Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 6, December 2024, pp. 1651-1662
DOI: https://doi.org/10.52436/1.jutif.2024.5.6.3859
p-ISSN: 2723-3863
e-ISSN: 2723-3871

WEBSITE VULNERABILITY TESTING USING THE PENETRATION TESTING METHOD REFERRING TO NIST SP 800 – 155 (CASE STUDY (Astonprinter.com Domain))

Ari Agustinus[*1], Irwan Sembiring[2]

[1,2]Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Indonesia
Email: [1]672018194@student.uksw.edu, [2]irwan.sembiring@uksw.edu

(Article received: October 02, 2024; Revision: November 27, 2024; published: December 29, 2024)

Abstract

Information security is a very important aspect in maintaining the confidentiality, integrity and availability of data on a system, especially on websites that are vulnerable to various cyber threats. This research aims to test website vulnerabilities using the penetration testing method by referring to the NIST SP 800-115 standard. The case study used in this research is the astonprinter.com website. The penetration testing method applied in this research follows the NIST SP 800-115 guidelines which include the Planning, Discovery, Attacking and Reporting stages. The results of the research show that the astonprinter.com website has 20 vulnerabilities that can be exploited, with details of 2 vulnerabilities which are in the high threat level, namely DNS Server Spoofed Request Amplification Ddos and Path Traversal, then it has 7 vulnerabilities which are in the medium threat level, including DNS Server Chace Snooping Remote Information Disclosure and Vulnerable Js Library and 11 vulnerabilities that are in the low threat level including ICMP Timestamp Request Remote Date Disclosure, SSH Server CBC Mode Ciphers Enabled, , Cookie No HttpOnly Flag and Cookie without SameSite Attribute. These findings can provide valuable insight for website managers in strengthening security systems and reducing the risk of cyber attacks in the future.

Keywords: *CIA TRIAD, NIST SP 800-115, Penetration Testing, Server Security.*

PENGUJIAN KERENTANAN WEBSITE MENGGUNAKAN METODE PENETRATION TESTING MERUJUK PADA NIST SP 800 – 155 (STUDI KASUS (Domain Astonprinter.com))

Abstrak

Keamanan informasi merupakan aspek yang sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data pada sebuah sistem, terutama pada website yang rentan terhadap berbagai ancaman siber. Penelitian ini bertujuan untuk menguji kerentanan website menggunakan metode penetration testing dengan merujuk pada standar NIST SP 800-115. Studi kasus yang digunakan dalam penelitian ini adalah website astonprinter.com. Metode penetration testing yang diterapkan dalam penelitian ini mengikuti panduan NIST SP 800-115 yang meliputi tahap Planning, Discovery, Attacking, dan Reporting. Hasil penelitian menunjukkan bahwa website astonprinter.com memiliki 20 kerentanan yang dapat dieksploitasi dengan rincian 2 kerentanan yang berada dalam threat level high yaitu DNS Server Spoofed Request Amplification Ddos dan Path Traversal, kemudian memiliki 7 kerentanan yang berada dalam threat level medium diantaranya DNS Server Chace Snooping Remote Information Disclosure dan Vulnerable Js Library dan 11 kerentanan yang berada dalam threat level low diantaranya ICMP Timestamp Request Remote Date Disclosure, SSH Server CBC Mode Ciphers Enabled, , Cookie No HttpOnly Flag dan Cookie without SameSite Attribute. Temuan ini dapat memberikan wawasan yang berharga bagi pengelola website dalam memperkuat sistem keamanan dan mengurangi risiko serangan siber di masa depan.

Kata kunci: *CIA TRIAD, Keamanan Server, NIST SP 800-115, Penetration Testing.*

1. PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi saat ini semakin lama semakin berkembang. Komunikasi yang dulunya

membutuhkan waktu lama untuk penyampaiannya, namun dengan kemunculan teknologi, kini komunikasi menjadi sangat cepat, dikutip dari artikel[1]. Seiring perkembangan Sistem Informasi sangat diperlukan keamanan untuk melindungi kita dari hal – hal yang tidak diinginkan, maka dari itu data dan informasi yang dimiliki perlu disimpan dengan baik sehingga tidak akan disalahgunakan[2]. Dikutip dalam Kompas Harian (2024) menuliskan bahwa peningkatan serangan siber yang semakin canggih dan beragam, perlindungan data tidak dapat lagi diabaikan. Menghadapi situasi ini, penetration testing muncul sebagai salah satu strategi krusial dalam mengidentifikasi kerentanan sistem[3].

Website Astonprinter.com, sebagai bagian dari infrastruktur digital perusahaan yang mengelola informasi sensitif pelanggan. Seiring meningkatnya adopsi teknologi seperti cloud computing, Internet of Things (IoT), dan kecerdasan buatan (AI) untuk mendukung efisiensi dan daya saing, risiko keamanan siber terhadap aplikasi web menjadi semakin signifikan. Seperti yang dibahas dalam jurnal "Cyber Security in the Age of Digital Transformation", ancaman terhadap aplikasi web dapat mengakibatkan kebocoran data, modifikasi informasi, atau penonaktifan layanan—masalah yang seringkali disebabkan oleh celah keamanan yang dieksploitasi oleh serangan siber yang semakin canggih. Oleh karena itu, implementasi strategi keamanan siber yang proaktif dan kepatuhan terhadap standar keamanan menjadi sangat krusial untuk melindungi aset digital dan kepercayaan pelanggan dalam ekosistem bisnis modern[4].

Penetration testing atau uji penetrasi adalah aktivitas di mana seseorang mencoba untuk melakukan serangan terhadap suatu jaringan organisasi/perusahaan untuk mengidentifikasi kelemahan dalam sistem tersebut. Pada penelitian ini, akan dilakukan *penetration testing* terhadap aplikasi yang berbasis web untuk menemukan celah keamanan[5].

Untuk mengatasi ancaman ini, *NIST SP 800-115* menyediakan panduan komprehensif dalam pelaksanaan *penetration testing*, yang tidak hanya bertujuan mengidentifikasi kelamahan teknis, tetapi juga memberikan pendekatan yang sistematis untuk mengevaluasi dan meningkatkan kontrol keamanan yang diterapkan dalam sistem. Penelitian ini bertujuan untuk menguji kerentanan pada website Astonprinter.com dengan menggunakan metode *penetration testing*, mengacu pada panduan dari *NIST SP 800-115*, guna mengidentifikasi potensi kelemahan dan memberikan rekomendasi mitigasi yang relevan[6].

1.2. Tinjuan Pustaka

Penelitian yang dilakukan oleh Esti Zakia Darojat et al., ini mengidentifikasi kerentanan pada dua situs *web e-Government*, semarang.go.id dan gunungtumpeng.id, menggunakan standar keamanan *NIST SP 800-115* dan *OWASP Top 10*, dengan alat pemindaian *Acunetix* dan *Pentest-Tools*. Hasil pemindaian menunjukkan kerentanan tingkat menengah dan rendah, seperti *Cross-site Scripting (XSS), Clickjacking, dan Security Missconfiguration* pada kedua situs. Selain itu, masalah kemanan seperti pengunaan koneksi yang tidak terenkripsi dan konfigurasi cookie yang tidak aman juga ditemukan. Rekomendasi untuk meningkatkan keamanan termasuk penerapan header keamanan seperti *HSTS* dan *Content Security Policy 9CSP)*, serta penggunaan *HTTPS* dan pengaturan *cookie* yang lebih aman[7].

