Analisis Keamanan Sistem Informasi Website ABC Dengan Penetration Testing Menggunakan OWASP Top 10

1st Hisyam Mahendra Putera
Department of Information System
Universitas Telkom
Surabaya,Indonesia
hisyammp@student.telkomuniversity.ac.id

2nd Muhammad Nasrullah
Department of Information System
Universitas Telkom
Surabaya,Indonesia
emnasrul@telkomuniversity.ac.id

3rd Rizky Fenaldo Maulana
Department of Informatics
Universitas Telkom
Surabaya,Indonesia
rizkyfenaldom@telkomuniversity.ac.id

***Abstrak* — Perkembangan teknologi informasi telah mengubah cara organisasi beroperasi dan berkomunikasi. Salah satu implementasi penting dari teknologi informasi adalah sistem informasi berbasis *website*. Pada perusahaan PT. XYZ, sistem informasi telah diterapkan untuk menyediakan pelayanan kepada pelanggan. Serangan *cyber* seperti kebocoran data maupun akses terhadap layanan *website* dapat merugikan pihak perusahaan dan juga dapat mengganggu kegiatan operasioanl. Selain itu, keamanan *cyber* yang buruk atau sering diserang dapat merusak reputasi perusahaan. Penelitian ini bertujuan untuk menganalisis keaman sistem informasi *website* ABC pada PT. XYZ menggunakan meotde *penetration testing* dan *Open Web Application Security Project* (OWASP) Top-10 2021. Metode ini membantu mengidentifikasi potensi kerentanan keamanan yang terdapat pada *website* tersebut. Tahapan yang dilakukan pada penelitian ini yaitu identifikasi *website*, pengujian *penetration testing*, hasil pengujian, analisis, dan kesimpulan. Dari proses pengujian dan analisis yang telah dilakukan, hasil dari 10 daftar kerentanan yang dimiliki oleh OWASP Top 10 peneliti menemukan 4 daftar kerentanan yang berhasil ditemukan, yaitu *Insecure Design (medium), Vulnerable and Outdated Components (Medium), Software and Data Integrity Failures (High), dan Security Logging and Monitoring Failures (Medium)*.**

***Kata kunci*— Keamanan Sistem Informasi;*Penetration Testing*;OWASP Top 10;*Website*.**

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat dalam beberapa tahun terakhir telah menjadi faktor utama dalam transformasi berbagai sektor, baik pemerintahan, swasta maupun public[1]. Implementasi sistem informasi berbasis web menjadi tonggak penting dalam mempercepat layanan dan proses operasional, memungkinkan perusahaan-perusahaan untuk lebih efisien dan responsif terhadap kebutuhan masyaraka[2]. Namun, di balik progres tersebut, tantangan keamanan siber semakin kompleks dan muncul sebagai ancaman serius terhadap integritas, kerahasiaan, dan ketersediaan data[2].

Pentingnya evaluasi keamanan sistem informasi semakin mendesak mengingat eskalasi serangan siber yang telah terjadi pada tahun 2022. Menurut artikel Surfsjark, Indonesia merupakan negara dengan penduduk 275 juta jiwa per Juni 2022 dan merupakan salah satu negara dengan jumlah pengguna internet terbesar di dunia. Menurut global data breach statistics, Indonesia menempati peringkat ke 3 dunia dengan kasus kebocoran data tertinggi[3]. Dalam enam bulan pertama pelaku peretasan siber melakukan aksinya di Asia Tenggara pada website company sebanyak lebih dari 11,2 juta kali. Indonesia menjadi salah satu negara dengan serangan terbanyak yaitu (5 juta serangan) disusul dengan negara Vietnam (2 juta serangan) dan Thailand (1,5 juta serangan[4], hal tersebut menandakan tingginya risiko yang harus diatasi. Kasus serangan siber yang meningkat signifikan membuka peluang bagi kebocoran data dan akses yang tidak legal, mengancam operasional dan reputasi perusahaan.

