Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing* (*Pentest*)

Yudi Mulyanto[1], Mohammad Taufan Asri Zaen[2,*], Yuliadi[1], Safwan Sihab[1]

[1]Fakultas Rekayasa Sistem, Informatika, Universitas Teknologi Sumbawa, Sumbawa
Jl. Raya Olat Maras, Batu Alang, Moyo Hulu, Pernek, Kec. Moyo Hulu, Kabupaten Sumbawa, Nusa Tenggara Barat, Indonesia
[2]Sistem Informasi, STMIK Lombok, Lombok Tengah
Jalan Basuki Rahmat Praya Mataram, Praya, Kec. Praya, Kabupaten Lombok Tengah, Nusa Tenggara Barat, Indonesia
Email: [1]yudi.mulyanto@uts.ac.id, [2,*]opanzain@gmail.com, [3]yuliadi@uts.ac.id, [4]s.sihab@gmail.com
Email Penulis Korespondensi: opanzain@gmail.com
Submitted: **07/10/2022**; Accepted: **30/10/2022**; Published: **31/10/2022**

Abstrak−Keamanan website menjadi aspek yang sangat penting seiring dengan peningkatan volume data yang dipertukarkan di internet. SMA Negeri 2 Sumbawa Besar menyediakan informasi dalam sebuah *website*, baik informasi untuk pengenalan sekolah atau informasi yang berkaitan dengan sekolah dapat melalui beberapa media. Beberapa waktu yang lalu websitesekolah diserang oleh penjahat informasi yang mengakibatkan tampilan website berubah dan mencuri beberapa data penting sekolah. Sistem keamanan website yang lemah dapat menjadi target sasaran yang mudah bagi para pelaku *cyber criminal*. Mereka mengetahui berbagai macam cara untuk masuk ke dalam sistem keamanan website dan melakukan berbagai macam tindakan yang dapat merugikan organisasi. Berdasarkan kondisi yang terjadi pada website sekolah, maka dilakukan penelitian melakukan menganalisis tingkat keamanan dan mencari celah pada kelemahan *website* SMA Negeri 2 Sumbawa Besar. Dalam analisis ini, peneliti melakukan pengujian *website* sekolah dengan menggunakan metode *Penetration Testing*. Pengujian dilakukan dengan beberapa tahapan yakni *Footprinting*, *Scanning Fingerprinting*, *Exploit* dan *Reporting*. Proses pengujian keamanan *website* SMA Negeri 2 Sumbawa didapatkan beberapa celah yang mendeteksi 13 sub *file vulnerability* dengan status *low* dan *medium*. Hasil penelitian ini berupa hasil pengujian keamanan berupa daftar celah kerentanan yang dapat menjadi rekomendasi bagi pihak sekolah dalam perbaikan keamanan *website.*

Kata Kunci: Website; Sekolah; Cyber Criminal; Analisa; Metode Pentest

Abstract−Website security is becoming a very important aspect along with the increasing volume of data exchanged on the internet. High School 2 Sumbawa Besar provides information on a website, both information for school introductions or information related to schools can be through several media. Some time ago the school's website was attacked by information criminals who caused the appearance of the website to change and steal some important school data. Weak website security systems can be easy targets for cyber criminals. They know various ways to get into the website security system and perform various actions that can harm the organization. Based on the conditions that occurred on the school's website, a research was conducted to analyze the level of security and look for loopholes in the weaknesses of the High School 2 Sumbawa Besar website. In this analysis, researchers tested the school's website using the Penetration Testing method. Test is carried out in several stages, namely *Footprinting*, Scanning Fingerprinting, Exploit and Reporting. The process of testing the website security of High School 2 Sumbawa Besar found several loopholes that detected 13 sub-file vulnerabilities with low and medium status. Results of this study are the results of security testing in the form of a list of vulnerabilities that can be a recommendation for the school in improving website security.

Keywords: Website; School; Cyber Crime; Analysis; Pentest Method

1. PENDAHULUAN

Teknologi informasi menjadi kebutuhan mutlak, bagi seluruh lapisan masyarakat terlebih pemerintahan untuk mendukung memperoleh informasi yang cepat, mudah, akuntabel, serta layanan yang perima. Jaringan komputer yang digunakan dalam pertukaran informasi pada ranah ruang publik [1]. Internet bagian dari kemajuan teknologi informasi menjadi media informasi yang pertumbuhannya sangat cepat tanpa terkendala ruang dan waktu. Salah satu bagian dari internet yang pertumbuhannya sangat cepat adalah *world wide web* (www). WWW adalah teknologi yang perkembangan cepat sebagai mediakomunikasi berisi informasi berupa suara, gambar, animasi, text, dan programperangkat lunak yang menyusunnya menjadi dokumen yang dinamis [2].

