hanya menciptakan revolusi dalam cara manusia berkomunikasi, tetapi juga memberikan manfaat mulai dari dunia bisnis, industri, pendidikan dan pergaulan sosial [2].

Perkembangan teknologi informasi yang kian pesat telah membawa banyak manfaat bagi peradaban manusia. Namun, di sisi lain, menimbulkan masalah baru, salah satunya adalah keamanan siber [3]. Kejahatan siber menjadi sebuah masalah serius yang dapat mengancam di bidang ekonomi, politik, hingga pertahanan negara [4]. Di tahun 2022, kerugian akibat kejahatan siber di seluruh dunia mencapai US$ 8,44 triliun atau sekitar Rp 130 triliun. Nominal tersebut menunjukkan peningkatan sebesar 40,9 persen dibanding tahun sebelumnya yang sebesar US$ 6 triliun [5]. Peningkatan ini menegaskan urgensi perlindungan dan keamanan siber global, yang berdampak besar terhadap perekonomian dunia.

Di indonesia, menurut Badan Siber dan Sandi Negara (BSSN), jumlah anomali lalu lintas internet mencatat angka yang sangat tinggi. Sepanjang tahun 2021, Sebanyak 1,6 miliar anomali, kemudian mengalami penurunan pada tahun 2022 menjadi 976,4 juta [6]. Di semester 1 tahun 2023, telah terjadi empat kali kebocoran data RI yang terkemuka. Pertama, BPJS Ketenagakerjaan Indonesia dengan 19,5 juta pelanggan pada 12 Maret 2023. Kedua, Bank Syariah Indonesia (BSI) alami kebocoran data karena serangan ransomware Lockbit dan berhasil mencuri data pribadi pengguna BSI dengan ukuran data sebesar 1,5 terabyte (TB). Ketiga, dugaan kebocoran 35 juta data dari pengguna My IndiHome pada Juni 2023 oleh Bjorka. Keempat, pada Juli 2023, Bjorka diduga membocorkan sebanya 34,9 juta data paspor WNI [7]. Kurangnya kesadaran keamanan siber pada pengguna digital juga menjadi faktor yang memperburuk situasi ini. Selain itu kebijakan dan regulasi yang tidak memadai dalam menangani kejahatan siber, kurangnya kemampuan teknis dalam melawan serangan siber, dan rendahnya tingkat sinergi antara sektor publik dan swasta dalam menghadapi kejahatan siber [3].

Lembaga XYZ mengandalkan situs web resmi sebagai sarana menyediakan layanan mengenai informasi Lembaga. Situs tersebut meyimpan data pibadi seperti alamat email, nomor telepon, dan KTP. Data tersebut tidak boleh bocor sehingga dibutuhkan Langkah proaktif untuk mengidentifikasi dan mengatasi potensi celah keamanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab, dilakukan uji penetrasi dengan panduan OWASP Top 10 2021. Panduan ini dipilih karena memberikan wawasan mendalam mengenai kerentanan keamanan yang paling umum serta merefleksikan tren terkini dalam dunia keamanan web. Dengan penerapan standar keamanan yang lebih baik,

risiko peretasan dapat diminimalkan, sehingga integritas dan kredibilitas situs web tetap terjaga serta memberikan rasa aman bagi pengguna dalam mengakses layanan yang disediakan.

II. KAJIAN TEORI

A. Sistem Informasi

Sistem informasi adalah perpaduan dari berbagai sumber daya, seperti hardware, software, netware, brainware, dan data. Terdapat elemen-elemen seperti input, model, proses, output, penyimpanan, dan kontrol. Sistem informasi berguna untuk merencanakan, mengolah, mengendalikan, serta meracik data dalam suatu organisasi berdasarkan critical sukses untuk menentukan keberhasilan Perusahaan [8].

B. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan bagian internal dari organisasi yang bertanggung jawab untuk mengelola risiko yang terkait dengan sistem informasi yang terkomputerisasi. Mengontrol keamanan sistem informasi merupakan salah satu strategi dalam melindungi data perusahaan dari potensial yang timbul dari akses oleh pihak yang tidak sah. Jika seseorang yang tidak berwenang berhasil masuk ke dalam sistem dan mengakses data perusahaan, hal tersebut dapat menimbulkan ancaman serius karena data tersebut dapat tereksploitasi [9].

