Analisis Keamanan *Website* Desa Budaya DIY Dengan Metode *Penetration Testing (Pentest)* dan OWASP ZAP

Muhammad Arifai Nurrizki[1*], Erik Iman Heri Ujianto[2], Rianto[3]
[1,2,3]Studi Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
[1]manrzmz31@gmail.com, [2]erik.iman@uty.ac.id, [3]rianto@staff.uty.ac.id
*Penulis Korespondensi

ABSTRAK

Website yang bertujuan menyampaikan informasi sangat membutuhkan keamanan agar informasi yang diterima tidak di curi atau di rusak. Beberapa waktu lalu *website* Desa Budaya diserang oleh peretas yang mengakibatkan tampilan pada *website* berubah dan rusak. Berdasarkan kondisi tersebut akan dilakukan penelitian yang berguna untuk menganalisis serta mengetahui keamanan dan kelemahan *website* Desa Budaya. Cara yang dapat digunakan untuk menganalisis keamanan *website* adalah metode *Penetration Testing (Pentest)*. Metode *Penetration Testing* ialah sebuah kegiatan yang berfungsi mengeksploitasi dan mengidentifikasi kerentanan keamanan. Cara ini digunakan untuk memindai target dan mengecek kerentanan, serta memiliki proses berorientasi dengan beberapa fase. Penelitian ini dilakukan dengan menggunakan cara *Footprinting*, *Scanning Fingerprinting*, *Exploit* dan *Report*. Pada pengujian dengan *tool* Nslookup mendapatkan informasi IP yaitu "103.102.146.107". Proses selanjutnya dengan *tool* OWASP (*Open Web Application Security Project*) ZAP mendapatkan beberapa celah keamanan yaitu mendeteksi 17 *sub-file vulnerability*. Sebanyak 6 *sub-file vulnerability* statusnya medium dan 11 *sub-file vulnerability* statusnya *low*. Hasil pengujian pada *website* tersebut dapat memberikan rekomendasi kepada pengelola agar mengecek konfigurasi di *sub-file vulnerability* supaya bisa meningkatkan keamanan sistem pada *website*.

Kata kunci: analisis keamanan, *penetration testing (pentest), website.*

ABSTRACT

Cultural Village website is a very important to support the activities and development of the Cultural Village in Yogyakarta, especially in the field of Information Technology. Website that aim to convey information really need security so that the information received is not stolen or damaged. Some time the Culture Village website, attacked a hackers which resulted in the appearance of the website changing and breaking. Based on these conditions, a study was conducted to analyze the security website, then find loopholes for the Cultural Village website weaknesses. The method can be used to analyze is Penetration Testing (Pentest). Penetration Testing is an activity carried out to exploit and identify security vulnerabilities. This method is used to scan targets and check for vulnerability, and has an oriented process with several phases. This research was conducted using Footprinting, Scanning Fingerprinting, Exploit and Report. In testing with Nslookup tool, IP information is "103.102.146.107". The next process with the OWASP (Open Web Application Security Project) ZAP tool found several security holes, namely detecting 17 sub-file vulnerability. A total of 6 vulnerability sub-files have medium status and 11 vulnerability sub-files have low status. The test results on the website can provide recommendations to managers to reconfigure the vulnerability sub-file to improve the website's security system.

Keywords: *analyze the security, penetration testing (pentest), website*

1. PENDAHULUAN

Perkembangan Teknologi di era sekarang sangat dibutuhkan bagi pemerintahan maupun masyarakat yang mendukung kegiatan untuk mendapatkan suatu informasi yang baik, cepat dan tepat. Suatu perkembangan teknologi yang sangat dibutuhkan yaitu Internet. Internet merupakan suatu bagian dari perkembangan teknologi informasi yang memiliki tujuan memberikan informasi secara cepat tanpa adanya kendala ruang dan waktu. Teknologi internet merupakan gabungan berbagai macam bentuk layanan: *World Wide Web* (WWW) [1]. Fungsi dari WWW adalah menjadi media komunikasi seperti berupa gambar, suara, teks, animasi dan sekumpulan perangkat lunak di internet. *Website* merupakan perwujudan perkembangan teknologi informasi yang membawa dampak bagi pemerintahan, baik yang berdampak positif ataupun negatif. Dampak positif dari sebuah *website* adalah dapat memperoleh berbagai macam informasi secara luas dengan cepat dan mudah. Namun, di lain sisi perkembangan dari teknologi yang sangat cepat dapat menimbulkan suatu ekses yang negatif [2]. Contohnya dapat memberikan ruang bagi pelaku kejahatan seperti pencurian data, pencemaran nama baik dan perusakan terhadap