Berdasarkan fungsinya website sebagai media yang menyampaikan informasi, membutuhkan sebuah keamanan agar informasi utuh diterima oleh penerima informasi. Bila pemilik website mengabaikan keamanan tersebut, maka seorang *cracker*mampu membuat suatu program bagi kepentingan dirinya sendiri dan bersifat merusak informasi tersebut. Beberapa contoh kasus yang dilakukan oleh *cracker* meliputi Virus, Pencurian Kartu Kredit, Pembobolan Rekening Bank, Pencurian Password E-mail/*Web Server*.*Cracker* mengambil data-data penting pada suatu *website* dan bahkan pula mengacak-acak tampilan *web* tersebut di *website* disebuah organisasi, instansi, dan sekolah [3].

Teknologi informasi (*information technology*) yang perwujudannya dalam bentuk *website* membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya adalah dapat memperoleh berbagai informasi, baik dari dalam maupun luar negeri, transaksi jarak jauh. Sedangkan dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan, seperti penipuan, pencurian,

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

pencemaran nama baik, kesusilaan, perjudian, pengancaman, perusakan dan teror yang seluruhnya dikenal dengan *cyber crime* [4].

Keamanan website menjadi aspek yang sangat penting seiring dengan peningkatan volume data yang dipertukarkan di internet. Setiap organsiasi maupun perusahaan dituntut untuk selalu menjaga kerahasiaan, integritas dan otentikasi data pada sebuah website sesuai standar keamanan. Hal ini salah satunya disebabkan oleh meningkatnya ketergantungan masyarakat pada website sehingga keamanan keseluruhan dari sistem harus selalu diukur dan ditingkatkan [5]. Tidak adanya keamanan pada sistem website akan berdampak buruk. Hacker dengan mudah dapat mengambil alih sistem yang dibangun. Hal ini menimbulkan permasalahan pada data yang bersifat pribadi, maupun data yang sangat penting sebuah perusahaan atau lembaga yang seharusnya tidak diketahui oleh orang lain, akan tetapi dapat di akses oleh *hecker* [6].

SMA Negeri 2 Sumbawa Besar merupakan salah satu Sekolah menengah atas negeri yang ada di sumbawa yang telah terakreditasi A, yang beralamat di Jln. Garuda 102 Sumbawa Besar, Lempeh, Kecamatan Sumbawa, Kabupaten Sumbawa Nusa Tenggara Barat. SMA Negeri 2 Sumbawa Besar menyediakan informasi dalam sebuah *website*, baik informasi untuk pengenalan sekolah atau informasi yang berkaitan dengan sekolah dapat melalui beberapa media. *Website* sekolah dapat dibuka melalui *domain https://sman2sumbawabesar.sch.id/*.Selain itu juga terdapat profil sekolah yang ditampilkan dalam sebuah *website* tersendiri dengan subdomain yang sama[7].

Berdasarkan hasil observasi, SMA Negeri 2 Sumbawa Besar pada tahun 2012 website SMA Negeri 2 Sumbawa Besar pernah diserang. Penyerangan tersebut mengakibat tampilan website berubah dan beberapa data diambil oleh penjahat informasi. Kejadian tersebut sangat merugikan pengelola dan pengguna yang sering berinteraksi dengan *website* tersebut untuk mendapatkan informasi. Selain itu, sistem keamanan website yang lemah dapat menjadi target sasaran yang mudah bagi para pelaku *cyber criminal*. Mereka mengetahui berbagai macam cara untuk masuk ke dalam sistem keamanan website dan melakukan berbagai macam tindakan yang dapat merugikan organisasi.

Berangkat dari permasalahan tersebutpenulis melakukan menganalisis tingkat keamanan dan mencari celah pada kelemahan *website* di SMA Negeri 2 Sumbawa Besar. Dalam menganalisa keamanan *website* menggunakan *tool Zed Attack* Proxy *(ZAP)*) dan metode *Pentest*. Dengan analisa keamanan *website* SMA Negeri 2 Sumbawa, diharapkan dapat menjadi rekomendasi bagi pihak SMA Negeri 2 Sumbawa Besar agar dapat meningkatkan keamanan *website.*

Adapun penelitan yang terdahulu menajdi rujukan dalam penelitian ini, yakni penelitian tentang Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing dan Dast (*Dynamic Application Security Testing*). Kejahatan siber banyak ditemukan pada kasus penyerangan situs web untuk mendapatkan data penting pada situs web. Ancaman kejahatan siber berasal dari *malware*, *supply chain attact*, hingga *ransomware*. Penelitian dilakukan untuk mengetahui celah keamanan pada situs web, dengan metode *Penetration Test* dan *Dynamic Application Security Testing* (DAST). Celah keamanan yang diuji khususnya *Broken Access Control*, *Cross Site Scripting* (XSS), dan *Sql Injection* dan kemudian dilakukan upaya perbaikan pada situs web [8].