C. Penetration Testing

Penetration testing adalah simulasi serangan siber yang bertujuan untuk mengidentifikasi kerentanan dan merancang strategi agar bisa menembus dari sistem pertahanan. Penyerangan dilakukan tim keamanan untuk mencegah pelanggaran data yang dapat menyebabkan kerugian finansial [10].

D. VAPT *(Vulnerability Assessment & Penetration Testing)*

VAPT merupakan suatu pendekatan untuk melindungi organisasi dari potensi ancaman baik dari luar maupun dalam dengan cara mengidentifikasi potensi kerentanan keamanan. Metode ini bertujuan untuk mengamankan infrastruktur jaringan organisasi, aplikasi web, serta melakukan penilaian keamanan pada aplikasi seluler guna mendeteksi dan mengukur kerentanan keamanan [11].

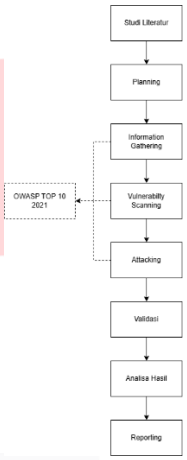
E. OWASP Top 10 2021

OWASP Top 10 merupakan standar dokumen bagi pengembang web dan keamanan web yang didasarkan pada kesepakatan umum komunitas mengenai ancaman keamanan yang paling serius pada situs web [12]. Dokumen ini berisi daftar sepuluh jenis serangan situs web yang umumnya dimanfaatkan oleh para penyerang. Dalam daftar ini setiap jenis serangan dalam daftar ini merinci risiko tertentu yang dapat mempengaruhi integritas, kerahasiaan, dan ketersediaan data dalam suatu sistem. Dengan pemahaman mendalam tentang OWASP Top 10, organisasi dapat mengambil langkah proaktif untuk memitigasi risiko, membangun sistem yang lebih aman, dan melindungi informasi sensitif dari penyerang yang tidak bertanggung jawab. Berikut ini adalah kesepuluh kategori OWASP TOP 10 2021 disebutkan di bawah ini:

1. A01:2021 Broken Access Control
2. A02:2021 Cryptographic Failures
3. A03:2021 Injection
4. A04:2021 Insecure Design
5. A05:2021 Security Misconfiguration
6. A06:2021 Vulnerable and Outdated Components
7. A07:2021 Identification and Authentication Failures
8. A08:2021 Software and Data Integrity Failures
9. A09:2021 Security Logging and Monitoring Failures
10. A10:2021 Server-Side Request Forgery

III. METODE

A. Alur Penelitian



GAMBAR 1
(ALUR PENELITIAN)

Penelitian ini diawali dengan studi literatur untuk memperoleh wawasan mendalam mengenai aspek keamanan sistem dari berbagai jurnal relevan. Selanjutnya, tahap Planning dilakukan untuk menetapkan target situs web, ruang lingkup penelitian, serta alat yang digunakan. Pada tahap *information gathering*, informasi terkait sistem target seperti arsitektur jaringan, dan teknologi yang digunakan, dikumpulkan guna mengidentifikasi potensi celah keamanan. Setelah itu, dilakukan vulnerability scanning dengan berbagai alat uji penetrasi untuk mendeteksi kelemahan dalam sistem. Tahap *attacking* mensimulasikan serangan berdasarkan skenario OWASP Top 10 2021 guna mengidentifikasi celah keamanan yang dapat dieksploitasi. Hasil pengujian kemudian divalidasi oleh profesional uji penetrasi untuk memastikan keakuratan temuan. Analisis hasil dilakukan untuk mengevaluasi penyebab serta mitigasi terhadap kerentanan yang ditemukan, sekaligus memberikan rekomendasi perbaikan. Tahap akhir adalah *reporting*, di mana seluruh temuan, analisis, dan rekomendasi terdokumentasi dalam laporan penelitian. Penelitian ini diharapkan memberikan pemahaman komprehensif mengenai risiko keamanan sistem serta menjadi dasar dalam penguatan keamanan situs web XYZ.

