

Pengujian Keamanan Website XYZ Menggunakan Metode Vulnerability Assessment & Penetration Testing

Security Testing of the XYZ Website Using Vulnerability Assessment and Penetration Testing Methods

Ian Vemas Silalahi¹, Kasmawi²

^{1,2}Politeknik Negeri Bengkalis, Jl. Bathin Alam, Sungai Alam, Bengkalis, +62822 3572 0044

E-mail : iansilalahi28@gmail.com¹, kasmawi@polbeng.ac.id²

Received 16 July 2025; Revised 6 August 2025; Accepted 8 August 2025

Abstrak - Keamanan website khususnya pada bidang *e-commerce* menjadi aspek yang perlu diperhatikan dalam menerapkan *Cloudflare* dan *Strict-Transport-Security Header* untuk menjaga ketersediaan data guna meningkatkan kepercayaan *customer* ataupun *supplier*. Penelitian ini bertujuan untuk menguji keamanan website XYZ dengan menggunakan metode *Vulnerability Assessment Penetration Testing* (VAPT). Penerapan metode VAPT memiliki 4 tahapan yang dimulai dari *information gathering*, *vulnerability scanning*, *penetration testing*, dan *report and result*. Metode pengujian yang digunakan dengan teknik *Disributed Denial of Service* (DDoS), *Clickjacking* dan *Cross Site Request Forgery* (CSRF). Hasil penelitian menunjukkan bahwa website tidak aman dari serangan DDoS yang ditemukan pada port 80 berdasarkan hasil *scanning port* yang terbuka menggunakan *nmap*, dan dengan teknik CSRF pada elemen *login* yang tidak menggunakan anti-token CSRF. Untuk menghindari serangan DDoS dan CSRF maka pencegahannya adalah menggunakan *Cloudflare*, *framework Laravel*, konfigurasi *X-Frame-Option-Header*, menerapkan *Content Security Policy* (CSP) dan *HTTP Strict-Transport-Security* (HSTS).

Kata kunci - Keamanan Website, VAPT, DDoS Attack, Clickjacking, CSRF Attack

Abstract - Website security, especially in the e-commerce sector, is an aspect that needs to be considered in implementing Cloudflare and Strict-Transport-Security Header to maintain data availability to increase customer or supplier trust. This study aims to test the security of the XYZ website using the Vulnerability Assessment Penetration Testing (VAPT) method. The implementation of the VAPT method has 4 stages starting from information gathering, vulnerability scanning, penetration testing, and report and result. The testing method used is the Disributed Denial of Service (DDoS), Clickjacking and Cross Site Request Forgery (CSRF) techniques. The results of the study showed that the website was not safe from DDoS attacks found on port 80 based on the results of scanning open ports using nmap, and with the CSRF technique on login elements that did not use CSRF anti-tokens. To avoid DDoS and CSRF attacks, the prevention is to use Cloudflare, the Laravel framework, the X-Frame-Option-Header configuration, implementing Content Security Policy (CSP) and HTTP Strict-Transport-Security (HSTS).

Keywords - Website security, VAPT, DDoS Attack, Clickjacking, CSRF Attack.

1. PENDAHULUAN

Web adalah jenis layanan informasi yang sering diakses oleh pengguna yang terhubung ke jaringan *internet*. Suatu website harus dapat menangani permintaan pengguna dengan baik, jadi tidak jarang terjadi kesalahan keamanan saat dibangun yang dapat dimanfaatkan oleh pencuri untuk merusak sistem. Untuk menjamin kerahasiaan, integritas, dan ketersediaan data, lembaga harus memiliki keamanan teknologi informasi. [1]

Keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat (*right form*). [2]

Vulnerability Scanning adalah proses mengumpulkan informasi tentang kelemahan jaringan dengan menggunakan berbagai alat pemindaian dan pemindaian kelemahan jaringan, seperti *bug* aplikasi *server* dan *port* yang terbuka, [3] *Penetration Testing* adalah pemeriksaan keamanan sistem jaringan komputer. Evaluasi tersebut akan menentukan kelemahan sistem keamanan jaringan yang dapat dimanfaatkan oleh pencuri[4]. Pengujian sistem keamanan aplikasi berbasis *website* sangatlah penting. Ini karena pertumbuhan pesat aplikasi berbasis *web* diluncurkan dengan peningkatan serangan keamanan dari berbagai teknik ancaman. Keamanan seringkali hanya terlihat di urutan kedua atau bahkan terakhir dalam daftar hal-hal penting. Oleh karena itu, evaluasi aplikasi berbasis *web* harus dilakukan oleh organisasi agar organisasi dapat menemukan *bug* dan memahami risiko yang dihadapi [5].

Vulnerability Assessment and Penetration Testing (VAPT) terbukti berguna untuk memastikan keamanan *Cyber* perusahaan. Ini adalah cara terbaik untuk mematuhi peraturan keamanan yang berlaku untuk mengatasi ancaman *Cyber*. Ini sudah menjadi bagian integral dari teknik pengamanan kualitas untuk keamanan sistem yang digunakan oleh Perusahaan. *Assessment Vulnerability* bertujuan untuk mengidentifikasi potensi ancaman dan *subset* yang dapat digunakan *hacker* untuk mengeksloitasi kesalahan logis dalam sistem untuk mendapatkan keuntungan dengan mengarahkan sistem ke kondisi yang tidak aman [6]. Keamanan sistem berbasis *web* sangat penting saat membangun sebuah *website*. Bahkan sudah dipersiapkan dari awal pengembangan untuk mengurangi kemungkinan serangan yang disebabkan oleh banyaknya celah dan kerentanan yang tidak diperhitungkan selama proses pengembangan, yang memungkinkan orang yang tidak bertanggung jawab untuk mengeksloitasi *web* yang dibangun [7]. Analisis Metode *Open Web Application Security Project* (OWASP) Menggunakan *Penetration Testing* pada Keamanan *Website E-commerce* yang menghasilkan beberapa data yang telah disajikan berupa informasi tingkat kerentanan, resiko, dan tindakan perbaikan pada *url* yang tingkat kerentanan nya tinggi. [8]