Penelitian tentang Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. Lembaga X adalah lembaga pemilihan umum yang memiliki situs web sebagai media penyampaian informasi dan penataan data pemilih. Sebagai situs web yang menyimpan data sensitif, perlu dilakukan peningkatan keamanan untuk mencegah terjadinya serangan pihak luar. Metode yang dapat digunakan untuk menguji keamanan sistem adalah pengujian penetrasi. Hasil dari penelitian ini adalah diperoleh 18 celah keamanan yang terdapat pada website Lembaga X. Pemberian rekomendasi diberikan untuk meningkatkan keamanan website Lembaga X [9].

Penelitian tentang Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web. Aplikasi web dapat berjalan pada berbagai sistem operasi dengan bantuan perambah web. Aplikasi web merupakan platform aplikasi yang cukup rentan terhadap serangan dari peretas. *SQL Injection, Phising,* dan *Cross-Site Scripting* (XSS) merupakan beberapa jenis serangan yang dapat menyerang aplikasi berbasis web. Dalam meningkatkan sistem keamanan dari sebuah aplikasi berbasis web maka perlu dilakukan sebuah tahapan pengujian keamanan dari aplikasi berbasis web tersebut. Pengujian keamanan dilakukan dengan melakukan uji teknik-teknik serangan yang mungkin terhadap aplikasi target. Penelitian ini akan mengusulkan sebuah rancangan aplikasi terintegrasi yang dapat digunakan untuk melakukan pengujian terhadap aplikasi berbasis web [10].

Penelitian tentang Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box. Penetration testing merupakan pengujian pada sistem yang memiliki elemen yang bersifat kritis membahayakan apalikasi *Open Journal System* (OJS) yang berjalan pada internet. Tahap uji coba melibatkan langkah-langkah berikut: pengumpulan informasi, analisis kerentanan, dan kerentanan mengeksploitasi. Pengujian Penetration testing. Pengujian yang telah dilakukan mengidetifikasi 1 kerentanan high risk, 7 kerentanan medium *risk*, 90 pada kerentanan *low risk* pada OJS. Total vulnerability pada pengujian berjumlah 98 *vulnerability file* sistem dengan tambahan informasi 1043 file sistem untuk ditindaklanjuti dalam perbaikan [11].

Keamanan adalah hal yang paling mutlah dilakukan bila dilakukan pertukaran informasi ke ranah publik. Pentingnya pengamanan pada media *website* yang digunakan pengguna dalam pertukaran informasi [12]. Keamanan *Website* adalah suatu aktivitas sebagai perlindungan terhadap informasi/data. Kejahatan dunia maya

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

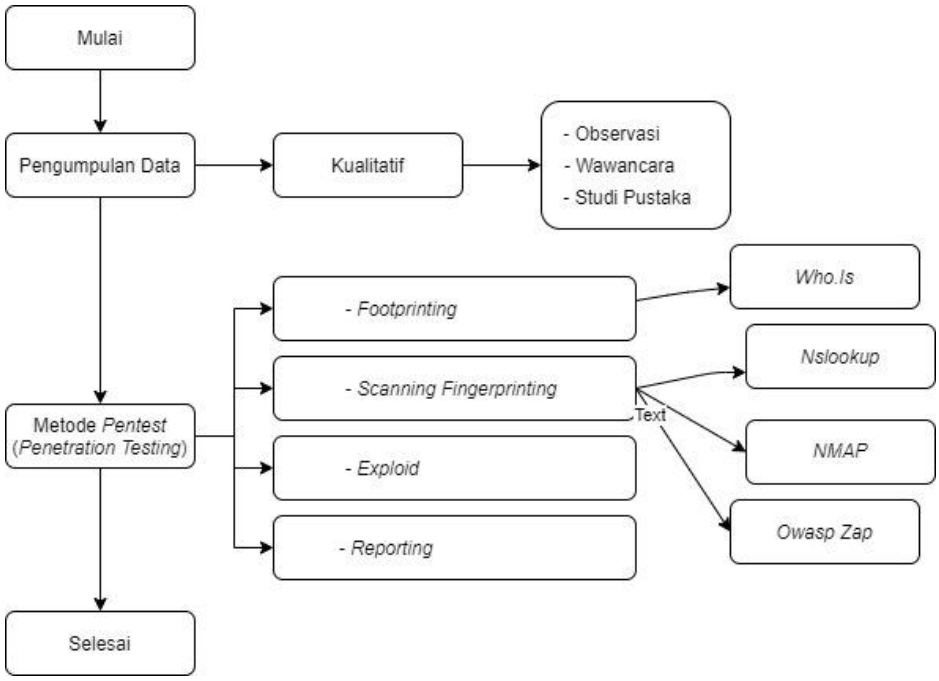
merupakan kejahatan yang dilakukan oleh seseorang dengan menggunakan fasilitas internet yang bersifat melintasi batas negara, dilakukan secara ilegal, menggunakan peralatan komputer dan internet, menyebabkan kerugian, dan sulit dibuktikan secara hukum [13].