website itu sendiri. *Website* yang bertujuan untuk menyampaikan informasi, tentu membutuhkan keamanan agar informasi yang diterima tidak dicuri atau dirusak. Keamanan pada sebuah *website* menjadi aspek yang penting untuk mejaga kerahasiaan data. Pemerintahan di tuntut untuk menjaga kerahasiaan data pada *website* sesuai dengan standar keamanan. Setara dari tingkat pemakaian *website* yang sangat tinggi, di imbangi dengan timbulnya kerentanan pada *website*, terdapat resiko akan di serang oleh *hacker* sehingga terjadilah peretasan pada *website* [3]. Pengujian sistem keamanan pada *website* adalah hal yang penting di era sekarang. Terdapat banyak metode metode yang bisa dilakukan dalam menguji keamanan dari *website*, antara lain *Penetration Testing (Pentest)* [4].

Penetration Testing (Pentest) merupakan kegiatan yang dilakukan untuk mengeksploitasi dan mengidentifikasi kerentanan keamanan. Cara ini digunakan tidak hanya intuk memindai target untuk mengecek kerentanan, namun juga memiliki proses pengenalan yang memiliki berbagai fase [5]. Metode *Pentest* juga membantu mengecek langkah-langkah keamanan yang telah dilakukan agar efektif atau tidak, sehingga dapat membantu pengembang untuk tidak memberi akses *code* yang bahaya serta berpontensi diserang hacker. *Website* desa budaya merupakan sebuah website yang sangat penting untuk menunjang kegiatan pengembangan dan kegiatan desa budaya di yogyakarta dalam bidang Teknologi Informasi. Maka dari itu peneliti ingin menganalisis keamanan website desa budaya agar dapat menjadi acuan untuk meningkatkan keamanan *website* tersebut.

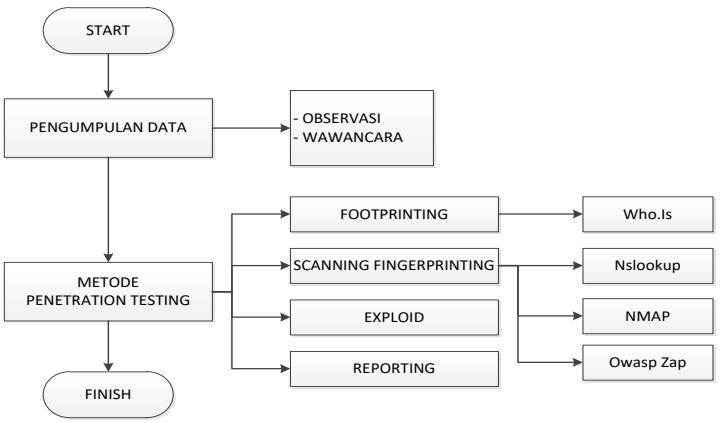
Penelitian oleh [6] mengatakan penelitian ini menganalisis tingkat keamanan dan mencari celah pada kelemahan *website* SMA Negeri 2 Sumbawa Besar menggunakan metode *Penetration Testing*. Ujicoba sistem dilakukan dengan beberapa cara yaitu *footprinting*, kemudian tahap *scanning fingerprinting*, kemudian dilanjutkan proses *exploit* serta *reporting*. Pengujian keamanan *website* ini mendapatkan hasil dengan mendeteksi 13 *sub-file vulnerability* yang mempunyai status medium dan *low*. Hasil pengujian ini berupa daftar celah kerentanan yang dihasilkan untuk merekomendasikan pihak SMA untuk memperbaiki sistem keamanan pada *website*. Penelitian oleh [7] mengatakan penelitian ini menerapkan metode *Penetration Testing* dengan beberapa proses yaitu *Pre-engagement Interaction*, kemudian *intelegence gathering*, kemudian *vulnerabillity analysis*, kemudian *exploitation* serta *reporting*. Pengujian dilakukan dengan *tool* zenmap dan mendapatkan hasil berupa 6 port mempunyai status terbuka di elearning.unp2.ac.id. Dapat disimpulkan tahap scanning dari hasil pengujian kerentanan keamanan website yaitu sejumlah 96.