Sistem informasi berbasis *web* ini menawarkan banyak keuntungan dan kemudahan bagi penggunanya. Namun, tidak dapat dihindari bahwa sebuah situs *web* dapat terintimidasi oleh serangan keamanan yang dapat menyebabkan kerugian. *Clickjacking*, *SQL Injection*, XEE, XSS, dan *Brute Force* adalah beberapa ancaman yang mungkin terjadi. Dengan hal itu, sistem keamanan *website* harus diuji. Metode pengujian penetrasi adalah salah satu pengujinya. Simulasi serangan yang terkendali disebut uji penetrasi untuk mengidentifikasi kerentanan pada aplikasi, jaringan, dan cabang sistem informasi. Hal ini dilakukan untuk memastikan bahwa jika ada celah keamanan, hal itu dapat segera ditemukan dan ditangani sebelum orang yang tidak bertanggung jawab memanfaatkannya [9].

Dengan berkembangnya teknologi informasi dan *internet*, banyak aspek kehidupan telah berubah, termasuk dunia bisnis. Munculnya *e-commerce*, juga dikenal sebagai perdagangan elektronik, adalah salah satu perubahan yang paling menonjol. *e-commerce* memungkinkan orang untuk membeli barang secara *online*, menghilangkan batasan geografis dan waktu, dan membuat belanja lebih mudah. Sebagai salah satu *platform e-commerce*, XYZ berkomitmen untuk memberikan pengalaman berbelanja *online* yang aman dan nyaman bagi penggunanya. Pelanggan penting *customer* memiliki data sensitif seperti data pribadi, detail kontak, saldo dan rincian data transaksi. Dan celah keamanan yang belum diidentifikasi, menjadi masalah utama dan sebagai alasan untuk dilakukannya uji penetrasi pada *website*. Keamanan data ini sangat penting untuk menjaga integritas dan kepercayaan dalam hubungan penjual dan pembeli.

Penelitian yang telah dilakukan oleh Rui Ventura, dkk pada tahun 2023 dengan judul “A Novel VAPT Algorithm: *Enhancing Web Application Security Trough OWASP TOP 10 Optimization*” membahas tentang audit keamanan siber dan menyelidiki pengoptimalan algoritma OWASP TOP 10 untuk keamanan *Web Application* (WA) menggunakan proses VAPT. Namun kelemahan penelitian ini hanya berfokus pada satu alat tools VA saja yang sesuai dengan objek judulnya yaitu OWASP. Dan dari penelitian ini, tujuannya adalah memperoleh pengetahuan tentang audit keamanan siber WA dengan menggunakan proses VAPT berbasis algoritma OWASP TOP 10. Penelitian ini menemukan hasil bahwa algoritma OWASP menunjukkan tingkat presisi yang mengesankan, mencapai tingkat presisi yaitu 90% pada WA. [10]

Kemudian penelitian selanjutnya yang dilakukan oleh Ahmad Almaarif, dan Muharman Lubis pada tahun 2020 dengan judul “VAPT Framework: Case Study of Government’s Website” yang membahas tentang identifikasi kerentanan yang telah dilakukan yang merujuk pada konsesi bisnis dan mencegah risiko yang berdampak *negative* pada Perusahaan. Namun, objek yang berfokus penelitian ini hanya berdasarkan hasil pemindaian kerentanan dan merujuk pada teknik SQL *Injection* dan XSS yang sesuai dari hasil *scanning* untuk menemukan celah dari kerentanan tersebut. Adapun tujuan yang dilampirkan dari penelitian ini adalah mengungkap ancaman yang kemungkinan berdampak potensial yang akan dilaporkan sistem melalui kerangka kerja yang tepat dan pengukuran sistematis. Dan hasil yang diperoleh dari penelitian ini berupa kerentanan pada bagian *directory listing*, *full path revealed*, *PHP info disclosure*, *folder webserver revealed*, dan potensi ancaman lainnya, yang dimana terdapat 2 risiko kritis, 6 risiko sedang, 2 risiko rendah. [11]

Berikutnya ada penelitian yang telah dilakukan oleh Afif Saktiansyah dan Muhammad Muharrom pada tahun 2023 dengan judul “Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVAS” yang mendiskusikan tentang pemindaian jaringan PT. Dutakom Wibawa dan melakukan identifikasi kerentanan yang ada, kemudian mereka melakukan evaluasi terhadap kerentanan yang telah teridentifikasi, termasuk penilaian risiko dan rekomendasi mitigasi yang diperlukan. Namun kelemahan dari penelitian ini dimana objek VA yang difokuskan pada penelitian ini hanyalah pada *OpenVAS*, tidak merujuk pada *tools* VA lainnya. Tujuan dari penelitian ini adalah mengidentifikasi kerentanan keamanan dalam jaringan yang dimiliki oleh PT. Dutakom Wibawa Putra dengan menggunakan *OpenVAS*, dan mereka memperoleh hasil penemuan dari penelitian yaitu ancaman 1 risiko *high*, 3 risiko *medium*, 4 risiko *low*. [12]