Penetration testing merupakan suatu aktvitas proses mensimulasikan serangan terhadap jaringan organisasi/perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut [14]. Uji penetrasi dilakukan untuk mengukur dampak dan kemungkinan kerentanan sehingga memungkinkan organisasi untuk memprioritaskan langkah-langkah korektif untuk perbaikan sistem. Proses uji memerlukan banyak waktu, tenaga dan pengetahuan dalam menangani kompleksitas ruang pengujian [15].

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

Dalam penelitian Analisis Keamanan *Website* di SMA Negeri 2 Sumbawa Besar menggunakan Metode *Penetration Testing (pentest)* sesuai dengan tahapan-tahapan yang ditetapkan untuk mendapatkan informasi yang diperlukan dalam penyelesian masalah. Adapun tahapan penelitian tersebut dapat dilihat pada diagram penelitian dibawah adalah :



Gambar 1. Diagram Penelitian

2.2 Metode Pengumpulan Data

Berikut beberapa metode pengumpulan data yang digunakan peneliti dalam melakukan penelitian Analisis Keamanan *Website* di SMA Negeri 2 Sumbawa Besar menggunakan Metode *Penetration Testing (pentest)*, yaitu observasi, wawancara dan studi Pustaka.

2.3 Metode *Penetration Testing*

Analisis website SMA Negeri 2 Sumbawa menggunakan *Penetration Testing* digunakan mencari kerentanan yang ada pada Web server. Hasil dari pengujian ini diharapkan dapat dicermati pola serangan yang dilakukan oleh para Hacker dan tindakan yang dapat dilakukan dalam mengamankan sebuah *Web Server*[16]. Adapun tahapan-tahapan *Penetration Testing*, yakni:

a. *Footprinting*

Tahap ini dilakukan bertujuan untuk mendapatkan informasi mengenai *domainwebite,* alamat, No. Telepon alamat email, kapan domain didaftarkan dan kapan domain kadaluarsa. Dengan cara ketik *who.is* di *google chrome* Salin *link* dariwebsitetersebut dan *paste* pada pencarian *who.is.*

b. *Scanning Fingerprinting*

Setelah melakukan analisa masalah, adapun langkah untuk pemecahan masalah tersebut dengan beberapa aktivitas adalah:

1. *Nslookup* yaitu bertujuan mengetahui IP dari sebuah domain. Dengan cara ketik *Nslookup* di *google crom* Salin *link* dari *website* tersebut dan *paste* pada pencarian *Nslookup.*
2. *Nmap* yaitu bertujuan untuk *Port Scanning* atau mengetahui port terbuka. Dengan cara memasukan ip

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

dari website, lalu pilih *scan* maka akan mucul port mana yang terbuka.

3. *Owasp Zap* yaitu Untuk mencari celah kerentanan yang ada pada sebuah *Website*. Salin *link* dari *website* tersebut dan *paste* pada *tool Owaps zap*, lalu klik *attack*. Dan akan muncul jenis serangan *website* tersebut.

c. *Exploit*

Pada tahapan ini penulis akan melakukan berbagai percobaan dan pengujian terhadap sistem keamanan yang telah diterapkan dengan menggunakan berbagai cara dan teknik berdasarkan informasi yang didapat dalam melakukan tahapan *footprinting, and scanning* sebelumnya.

d. *Reporting*

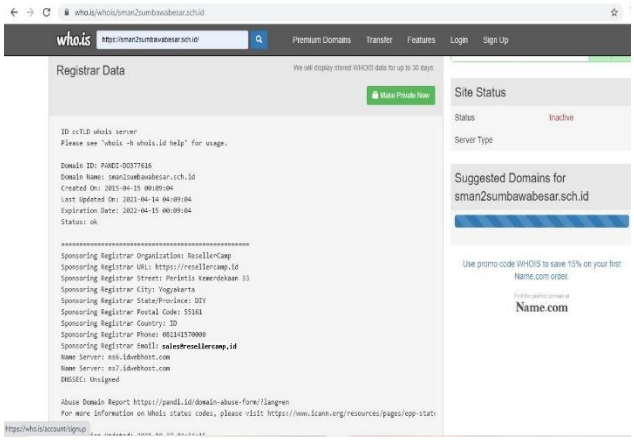
Setelah ditemukan acaman atau seranagan, maka selanjutnya adalah melakukan *report* dan merekomendasikan penangan keamanan *webset* tersebut sebagai hasil akhir analisis.