Penelitian yang dilakukan oleh Yosua Ade Pohan melakukan dua tahapan yang dilakukan dalam penelitian terkait pencarian informasi *webserver* aplikasi yaitu *IP Whois* dan *Nmap*. Peran *IP whois* mencari tahu informasi mengenai *IP Publik webserver* yang digunakan, dan peran dari Nmap, melakukan pemindaian port pada sistem. Pada tahapan *Vulnerability Analysis* ini dilakukan untuk megidentifikasi potensi kelemahan dengan melakukan pemindaian aplikasi menggunakan *tool Acunetix* yang berfungsi untuk menguji keamanan situs web. Dari hasil Analisa terdapat 7 jenis kerentanan yang dapat dilakukan exploitasi terhadap *webserver* aplikasi. Dari 7 jenis kerentanan yang sudah dieksploitasi maka dilakukan tindakan perbaikan berdasarkan solusi yang tepat untuk mengatasi kerentanan. Salah satu contoh yang dilakukan peneliti dalam mengatasi kerentanan yaitu, jenis kerentanan: *X-Frame Header Options Is Missing*, solusinya mengatur opsi *Header ke SAMEOTIGIN* dan *DENY*, serta menambahkan *SSL* pada *webserver* aplikasi untuk meningkatkan keamanan pertukaran data dengan menggunakan *protocol HTTPS*. Hasil perbaikan peneliti menyimpulkan "Aplikasi memblock Serangan *Clickjacking*"[8].

Penelitian yang dilakukan oleh Vriano dalam penelitiannya melakukan tahapan dari *Ethical Hacking*, metode ini memiliki 5 tahapan dalam penerapannya, yaitu *Reconnaisance*, *scanning* & *enumeration*, *Gainning Access*, *Maintaining Access Covering Tracks*. Dari hasil pengujian kerentanan website dengan menggunakan metode *ethical hacking*, pengujian dilakukan sesuai dengan prinsip – prinsip etika dalam *ethical hacking*[9].

Penelitian Wardana menggunakan *NIST SP 800-115* sebagai acuan dalam pengujian *penetration testing* pada situs *web XYZ* dengan empat tahapan: *Planning*, *Discovery*, *Attack*, dan *Reporting*. Pada tahap *discovery*, Nmap menemukan dua port terbuka, yaitu port 80 (HTTP) dan port 443 (HTTPS). Pengujian dengan *OWASP ZAP* mengidentifikasi 7 kerentanan, termasuk *SQL Injection* dengan risiko tinggi. Pengujian lanjutan menggunakan *Burp Suite* dengan 198 kombinasi kode injeksi menunjukkan bahwa 11% berhasil mengakses data, 42% memperoleh informasi direktori, dan 47% gagal mendapatkan data[10].

Penelitian oleh Fahmi Fachri, Abdul Fadlil, dan Imam Riadi mengevaluasi kelemahan *server web* pada institusi perguruan tinggi, yang sering mengalami hacking melalui penyisipan *backdoor*. Pengujian dilakukan menggunakan *Parrot OS*, distriusi *Linux* yang dirancang untuk keamanan komputer dan *penetration testing*. Metode pengumpulan data menggunakan *Nmap* dan *Whois Lookup*. Hasil penelitian menunjukkan bahwa Sistem Informasi Akademik memiliki kerentanan pada level *High*, *Medium*, dan *Low*, terutama pada port 22 (SSH). Simulasi serangan menggunakan *Parrot OS* berhasil mendapatkan akses sistem dengan menemukan kombinasi *username* dan *password* yang valid[11].

Keamanan sistem informasi adalah aset penting yang harus dilindungi. Secara umum, keamanan berarti kondisi atau kualitas terlindungi dari ancaman atau bahaya. Adapun tinjauan atau poin penting dalam keamanan infromasi :

Physical Security, personal Security, Operation, Identification, Authentication, Accountability, Communications Security, Network Security[12].

Nmap (Network Mapper) adalah alat open-source gratis untuk pemindaian port, pemeriksaan kerentanan, dan pemetaan jaringan. Nmap memiliki kode sumber Fleksibel yang bisa dikustominasi untuk berbagai sistem operasi seperti Windows, Mac, Linux, serta sistem yang kurang umum seperti Solaris dan AIX[13].

Nessus adalah program yang berfungsi sebagai security scanner yang mengaudit jaringan dan menentukan kelemahan-kelemahan dari jaringan yang dituju. Nessus dibuat dengan pemahaman mendalam tentang cara kerja praktisi keamanan. Setiap fitur di *Nessus* dirancang untuk membuat penilaian kerentanan menjadi sederhana, mudah, dan intuitif. Hasilnya lebih sedikit waktu dan upaya untuk menilai, memprioritaskan, dan memperbaiki masalah[14].

ZAP atau *OWASP Zed Attack Proxy*, adalah alat keamanan gratis yang dapat anda gunakan untuk menemukan kerentanan keamanan dalam aplikasi web, dan beberapa prinsip yang menjadi dasar *ZAP* Menyediakan platform yang fleksibel untuk pengujian, Membangun platform yang kompetitif, berbasis *open source* dan berorientasi pada komunitas[15].

CIA TRIAD adalah keamanan informasi memiliki tiga aspek utama yang dapat diingat dengan singkatan *CIA*:

1. *confidentiality* adalah aspek yang memastikan bahwa data atau informasi tetap rahasia, serta menjaga kerahasiaan data yang dikirim, diterima, dan disimpan.
2. *Integrity* adalah aspek yang menjamin bahwa data tidak mengalami perubahan tanpa izin dari pihak yang berwenang (authorized), memastikan keakuratan dan keutuhan informasi tetap terjaga.
3. *Availability* adalah aspek yang memastikan bahwa data akan tersedia ketika diperlukan, memungkinkan pengguna yang berhak untuk mengakses informasi dan perangkat terkait sesuai kebutuhan[16].

Website adalah sekumpulan halaman web yang tersimpan di internet dan dapat diakses secara online oleh siapapun. Sebagaimana lokasi pada umumnya, website memiliki alamat yang menunjukkan lokasinya di internet, sehingga dapat diakses melalui web browser. Layanan web menggunakan teknologi seperti Hypertext Transfer Protocol (HTTP) dan File Transfer Protocol (FTP) untuk melakukan proses pengambilan data ini[17].

Kali linux, yang dirilis pertama kali oleh Offensive Security pada tahun 2013, adalah sistem operasi (OS) yang dirancang untuk memenuhi kebutuhan keamanan jaringan dan digunakan untuk pengujian penetrasi dan hacking jaringan. Kali linux telah menjadi standar industri dalam pengujian penetrasi dan forensik digital, serta terintergrasi dengan berbagai perangkat keamanan[18].

Pengujian *black box testing* biasanya digunakan untuk menguji fungsi internal aplikasi tanpa memerlukan pemahaman tentang kode program. Metode ini digunakan untuk menguji aspek fungsional, termasuk proses input dan output pada aplikasi. Teknik pengujian ini ditujukan bagi penguji yang tidak memiliki pengetahuan mendalam tentang pemrograman[19].

Port dalam TCP/IP digunakan untuk mengidentifikasi aplikasi spesifik dan layanan melalui nomor port, memungkinkan pengelolaan lalu lintas data pada tingkat perangkat lunak. Port seperti 80 untuk HTTP dan 443 untuk HTTPS mengatur jenis lalu lintas jaringan sesuai dengan protokol yang digunakan[20].