Setelah itu, penelitian oleh Sari Prabandari pada tahun 2024 dengan judul “Vulnerability Scanning Website PMB Menggunakan Open Web Application Security Project (Owasp)” dengan pembahasan pemindaian kerentanan dan celah kerentanan yang ada pada website PMB dengan menggunakan metode VA. Namun, Pemindaian kerentanan yang dilakukan pada penelitian ini hanya berfokus pada metode OWASP saja dan juga alat *tools* VA yang digunakan hanya OWASP untuk mendukung metode yang digunakan pada penelitian. Tujuan dari penelitian ini adalah melakukan VA pada website penerimaan mahasiswa baru, dengan mengikuti konsep OWASP. Dan hasil yang ditemukan dari penelitian ini ialah 33,3% kerentanan tingkat risiko sedang (enam tanda), 38% kerentanan tingkat risiko rendah (tujuh tanda), 27,7% tingkat risiko informasional (5 tanda) dan tidak ada kerentanan tingkat tinggi. [13]

Penelitian yang selanjutnya dilakukan oleh Candra Darmawan, dkk pada tahun 2021 dengan judul “Penerapan Metode VA Untuk Identifikasi Keamanan *Website* berdasarkan OWASP ID” yang mendiskusikan tentang identifikasi keamanan yang ada website Universitas Papua dengan menggunakan OWASP. Metode penelitian ini menggunakan metode terbaru yaitu OWASP ID pada tahun 2021 untuk mendukung uji penetrasi yang sesuai dengan OWASP ID tahun 2021. Namun, penelitian ini hanya berfokus pada tools VA yaitu OWASP saja dengan tujuan membuktikan kerentanan pada klausula metode OWASP ID tahun 2021 itu saja. Dengan tujuan mengetahui celah keamanan *website* UNIPA berdasarkan OWASP ID tahun 2021 dan menerapkan mitigasi, dan dimana mereka menemukan hasil kerentanan *website* UNIPA

dipengaruhi dua faktor, kelemahan keamanan *website* dan kelalaian pengguna. Kerentanan dengan *alerts* ID A1, A2, A3, A4 A5, dan A6 merupakan kelompok kelemahan keamanan *website*. Solusinya yang mereka simpulkan yaitu memanfaatkan sistem khusus seperti anti-CSRF, CSP, CDN, *Strict-Transport-Security Header*, dan pengecekan timestamp agar website proporsional. Sedangkan kerentanan dengan alerts ID A7 adalah klasifikasi kelalaian pengguna. Solusinya, pengguna wajib menggunakan browser versi terbaru. Browser dengan versi terbaru memiliki mekanisme keamanan *X-Content-Type-Options*: nosniff untuk mencegah serangan sniffing. [14]

Sebagai penutup, penelitian yang terakhir dilakukan oleh Imam Riadi, dkk pada tahun 2020 dengan judul “Analisis Kerentanan Serangan *Cross Site Scripting (XSS)* pada aplikasi *Smart Payment* Menggunakan *Framework OWASP*”, dimana mereka membahas kerentanan yang ada pada *website e-commerce* dengan menggunakan teknik XSS metode *framework OWASP*. Namun, penelitiain ini berfokus hanya pada analisis XSS dan menggunakan *tools VA* yaitu OWASP, tidak ada tambahan teknik serangan ataupun *tools VA* agar mewujudkan tujuan penelitian ini yaitu untuk mengamankan aplikasi yang dijadikan sebagai rekomendasi tindak lanjut dalam pengamanan *Smart Payment*. Dari hasil penelitian mereka ditemukan hasil kerentanan *Information Disclosure-Suspicious Comments*, *X-Frame-Options Header Not Set*, *X-Content-Type-Options Header Missing*, *Timestamp Disclosure-Unix*, *Web Browser XSS Protection Not Enabled*, dan *Directory Browsing*. [15]

2. METODE PENELITIAN

VAPT (*Vulnerability Assessment and Penetration Testing*) adalah metode keamanan siber yang menggabungkan dua pendekatan utama. Tujuan daripada itu adalah untuk menemukan, menganalisis, dan mengatasi kerentanan dalam sistem, jaringan, dan aplikasi. Sehingga organisasi, lembaga, atau pihak manapun dapat memperkuat pertahanan mereka terhadap serangan dalam dunia nyata. VAPT membantu studi kasus kali ini dalam mengidentifikasi dan mengatasi kelemahan keamanan, serta memperkuat postur keamanan mereka secara keseluruhan.

Sebagai website yang terkemuka, dengan total ada 183 toko yang menjadi pilihan, 9 investor, 16 produk dan 218 subproduk serta 4 penyedia layanan jasa transportasi yang banyak digunakan oleh para *customer* untuk bermiaga secara online, *website* tersebut harus memberikan jaminan atas keamanan data privasi para *customer* agar mereka merasa aman dan nyaman terhadap data privasi mereka yang sudah mereka berikan setelah mendaftar sebagai pelanggan atau *customer*.