IV. HASIL DAN PEMBAHASAN

A. *Information Gathering*

Penggunaan *extension* Wappalyzer yang memberikan jabaran tentang komponen yang infrastruktur situs web. Informasi ini sangat penting untuk memahami teknologi yang digunakan. Selain itu, dengan mengetahui jenis teknologi yang spesifik, dapat menentukan langkah-langkah yang diambil pada tahap *attacking*.

TABEL 1
(HASIL WAPPALYZER.)

Teknologi	Keterangan
Analistik	Google Analytics
Rich Text Editor	Quill
Bingkai Kerja JavaScript	Vue.js
JavaScript Graphics	Chart.js
Server	Apache HTTP Server
Pemutar Video	YouTube VideoJS
Sistem Operasi	Ubuntu
Security	HSTS
JavaScript Libraries	jQuery OWL Carousel
UI Frameworks	Element UI Bootstrap
Serba Serbi	Popper HTTP/2

Situs web ini menerapkan mekanisme HTTP *Strict Transport Security* (HSTS) untuk memastikan bahwa seluruh komunikasi antara pengguna dan server selalu dilakukan melalui protokol HTTPS yang terenkripsi. Implementasi HSTS bertujuan untuk mencegah serangan *man-in-the-middle* (MITM) sehingga meningkatkan keamanan data yang dikirimkan antara klien dan server.

B. *Network Mapping*

Command kali Linux diisi perintah 'nmap -sS -sV [nama website]' untuk menampilkan port terbuka dan layanan yang berjalan yang terbuka serta keterangan versi layanan.

TABEL 2
(HASIL *NETWORK MAPPING*)

Port	Keterangan	Layanan	Versi
80	Open	http	Apache httpd 2.4.29 (Ubuntu)
443	Open	ssl/http	Apache httpd 2.4.29 (Ubuntu)

Dari hasil mapping ditemukan 2 port yang terbuka. Port 80 menjalankan layanan HTTP dengan server Apache versi 2.4.29 pada sistem operasi Ubuntu. Port 443 menjalankan layanan HTTPS dengan Apache HTTP Server versi 2.4.29 pada sistem operasi Ubuntu. Ini menunjukkan bahwa situs web dapat diakses melalui protokol HTTPS.

B. *Vulnerability Scanning*

Proses *vulnerability scanning* dilakukan menggunakan OWASP ZAP untuk mengidentifikasi potensi celah keamanan. Alat ini membantu dalam mendeteksi kelemahan yang dapat dieksploitasi oleh penyerang dengan melakukan analisis terhadap berbagai aspek keamanan situs web. Hasil pemindaian ini menjadi dasar dalam mengevaluasi tingkat risiko dan menyusun rekomendasi perbaikan guna meningkatkan keamanan sistem

TABEL 3
(HASIL VULNERABLE SCANNING)

Jenis Kerentanan	Tingkat Resiko	ID
Cloud Metadata Potentially Exposed	High	A05:2021
Script Served From Malicious Domain (polyfill)		A06:2021
Content Security Policy (CSP) Header Not Set	Medium	A05:2021
Missing Anti-clickjacking Header		A05:2021
Vulnerable JS Library		A06:2021
Application Error Disclosure	Low	A05:2021
Big Redirect Detected (Potential Sensitive Information Leak)		A04:2021
Cookie No HttpOnly Flag		A05:2021
Cookie Without Secure Flag		A05:2021
Cookie without SameSite Attribute		A01:2021
Cross-Domain JavaScript Source File Inclusion		A08:2021
Server Leaks Version Information via "Server" HTTP Response Header Field		A05:2021
Strict-Transport-Security Header Not Set		A05:2021
X-Content-Type-Options Header Missing		A05:2021
Information Disclosure - Sensitive Information in URL		A01:2021
Information Disclosure - Suspicious Comments		A01:2021
User Controllable HTML Element Attribute (Potential XSS)		A03:2021

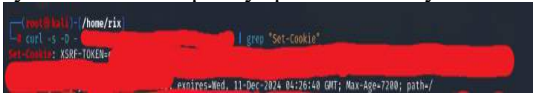
Tool OWASP ZAP menunjukkan bahwa situs B terdapat 21 kerentanan yang ditemukan. Diantaranya terdapat 2 kerentanan tingkat *High*, 3 kerentanan *medium*, 9 kerentanan tingkat *low*, dan 7 kerentanan dengan *informational.* Dari ditemukannya kerentanan ini, tidak semuanya masuk dalam OWASP top 10 2021

C. Attacking

1. A01:2021 – *Broken Access Control*

Cookie Without SameSite

Pemindaian yang dilakukan dengan menggunakan tool OWASP ZAP mengungkapkan bahwa situs B tidak menyetel atribut 'HttpOnly' pada cookie-nya.