2. METODE PENELITIAN

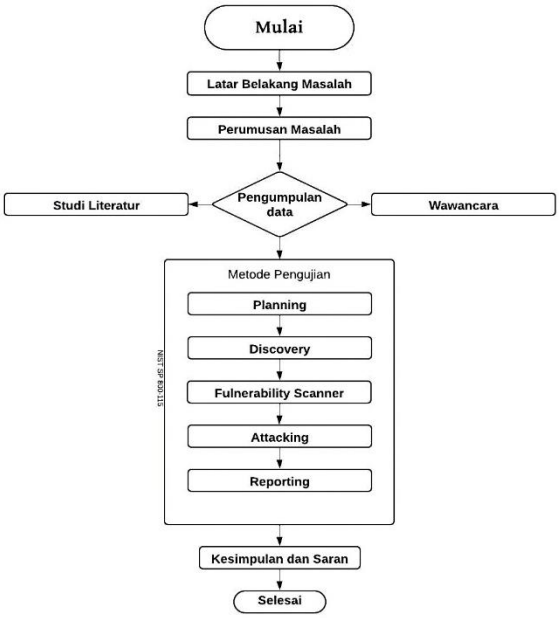
Latar belakang masalah pentingnya penelitian untuk memberikan pemahaman konteks dan relevansinya sebelum masuk ke metodologi, hasil, dan pembahasan.

Perumusan masalah adalah tahap dimana sebuah masalah dalam penelitian atau proyek didefinisikan secara rinci dan spesifik. Ini melibatkan mengidentifikasi, memahami, dan merumuskan pertanyaan yang menjelaskan masalah yang akan dipecahkan atau diteliti.

Pengumpulan data menggunakan studi literatur dari buku, jurnal, referensi online, serta tugas akhir. Wawancara non-truktural dilakukan dengan pengembang Astonprinter.com untuk mendapatkan wawasan mendalam tentang topik penelitian.

Metode pengujian yang digunakan dalam penelitian ini mengacu pada kerangka kerja *NIST SP 800-115* yang merupakan panduan untuk melakukan penetration testing. Metode ini terdiri dari beberapa tahapan penting, yaitu *Planning* (perencanaan), *Discovery* (penemuan), *Attack* (penyerangan), dan

Reporting (pelaporan). Berikut adalah deskripsi rinci dari tiap tahapan:



Gambar 1. Alur Penelitian

a. *Planning* (Perencanaan)

Pada tahap perencanaan , dilakukan persiapan menyeluruh terkait ruang lingkup dan tujuan pengujian penetrasi. Tahap ini bertujuan untuk memastikan bahwa pengujian penetrasi dilakukan secara terstruktur dengan mempertimbangkan risiko dan dampak yang mungkin terjadi.

b. *Discovery* (Penemuan)

Tahap ini melibatkan pengumpulan informasi penting tentang target sistem. Informasi yang diperoleh digunakan untuk tahap pengujian. Aktivitas pada tahap ini meliputi:

1. *Information Gathering* (Pengumpulan Informasi) : dilakukan pengujian dengan menggunakan *tools ping*, mencari informasi dari target Domain Astonprinter.com, ping adalah teknik dasar dalam mencari informasi suatu situs web, teknik ini membantu mengidentifikasi perangkat yang aktif dan memberikan informasi awal mengenai delay serta masalah jaringan.
2. *Vulnerability Scanning* (Pemindaian Kerentanan): Menggunakan *Nessus* dan *OWASP ZAP* untuk melakukan pemindaian otomatis. Alat-alat ini membantu dalam mendeteksi kerentanan yang mungkin terdapat dalam sistem.
3. *Network Scanning* (Pemindaian Jaringan): Menggunakan Nmap untuk melakukan pemetaan port dan layanan yang berjalan di server. Hal ini bertujuan untuk mengidentifikasi port terbuka yang dapat menjadi pintu masuk bagi serangan.

c. *Attack* (Penyerangan)

Tahap penyerangan dilakukan setelah informasi dan kerentanan ditemukan pada tahap sebelumnya. Pada tahap ini, dilakukan eksploitasi kerentanan yang telah terdeteksi guna mengevaluasi dampak potensial dari serangan siber yang nyata. Aktivitas dalam tahap ini meliputi:

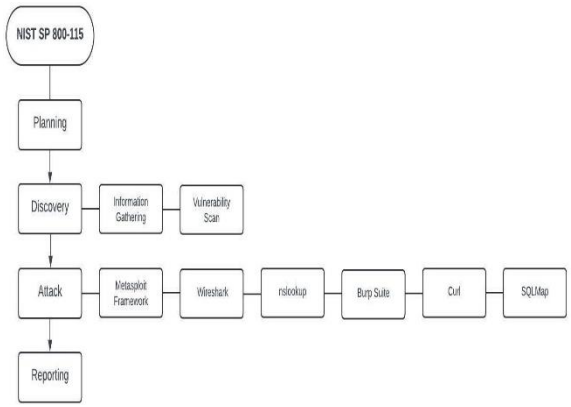
1. *Exploitation* (Eksploitasi): pada tahap ini, kerentanan yang ditemukan dieksploitasi untuk memvalidasi apakah kelemahan tersebut dapat digunakan untuk mencuri data, mendapatkan akses yang tidak sah, atau menyebabkan gangguan layanan.

d. *Reporting* (Pelaporan)

Tahap akhir dari penetration testing adalah penyusunan laporan hasil pengujian. Laporan ini harus mendokumentasikan seluruh proses pengujian, temuan kerentanan, eksploittasi yang dilakukan, serta rekomendasi mitigasi.

Alur Pengujian Penetration Testing Menggunakan Metode NIST SP 800-115

Metode ini melibatkan beberapa tahap pengujian yang terstruktur. Langkah-langkah dalam proses pengujian diilustrasikan pada gambar sebagai berikut:



Gambar 2. Perancangan Sistem

Gambar tersebut menunjukkan alur pengujian kerentanan situs Astonprinter.com menggunakan metode *NIST SP 800-115*. pada tahap *planning*, dilakukan perencanaan *penetration testing*, meliput:.

2.1. Tahap Planning

a. Ruang Lingkup

Komunikasi dengan tim IT Perusahaan Aston Printer untuk menentukan langkah-langkah yang akan diambil dalam penelitian ini. Adapun hasil kesepakatan yang dicapai pada tahap penelitian ini adalah :

1. Indentifikasi sistem atau aplikasi web yang akan menjadi fokus *penetration testing*.
2. Kesepakatan tentang akses data yang diperlukan untuk pengujian.
3. Metode dan pendekatan yang akan digunakan dalam pengujian.

4. Kesepakatan penggunaan tools dalam melakukan *penetration testing*.
5. Penyerahan hasil *report* kepada pihak IT kantor dan pihak pengembang web.

b. Persiapan Pemasangan Software

Penelitian ini memerlukan instalasi *kali linux* dengan menggunakan *VirtualBox* serta penggunaan tools pendukung pengujian. Alat – alat ini akan digunakan untuk melakukan *penetration testing* pada situs web.

c. Pemilihan website yang dijadikan target pengujian

Pada penelitian ini website yang akan dijadikan target pengujian adalah web Astonprinter.com untuk melakukan kerentanan ketahanan.

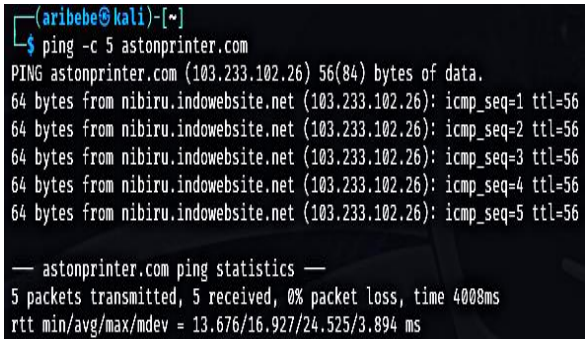
3. HASIL DAN PEMBAHASAN

3.1. Tahap Discovery

3.1.1. Information Gathering

a. Pengujian Ping

Hasil pengujian ping pada domain Astonprinter.com berhasil mendapatkan respons dari web server, dengan rata-rata *round-trip time (RTT)* berkisar antara 13,7 ms hingga 24,5 ms. Hasil selengkapnya ditambilkan pada gambar 3, dan tabel 1.