Melalui penjelasan tersebut, memperkuat alasan untuk menggunakan metode VAPT dengan tujuan untuk menemukan potensi celah keamanan dan menjaga keamanan data privasi para *customer* dengan mewujudkan kinerja OWASP ZAP dan Acunetix dalam melakukan *Vulnerability Scanning*. Penerapan metode VAPT ini pada *website XYZ* sangat berpengaruh pada kestabilan *website* untuk melindungi privasi yang dimiliki customer. Oleh karena itu, diharapkan bahwa penelitian ini membantu meningkatkan kesadaran tentang keamanan informasi di *e-commerce* dan *Penetration Testing* merupakan proses yang aktif untuk mengevaluasi kekuatan dan kelemahan *website* melalui serangkaian tes yang mencoba menembus lapisan keamanan yang ada. Dalam metode VAPT, ada lima langkah atau tahap yang digunakan meliputi tahap perencanaan, tahap pengumpulan informasi, tahap pemindaian kerentanan, tahap uji penetrasi, dan terakhir ada tahap laporan. Adapun tahap-tahap dalam menggunakan metode Vulnerability Assessment dan Penetration Testing (VAPT) berikut dijelaskan:

1. Perencanaan (*Planning*)

Tahap pertama dalam melakukan penilaian VAPT adalah menentukan ruang lingkup penilaian dan sejauh mana eksplorasi yang akan diselidiki, Dalam eksplorasi penelitian ini melibatkan sebuah website *e-commerce* sebagai objek eksplorasi yang akan dilakukan. Pada langkah ini dilakukan identifikasi bahwa objek yang akan diteliti adalah *website e-commerce*.

Aspek yang diteliti dalam lingkup penelitian ini dari login (perangkat user) dan server website. Untuk mengidentifikasi masalah pada atau penerapannya, maka ditetapkan tujuan serta sasaran.

2. Pengumpulan Informasi (*Information Gathering*)

Tahap kedua adalah langkah perencanaan untuk mengidentifikasi kerentanan. Pada langkah ini dilakukan teknik pengumpulan informasi untuk mendapatkan informasi penting terkait website yang diteliti. Informasi penting yang dimaksud meliputi , seperti alamat IP, nama *domain*, *port* terbuka, *Domain Name System* atau protokol jaringan yang digunakan. Dengan informasi ini, dapat dengan mudah mengidentifikasi potensi kerentanan serta merencanakan pendekatan pengujian melalui *tools whois*, *virusTotal*, *nmap*, dan *DNS Checker*.

3. Pemindaian Kerentanan (*Vulnerability Scanning*)

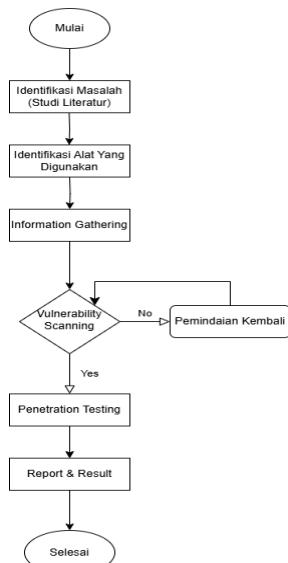
Tahap ketiga adalah *vulnerability scanning* adalah tahap proses melakukan identifikasi dan evaluasi dari kerentanan keamanan dalam *website*. Pada penelitian kali ini, tahap pemindaian kerentanan dilakukan dengan tools VA berupa *tools Owasp Zap* dan *Acunetix* menjadi pilihan utama untuk melakukan pemindaian terhadap objek penelitian. Pemindaian dilakukan sesuai dengan ruang lingkup penelitian yang mungkin dapat dieksplorasi oleh *attacker*. Tahapan ini akan menghasilkan berupa daftar celah kerentanan beserta informasi rinci tingkat kerentanan dan dampak yang diakibatkan. Pemindaian dilakukan secara komprehensif untuk komponen *login* dan *server website*.

4. Uji Penetrasi (*Penetration Testing*)

Tahap keempat adalah pengujian penetrasi. Di sini, peneliti penetrasi mensimulasikan serangan cyber berupa *Clickjacking*, *CSRF*, dan *DDoS* untuk menemukan ikhtisar kelemahan dari penyisiran yang sebelumnya sudah melakukan pemindaian kerentana. Pada langkah ini berupaya mengeksplorasi kerentanan dalam ruang lingkup terkendali untuk menilai ketahanan sistem terhadap serangan. Hal ini dilakukan untuk membuktikan celah kerentanan yang ditemukan pada pemindaian kerentanan dengan teknik *Clickjacking*, *CSRF*, dan *DDoS* yang sesuai dengan scope yang ditujuan. Satu-satunya tujuan pengujian penetrasi adalah untuk membantu mengidentifikasi celah keamanan yang perlu diatasi.

5. Pelaporan (*Report*)

Tahap kelima ialah tahap pelaporan untuk menyusun laporan secara rinci dari penelitian, termasuk kerentanan yang teridentifikasi, potensi risiko, dan rekomendasi tindakan yang dapat diambil untuk memperkuat *website*. Laporan ini membantu *owner website* memahami status keamanan mereka, memprioritaskan langkah-langkah keamanan, dan pada akhirnya, meningkatkan keamanan sistem mereka secara keseluruhan.



Gambar 1 Desain Metode VAPT

3. HASIL DAN PEMBAHASAN

Dalam analisis ini, setelah melakukan pengumpulan informasi dan pengujian pada website XYZ yang memiliki standar keamanan umum dengan menerapkan *firewall* berupa *IP Blacklist* maka dilakukan identifikasi celah keamanan berdasarkan sesuai penerapan metode VAPT, dapat diberikan suatu kesimpulan bahwasanya metode VAPT ini sangat direkomendasikan untuk menguji celah keamanan *website*. Pada proses scanning hasil temuan kerentanan dari *Acunetix* dan *OWASP ZAP* disertakan masing-masing tingkat kerentanan. Sedangkan pada proses pengujian, hasil temuan celah keamanan dari serangan *DDoS Attack* dan *CSRF Attack* pada *web server* dan elemen *login*.