GAMBAR 2
(COOKIE XSRF-TOKEN TIDAK ADA ATRIBUT HTTPONLY)

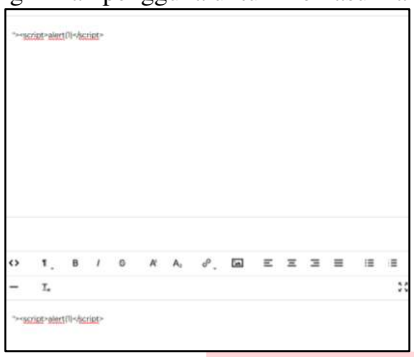
Dari hasil menggunakan *tool* curl menunjukkan bahwa cookie XSRF-Token pada situs B yang tidak menggunakan atribut HttpOnly

Cookie without SameSite Attribute

2. A03:2021 – *Injection*

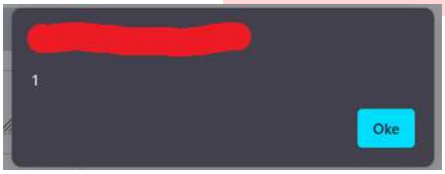
XSS Injection

Situs web memiliki kolom input yang memungkinkan pengguna untuk memasukkan data.



GAMBAR 3
(KOLOM INPUT)

Percobaan dilakukan dengan mengisikan skrip XSS di kolom terebut untuk menguji apakah sistem rentan terhadap serangan ini.



GAMBAR 4
(XSS BERHASIL)

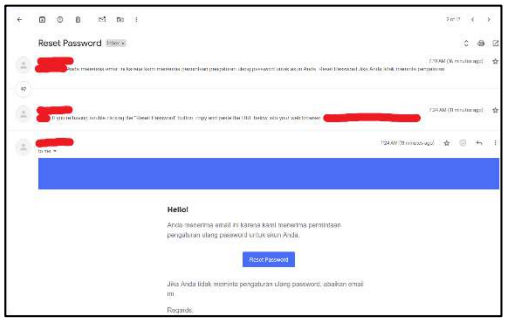
Hasil inputan yang telah disimpan sebagai draft diakses kembali dengan edit input, hasilnya muncul sebuah *pop-up* yang menunjukkan bahwa serangan XSS berhasil dieksekusi

3. A04:2021 – *Insecure Design*

No Rate Limit on Reset Password

GAMBAR 5
(MENGATUR PAYLOAD)

Serangan ini dilakukan dengan bantuan Burp Suite, di mana sebanyak 100 permintaan reset password dikirimkan melalui tool tersebut.



GAMBAR 6
(PERMINTAAN RESET PASSWORD MASUK EMAIL)

Hasil dari serangan ini menunjukkan bahwa semua 100 permintaan berhasil diproses dan sebanyak 100 email permintaan reset password masuk ke alamat email yang ditargetkan. Temuan ini mengindikasikan bahwa sistem tidak memiliki mekanisme pembatasan atau deteksi terhadap permintaan reset password yang berulang dalam jumlah besar.

4. A05:2021 – *Security Misconfiguration*

Content Security Policy (CSP) Header Not Set

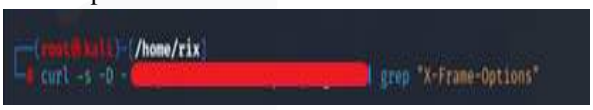
Hasil pemindaian menggunakan OWASP ZAP menunjukkan bahwa situs web tidak memiliki header Content Security Policy (CSP).