Gambar 3. Hasil Pengujian Ping

Tabel 1. Hasil Pengujian Ping

Domain Name System	Bytes	IP Address	ICMP Sequence	Time to Live	Time
Astonprinter.com	64	103.233.102.26	1	56	15.4 ms
	64	103.233.102.26	2	56	24.5 ms
	64	103.233.102.26	3	56	16.3 ms
	64	103.233.102.26	4	56	14.7 ms
	64	103.233.102.26	5	56	13.7 ms

b. Pengujian *Whois*

Pengujian *Whois* menggunakan alamat IP yang diperoleh dari pengujian ping menemukan bahwa website Astonprinter.com dikelola oleh PT. Tujuh Ion Indonesia. Detail informasi mengenai alamat IP, lokasi, dan kontak pengembang juga ditemukan. Hal ini ditampilkan pada tabel 2.

Tabel 2. Hasil Rangkuman Whois.

Parameter	Detail
Inetnum (Rentang IP)	103.233.102.0 - 103.233.103.255
Nename (Nama jaringan)	IDNIC-T7ION-ID
Organization (Organisasi Pemilik)	PT. Tujuh Ion Indonesia
Description (Deskripsi)	Corporate / Direct Member IDNIC
Address (Alamat)	Bekasi Regensi 2 Blok ii 1 No. 3 Cibitung, Bekasi 17520, Indonesia
Admin-c dan Tech-c (Kontak Administratif dan Teknis)	YP767-AP
Mnt-by, Mnt-routes, Mnt-irt (Maintenance Information)	MAINT-ID-T7ION dan IRT-T7ION-ID
Status	ASSIGNED PORTABLE
Abuse Contact (Kontak Penyalahgunaan)	email abuse@7ion.co.id
Person (Individu yang Bertanggung Jawab)	Yanwar Purnama
Last-modified	2020-09-01

3.1.2. Vulnerability Scanning

a. Network Scanning

1. *Network Mapping*

Tahap awal dalam *vulnerability scanning* menggunakan *Nmap*. Perintah '-Ss -Sv' digunakan untuk mengidentifikasi port terbuka dan versi layanan, '-Su' untuk memindai layanan UDP, dan '-O' untuk mendeteksi sistem operasi. *Nmap* memberikan informasi rinci tentang potensi kerentanan.

1.1 Hasil TCP Scan

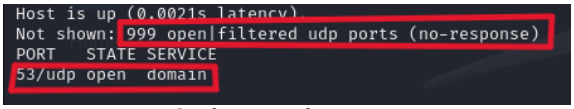
Hasil pengujian dengan perintah -Ss -Sv pada IP 103.233.102.26 (Astonprinter.com) menunjukkan beberapa layanan port bertuliskan *"tcpwrapped"*, yang dicurigai karena jaringan tidak stabil. Pemindaian diulang pada waktu berbeda untuk hasil lebih akurat. Hasilnya dirangkum dalam tabel:

Tabel 3. Hasil TCP Scan Rangkuman

IP Addess		103.233.102.26	
Nama Domain		Astonprinter.com	
Port	**Layanan**	**Status**	**Versi**
21	ftp	Open	Pure-FTPd
53	domain	Open	PowerDNS Authoritative Server 4.7.3
80	http	Open	Apache httpd
110	Pop3	Open	Dovecot pop3d
143	imap	Open	Dovecot imapd
443	Ssl/http	Open	Apache httpd
80	http	Open	Apache httpd
587	smtp	Open	Exim smtd 4.97.1
993	Ssl/imap	Open	Dovecot imapd
995	Ssl/pop3	Open	Dovecot pop3d
3306	mysql	open	Mysql (blocked - too many connection erors)

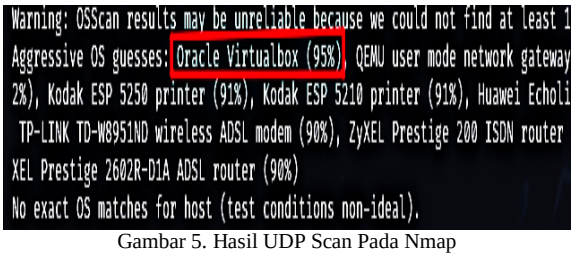
1.2 Hasil UDP Scan

Hasil rangkuman pada tabel 3. ditemukan beberapa port selain HTTP/HTTPS, dan akan dilakukan UDP scan (-Su), yang menunjukkan 999 port terbuka/difilter, menandakan adanya *firewall*, Port UDP 53 terbuka menjalankan DNS, dapat dilihat pada gambar 4.



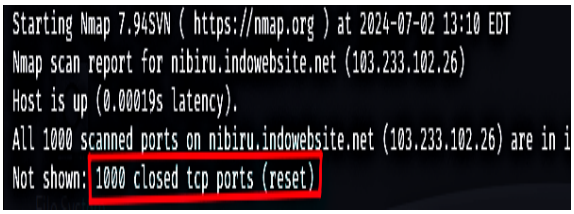
Gambar 4. Hasil UDP scan

1.3 Hasil Deteksi Sistem Operasi & Hasil TCP Maimon



Gambar 5. Hasil UDP Scan Pada Nmap

Dari hasil tools *Nmap* dengan menggunakan perintah '-O [IP Address], ditemukan bahwa sistem operasi yang digunakan *Oracle Virtualbox* dengan tingkat akurasi (95%). Kemudian pada gambar 6 dilakukan TCP maimon scan dengan menggunakan perintah -Sm [*IP Address*].



Gambar 6. Hasil Deteksi Sistem Operasi Pada Nmap

TCP Maimon scan (-Sm) menunjukkan bahwa 100 port TCP tertutup (reset), menandakan *firewall* mendeteksi aktivitas mencurigakan dan melindungi jaringan dengan baik.

b. Aplikasi web

1. *Nessus*

Pengujian *Basic Network Scan* menggunakan Nessus dilakukan 4 kali karena kondisi jaringan yang kurang stabil. Hasil pengujian terakhir (tes4) dipilih karena berhasil mendeteksi seluruh kelemahan protokol jaringan.

Gambar 7. Hasil Pengujian Nessus (tes4)

Hasil menunjukkan 1 ancaman *High*, 3 *Medium*, 4 *Low*, dan 45 informasi tambahan. Berikut rangkuman ancaman dari tes4

Tabel 4. Hasil Pengujian Nessus

No	Vulnerability	Threat Level	Analisis
1	DNS Server Spoofed Request Amplification DDos	High	DNS digunakan untuk amplifikasi serangan DdoS dengan IP palsu.
2	DNS Server Recursive Query Cache Poisoning Weakness	Medium	Manipulasi cache DNS Resolver dengan data berbahaya.
3	HSTS Missing From HTTPS Server (RFC 6797)	Medium	Tidak ada HSTS, rentan terhadap MITM dan downgrade attacks.
4	DNS Server Cache Snooping Remote Information Disclosure	Medium	Eksploitasi DNS Cache Snooping untuk pengambilan informasi secara remote.
5	ICMP Timestamp Request Remote Date Disclosure	Low	Informasi waktu sensitif dapat diambil melalui permintaan timestamp ICMP.
6	SSH Server CBC Mode Ciphers Enabled	Low	Konfigurasi cipher block chaining (CBC) aktif, rentan serangan.
7	SSH Weak Key Exchange Algorithms Enabled	Low	Konfigurasi SSH (Secure Shell) Weak Key Exchange Algorithms masih diaktifkan.
8	SMTP Service Cleartext Login Permitted	Low	Proses login SMTP tidak dienkripsi, dan mengakibatkan rentan terhadap pencurian informasi.