3.1 Hasil Pengumpulan Informasi

Whois Record for [REDACTED]	
— Domain Profile	
Registrar	WEBCC Web Commerce Communications Limited dba WebNic.cc IANA ID: 460 URL: http://www.webnic.cc Whois Server: whois.webnic.cc compliance_abuse@webnic.cc (p) +60.389966799
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	1,425 days old Created on 2020-12-18 Expires on 2024-12-19 Updated on 2021-10-09
Name Servers	NS1.HOSTER.CO.ID (has 5,319 domains) NS2.HOSTER.CO.ID (has 5,319 domains) NS3.HOSTER.CO.ID (has 5,319 domains) NS4.HOSTER.CO.ID (has 5,319 domains)
IP Address	103.16.198.18 - 851 other sites hosted on this server
IP Location	Indonesia - Jakarta Raya - Jakarta Selatan - Jalanet - Connecting U
ASN	AS131775 IDNIC-JALANET-AS-ID PT. Jupiter Jala Arta, ID (registered Jul 25, 2011)
Domain Status	Registered And No Website
IP History	8 changes on 8 unique IP addresses over 3 years
Hosting History	1 change on 2 unique name servers over 4 years

Gambar 2 Whois

The screenshot shows the VirusTotal analysis interface. It includes sections for History, HTTP Response, Final URL, and Serving IP Address. The History section displays submission and analysis dates. The HTTP Response section shows the final URL as a redacted black box. The Serving IP Address section shows the IP address 103.16.198.18.

Gambar 3 virusTotal

```
(root㉿kali)-[~/home/kali]
└─# nmap 103.16.198.14
Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-04 05:36 EST
Nmap scan report for bonecrusherserver.hosterserver.com (103.16.198.14)
Host is up (0.034s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 7.32 seconds
```

Gambar 4 Nmap

Type	Domain Name	TTL	Canonical Name
NS	[REDACTED]	21600	ns1.hoster.co.id. (89.116.156.92) Check IP Blacklist Owner: SC Lithuanian Radio and TV Center  WHOIS
NS	[REDACTED]	21600	ns3.hoster.co.id. (89.116.44.81) Check IP Blacklist Owner: Ethernet Servers  WHOIS
NS	[REDACTED]	21600	ns4.hoster.co.id. (103.131.51.196) Check IP Blacklist Owner: PT Ardetamedia Global Komputindo  WHOIS
NS	[REDACTED]	21600	ns2.hoster.co.id. (103.131.51.220) Check IP Blacklist Owner: PT Ardetamedia Global Komputindo  WHOIS

Gambar 5 DNSChecker

3.2 Hasil Pemindaian Kerentanan

Table 1 Hasil Scanning Acunetix

Vulnerability	Severity	Confidence
<i>Slow HTTP Denial of Service Attack</i>	Medium	80
<i>Clickjacking X-Frame-Options header missing</i>	Low	95
<i>Cookie(s) without HttpOnly flagset</i>	Low	100
<i>Cookie(s) without Secure flagset</i>	Low	100
<i>Possible virtual host found</i>	Low	95
<i>Unencrypted Connection</i>	Low	100
<i>Content Security Policy (CSP) Not Implemented</i>	Low	95

Table 2 Hasil Scanning OWASP

Jenis Kerentanan	Risk Level
<i>Absence of Anti-CSRF Tokens</i>	Medium
<i>Content Security Policy (CSP) Header Not Set</i>	Medium
<i>Missing Anti-clickjacking Header</i>	Medium
<i>Vulnerable JS Library</i>	Medium
<i>Big Redirect Detected (Potential Sensitive Information Leak)</i>	Low

<i>Cookie No HttpOnly Flag</i>	<i>Low</i>
<i>Cookie without SameSite Attribute</i>	<i>Low</i>
<i>Cross-Domain JavaScript Source File Inclusion</i>	<i>Low</i>
<i>Strict-Transport-Security Header Not Set</i>	<i>Low</i>
<i>X-Content-Type-Options Header Missing</i>	<i>Low</i>

Hasil dari tahapan penetration testing yang telah dilakukan pengujinya pada target. Dari daftar kerentanan pada kedua aplikasi atau *tools* kerentanan *Vulnerability Assessment*. Berikut dibuktikan hasil pengujinya Ditemukan (Ya) dan Tidak ditemukan (Tidak).