3. HASIL DAN PEMBAHASAN

3.1 *Proses Penetration Testing*

3.1.1 *Footprinting*/pencarian informasi

Adapun proses *footprinting* menggunakan aplikasi ***Who.is***. Untuk mengambil informasi sebuah alamat domain dari *website* SMA Negeri 2 Sumbawa besar, maka penulis menggunakan w*ebsite Who.is.* Adapun hasil informasi domain yang didapatkan yaitu *https://sman2sumbawabesar.sch.id/* adalah:



Gambar 2. Hasil Pengecekan *Website* SMA Negeri 2 Sumbawa besar

3.1.2 *Scanning Fingerprinting*

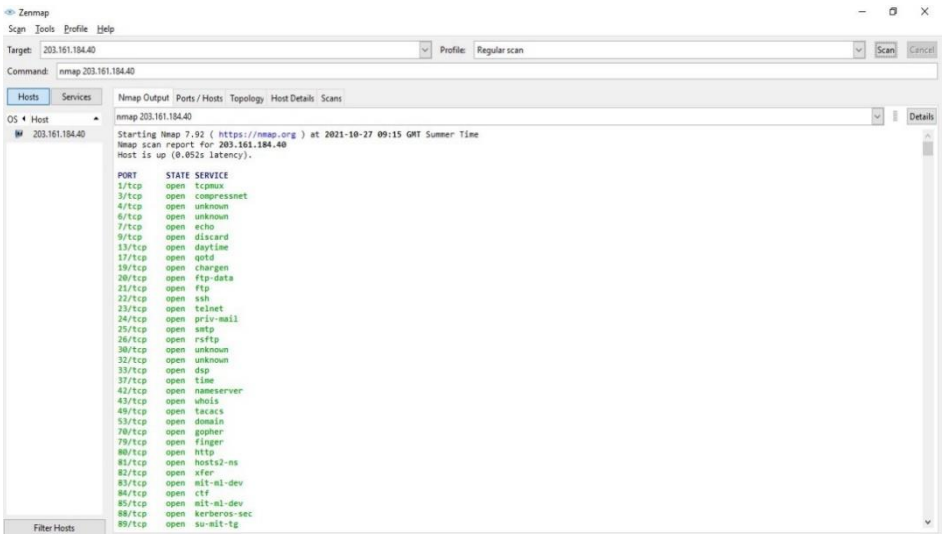
Untuk mengetahui IP dari sebuah *domain* pada *website* SMA Negeri 2 Sumbawa penulis menggunakan *tools Nslookup*. Berikut hasil Scanning dengan *tool Nslookup* pada gambar dibawah:

Gambar 3. *Hasil Scanning* dengan tool *Nslookup*

Berdasarkan pengujian*port scaning* diatas, dapat terlihat alamat *website* dan IP *adress* pada *website* SMA Negeri 2 Sumbawa. Adapun hasil *Scanning* oleh *tool Nslookup* pada *website* SMA Negeri 2 Sumbawa menampilkan informasi IP yaitu "203.161.184.40".

Untuk melihat *server* atau *port* terbuka pada SMA Negeri 2 Sumbawa penulis menggunakan *tool (NMAP) Network Mapper.* Adapun hasil dari pengujian menggunakan *tool (Network Mapper) NMAP* dengan *port Scanning* sebagai berikut:

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335



Gambar 4. Hasil *Port Scanning* dengan *Tool Nmap*

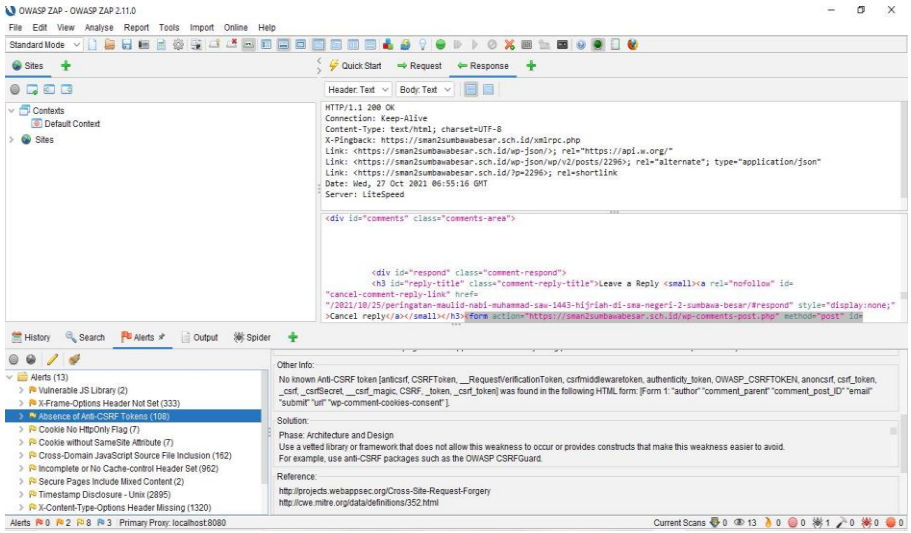
Berdasarkan pengujian *port scaning* diatas dapat terlihat *port Service* seperti *tcpmux, compressnet, whois, finger, multidropper, neod1, neod2, qsm-proxy dll* yang statusya terbuka.