Nessus berhasil mendeteksi berbagai kerentanan yang berdampak pada keamanan jaringan, terutama terkait DNS, SSH, dan konfigurasi enkripsi yang lemah.

2. *OWAZP ZAP*

Dalam pengujian ini penulis menggunakan pemindaian otomatis untuk menemukan kerentanan terhadap web target. Adapun hasil yang ditemukan pada pemindaian kerentanan pada tabel 5. Dari hasil pemindaian tersebut, terdapat beberapa kerentanan yang ditemukan, seperti level ancaman *high* (1), *medium* (4) *low* (7). Dibahas pada tabel berikut;

Tabel 5. Hasil Pengujian OWAZP ZAP

No	Vulnerability	Threat Level	Analisis
1	Path Traversal	High	Kelemahan validasi input memungkinkan akses direktori sistem file dengan karakter khusus seperti "../".
2	Absence of Anti-CSRF Tokens	Medium	Tidak adanya Token Anti-CSRF
3	Content Security Policy (CSP) Header Not Set	Medium	Tidak adanya implementasi Content Security Policy (CSP)
4	Missing Anti-clickjacking Header	Medium	Header Anti-clickjacking tidak diatur.

5	Vulnerable JS Library	Medium	Pustaka JavaScript tidak diperbarui dan rentan.
6	Cookie No HttpOnly Flag	Low	Cookie tidak memiliki atribut HttpOnly.
7	Cookie without SameSite Attribute	Low	Cookie tidak memiliki atribut SameSite.
8	Cross-Domain JavaScript Source File inclusion	Low	JS dimuat dari sumber yang tidak aman atau tanpa CSP.
9	Server Leaks Information via "X-Powered-By" HTTP Response Header Filed(s)	Low	Pengungkapan informasi tentang teknologi server yang digunakan
10	Stirct-Transport-Security Header Not Set	Low	Strict-Transport-Security (HSTS) tidak diterapkan.
11	Timestamp Disclosure - Unix	Low	Pengungkapan waktu dan tanggal melalui file, log, atau response header.
12	X-Content-Type-Options Header Missing	Low	Header "X-Content-Type-Options" tidak ada.

3.2. Tahap Attack

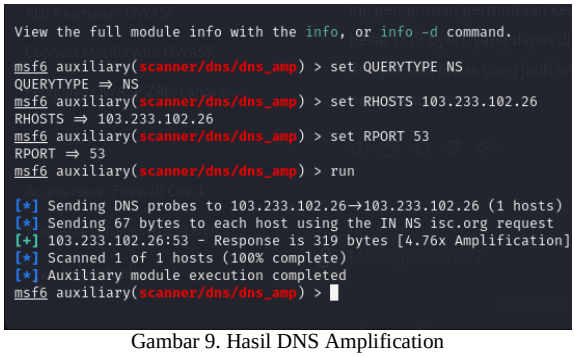
Penetration testing fokus kepada kerentanan dengan risiko tinggi (*high*) dan sedang (*medium*) yang memiliki potensi dampak besar terhadap keamanan sistem.

a. Kerentanan pada Nessus

1. *DNS Server Spoofed Request Amplification Ddos*

Pengujian *DNS Amplification* menggunakan *Metaspoit Framework* diawali dengan mencari madul DNS dengan perintah Search dns-amp, lalu memilihi modul use auxiliary/scanner/dns/dns_amp. Setelah itu, parameter dikonfigurasi menggunakan show options. Serangan ini menggunakan set QUERYTYPE NS untuk meminta informasi name server dari domain target, dengan IP target RHOSTS 103.233.102.26 dan port DNS RPORT 53, dapat dilihat pada gambar 8 dan 9.

Gambar 8. Hasil Pengujian Serangana DNS

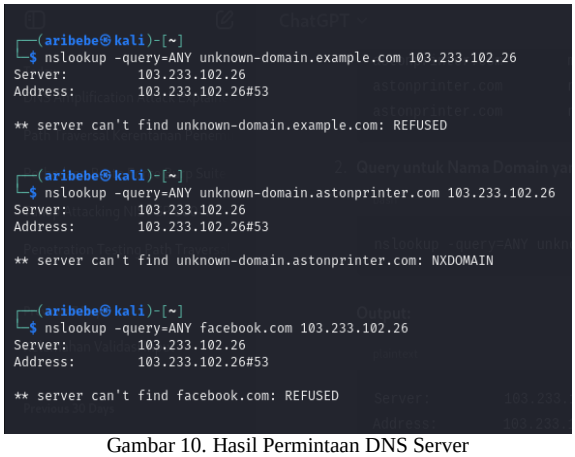


Gambar 9. Hasil DNS Amplification

Hasil pengujian menunjukkan bahwa server DNS tersebut dapat dieksploitasi, dengan paket permintaan 67 byte menghasilkan respons sebesar 319 byte, memberikan rasio amplifikasi 4,76 kali lipat, yang artinya ekploitasi berhasil dilakukan.

2. DNS Server Cache Snooping Remote Information Desclosure

Tools yang digunakan nslookup. Pada Gambar 10, saat dilakukan pengujian dengan domain tidak umum, server memberikan respons REFUSED dan NXDOMAIN, menandakan penolakan dan tidak adanya cache untuk domain tersebut. Ini menunjukkan serangan Cache Snooping tidak berhasil.

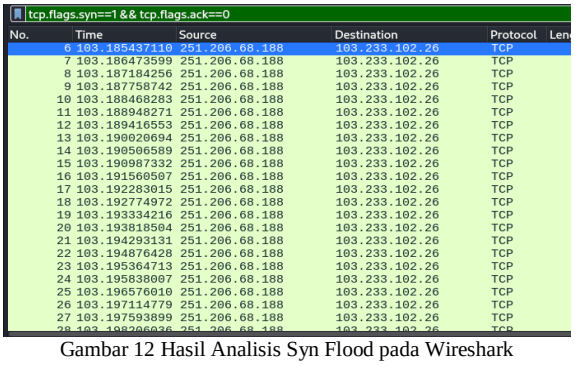


Gambar 10. Hasil Permintaan DNS Server

3. *Deniel of Service SynFlood*

Serangan dimulai dengan mencari modul menggunakan perintah *search dos synflood* lalu menjalankan use *auxiliary/dos/tcp/synflood*. Target dikonfigurasi dengan set RHOSTS 103.233.102.26 dan port set RPORT 80, kemudian serangan diluncurkan dengan run.