Penting untuk digaris bawahi bahwa serangan siber tidak hanya mencakup ancaman terhadap keamanan data, tetapi juga dapat mengganggu kelancaran operasional dan merusak reputasi perusahaan[5]. Keberlanjutan operasional perusahaan dan pelayanannya kepada pelanggan sangat tergantung pada ketahanan sistem informasi mereka terhadap ancaman siber.

Lebih lanjut, situasi ini semakin memperoleh urgensi mengingat perusahaan di Indonesia merupakan tulang punggung ekonomi yang berperan sebagai penggerak pertumbuhan ekonomi, membuka lapangan pekerjaan, dan memberi pelayanan kepada pelanggan[6]. Dengan mengidentifikasi dan mengatasi potensi kerentanan keamanan, diharapkan perusahaan dapat memperkuat pertahanan mereka dan memberikan contoh bagi instansi maupun perusahaan lainnya.

Salah satu platform yang memiliki peran dalam memberikan pelayanan di bidang penjualan barang dan distribusi, PT. XYZ mempunyai sistem informasi berupa website. Pada sistem informasi tersebut memiliki beberapa fitur seperti halaman profil, fitur belanja untuk berbelanja pada website tersebut, fitur career untuk membuka rekrutment pegawai, E-Commerce yang

terhubung dengan platform Shopee dan Tokopedia. Di tengah pemberlakuan sistem informasi, seperti website ABC sebagai sarana interaksi dengan pelanggan, keamanan sistem informasi menjadi krusial untuk menjaga kepercayaan publik dan integritas data yang dimiliki oleh perusahaan.

Menurut data Statista menunjukkan, Indonesia menjadi negara dengan pengguna rokok elektrik atau biasa dikenal dengan vape terbanyak di dunia[7]. Website ABC menjadi media penting yang menghubungkan perusahaan dengan pelanggan maupun pengguna yang memiliki minat membeli produk ABC. Namun, potensi serangan siber pada website ini menimbulkan risiko besar terhadap kerahasiaan dan integritas data. Sebelumnya website ABC pernah menjadi sasaran hacker yang mencoba masuk pada bagian admin website dan berhasil menemukan celah yang dimiliki pada website ABC. Oleh karena itu, analisis keamanan yang menyeluruh dan sistematis menjadi suatu kebutuhan yang penting untuk mengurangi resiko keamanan dan kebocoran data pada website.

Penelitian ini bertujuan untuk mencari kerentanan pada website tersebut dengan menerapkan metode penetration testing, yang merupakan pendekatan praktis dan efektif dalam mengidentifikasi dan mengevaluasi kerentanan keamanan suatu sistem. Penggunaan Open Web Application Security Project (OWASP) Top-10 2021 sebagai alat utama [8] dalam penelitian ini diharapkan dapat memberikan gambaran yang komprehensif tentang keamanan website ABC.

Penelitian ini juga relevan dengan kebutuhan mendesak untuk meningkatkan literasi keamanan siber di lingkungan perusahaan. Dengan memahami kerentanan dan resiko yang mungkin dihadapi, perusahaan dapat memperkuat kapasitas internal mereka dalam melindungi informasi yang mereka kelola dan memberikan layanan yang andal kepada pelanggan[5].

Melalui tahapan identifikasi website, penggunaan metode OWASP Top-10 2021, serta pengujian penetration testing menggunakan pengujian blackbox testing[11] penelitian ini diharapkan dapat memberikan pemahaman mendalam tentang keamanan sistem informasi pada website ABC. Hasil analisis kerentanan yang dihasilkan nantinya dapat memberikan dasar untuk rekomendasi perbaikan yang tepat dan praktis, serta membantu pihak terkait dalam mengurangi resiko serangan siber dan melindungi data rahasia yang dimiliki oleh perusahaan.