GAMBAR 7
(CURL TIDAK MENAMPILKAN HEADER CSP)

Penggunaan *tool* curl pada situs web tersebut menunjukkan bahwa memunculkan output header CSP. CSP berguna sebagai lapisan keamanan tambahan yang dapat mengurangi jenis serangan XSS dan serangan penyisipan data lainnya

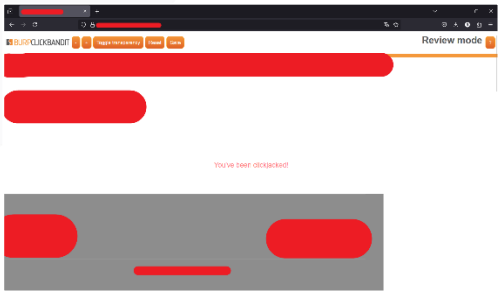
Missing Anti-clickjacking Header

Pemindaian menggunakan OWASP ZAP menemukan kerentanan "Missing Anti-Clickjacking Header" pada situs web.



GAMBAR 8
(CURL TIDAK MENAMPILKAN HEADER X-FRAME-OPTIONS)

Penggunaan *tool* curl tidak menampilkan output yang diminta menandakan situs web tidak menggunakan header Anti-clickjacking. Tanpa header ini memungkinkan penyerang untuk mendorong pengguna agar melakukan tindakan yang tidak mereka inginkan, dengan klik tombol atau tautan berbahaya yang terletak tersembunyi di balik lapisan tampilan.



GAMBAR 9
(CLICKJACKING BERHASIL)

Untuk menguji kerentanan ini, digunakan tool Burp Suite dengan fitur Burp Clickbandit yang dirancang untuk mendeteksi kerentanan *clickjacking*. Hasilnya menunjukkan bahwa situs web tersebut terdapat tulisan "*You've been clickjacked*" yang menandakan bahwa situs web rentan diserang *clickjacking*.

Cookie No HttpOnly Flag

Pemindaian yang dilakukan dengan menggunakan tool OWASP ZAP mengungkapkan bahwa situs web tidak mengatur atribut 'HttpOnly' pada cookie-nya.

GAMBAR 10
(COOKIE XSRF-TOKEN TIDAK ADA ATRIBUT HTTPONLY)

Dari hasil menggunakan tool curl menunjukkan bahwa cookie XSRF-Token pada situs web tidak menggunakan atribut HttpOnly. Flag HttpOnly adalah lapisan pertahanan yang dapat mengurangi risiko pencurian cookie melalui XSS

Cookie Without Secure Flag

Pemindaian menggunakan OWASP ZAP menemukan kerentanan yang menunjukkan bahwa Set-cookie yang diatur tanpa *secure* flag.

GAMBAR 11
(TIDAK ADA ATRIBUT FLAG PADA SET COOKIE)

Hasil pemeriksaan dengan tool curl menunjukkan seluruh Set-Cookie tidak menggunakan atribut *secure*. Tanpa atribut tersebut menyebabkan cookie dapat diakses melalui koneksi yang tidak terenkripsi, sehingga cookie dapat dicuri yang dapat meningkatkan risiko pencurian akun.

Server Leaks Version Information via "Server" HTTP Response Header Field

Hasil pemindaian menggunakan OWASP ZAP diketahui bahwa situs web terdapat informasi servermelalui header respon HTTP.

GAMBAR 12
(INFORMASI SERVER TERLIHAT PADA HEADER)

Selain itu, penggunaan tool curl dalam pengujian menunjukkan bahwa informasi terkait server situs web dapat diakses melalui header HTTP. Tool curl berhasil mengungkapkan detail dari header server yang mencakup informasi tentang versi perangkat lunak server yang digunakan.

X-Content-Type-Options Header Missing

Pemindaian menggunakan OWASP ZAP menemukan kerentanan "*X-Content-Type-Options Header Missing*". Kerentanan ini menunjukkan bahwa situs web tidak menggunakan header 'X-Content-Type-Options' yang merupakan header yang penting untuk keamanan

GAMBAR 13
(INFORMASI SERVER TERLIHAT PADA HEADER)

Hasil pemeriksaan dari tool curl menujukkan bahwa tidak menunjukkan output. Yang mengindikasikan tidak adanya header 'X-Content-Type-Options'. Tanpa header header tersebut, memungkinkan situs web dapat diserang MIME-sniffing dengan menggunakan browser versi lama.