Penetration Testing ialah cara yang digunakan pada pengujian suatu sistem yang bertujuan untuk mencari kelemahan pada sebuah sistem agar sistem dapat di kembangkan lebih baik. Tujuan dari *Penetration Testing* adalah mengantisipasi adanya penyerangan atau peretasan pada sebuah sistem. Tingkat keberhasilan proses *Penetration Testing* terhadap sistem ditentukan oleh tingkat keahlian penyerang untuk memperoleh hasil paling akuran dari kelemahan server [8].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Pada tahapan penelitian dari Menganalisis Keamanan *website* Desa Budaya Dengan Menggunakan Metode Penetration Testing (Pentest) dan OWASP ZAP mempunyai tahapan-tahapan yang digunakan untuk menyelesaikan penelitian agar dapat mendapatkan informasi yang diperlukan dalam menganalisis keamanan website. Tahapan pertama yaitu Pengumpulan data. Hal pertama yang dilaksanakan yaitu dengan mendatangi Dinas Kebudayaan untuk Obeservasi agar mengetahui tentang website Desa Budaya. Tahapan kedua yaitu wawancara yang dilakukan dengan bertanya kepada narasumber untuk mengetahui apakadh website Desa Budaya pernah mendapatkan ancaman keamanan atau belum. Tahapan ke 3 yaitu melakukan metode Penetration Testing dengan mencoba beberapa cara seperti footprinting, scanning fingerprinting, exploit, dan reporting untuk menganalisis keamanan web Desa Budaya. Alur tahapan penelitian ini bisa dilihat pada gambar 1 dibawah ini.



Gambar 1. Tahapan Penelitian

2.2 Metode Pengumpulan Data

Pada metode pengumpulan data, observasi dilakukan di Dinas Kebudayaan DIY untuk mengetahui tentang *website* Desa Budaya. Tahapan kedua yaitu wawancara yang dilakukan dengan bertanya kepada narasumber untuk mengetahui apakah website Desa Budaya pernah mendapatkan ancaman keamanan atau belum. Hasil pengumpulann data ini selanjutnya dapat digunakan pada tahapan *Penetration Testing* yang akan menguji keamanan *website* tersebut.

2.3 Metode *Penetration Testing (Pentest)*

Penetration Testing (Pentest) ialah pendekatan proaktif yang bertujuan mengevaluasi keamanan aset digital dengan sangat aktif mengidentifikasi serta mengeksploitasi celah keamanan yang terdapat pada *asset digital* [9]. *Penetration Testing (Pentest)* merupakan serangan pada sistem yang bertujuan mecari celah ancaman dan resiko pada suatu sistem perangkat lunak, web aplikasi dan jaringan yang dapat dimanfaatkan oleh penyerang [10]. Metode *Penetration Testing (Pentest)* yang baik selalu akan merekomendasikan kepada pemilik website terkait mengatasi dan memperbaiki masalah yang ada atau ditemukan saat pengujian berlangsung. Secara umum, proses ini digunakan untuk mencegah dan mengamankan website dari serangan keamanan dimasa mendatang. Metode *Penetration Testing (Pentest)* memiliki beberapa tahapan tahapan yang harus dijalankan atau dilakukan saat pengujian. Adapun beberapa langkah langkahnya yaitu sebagai berikut.

a. *Footprinting*

Footprinting merupakan suatu cara yang memiliki tujuan untuk mengetahui atau mendapatkan informasi mengenai info yang ada pada sebuah website, antara lain untuk mengetahui domain website, alamat website, nomor telepon, alamat email, masa aktif domain website yang didaftarkan dan info mengenai kapan kadaluarsanya domain sebuah website. Pada tahapan ini menggunakan sebuah program aplikasi yang ada di internet bernama who.is (bisa dicari pada google chrome). Masukkan link dari website tersebut pada pencarian di who.is maka akan mendapatkan informasi tentang website tersebut.

b. *Scanning Fingerprinting*

Setelah dilakukan analisa untuk mengetahui masalah pada website, selanjutnya mencoba untuk memecahkan masalah tersebut dengan cara :