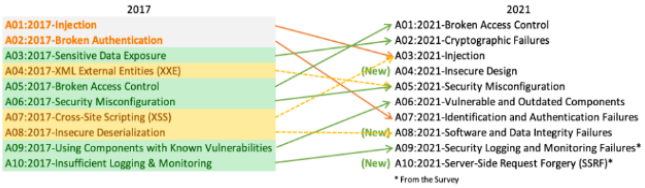
Pada akhirnya, kesimpulan dari penelitian ini akan memberikan gambaran menyeluruh serta rekomendasi perbaikan tentang keamanan sistem informasi pada website ABC dan dapat menjadi panduan bagi pihak serupa yang berkomitmen untuk meningkatkan keamanan siber mereka.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan Sistem Informasi adalah Keamanan Sistem Informasi adalah segala bentuk aktivitas yang dilakukan untuk memastikan bahwa data pada suatu sistem dapat terlindungi dari berbagai ancaman, di mana ancaman tersebut dapat berupa serangan dari luar seperti peretasan atau *hacking*, *virus* atau *malware*, dan serangan dari dalam seperti kebocoran data akibat dari oknum internal perusahaan seperti pegawai. Aspek keamanan sistem informasi meliputi Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan)(Ary et al., n.d.).

B. *Open Web Application Security Project* (OWASP) Top 10



Gambar 1. OWASP Top 10

OWASP *(Open Web Application Security Project)* adalah sebuah organisasi yang mendedikasikan metodenya untuk meningkatkan keamanan pada aplikasi berbasis *website*. OWASP Top 10 memiliki daftar sepuluh kerentanan keamanan teratas aplikasi website yang berfungsi sebagai panduan bagi pengembang aplikasi web, professional keamanan informasi, dan organisasi untuk memahami resiko keamanan siber dan bagaimana cara untuk mengatasinya.

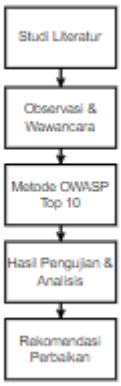
C. *Penetration Testing*

Penetration testing atau bisa disebut dengan pentest adalah aktivitas yang dilakukan untuk mencoba serangan terhadap suatu jaringan target untuk menemukan kelemahan pada sistem tersebut[9]. Sebuah sistem pada umumnya mempunyai mekanisme keamanan yang diterapkan oleh pihak pengembang, tetapi pada kenyataannya terdapat banyak informasi penting dan critical yang masih bisa diakses tanpa izin akibat dari ada celah keamanan pada sistem tersebut.

III. METODE

Dalam memaparkan masalah pada penelitian diperlukan alur penelitian untuk mempermudah pemahaman dalam penelitian tersebut. Berikut merupakan alur penelitian yang digunakan, mulai dari studi literatur, observasi & wawancara, Metode OWASP Top 10, hasil pengujian & analisis, rekomendasi

perbaikan.



Gambar 1. Alur penelitian

3.1 Studi Literatur

Studi literatur atau juga disebut studi Pustaka dilakukan dengan cara mempelajari literatur-literatur seperti buku, jurnal, laporan penelitian, skripsi/tugas akhir, internet, ataupun referensi lain yang berkaitan dengan penelitian. Dari studi literatur yang didapatkan oleh penulis yang kemudian dijelaskan pada Bab 2 sub bab dasar teori, seperti Sistem Informasi, Keamanan Sistem Informasi, OWASP Top 10, Cybercrime, Cross Site Scripting (XSS), SQL Injection, Blackbox Testing, Penetration Testing, ZAP, WHOIS, Nmap, Nslookup[(Yudiana et al., 2021)].

3.2 Observasi dan Wawancara

Setelah melakukan studi literatur selanjutnya dilakukan pengumpulan data dengan cara observasi dan wawancara secara langsung ke instansi atau perusahaan terkait. Beberapa informasi yang didapatkan setelah melakukan observasi dan wawancara adalah mendapatkan izin atau akses untuk meneliti website ABC.co.id sebagai objek tugas akhir yang digunakan.