3.1.3 *Exploit*

Proses ini bagian untuk pengujian sistem keamanan *website*pada *MySQL* pentesting menggunakan *MetasploitFramework*. Aktivitas proses ini berupa mengecek apakah *databaseMYSQL* berjalan dengan menggunakan semua modul MYSQL untuk membantu menghasilkan *exploit.*

3.2 Proses Pengujian

Pada peroses ini dikerjakanuntuk mencari celah kerentanan keamanan pada *Website* SMA Negeri 2 Sumbawa penulis menggunakan *tool Open Web Aplication Security Project* (OWASP). Berikut tampilan pengujian kerentanan keamanan *Website* yang telah dilakukan oleh penlis.



Gambar 5. Hasil *scanning OWASPZAP*

Berdasarkan hasil pengujian yang dilakukan pada *tool Open Web Aplication Security Project (OWASP),* didapatkan beberapa celah keamana yang ada di *Website* SMAN Sumbawa diantaranya berupa : *Vulnerable javascript Library, X-Frame-Options Header Not Set, Absence of Anti-cross-site request forgery Tokens, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Timestamp Disclosure – Unix, Information Disclosure - Sensitive Information in Uniform Resource Locator, Information Disclosure -Suspicious Comments*.

Adapun hasil *scaning* yang didapatkan adalah 13 *alerts,* dan 2 level kerentanan, diantaranya: *low* dan *medium.*Bx erikut adalah kolom hasil dari pengujian kerentanan keamanan *Website* SMA Negeri 2 Sumbawa yang mendeteksi 13 sub *file vulnerability* diantaranya dapat dilihat pada tabel berikut.:

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

Tabel 1. Tabel Hasil pengujian KerentananMendeteksi 13 sub *file vulnerability, high, medium, low, informational.*

No	*Alert*	*Risk*		Keterangan
		Medium	*Low*	
1.	*Vulnerable JS Library*	√		Untuk*medium Risk* pada Website SMA Negeri 2 Sumbawa ini adalah tahap menghawatirkan harus segera untuk diperbaiki oleh admin pengelolah SMAN 2 Sumbawa
2.	*X-Frame-Options Header Not Set*	√		
3.	*Absence of Anti-CSRF Tokens*	√		
4.	*Cookie No HttpOnly Flag*	√		
5.	*Cookie without SameSite Attribute*	√		Untuk*medium Risk* pada Website SMA Negeri 2 Sumbawa ini adalah tahap menghawatirkan harus segera untuk diperbaiki oleh admin pengelolah SMAN 2 Sumbawa
6.	*Cross-Domain JavaScript Source File Inclusion*	√		
7.	*Incomplete or No Cache-control Header Set*	√		
8.	*Secure Pages Include Mixed Content*	√		
9.	*Timestamp Disclosure - Unix*		√	Sementara pada posisi low Risk masih berada pada keadaan kerusakan ringan
10.	*X-Content-Type-Options Header Missing*	√		Untuk*medium Risk* pada *Website* SMA Negeri 2 Sumbawaini adalah tahapmenghawatirkan harus segera untuk diperbaiki oleh admin pengelolah SMA Negeri 2 Sumbawa
11.	*Charset Mismatch*		√	Sementara pada posisi low Risk masih berada pada keadaan kerusakan ringan
12.	*Information Disclosure - Sensitive Information in URL*	√		Untukmedium Risk pada *Website* SMA Negeri 2 Sumbawaini adalah tahapmenghawatirkan harus segera untuk diperbaiki oleh admin pengelolah SMA Negeri 2 Sumbawa
13.	*Information Disclosure -Suspicious Comments disclosure*		√	Sementara pada posisi low Risk masih berada pada keadaan kerusakan ringan

3.3 *Rekomendasi Hasil Pengujian Keamanan Website*

Berikut sebuah saran yang direkomendasikan oleh *tool Open Web Aplication Security Project (OWASP).*