5. A06:2021 – *Vulnerable and Outdated Components*

Script Served From Malicious Domain (polyfill)

Hasil pemindaian situs web menggunakan OWASP ZAP ditemukan kerentanan Script Served From Malicious Domain terkait pencantuman skrip dari domain 'polyfill.io'. Domain ini memiliki potensi untuk menyajikan konten berbahaya. Temuan ini menunjukkan bahwa pemuatan skrip dari sumber yang tidak terpercaya dapat menjadi celah keamanan yang berisiko tinggi.

Vulnerable JS Library

Berdasarkan hasil pemindaian dari OWASP ZAP, ditemukan bahwa situs web memiliki kerentanan "Vulnerable and Outdated Components", *library* versi lama yang telah diketahui memiliki kelemahan keamanan. Terdapat lima library versi lama yang digunakan, yaitu jQuery Validation 1.14.0, moment.js 2.21.0, moment.js 2.29.1, jQuery 3.3.1, jQuery 3.4.1, Bootstrap 4.0.0, dan jQuery 2.1.4.

V. KESIMPULAN

Penelitian ini mencakup beberapa tahapan, mulai dari studi literatur, planning, information gathering, vulnerability scanning, attacking, validasi, analisa hasil, hingga reporting, dengan mengacu pada framework OWASP Top 10 2021 yang berfokus pada jenis kerentanan yang paling sering ditemukan. Pengujian dilakukan menggunakan berbagai tool serta secara manual tanpa tool, menghasilkan temuan 11 jenis terdiri dari 2 high, 4 medium, dan 5 low.

REFERENSI

[1] S. Rohaya, "INTERNET: Pengertian, Sejarah, Fasilitas, dan Koneksi" 2008. [Online]. Available: http://dhani.shingcat.com

[2] R. Mochamad, "Literasi Internet Sehat Terhadap Siswa Sekolah Dasar Di Desa Tanjakan Banten", *Community Engagement and Emergence Journal (CEEJ)*, vol. 2, no. 1, pp. 116–119, Sep. 2020.

[3] A. . Muftiadi, T. P. M. . Agustina, and M. . Evi, “Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phishing terhadap Layanan Online Banking”, *Jurnal Ilmiah Teknik*, vol. 1, no. 2, pp. 60–65, Aug. 2022.

[4] M. DI Kejahatan Siber Indonesia, M. Rizki Hapizon, and K. Rizki, “Analisis Kerjasama Cybersecurity Indonesia-Australia dalam.” [Online]. Available: https://media.neliti.com/

[5] Bisnis Tekno, “Kerugian Akibat Kejahatan Siber di Dunia Tembus Rp129.643 Triliun Artikel ini telah tayang di Bisnis.com dengan judul "Kerugian Akibat Kejahatan Siber di Dunia Tembus Rp129.643 Triliun.” [Online]. Available: https://teknologi.bisnis.com/read/20221212/84/1607768/kerugian-akibat-kejahatan-siber-di-dunia-tembus-rp129643-triliun

[6] Antara News, “BSSN harapkan perbankan respon cepat pemberitahuan anomali internet.” Nov. 13, 2023. [Online]. Available: https://www.antaranews.com/berita/3823224/bssn-harapkan-perbankan-respon-cepat-pemberitahuan-anomali-internet

[7] dataindonesia.id, “Deret Kasus Kebocoran Data RIpada 2023, dari BSI hingga Paspor.” [Online]. Available: https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.

[8] R. Rahmahwati Sidh, "Peranan brainware dalam sistem informasi manajemen," Jurnal Computech & Bisnis, vol. 7, no. 1, pp. 19-29, 2013.

[9] E. Novianto, E. I. Heri Ujianto, and R. Rianto, “Keamanan Informasi (Information Security) pada Aplikasi Sistem Informasi Manajemen,” Jurnal Komputer dan Informatika, vol. 11, no. 1, pp. 1–6, Mar. 2023, doi: 10.35508/jicon.v11i1.9139.

[10] E. M. Safitri, A. S. Larasati, and S. R. Hari, “Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur.”

[11] “Vapt Testing: The Complete Guide 2023.” [Online]. Available: https://qualysec.com/vapt-testing-the-complete-guide-2023/

[12] “OWASP Top Ten.” [Online]. Available: https://owasp.org/www-project-top-ten