3.3 Metode OWASP Top 10

OWASP Top 10 terdiri dari sepuluh daftar kerentanan yang dikembangkan oleh Open Web Application Security Project (OWASP) untuk mengidentifikasi serta menilai sepuluh risiko keamanan pada suatu website. Tujuan dari tahapan ini adalah agar pentester mendapat akses maupun informasi berharga dan rahasia dari suatu website. Berikut merupakan daftar sepuluh risiko keamanan dalam web app exploitation menurut OWASP Top 10 2021, yakni;

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

3.4 Hasil Pengujian & Analisis

Tahap ini merupakan penjelasan terkait metode OWASP Top 10 dengan mendapatkan hasil dan pembahasan data melalui tahap observasi hingga pengujian yang telah dilakukan.

3.5 Rekomendasi Perbaikan

Rekomendasi perbaikan merupakan suatu usulan atau solusi yang diberikan untuk mengatasi serta memperbaiki sebuah sistem maupun permasalahan yang terdapat pada sistem tersebut. Rekomendasi perbaikan ini dihasilkan dari proses hasil pengujian dan analisis terhadap objek yang akan dilakukan pengujian.

IV. HASIL DAN PEMBAHASAN

4.1 Pengujian OWASP Top 10

Tahapan pada pengujian ini adalah suatu tahapan atau fase dalam pengujian *penetration testing* maupun serangan siber di mana penulis melakukan percobaan penyerangan untuk mendapatkan akses yang tidak sah/*illegal* ke dalam sistem, aplikasi, atau sebuah data yang telah ditargetkan. Penyerang memanfaatkan data serta informasi yang telah dikumpulkan selama tahap-tahap sebelumnya, yaitu tahapan observasi dan wawancara untuk melakukan eksploitasi kerentanan yang ditemukan. Pengujian yang dilakukan berdasarkan sepuluh daftar kerentanan yang terdapat pada OWASP Top 10 2021.

1. A01: *Broken Access Control*

   Pada pengujian Broken Access Control, peneliti menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Burp Suite dan Dirsearch, yang mana Burp Suite digunakan untuk melakukan teknik Insecure Direct Object References dan Dirsearch digunakan untuk menemukan file dan direktori tersembunyi.

Table 1 Hasil Broken Access Control

ID	Testing	Parameter	Keterangan
A01	IDOR	• https://ABC.co.id/order/cart	Tidak ditemukan kerentanan pada percobaan ini
	Dirsearch	• https://ABC.co.id/member/Login/js.php • https://ABC.co.id/member/Login/!.htpasswd	Tidak ditemukan kerentanan pada percobaan ini

2. A02: *Cryptographic Failures*

Pada pengujian Cryptographic failures, peneliti mengidentifikasi kerentanan pada kegagalan kriptografi menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Dirb dan Xerosploit3, yang mana Dirb digunakan untuk melakukan teknik brute force yang dilakukan untuk mencari direktori terbuka dan Xerosploit3 digunakan untuk melakukan serangan Man In The Middle (MITM).

Tabel 2. Hasil Cryptographic Failures

ID	Testing	Parameter	Keterangan
A02	Dirb	• 103.247.10.94/~administrator/ • 103.247.10.94/~sysadmin/ • 103.247.10.94/~mail/ • 103.247.10.94/~user/	Tidak ditemukan kerentanan pada percobaan ini
	Xerosploit	• https://ABC.co.id/member/Dashboard • https://ABC.co.id/member/Login	Tidak ditemukan kerentanan pada percobaan ini

3. A03: *Injection*

Pada pengujian Injection, peneliti mengidentifikasi kerentanan pada kegagalan kriptografi menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Parampsider dan Dalfox, yang mana Paramspider digunakan untuk mencari parameter URL dan Dalfox digunakan untuk melakukan serangan eksploitasi.