Table 3. Analisa temuan celah kerentanan

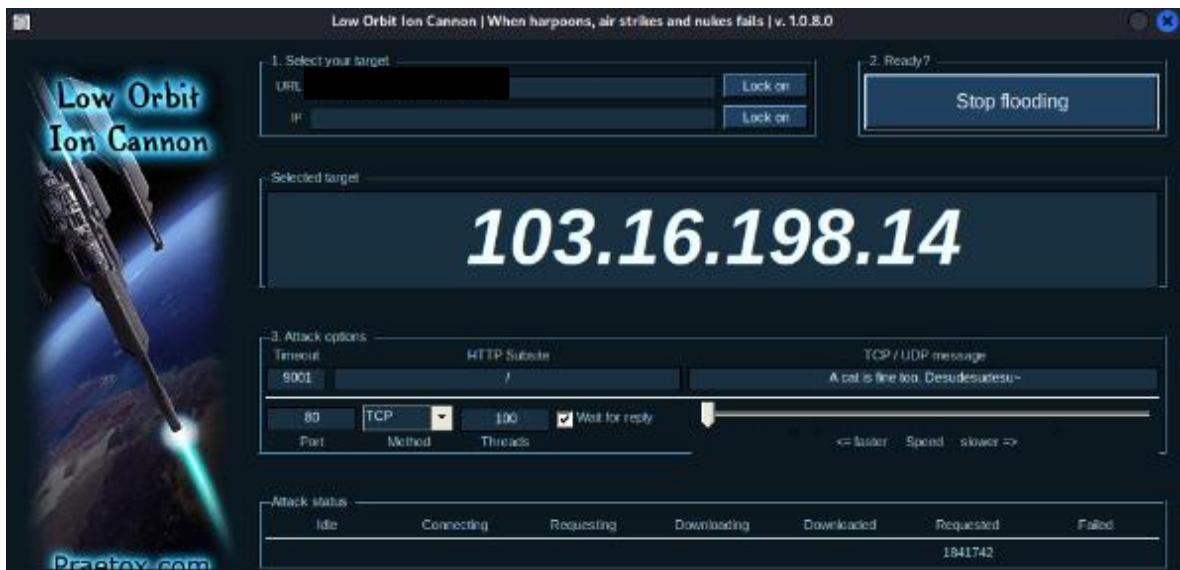
Nama Kerentanan	Tingkat Kerentanan	Ditemukan	Tidak ditemukan
<i>Slow HTTP Denial of Service Attack</i>	<i>Medium</i>	Ya	
<i>Absence of Anti-CSRF Tokens</i>	<i>Medium</i>	Ya	
<i>Content Security Policy (CSP) Header Not Set</i>	<i>Medium</i>	Ya	
<i>Missing Anti-clickjacking Header</i>	<i>Medium</i>		Tidak
<i>Vulnerable JS Library</i>	<i>Medium</i>		Tidak
<i>Clickjacking: X-Frame-Options Header Missing</i>	<i>Low</i>		Tidak
<i>Cookies without HttpOnly flagset</i>	<i>Low</i>		Tidak
<i>Cookies without Secure flagset</i>	<i>Low</i>		Tidak
<i>Possible virtual host found</i>	<i>Low</i>		Tidak
<i>Unencrypted Connection</i>	<i>Low</i>		Tidak
<i>Content Security Policy (CSP) Not Implemented</i>	<i>Low</i>	Ya	
<i>Big Redirect Detected (Potential Sensitive Information Leak)</i>	<i>Low</i>		Tidak
<i>Cookie No HttpOnly Flag</i>	<i>Low</i>		Tidak

<i>Cookie without SameSite Attribute</i>	<i>Low</i>		Tidak
<i>Cross-Domain JavaScript Source File Inclusion</i>	<i>Low</i>		Tidak
<i>Strict-Transport-Security Header Not Set</i>	<i>Low</i>	Ya	
<i>X-Content-Type-Options Header Missing</i>	<i>Low</i>	Ya	
Total Kerentanan	17	6	11

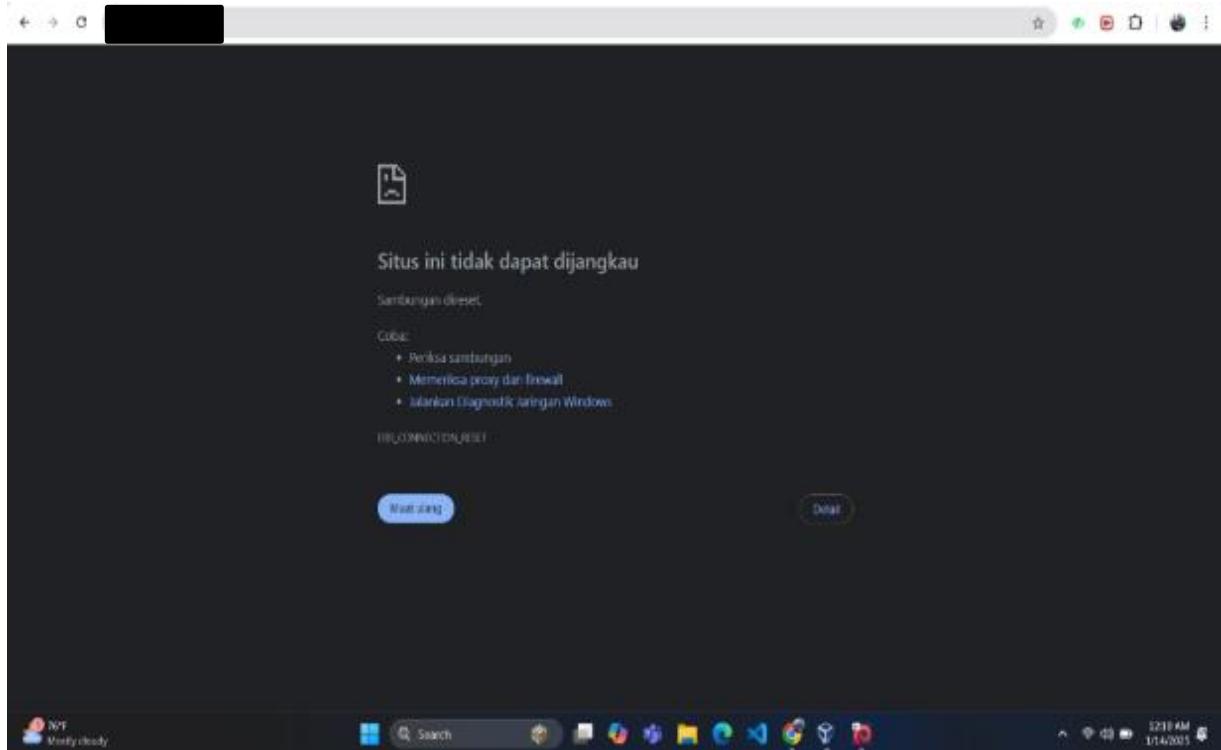
3.3 Hasil Penetration Testing

Berdasarkan kerentanan yang berhasil, uji penetrasi yang telah dilakukan dengan melalukan pengujian serangan DDoS *Attack*, *Clickjacking Attack*, dan *CSRF Attack*, bahwasanya, pengujian DDoS *Attack* dan *CSRF Attack* berhasil menemukan titik celah keamanan. Hasil dari dua pengujian dapat dilihat sebagai berikut.