Tabel 2. Rekomenasi Oleh *Tool OWAPS*

No	Nama sub file Sistem *Vulnerability*	Jumlah *Vulnerabiliy*	Rekomendasi Perbaikan *(Countermeasure)*
1.	*Vulnerable JS Library*	2	Harap tingkatkan ke *bootstrap* versi terbaru
2.	*X-Frame-Options Header Not Set*	370	Sebagian besar*browser Web* modern mendukung header *HTTP X-Frame-Options.* Pastikan itu disetel di semua halaman *web* yang dikembalikan oleh situs Anda (jika Anda mengharapkan halaman dibingkai hanya oleh halaman di *server* Anda (misalnya itu bagian dari *FRAMESET*) maka Anda akan ingin menggunakan *SAMAORIGIN*, jika tidak, jika Anda tidak pernah mengharapkan halaman untuk dibingkai, Anda harus menggunakan DENY. Atau pertimbangkan untuk menerapkan arahan "*frame-ancestors*" Kebijakan Keamanan Konten.
3.	*Absence of Anti-CSRF Tokens*	109	Arsitektur dan DesainGunakan perpustakaan atau kerangka kerja yang diperiksa yang tidak memungkinkan kelemahan ini terjadi atau menyediakan konstruksi yang membuat kelemahan ini lebih mudah untuk dihindari.Misalnya, gunakan paket anti *CSRF* seperti *OWASP CSRFGuard.*
4.	*Cookie No HttpOnly Flag*	7	Pastikan bahwa *flag HttpOnly* disetel untuk semua *cookie*
5.	*Cookie without SameSite Attribute*	7	Pastikan atribut *SameSite* diatur ke *'lax'* atau idealnya *'strict'* untuk semua *cookie*.
6.	*Cross-Domain JavaScript Source File Inclusion*	168	Pastikan file sumber *JavaScript* dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi.
7.	*Incomplete or No Cache-control Header Set*	1003	Kapan pun memungkinkan, pastikan *header HTTP kontrol-cache* disetel dengan *no-cache, no-store, must-revalidate.*
8.	*Secure Pages Include*	2	Halaman yang tersedia melalui *SSL/TLS* harus sepenuhnya terdiri

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

No	Nama sub file Sistem *Vulnerability*	Jumlah *Vulnerabiliy*	Rekomendasi Perbaikan (*Countermeasure*)
	Mixed Content		dari konten yang dikirimkan melalui *SSL/TLS*. Halaman tidak boleh berisi konten apa pun yang dikirimkan melalui *HTTP* yang tidak terenkripsi. Ini termasuk konten dari situs pihak ketiga.
9.	*Timestamp Disclosure – Unix*	2992	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungkan untuk mengungkapkan pola yang dapat *dieksploitasi*.
10.	*X-Content-Type-Options Header Missing*	1412	Pastikanaplikasi/*server web* menyetel *header Content-Type* dengan tepat, dan menyetel *header X-Content-Type-Options ke 'nosniff'* untuk semua halaman *web*.Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan *browser web* yang sesuai standar dan modern yang tidak melakukan sniffing *MIME* sama sekali, atau yang dapat diarahkan oleh aplikasi *web/server web* untuk tidak melakukan *sniffing MIME. 'nosniff'* untuk semua halaman *web*.Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan *browser web* yang sesuai standar dan modern yang tidak melakukan *sniffingMIME* sama sekali, atau yang dapat diarahkan oleh aplikasi *web/server web* untuk tidak melakukan *sniffing MIME.*
11.	*Charset Mismatch*	170	Paksa *UTF-8* untuk semua *konten teks di header HTTP* dan tag meta dalam *HTML* atau deklarasi penyandian *dalam XML.*
12.	*Information Disclosure - Sensitive Information in URL*	6	Jangan berikan *informasi* sensitif dalam *URI*
13.	*Information Disclosure - Suspicious Comments*	1051	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.

4. KESIMPULAN

Penelitian tentang Analisis keamanan *Website* SMA Negeri 2 Sumbawa Besar telah selesai dilakukan. Proses analisis website SMA Negeri 2 Sumbawa Besar dengan beberapa kegiatan, yakni *Footprinting, Scanning Fingerprinting* dan *Ekploit.* Pada tahapan *exploit* ini tidak bisa masuk karena sistem keamanan *website* SMA Negeri 2 Sumbawa memiki standar keamanan yang sangat tinggi yaitu menggukan *HTTPS (Hypertext Transfer Protocol Secure)* denganprotokol yang digunakan *HTTPS* adalah *Transport Layer Security(TLS).Website* SMA Negeri 2 Sumbawa sudah memikili integritas yang baik terkait *website* yang di gunakan karena pada percobaan pencarian *password* menggunakan metode *penetration testing (pentest)* gagal di lakukan dan hanya saja perlu pemantauan ulang di karenakan masih terdapat kerentanan-kerentanan pada percobaan OWASP. Proses pengujian keamanan website didapatkan beberapa celah yang mendeteksi 13 sub *file vulnerability* dengan status low dan medium. Dari hasil tersebut di berikan rekomendsi pengelola website melakukan konfigurasi ulang *file vulnerability* untuk meningkatkan keamanan website. Selain itu, pengelola secara terus menerus melakukan peningkatkan keamanan *website* ke jenjang yang lebih tinggi, agar tidak ada serangan yang akan datang nantinya.