Tabel 3. Hasil Injection

ID	Testing	Parameter	Keterangan
A03	Paramspider	• result/ABC.co.id.txt	Terdapat tiga parameter yang teridentifikasi
	Dalfox	• https://ABC.co.id/all-news/category/education?start=FUZZ • https://ABC.co.id/all-news/filter/?date=FUZZ • https://ABC.co.id/products?=FUZZ	Tidak ditemukan kerentanan pada percobaan ini

4. A04: *Insecure Design*

Pada pengujian Insecure Design, peneliti mengidentifikasi kerentanan pada desain website menggunakan tools Burp Suite untuk melakukan pengujian penetration testing. Tools tersebut digunakan untuk melakukan teknik clickjacking untuk mengetahui kerentanan yang terdapat pada website.

Tabel 4. Hasil Insecure Design

ID	Testing	Parameter	Keterangan
A04	Clickjacking	https://ABC.co.id/order/cart	Tidak ditemukan kerentanan pada percobaan ini.

5. A05: *Security Misconfiguration*

Pada pengujian Security Misconfiguration, peneliti mengidentifikasi kerentanan menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Gobuster dan SQL Map, yang mana Gobuster digunakan untuk menemukan teknik direktori tertentu yang tersembunyi dan tak dilindungi dengan baik dan SQL Map digunakan untuk menemukan direktori database pada website target.

Tabel 5. Hasil Security Misconfiguration

ID	Testing	Parameter	Keterangan
A05	Gobuster	https://ABC.co.id	Tidak ditemukan kerentanan pada percobaan ini.
	SQL Map	https://103.24710.94:2096/	Tidak ditemukan kerentanan

			pada percobaan ini.

6. A06: *Vulnerable and Outdated Components*

Pada penguj Vulnerable and Outdated Components, peneliti mengidentifikasi kerentanan menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Wappalyzer dan secara manual menggunakan Inspect Element, yang mana Wappalyzer digunakan untuk melakukan mengidentifikasi perangkat dan komponen yang telah usang atau kadaluarsa dan Inspect Element digunakan untuk mengtahui kapan website terakhir kali dilakukan pembaruan.

Tabel 6. 1 Hasil Vulnerable and Outdated Components

ID	Testing	Parameter	Keterangan
A06	*Website*	https://ABC.co.id	Ditemukan kerentanan pada percobaan ini
	Console	https://ABC.co.id	Ditemukan kerentanan pada percobaan ini

7. A07: *Identification and Authentication Failures*

Pada pengujian Identification and Authentication Failures, peneliti mengidentifikasi kerentanan menggunakan tools Burp Suite untuk melakukan pengujian penetration testing. Burp Suite digunakan oleh peneliti untuk mendapatkan email dan password yang diinputkan dengan teknik brute force menggunakan kombinasi payload.

Tabel 7. Hasil Identification and Authentication Failures

ID	Testing	Parameter	Keterangan
A07	*Brute Force*	https://ABC.co.id/member/Login	Tidak ditemukan kerentanan pada percobaan ini

8. A08: *Software and Data Integrity Failures*

Pada pengujian Software and Data Integrity Failures, peneliti mengidentifikasi kerentanan secara manual menggunakan inscpect element untuk melakukan pengujian penetration testing. Inspect element digunakan oleh peneliti untuk menemukan kerentanan secara manual dengan cara membuka file dan direktori satu persatu[11].

Tabel 8. Hasil Software and Data Integrity Failures

ID	Testing	Parameter	Keterangan
A08	*Software Integrity*	https://ABC.co.id/searching?	Ditemukan kerentanan pada percobaan ini

9. A09: *Security Logging and Monitoring Failures*

Pada pengujian security Logging and Monitoring, peneliti mengidentifikasi kerentanan akses login pada website menggunakan teknik brute force untuk melakukan pengujian penetration testing. Teknik tersebut dilakukan secara manual oleh peneliti dengan melakukan akses login secara berkali-kali untuk mengetahui kerentanan pada website, apakah terdapat pemblokiran sementara terhadap penggunaan email dan password pada akses login ketika dilakukan secara beruntun.