1. DDoS Attack



Gambar 6 Pengujian pada port 80



Gambar 7 Serangan DDoS port 80

Setelah melakukan pengujian DDoS *Attack* pada port 80 menggunakan *tool* LOIC, terbukti adanya bahwa kerentanan *Slow HTTP Denial of Service Attack* berhasil ditembus celahnya. Seperti gambar di atas dijelaskan “Situs ini tidak dapat dijangkau”.

Pengujian DDoS juga dilakukan dengan slowhttptest untuk memperkuat bukti bahwa port 80 pada website tersebut masih rentan.

Untuk melakukan serangan DDoS menggunakan slowhttptest, perintah yang digunakan ialah “slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://103.16.198.14/home.php -x 24 -p 3” pada terminal kali linux,

```
root@kali:/home/kali# slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 200 -t GET  
-u http://103.16.198.14/index.php -x 24 -p 3
```

Gambar 8 Perintah slowhttptest ke ip address website

```
test type:          SLOW_HEADERS
number of connections: 1000
URL:               http://103.16.198.14/home.php
verb:              GET
cookie:
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration:      240 seconds
using proxy:        no proxy

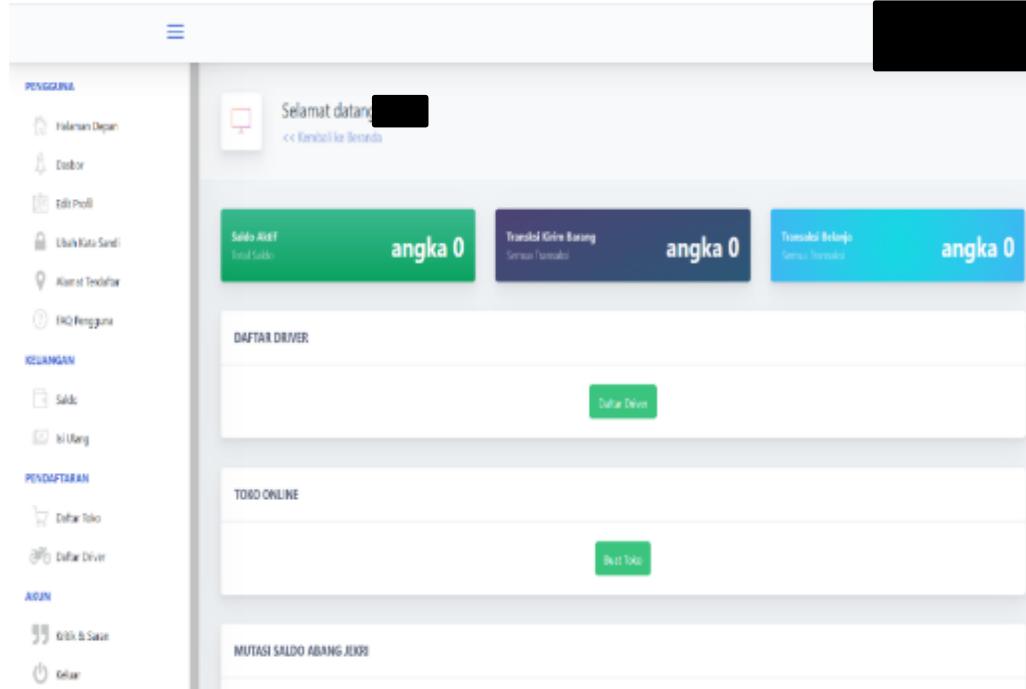
Thu Dec 5 01:20:42 2024:
slow HTTP test status on 70th second:

initializing:      0
pending:           0
connected:         1000
error:             0
closed:            0
service available: YES
```

Gambar 9 Hasil slowhttptest

Berdasarkan serangan DDoS menggunakan slowhttptest, keterangan ‘YES’ pada service available menandakan bahwa slowhttptest juga dapat menembus celah kerentanan pada DDoS pada port 80 yaitu https.

2. CSRF Attack



Gambar 10 Berhasil masuk dari request PoC



Gambar 11 Eksploitasi Password

Setelah dilakukan analisa berdasarkan pengujian yang telah dilakukan, bahwa melalui CSRF PoC yang diperoleh melalui *tools burpsuite* dan *CSRFShark*, telah berhasil mendapatkan hak akses *user* dengan mengirimkan informasi intercept dan menyimpan informasi dalam bentuk sebuah *file* dan dieksekusi dalam bentuk *request CSRF PoC*. Dan dapat diambil kesimpulan bahwa target masih dalam bentuk *native php* dan tidak menggunakan *framework*, sehingga pengujian CSRF Attack berhasil dilakukan seperti pada *form login*. Dan website juga tidak menerapkan HSTS (HTTP Strict Transport Security) sehingga aktivitas *intercept* seperti *Burpsuite* dapat dilakukan untuk melakukan pengujian serangan cyber.