Gambar 11 proses pengujian serangan Syn Flood



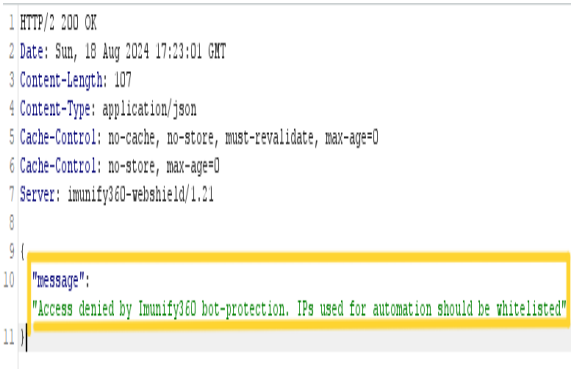
Gambar 12 Hasil Analisis Syn Flood pada Wireshark

Pada Gambar 12, Analisis menunjukkan banjir lalu lintas menyebabkan website sulit diakses. Serangan berhasil mengeksploitasi proses *Three-way Handshake TCP* dengan paket SYN yang tidak terselesaikan, memperlihatkan efek dari serangan *SYN Flood*.

b. Kerentanan pada OWASP ZAP

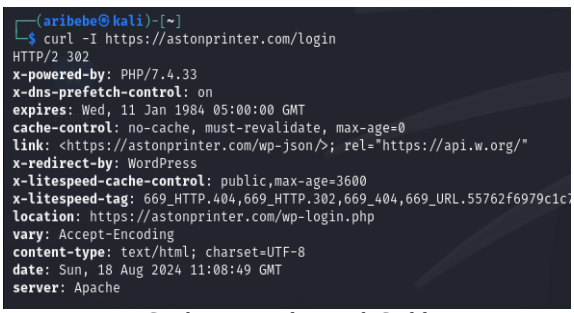
1. Path Traversal

Tools yang digunakan dalam pengujian ini adalah *Burp Suite*. Serangan *Path Traversal* menggunakan payload seperti ../../../etc/passwd tidak berhasil. Respons menunjukkan "*Access denied by Imunify360 bot-protection*," yang berarti *Imunify360* berhasil mendeteksi dan memblokir permintaan otomatis.



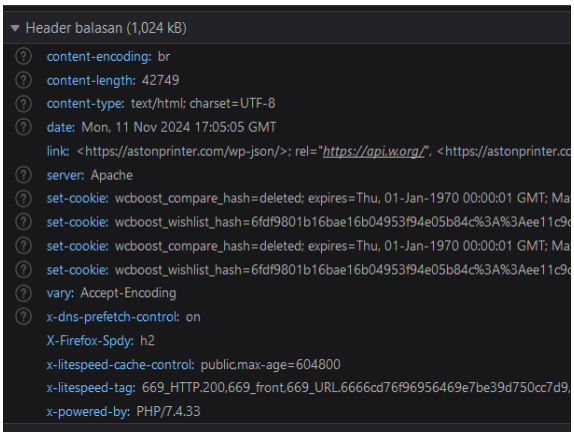
Gambar 13. Hasil Pengujian Path Traversal

2. Content Security Policy (CSP) Header Not Set & Missing Anti-clickjacking Header



Gambar 14. Hasil Perintah Curl-l

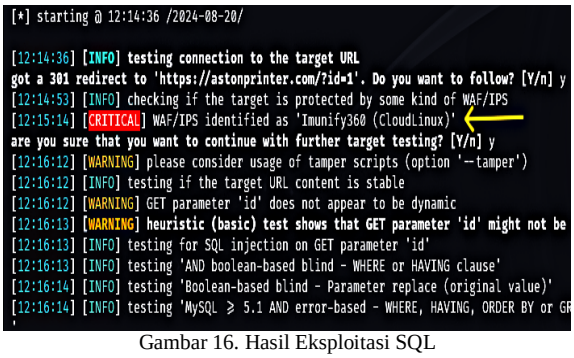
Hasil pada gambar 14 dapat dilihat, Perintah curl -I https://astonprinter.com digunakan untuk memeriksa header "*Content-Security-Policy*" dan "*X-Frame-Options*". Hasilnya, kedua header tersebut tidak ditemukan, menunjukkan CSP dan perlindungan *Clickjacking* belum diatur. Gambar 15, Analisis menggunakan *Mozilla Firefox* juga mengonfirmasi bahwa header "*Content-Security-Policy*" dan "*X-Frame-Options*" tidak ada, memperkuat hasil sebelumnya.



Gambar 15. Hasil Exploitasi Mozila

3. *Attacking SQL Injection*

Tools yang digunakan adalah *Sqlmap*, dapat dilihat pada gambar 16, Perintah sqlmap -u "https://astonprinter.com/index.php?id=1" --dbs digunakan untuk mengecek kerentanan *SQL Injection* pada astonprinter.com. Hasilnya, serangan tidak berhasil karena *WAF Imunify360* teridentifikasi memblokir atau menyaring serangan sebelum mencapai server.



Gambar 16. Hasil Eksploitasi SQL

3.3. Tahap Reporting

Pada tahap *reporting*, kerentanan yang ditemukan pada pengujian *Nessus* dan *Owasp ZAP* akan dilakukan analisis dengan melihat bagaimana kerentanan tersebut mempengaruhi tiga hal penting dalam keamanan informasi: Kerahasiaan, Integritas, dan Ketersediaan *(CIA Triad*). Penulis akan mengkategorikan masing - masing kerentanan dari ketiga aspek keamanan (*CIA Triad*) serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan sistem.

Tabel 6. Hasil Reporting

No	Vulnerability	Analisis Dampak Terhadap CIA Triad	Rekomendasi	Tingkat Risiko
1	DNS Server Spoofed Request Amplification DDos	**Availability :** Gangguan layanan akibat serangan DDoS.	Batasi dan filter query DNS untuk mencegah amplifikasi.	High
2	DNS Server Recursive Query Cache Poisoning Weakness	**Integrity :** Kerusakan cache DNS menyebabkan data salah.	Aktifkan DNSSEC untuk melindungi integritas data DNS.	Medium
3	HSTS Missing From HTTPS Server (RFC 6797)	**Confidentiality :** Risiko kebocoran data melalui man-in-the-middle.	Konfigurasikan header HSTS.	Medium
4	DNS Server Cache Snooping Remote Information Disclosure	**Confidentiality :** Pengungkapan informasi domain yang dikunjungi.	Terapkan pengaturan privasi DNS.	Medium
5	ICMP Timestamp Request Remote Date Disclosure	**Confidentiality :** Pengungkapan waktu sistem server.	Nonaktifkan respons timestamp ICMP pada server.	Low
6	SSH Server CBC Mode Cihpers Enabled	**Confidentiality :** Risiko kebocoran data karena cipher CBC rentan.	Gunakan cipher modern yang lebih aman dari CBC.	Low
7	SSH Weak Key Exchange Algorithms Enabled	**Confidentiality :** Algoritma pertukaran kunci yang lemah dapat dimanfaatkan penyerang.	Konfigurasi server SSH untuk menggunakan algoritma pertukaran kunci yang lebih kuat	Low
8	SMTP Service Cleartext Login Permitted	**Confidentiality :** kredendial login dapat diintersepsi jika dikirim dalam bentuk teks biasa	Terapkan TLS untuk mengenkripsi kredensial saat login ke server SMTP	Low
9	Path Traversal	**Confidentiality :** Penyerang dapat mengakses file atau direktori di luar jalur yang diizinkan..	Validasi input pengguna dan gunakan kontrol akses berbasis peran.	High
10	Absence of Anti-CSRF Tokens	**Integrity** : Tanpa token anti-CSRF, penyerang dapat mengirim permintaan berbahaya.	Implementasikan token anti-CSRF di setiap foemulir atau permintaan yang mengubah data.	Medium
11	Content Security Policy (CSP) Header Not Set	**Confidentiality :** Risiko serangan Cross-Site Scripting (XSS).	Konfigurasikan header CSP.	Medium
12	Missing Anti-clickjacking Header	**Confidentiality :** Risiko serangan clickjacking yang dapat mengekspos data pengguna.	Tambahkan header X-Frame-Options dengan nilai “DENY” atau “SAMEORIGIN”.	Medium
13	Vulnerable JS Library	**Confidentiality :** Pustaka JavaScript yang rentan bisa dieksploitasi.	Perbarui pustaka JavaScript ke versi terbaru.	Medium
14	Cookie No HttpOnly Flag	**Confidentiality :** Cookie dapat diakses oleh skrip sisi klien, meningkatkan risiko pencurian cookie	Tambahkan flag HttpOnly pada cookie untuk mencegah akses melalui JavaScript	Low
15	Cookie without SameSite Attribute	**Integrity :** Risiko serangan CSRF dengan pengiriman cookie dari domain lain.	Gunakan atribut SameSite pada cookie dengan nilai Strict atau Lax untuk membatasi pengirim cookie.	Low
16	Cross-Domain JavaScript Source File Inclusion	**Confidentiality :** Memuat skrip dari domain lain dapat memanipulasi data.	Batasi sumber daya JavaScript hanya pada domain terpercaya dan gunakan Content Security Policy.	Low
17	Server Leaks Information via “X-Powered-By” HTTP Response Header	**Confidentiality :** pengungkapan teknologi yang digunakan server.	Nonaktifkan Header “X-Powered-By”.	Low
18	X-Content-Type-Options Header Missing	**Confidentiality :** Serangan yang memanfaatkan browser untuk menebak jenis konten.	Tambahkan header “X-Content-Type-Options” dengan nilai “nosniff”.	Low
19	Stirct-Transport-Security Header Not Set	**Confidentiality:** Tidak adanya header Strict-Transport-Security (HSTS) membuka risiko serangan man-in-the-middle (MITM).	Mengaktifkan Strict-Transport-Security (HSTS) untuk memastikan bahwa browser hanya dapat terhubung ke server melalui HTTPS.	Low
20	Timestamp Disclosure - Unix	**Confidentiality:** Pengungkapan timestamp sistem, seperti versi Unix atau waktu server.	Menonaktifkan ICMP Timestamp Response atau meminimalkan pengungkapan informasi yang tidak diperlukan di server Unix.	Low