Tabel 9. Hasil Security Logging and Monitoring Failures

ID	Testing	Parameter	Keterangan
A09	Fitur Login	https://ABC.co.id/member/Login	Ditemukan kerentanan pada percobaan ini

10. A10: *Server-Side Request Forgery*

Pada pengujian Server-Side Request Forgery (SSRF), peneliti mengidentifikasi kerentanan pada server website menggunakan dua tools untuk melakukan pengujian penetration testing. Tools yang digunakan yaitu Burp Suite dan SSRF Map, yang mana Burp Suite digunakan untuk menemukan kerentanan pada server website.

Tabel 10. Hasil Server-Side Request Forgery

ID	Testing	Parameter	Keterangan
A10	Fitur Cart	https://ABC.co.id//products/addCart/247?Qty=1&Label=	Tidak ditemukan kerentanan pada percobaan ini
	Home Page	https://ABC.co.id	Tidak ditemukan kerentanan

			pada percobaan ini

4.2 Analisis

Table 11 Tabel analisis kerentanan

	OWASP Top 10 2021	Kerentanan
A01-	Broken Access Control	Tidak Ditemukan
A02-	Cryptographic Failures	Tidak Ditemukan
A03-	Injection	Tidak Ditemukan
A04-	Insecure Design	Ditemukan
A05-	Security Misconfiguration	Tidak Ditemukan
A06-	Vulnerable and Outdated Components	Ditemukan
A07-	Identification and Authentication Failures	Tidak Ditemukan
A08-	Software and Data Integrity Failures	Ditemukan
A09-	Security Logging and Monitoring Failures	Ditemukan
A10-	Server-Side Request Forgery (SSRF)	Tidak Ditemukan

Dari serangkaian pengujian yang dilakukan menggunakan metode OWASP Top 10 2021, dapat dihasilkan analisa seperti yang di tampilkan pada Tabel IV-11. Pada tahapan ini peneliti menemukan, bahwa dari daftar sepuluh kerentanan yang dimiliki oleh OWASP Top 10 terdapat tiga daftar kerentanan yang dimiliki oleh website ABC.co.id. Daftar kerentanan yang ditemukan tersebut yakni, A04 – Insecure Design, A06 – Vulnerable and Outdated Components, A08 – Software and Data Integrity Failures, dan A09 – *Security Logging and Monitoring Failures.*

4.3 Rekomendasi Perbaikan

Pada tahap ini dilakukan analisis terhadap pengujian yang telah dilakukan dengan memberikan rekomendasi perbaikan sebagai acuan untuk melakukan perbaikan selanjutnya. Rekomendasi yang diberikan berdasarkan hasil pengujian dan analisis dari OWASP Top 10 2021.

Table 12 Tabel rekomendasi perbaikan

Kerentanan	Tindakan Perbaikan
Insecure Design	Menggunakan *header Conten Security Policy* (CSP) untuk menentukan perizinan pada bingkai laman, audit dan monitoring.
Vulnerable and Outdated Components	Menggunakan komponen versi *libraries* dengan versi yang baru dan lebih relevan seiring dengan perkembangan teknologi.
Software and Data Integrity Failures	Menggunakan script yang sesuai dengan bahasa pemrograman yang digunakan.
Security Logging and Monitoring Failures	Menggunakan script yang memiliki fitur maksimal pada percobaan akses *login.*

V. KESIMPULAN

Dari serangkaian proses yang telah dilakukan pada implementasi dan pengujian dapat diambil kesimpulan sebagai berikut :