3.4 Laporan dan Hasil

Dari hasil yang ditemukan berdasarkan pemindaian kerentanan dan uji penetrasi berikan laporan saran perbaikan dari hasil pengujian yang telah dilakukan.

Table 4 Laporan Saran Perbaikan

Nama Kerentanan	Saran Perbaikan
<i>Absence of Anti-CSRF Tokens</i>	Disarankan menggunakan <i>framework Laravel</i> karena memiliki fitur anti-CSRF karena berguna untuk mengantisipasi transmisi dari luar situs web.
<i>Slow HTTP Denial of Service Attack</i>	Disarankan untuk menggunakan <i>cloudflare</i> sebagai mitigasi dari serangan DDoS
<i>Strict-Transport-Security Header Not Set</i>	Disarankan untuk menerapkan HTTP Strict-Transport-Security (HSTS) untuk menghindari aktivitas intercept.
<i>X-Content-Type-Options Header Missing</i>	Disarankan menggunakan <i>firewall X-Content-Type-Options</i> untuk mencegah tindakan <i>intercept</i> pada website.
<i>Content Security Policy (CSP) Header Not Set</i>	Disarankan menerapkan Content Security Policy untuk menghindari <i>input iframe</i> pada website.
<i>Content Security Policy (CSP) Implemented</i>	Disarankan menerapkan Content Security Policy untuk menghindari <i>input iframe</i> pada website.

4. KESIMPULAN

Penggunaan *tools scanning* berupa OWASP ZAP dan Acunetix sangat efektif dalam menemukan total jumlah 6 celah kerentanan diantaranya, *Absence of Anti-CSRF Tokens*, *Slow HTTP Denial of Service Attack*, *Content Security Policy (CSP) Header Not Set*, *Strict-Transport-Security Header Not Set*, *X-Content-Type-Options Header Missing*, *Content Security Policy (CSP) Not Implemented*. Berdasarkan kerentanan berupa Slow HTTP Denial of Service Attack dan Absence of CSRF Tokens, ditemukan celah keamanan website pada server port 80 dan elemen login. Dari celah kerentanan ditemukan port 80 yang terbuka menggunakan nmap dan melakukan pengujian DDoS pada port tersebut. Celah keamanan dari sisi elemen login berhasil dieksploitasi dengan CSRF PoC menggunakan tool Burpsuite dan CSRFShark dengan mendapatkan akses login melalui cookie user. Dari celah kerentanan Strict-Transport-Security Header Not Set yang telah ditemukan, penggunaan tool Burpsuite sangat efektif dalam melakukan uji coba serangan menggunakan proxy dengan IP localhost. Serangan yang dilakukan melalui penghubungan antara proxy dan intercept agar dapat memberikan informasi yang tersembunyi dari website. Dari informasi tersebut, menjadi kunci utama dari keberhasilan serangan yang telah dilakukan

DAFTAR PUSTAKA

- [1] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF.”
- [2] S. Hidayatulloh and D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP).” [Online]. Available: <http://jurnal.itg.ac.id/>
- [3] E. Irawadi Alwi and F. Umar, “Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning,” 2020.
- [4] H. Jurnal, R. Farismana, and D. Pramadhana, “VULNERABILITY ASSESSMENT UNTUK ANALISIS TINGKAT KEAMANAN PADA SISTEM INFORMASI REPOSITORI KARYA ILMIAH POLITEKNIK XYZ,” Online, 2023.
- [5] A. Putra Armadhani, D. Nofriansyah, K. Ibnutama, S. Informasi, and S. Triguna Dharma, “Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab testing Menggunakan Penetration Testing Standart OWASP,” *Jurnal Sains Manajemen Informatika dan Komputer*, vol. 21, no. 2, pp. 80–88, 2022, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jis>
- [6] R. Sahtyawan, “PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING),” 2019.
- [7] Riyandhanu, “Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi,” *Jurnal Informatika dan Teknologi*, Oct. 2022, doi: 10.37034/jidt.v4i3.236.
- [8] I. O. Riandhanu, “Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi,” *Jurnal Informatika dan Teknologi*, Oct. 2022, doi: 10.37034/jidt.v4i3.236.
- [9] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, “Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar,” 2023.
- [10] R. Ventura, D. J. Franco, and O. K. Akram, “A Novel Vapt Algorithm: Enhancing Web Application Security Trough OWASP Top 10 Optimization,” Academy and Industry Research Collaboration Center (AIRCC), Nov. 2023, pp. 13–27. doi: 10.5121/csit.2023.132002.

- [11] A. Almaarif and M. Lubis, “Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government’s Website,” *Int J Adv Sci Eng Inf Technol*, vol. 10, no. 5, pp. 1874–1880, 2020, doi: 10.18517/ijaseit.10.5.8862.
- [12] M. Muhamrom and A. Saktiansyah, “Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVas,” *International Journal of Engineering and Computer Science Applications (IJECSA)*, vol. 2, no. 2, pp. 51–58, Sep. 2023, doi: 10.30812/ijecsa.v2i2.3297.
- [13] S. Prabandari, “VULNERABILITY SCANNING WEBSITE PMB MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP),” *Jakarta Gedung Sentra Kramat Jalan Kramat Raya*.
- [14] C. Darmawan, J. P. P. Naibaho, and A. De Kweldju, “Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021,” *Edumatic: Jurnal Pendidikan Informatika*, vol. 8, no. 1, pp. 272–281, Jun. 2024, doi: 10.29408/edumatic.v8i1.25834.
- [15] I. Riadi, R. Umar, and T. Lestari, “Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP,” *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 5, no. 3, pp. 146–152, Nov. 2020, doi: 10.14421/jiska.2020.53-02.