1) Nslookup yaitu mempunyai tujuan untuk mengetahui sebuah IP dari suatu domain. Caranya yaitu dengan mengetik Nslookup pada *browser*, kemudian masukkan link dari *website* tersebut pada pencarian Nslookup, maka akan mengetahui hasil IP dari suatu domain *website*.
2) Nmap memiliki tujuan untuk mengetahui *port* yang terbuka atau biasa disebuat sebagai *Port Scanning*. Caranya dengan memasukkan IP dari *website* tersebut pada pencarian di Nmap, kemudian *Scan* untuk mengetahui port dengan status *open* atau terbuka.
3) Owasp Zap bertujuan menemukan keamanan yang terdapat pada suatu website. Dengan cara menyalin link web tersebut, kemudian memasukkan di *tool* Owasp Zap, kemudian pilih menu untuk *attack*. Hasilnya berupa berbagai jenis jenis penyerangan pada *website*.

c. *Exploit*

Tahapan Exploit ini peneliti berusaha mencoba pengujian serta percobaan pada keamanan *website* yang telah dicoba dengan beberapa tahapan atau cara, berdasar pada hasil informasi pada saat melakukan *footprinting* dan *scanning*.

d. *Reporting*

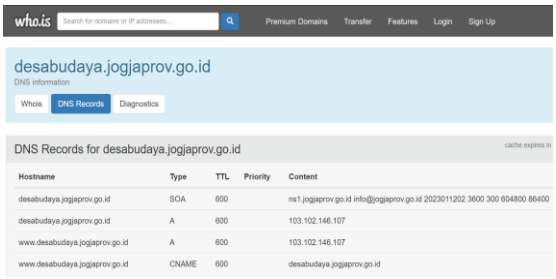
Pada tahapan Reporting setelah berbagai macam pengujian dan percobaan terhadap keamanan *website* hasil dari ancaman maupun serangan yang dilakukan pada *website* tersebut akan di *report* atau di laporkan. Hal ini bertujuan untuk merekomendasikan penanganan yang akan dilakukan terhadap keamanan *website* sebagai hasil dari analisis penelitian ini.

3. HASIL DAN PEMBAHASAN

3.1 *Footprinting*

Footprinting merupakan suatu cara yang memiliki tujuan untuk mengetahui atau mendapatkan informasi mengenai info yang ada pada sebuah *website*, pada tahapan *footprinting* adapun prosesnya menggunakan program

tool yang bernama who.is. Cara yang dilakukan pada tahapan ini yaitu memasukkan link *website* Desa Budaya yaitu https://desabudaya.jogjaprov.go.id kedalam *tool* who.is untuk mendapatkan informasi pada *website* tersebut. Hasilnya seperti pada Gambar 2



Gambar 2. Hasil *footprinting website* Desa Budaya

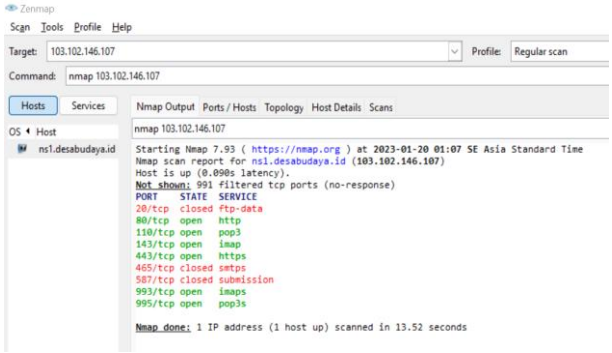
Gambar 2 merupakan hasil *footprinting* menggunakan *tool* who.is untuk mengetahui atau mendapatkan informasi *website* namun *register website* Desa Budaya di *private* oleh pembuatnya, hasilnya mendapatkan alamat IP dari *website* Desa Budaya tersebut.

3.2 *Scanning Fingerprinting*

Pada tahapan ini untuk mengetahui IP dari *website* Desa Budaya, peneliti menggunakan *tool* Nslookup. Dengan cara yaitu mengetik Nslookup pada *browser*, kemudian masukkan link *website* Desa Budaya pada pencarian Nslookup, maka akan muncul IP nya seperti yang ditunjukkan oleh gambar 3 dibawah ini.