Analisis Hasil: Dari tabel diatas, dapat dilihat bahwa ada 20 kerentanan yang ditemukan. Kerentanan - kerentanan ini dikategorikan berdasarkan kegagalan *CIA Triad*. Sebanyak 16 kerentanan terkait dengan kegagalan pada *Confidentiality*, 3 kerentanan terkait dengan kegagalan pada *Integrity*, dan 1 kerentanan terkait dengan kegagalan pada *Availability*.

Kemudian hasil pengujian *Nessus* dan *Owasp ZAP* berdasarkan urutan *Owasp Top 10 2021*. Pada tahap *Attacking* terdapat 6 kerentanan yang dieksploitasi . Eksploitasi ini menghasilkan data atau informasi yang dapat disajikan dalam tabel berikut:

Tabel 7. Hasil Pengujian Nessus dan Owazp Zap

NO	Daftar OWASP TOP 10 2021	Celah keamanan	Hasil pengujian
1	A01:2021 - Broken Access Control	Path Traversal	Payload "../../../etc/passwd" diblokir oleh Imunify360 dengan pesan "Access denied by Imunify360 bot-protection."
		DNS Server Cache Snooping Remote Information Disclosure	Respons terhadap permintaan domain tidak umum adalah REFUSED dan NXDOMAIN, menunjukkan bahwa server DNS menolak informasi tersebut.
2	A02:2021 - Cryptographic Failures	-	-
3	A03:2021 - Injection	SQL Injection	Pengujian menggunakan SQLmap menunjukkan serangan gagal karena adanya WAF (Imunify360) yang memblokirnya.
4	A04:2021 - Insecure Design	-	-
5	A05:2021 - Security Misconfiguration	Content Security Policy (CSP) Header Not Set & Missing Anti-clickjacking Header	Perintah 'curl -I https://astonprinter.com' menunjukkan bahwa header CSP dan Anti-clickjacking tidak ada, sehingga perlindungan tidak diatur.
		DNS Server Spoofed Request Amplification DDoS	Respons menunjukkan DNS pada IP target dapat dieksploitasi, dengan rasio respons 4.76 (67 byte permintaan menghasilkan 319 byte respons).
6	A06:2021 - Vulnerable anda Outdated Components	Deniel of Service (DoS) SYN Flood	Monitoring Wireshark menunjukkan lonjakan trafik yang membuat website sulit diakses, dengan grafik menunjukkan peningkatan paket SYN dan respons RST dari server.
7	A07:2021 - Indentification and Authentication Failures	-	-
8	A08:2021 - Software and Data Integrity Failures	-	-
9	A09:2021 - Security Logging and Monitoring Failures	-	-
10	A10:2021 - Server-Side Request Forgery (SSRF)	-	-

Hasil Temuan: Tingkat risiko yang ditetapkan (*High*, *Medium*, *Low*) menggambarkan potensi dampak kerentanan terhadap keamanan website yang diuji. Misalnya, kerentanan dengan tingkat risiko *High* seperti *Path Traversal* dan *DNS Server Spoofed Request Amplification DDoS* dapat menyebabkan akses tidak sah dan gangguan layanan, yang sangat berbahaya bagi situs *e-commerce* dan aplikasi kritikal lainnya. Sebaliknya, kerentanan dengan tingkat risiko *Low* meskipun tetap penting untuk diperbaiki, mungkin tidak langsung menyebabkan dampak signifikan terhadap operasional situs.

4. DISKUSI

Hasil penelitian ini menunjukkan adanya 20 kerentanan yang teridentifikasi melalui pengujian menggunakan *Nessus* dan *OWASP ZAP*, dengan analisis dampak terhadap tiga aspek penting dalam keamanan informasi, yaitu Kerahasiaan, Integritas, dan Ketersediaan *(CIA Triad)*. Dari hasil reporting, terlihat bahwa 16 kerentanan terkait dengan kerahasiaan, 3 dengan integritas, dan 1 dengan ketersediaan, menegaskan bahwa keamanan kerahasiaan data menjadi prioritas utama. Diskusi mengenai hasil pengujian ini dapat diperkuat dengan membandingkan hasil yang diperoleh dengan penelitian sebelumnya, seperti yang dilakukan oleh Esti Zakia Darojat et al.[7], yang juga mengidentifikasi kerentanan seperti *Cross-site Scripting (XSS)* dan *Clickjacking* pada situs *web e-Government*. Kerentanan serupa yang ditemukan dalam penelitian ini, seperti *X-Frame Header Options Is Missing* dan *Content Security Policy (CSP) Header Not Set*, menunjukkan bahwa masalah ini bersifat umum dan dapat terjadi di berbagai jenis situs web. Penelitian Yosua Ade Pohan[8] juga mencatat kerentanan *Path Traversal* yang kritis, sejalan dengan hasil penelitian ini, yang menyoroti pentingnya implementasi kontrol akses yang ketat dan validasi input untuk mencegah eksploitasi. Dalam hal dampak, kerentanan seperti *DNS Server Spoofed Request Amplification DDoS* dapat menyebabkan gangguan layanan yang signifikan, mengakibatkan hilangnya akses ke informasi penting. Rekomendasi untuk membatasi dan memfilter *query DNS* menjadi langkah mitigasi yang penting. Selain itu, kerentanan terhadap *SQL Injection* menjadi perhatian serius, seperti yang dicatat oleh Wardana[10], di mana potensi dampak dari serangan ini mencakup pencurian data sensitif dan ancaman terhadap integritas sistem. Pengungkapan informasi melalui *DNS Server Cache Snooping* dapat memberikan penyerang informasi sensitif mengenai domain yang dikunjungi, yang berpotensi dimanfaatkan untuk serangan lebih lanjut, sehingga penerapan pengaturan privasi DNS sangat relevan. Dengan demikian, analisis mendalam terhadap temuan ini tidak hanya mengidentifikasi kerentanan, tetapi juga menggambarkan dampak potensial terhadap keamanan sistem. Diskusi ini memberikan konteks yang lebih luas tentang pentingnya pengujian kerentanan dan tindakan mitigasi yang diperlukan untuk meningkatkan keamanan informasi di berbagai platform, serta menggambarkan urgensi untuk melakukan langkah pencegahan yang lebih baik

dalam menghadapi risiko yang dihadapi oleh sistem informasi saat ini.