UCAPAN TERIMAKASIH

Puji Syukur pada Allah SWT Tuhan Yang Maha Esa yang telah memberikan kemudahan penulis dalam menyelesaikan penelitian ini. Ucapan terima kasih yang tak terhingga buat Orang Tua dan seluruh pihak yang telah membantu dalam menyelesaikan penelitian ini. Penelitian ini tidak lepas dari kekurangan mohon kritikan dan saran untuk kesempurnaan dalam penelitian ini.

REFERENCES

[1] R. Rodianto, I. Idham, Y. Yuliadi, M. T. A. Zaen, and W. Ramadhan, “Penerapan Network Development Life Cycle (NDLC) Dalam Pengembangan Jaringan Komputer Pada Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD) Provinsi NTB,” *J. Ilm. FIFO*, vol. 14, no. 1, p. 35, 2022, doi: 10.22441/fifo.2022.v14i1.004.

[2] J. R. Situmorang, “Pemanfaatan Internet Sebagai New Media Dalam Bidang Politik, Bisnis, Pendidikan dan Sosial Budaya,” *J. Adm. Bisnis*, vol. 8, no. 1, pp. 77–91, 2012, doi: 10.26593/jab.v8i1.418.

[3] M. Reni Sehaffudin, N. Indrihastuti, and E. Gunawan, “Pengisi Air Minum Otomatis Dengan Gelas Khusus Berbasis Arduino Uno,” *Cahaya Bagaskara J. Ilm. Tek. Elektron.*, vol. 2, no. 1, pp. 17–23, 2017, [Online]. Available: https://journal.trunojoyo.ac.id/jim/article/download/3958/2883

Journal of Information System Research (JOSH)
Volume 4, No. 1, Oktober 2022, pp 202−209
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v4i1.2335

[4] M. H. Ali, "Cyber Crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Perspektif Hukum Pidana Islam)," UIN ALAUDDIN MAKASSAR, 2012. [Online]. Available: http://repositori.uin-alauddin.ac.id/5756/1/Tesis_Moh. Haidar Ali_opt.pdf

[5] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[6] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, p. 853, 2020, doi: 10.25126/jtiik.2020701928.

[7] I. SMANDA, "Website SMANDA Laman Resmi SMA Negeri 2 Sumbawa Besar," 2018. https://sman2sumbawabesar.sch.id/ (accessed Jan. 23, 2018).

[8] B. Wicaksono, Y. R. Kusumaningsih, and C. Iswahyudi, "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing Dan Dast (Dynamic Application Security Testing)," *Jarkom*, vol. 8, no. 1, pp. 1–9, 2020, [Online]. Available: http://bagusw.win.

[9] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[10] F. Yudha, A. Muhammad, and P. Muryadi, "Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web," vol. 1, no. 1, pp. 1–6, 2018, [Online]. Available: https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/1101/1153

[11] Y. Yunanri.W, Doddy Teguh Yuwono, Rodianto and 134Program, "Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box," *J. Dea Mas*, vol. 4, no. 1, pp. 68–77, 2021, [Online]. Available: www.uts.ac.id

[12] Y. C. Ika Yusnita Sari, Muttaqin, Jamaludin, Janner Simarmata, M. Arif Rahman, AKbar Iskandar, ANdrew Fernando Pakpahan, Abdul Karim, Sugianto, *Keamanan Data dan Informasi*, Cetakan 1. Yayasan Kita Menulis. [Online]. Available: https://www.google.co.id/books/edition/Keamanan_Data_dan_Informasi/WFoMEAAAQBAJ?hl=en&gbpv=1&dq=keamanan+data+dan+informasi&pg=PA96&printsec=frontcover

[13] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (SQL) Injection Untuk Keamanan Website," *J. Teknol. Inf.*, vol. VII, no. 1, pp. 111–124, 2013, [Online]. Available: https://jti.respati.ac.id/index.php/jurnaljti/article/download/53/46

[14] D. K. Abdul Kholiq, "Analisis Keamanan Wireless Local Area Network (WLAN) Dengan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus : PT. Win Prima Logistik)," *46 J. Ilm. Fak. Tek. LIMIT'S Vol.15*, vol. 15, no. 1, pp. 46–55, 2019, [Online]. Available: https://teknik.usni.ac.id/jurnal/ABDUL KHOLIQ.pdf

[15] B. V. Tarigan, A. Kusyanti, and W. Yahya, "Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 3, pp. 206–214, 2017, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/73/37

[16] F. Y. Fauzan, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak," *J. Vocat. Tek. Elektron. dan Inform.*, vol. 9, no. 2, 2021, [Online]. Available: http://ejournal.unp.ac.id/index.php/voteknika/article/download/111778/105248