Gambar 3. Pencarian IP menggunakan *tool* Nslookup

Gambar 3 diatas merupakan hasil pencarian IP pada *website* Desa Budaya. Berdasarkan pengujian *port scanning* tersebut, alamat web serta IP address web Desa Budaya dapat dilihat. Hasil *scanning tool* Nslookup menampilkan informasi IP nya yaitu "103.102.146.107". Kemudian untuk melihat server atau *port* yang memiliki kerentanan pada website Desa Budaya tool yang di gunakan peneliti yaitu Nmaps atau biasa di sebut *network mapper*. Dari pengujian yang dilakukan dengan Nmaps hasil yang didapatkan dapat dilihat pada gambar 4 berikut ini.



Gambar 4. *Scanning* menggunakan Nmaps

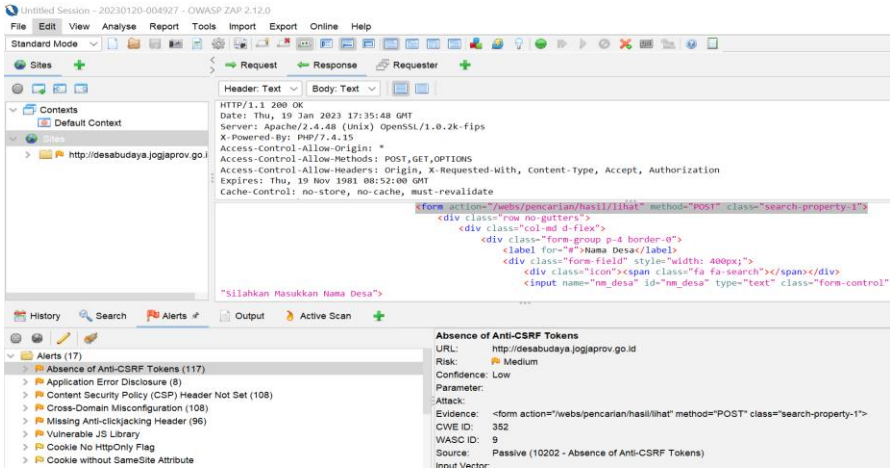
Hasil *port scanning* yang dilakukan pada pengujian dengan Nmaps terlihat *port* Service seperti http, pop3, imaps, https, pop3s yang status *port* nya terbuka. Kemudian *port* ftp-data, smtps dan *submission* tertutup.

3.3 Exploit

Pengujian pada tahap *exploit* yang dilakukan pada *website* Desa Budaya tidak dapat dilakukan karena sistem *website* Desa Budaya menggunakan keamanan dengan standar yang tinggi menggunakan *Hypertext Transfer Protocol Securen* (HTTPS) dengan menggunakan protokol yaitu *Transport Layer Security* (TLS).

3.4 Pembahasan

Proses pengujian digunakan untuk mencari celah keamanan atau kerentanan pada *website* Desa Budaya. Pada proses ini menggunakan tool OWASP ZAP atau biasa disebut *Open Web Application Security Project*. Hasil yag didapatkan saat pengujian keamanan atau kerentanan *website* yaitu pada gambar 5 dibawah ini.



Gambar 5. Pengujian dengan *tool* dari OWASP ZAP

Setelah dilakukan pengujian, pada penelitian ini dengan menggunakan *Open Web Application Security Project* (OWASP) ZAP mendapatkan hasil berbagai kerentanan keamanan di web Desa Budaya. Hasil *scanning* yang didapatkan saat pengujian *website* Desa Budaya adalah 17 *alert* dengan 2 level kerentanan yaitu 6 pada level : *medium risk*, 8 pada level : *low risk*, dan 3 pada level : *information risk*. *Adapun* hasilnya dapat dilihat pada Tabel 1 dibawah ini.