1. Dari proses pengujian yang telah dilakukan bahwa analisis keamanan sistem informasi *website* menggunakan metode OWASP Top 10 2021 terbukti mampu mengetahui kerentanan yang terdapat pada *website* ABC.co.id. Dari hasil pengujian, ditemukan kerentanan berdasarkan kategori OWASP Top 10 2021 yaitu pada *insecure design, vulnerable and outdated components, software and data integrity failures*, dan *security logging and monitoring failures.*
2. Tingkatan prioritas perbaikan keamanan sistem informasi pada *website* ABC.co.id berdasarkan kategori OWASP Top 10 2021 setelah dilakukan *penetration testing* yaitu, pada kerentanan *insecure design* memiliki tingkat prioritas perbaikan kerentanan menengah, pada kerentanan *vulnerable and outdated components* memiliki tingkat prioritas perbaikan kerentanan menengah, pada kerentanan *software and data integrity failures* memiliki tingkat prioritas perbaikan kerentanan tinggi, dan pada kerentanan *security logging and monitoring failures* memiliki tingkat kerentanan menengah.
3. Rekomendasi perbaikan yang harus dilakukan untuk meningkatkan keamanan sistem informasi pada perusahaan yaitu, dengan menggunakan *header Conten Security Policy* (CSP) untuk menentukan perizinan pada bingkai laman, audit dan monitoring, menggunakan komponen versi *libraries* dengan versi yang baru dan lebih relevan seiring dengan perkembangan teknologi, serta menggunakan script yang sesuai dengan bahasa pemrograman yang digunakan pada *website* dan menggunakan script yang memiliki fitur batasan maksimal pada percobaan akses *login.*

REFERENSI

[1] Miranda Atmanegara, “Perkembangan Teknologi di Era Digital,” Kompasiana. Accessed: Dec. 22, 2023. [Online]. Available: https://www.kompasiana.com/mirandaatmanegara8452/60f045ab06310e397504e432/perkembangan-teknologi-di-era-digital

[2] Y. Yuningsih, “Efektivitas Implementasi Pelayanan Publik Digital: Studi Kasus Pelayanan Perpustakaan Digital Puslatbang PKASN LAN,” Jurnal Wacana Kinerja: Kajian Praktis-Akademis Kinerja dan Administrasi Pelayanan Publik, vol. 25, no. 1, p. 43, Aug. 2022, doi: 10.31845/jwk.v25i1.727.

[3] Dancor, “Kebocoran Data Indonesia Tertinggi ke-3,” HYPERNET. Accessed: Nov. 27, 2023. [Online].

Available: https://hypernet.co.id/id/2023/03/03/kebocoran-data-indonesia-tertinggi-ke-3/

[4] bumialumni, " Isu Keamanan Siber Melanda Pelaku UMKM, Ini Penangkalnya," bumialumni. Accessed: Nov. 23, 2023. [Online]. Available: https://bumialumni.com/article/74/isu-keamanan-siber-melanda-pelaku-umkm-ini-penangkalnya

[5] Agustinus Mario Damar, "Survei Ungkap Phishing Masih Jadi Ancaman Siber Dominan di Perusahaan Indonesia," Liputan 6. Accessed: Dec. 22, 2023. [Online]. Available: https://www.liputan6.com/tekno/read/5483699/survei-ungkap-phishing-masih-jadi-ancaman-siber-dominan-di-perusahaan-indonesia?page=4

[6] Fanny Fajarianti, "4 Alasan Pentingnya Keamanan Siber bagi UMKM," ArmourZero Indonesia, Nov. 2023, Accessed: Nov. 23, 2023. [Online]. Available: https://id.linkedin.com/pulse/4-alasan-pentingnya-keamanan-siber-bagi-umkm-armourzero-indonesia-5etnc?trk=public_post

[7] Cindy Mutia Annur, "Indonesia Jadi Negara Pengguna Vape Terbanyak di Dunia, Kalahkan Negara-Negara Eropa hingga AS," Databoks. Accessed: Nov. 27, 2023. [Online]. Available: https://databoks.katadata.co.id/datapublish/2023/06/05/indonesia-jadi-negara-pengguna-vape-terbanyak-di-dunia-kalahkan-negara-negara-eropa-hingga-as

[8] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," Jurnal Informasi dan Teknologi, Oct. 2022, doi: 10.37034/jidt.v4i3.236.

[9] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF."

[10] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," CESS (Journal Comput. Eng. Syst. Sci., vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[11] Security Journey, "OWASP Top 10 Software and Integrity Failures Explained," securityjourney.com. [Online]. Available: https://www.securityjourney.com/post/owasp-top-10-software-and-integrity-failures-explained