5. KESIMPULAN

Penelitian ini bertujuan untuk menguji kerentanan pada *website e-commerce*, dengan domain astonprinter.com, menggunakan metode NIST SP 800-115 sebagai tahapan penelitian. Setelah melakukan pengujian kerentanan terhadap website astonprinter.com, dapat disimpulkan sebagai berikut. NIST SP 800-115 digunakan sebagai metode penelitian dalam pengujian website astonprinter.com, dengan mengikuti prinsip - prinsip dasar seperti *Planning*, *Discovery*, *Attack*, *Reporting*. Dalam konteks penelitian keamanan sistem informasi, NIST SP 800-115 tetap sangat relevan dan efektif untuk digunakan dalam tahapan pengujian. Aspek - aspek keamanan CIA TRIAD *(Confidentiality*, *Integrity*, *Availability*) pada website astonprinter.com masih belum dapat dikatakan aman, menunjukkan adanya kekurangan dalam menjaga Kerahasiaan, Integritas, dan Ketersediaan data serta Sistem. Khususnya pada *Confidentiality*, terdapat 20 kerentanan yang ditemukan.

Website e-commerce dengan domain astonprinter.com terdapat *firewall* atau perangkat keamanan jaringan yang melindungi dari berbagai ancaman dan serangan. Sebagai contoh, dapat dilihat pada tahapan *attacking*, terutama dalam eksploitasi *SQL Injection* dan *Path Traversal*, terdeteksi adanya *Imunify360* yang berfungsi sebagai *firewall*. Sehingga server tidak dapat diakses atau diblokir selama serangan terjadi.

DAFTAR PUSTAKA

[1] Saefullah, "Pengaruh Kemajuan Teknologi Komunikasi dan Informasi Terhadap Karakter Anak," *BDK Jakarta*, 2020. Accessed: Aug. 29, 2024. [Online]. Available: https://bdkjakarta.kemenag.go.id/pengaruh-kemajuan-teknologi-komunikasi-dan-informasi-terhadap-karakter-anak/

[2] M. Guntur, "Perencanaan Keamanan dalam Pengembangan Sistem Informasi," *Kemenkeu Learning Center*, Jakarta, pp. 1–7, 2021. Accessed: Sep. 02, 2024. [Online]. Available: https://klc2.kemenkeu.go.id/kms/knowledge/perencanaan-keamanan-dalam-pengembangan-sistem-informasi-1b26a827/detail/

[3] T. Yuniarto, "Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya," *Harian Kompas*, Banten, 2024. Accessed: Sep. 02, 2024. [Online]. Available: https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya

[4] and A. S. B. S. H. Shaikh, A. P. Datir, "Cyber security in the age of digital transformation," *IRE Journals*, vol. 7, no. 12, pp. 463–468, 2024.

[5] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," *Electronics*, vol. 12, no. 5, p. 1229, Mar. 2023, doi: 10.3390/electronics12051229.

[6] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment.," Gaithersburg, MD, 2008. doi: 10.6028/NIST.SP.800-115.

[7] E. Z. D. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.

[8] Y. A. Pohan, Y. Yunus, and Sumijan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, vol. 3, no. 1, pp. 1–6, 2021, Accessed: Sep. 07, 2024. [Online]. Available: https://doi.org/10.37034/jsisfotek.v3i1.36

[9] M. D. Al Vriano, "Pengujian keamanan website dengan teknik penetration testing berbasis OWASP Top 10 studi kasus subdomain UPNJATIM," *Kohesi J. Sains dan Teknol.*, vol. 1, no. 6, pp. 91–100, 2023, doi: 10.3785/kjst.v1i6.522.

[10] W. Wardana, Almaarif, and A. Widjajarto, "Vulnerability Assessment and Penetration Testing On The Xyz Website Using Nist 800-115 Standard," *Syntax Lit. J. Ilm. Indones.*, vol. 7, no. 1, pp. 520–529, 2022, doi: 10.36418/syntax-literate.v7i1.5800.

[11] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver Menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, Accessed: Sep. 07, 2024. [Online]. Available: https://doi.org/10.31294/ji.v8i2.10854

[12] Yel Mesra Betty dan Nasution Mahyuddin K. M., "Keamanan informasi data pribadi pada media sosial," *J. Infromatika Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, [Online]. Available: https://www.academia.edu/download/112035091/68.pdf

[13] I. Nedyalkov, "Study the Level of Network Security and Penetration Tests on Power Electronic Device," *Computers*, vol. 13, no. 3, p. 81, Mar. 2024, doi:

10.3390/computers13030081.

[14] Aristian and W. Cholil, "Analisis Vulnerability Terhadap Website Lembaga Bahasa LIA Palembang Menggunakan Nessus, Netsparker dan Acunetic," *J. Pendidik. Dan Konseling*, vol. 4, no. 4, pp. 2459–2473, 2022, doi: https://doi.org/10.31004/jpdk.v4i4.5821.

[15] W. Wahidin, D. N. Rahayu, and R. M. Yulianto, "Analisis Kerentanan Situs Web KopKar Syariah PT BSIN menggunakan OWASP Zed Attack Proxy," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 18, no. 4, pp. 25–31, 2024, doi: https://doi.org/10.35969/interkom.v18i4.321

[16] C. Kar Yee and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," *J. ICT Educ.*, vol. 8, no. 2, pp. 34–42, Jul. 2021, doi: 10.37134/jictie.vol8.2.4.2021.

[17] S. Anwar, M. R. Katili, and I. R. Padiku, "Penerapan Algoritma Dijkstra dalam Perancangan Sistem Informasi Pencarian dan Penyewaan Kamar Kost Berbasiskan Web," *J. Syst. Inf. Technol.*, vol. 4, no. 2, pp. 1–11, 2024, Accessed: Sep. 07, 2024. [Online]. Available: https://siskp.informatika.ft.ung.ac.id/assets/jurnal/20240704150223.pdf

[18] G. D. Singh, *Kali Linux*, 1st ed., vol. 1. Kompjuter Biblioteka, 2023. Accessed: Sep. 08, 2024. [Online]. Available: https://kombib.rs/preuzimanje/pog/562_KALI_LINUX_promo.pdf

[19] I. R. Dhaifullah, M. Muttanifudin, A. A. Salsabila, and M. A. Yakin, "Survei teknik pengujian software," *J. Autom. Comput. Inf. Syst.*, vol. 2, no. 1, pp. 1–8, 2022, [Online]. Available: https://jacis.pubmedia.id/index.php/jacis/article/view/42

[20] Annu and Anil Dudy, "Review of the OSI Model and TCP/IP Protocol Suite on Modern Network Communication," *Int. J. Curr. Sci. Res. Rev.*, vol. 07, no. 02, pp. 1230–1239, Feb. 2024, doi: 10.47191/ijcsrr/V7-i2-41.