Tabel 1. Hasil pengujian OWASP

No	*Alert*	*Risk*	
		Low	*Medium*
1	*Absence of Anti-CSRF Tokens*		√
2	*Application Error Disclosure*		√
3	*Content Security Policy Header Not Set*		√
4	*Cross-Domain Misconfiguration*		√
5	*Missing Anti-clickjacking Header*		√
6	*Vulnerable JS Library*		√
7	*Cookie No HttpOnly Flag*	√	
8	*Cookie without SameSite Attribute*	√	
9	*Cross Domain JavaScript Source File Inclusion*	√	
10	*Information Disclosure – Debug Error Messages*	√	
11	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*	√	
12	*Server Leaks Version Information via "Server" HTTP Response Header Field*	√	
13	*Timestamp Disclosure-Unix*	√	
14	*X-Content-Type Options Header Missing*	√	
15	*Information Disclosure – Suspicious Comments*	√	
16	*Modern Web Application*	√	
17	*User Controllable HTML Element Attribute*	√	

Pengujian yang telah dilalui pada *website* Desa Budaya berdasarkan *Open Web Applications Security Project* (OWASP) ZAP dapat memberikan rekomendasi kepada administrasi *website* Desa Budaya untuk

mengecek kembali konfigurasi pada *sub-file vulnerability* agar keamanan *website* lebih terjaga dan tidak mudah diretas orang.

4. KESIMPULAN

Pengujian dan analisis keamanan *website* Desa Budaya telah berhasil. Tahapan yang dilalui dalam analisis keamanan *website* ini yaitu menguji sistem dengan menggunakan cara *Footprinting, Scanning Fingerprinting, Exploit serta Report*. Pengujian di keamanan *website* Desa Budaya dilakukan dengan menggunakan beberapa *tools* yaitu *Who.is*, NSlookup, Nmaps dan OWASP (*Open Web Application Security Project*) ZAP. Berdasarkan pengujian dengan tool Nslookup terdapat IP Address pada Website Desa Budaya. Hasil scanning *tool* Nslookup menampilkan informasi IP nya yaitu "103.102.146.107". Pada tahapan pengujian dengan *tool* OWASP (*Open Web Application Security Project*) ZAP hasilnya mendapatkan beberapa kerentanan keamanan serta mendeteksi 17 *sub-file vulnerability*, yang mempunyai status *medium* ataupun *low*. Sebanyak 6 *sub-file vulnerability* mempunyai tingkatan *medium* dan 11 *sub-file vulnerability* mempunyai status *low*. Pengujian pada tahap *exploit* yang dilakukan pada *website* Desa Budaya tidak dapat dilakukan karena sistem *website* Desa Budaya menggunakan keamanan dengan standar yang tinggi menggunakan *Hypertext Transfer Protocol Secure* (HTTPS) dengan menggunakan protokol yaitu *Transport Layer Security* (TLS). Dari hasil pengujian dapat memberikan rekomendasi kepada administrasi *website* Desa Budaya untuk mengecek kembali konfigurasi pada *sub-file vulnerability* agar keamanan website lebih terjaga dan tidak mudah diretas orang.

DAFTAR PUSTAKA

[1] T. L. Marselino, "Kajian Ekspresi Diri pada Ruang Publik Dunia Maya dalam Perspektif Ontologis Layanan Internet World Wide Web," vol. 9, no. 1, pp. 14–23, 2022.

[2] N. Sulisrudatin, "Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit," *J. Ilm. Huk. Dirgant.*, vol. 9, no. 1, pp. 26–39, 2014, doi: 10.35968/jh.v9i1.296.

[3] S. Eko Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf," *J. Ilm. Inform.*, vol. 9, no. 02, pp. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.

[4] M. F. Susanto, A. Nurcahyo, and ..., "Website Threat Monitoring Untuk Pemantauan dan Analisis Ancaman Pada Web Server," *... Res. Work. ...*, pp. 13–14, 2022, [Online]. Available: https://jurnal.polban.ac.id/ojs-3.1.2/proceeding/article/view/4213%0Ahttps://jurnal.polban.ac.id/ojs-3.1.2/proceeding/article/view/4213/2937

[5] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 2, p. 80, 2022, doi: 10.53513/jis.v21i2.6119.

[6] Y. Mulyanto, M. Taufan Asri Zaen, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res.*, vol. 4, no. 1, pp. 202–209, 2022, doi: 10.47065/josh.v4i1.2335.

[7] F. Y. Fauzan and S. Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 9, no. 2, p. 105, 2021, doi: 10.24036/voteteknika.v9i2.111778.

[8] I. G. Arya Kukuh Y, Geraldo Alfarenb, "Analisis Serangan Sistematik Penetration Testing : Sebuah Review," *J. Ilm. Inform. Komput.*, vol. 1 no. 2, pp. 21–26, 2022.

[9] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[10] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, 2022, doi: 10.47970/siskom-kb.v5i2.268.