Analisis Kerentanan Menggunakan *Vulnerability Assessment* pada Situs Web Perguruan Tinggi

Danang Prihanto*[1], Adkhan Sholeh [2], Chanief Budi Setiawan[3], M. Abu Amar Al Badawi[4]
[1,2,3]Teknologi Informasi, FTTI Unjaya, Yogyakarta, Indonesia
[4]Informatika, FTTI Unjaya, Yogyakarta, Indonesia
e-mail: ***[1]danangprihanto1997@gmail.com**, [2]adkhan2006@gmail.com, [3]chanief.b.s@gmail.com, [4]abuamar.albadawi@gmail.com

Abstract* - In Indonesia, instances of low digital security have become increasingly prevalent. In 2021, the country witnessed 5,940 cases of web defacement across various sectors, with the academic domain, particularly universities, being a primary target, accumulating a total of 2,217 cases, the highest among all sectors. Consequently, this research focused on scanning the FTTI (Faculty of Engineering and Information Technology) websites. The study aims to analyze and assess the security level and vulnerabilities present on the FTTI website at Jenderal Achmad Yani University, Yogyakarta, specifically ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, and app.ftti.unjaya.ac.id. The obtained results are to be reported to the Head of Pusat Sistem Informasi (PUSI) FTTI. A vulnerability assessment was conducted using tools such as Nmap, Nessus, and WPScan. The process involved tool installation, data collection, vulnerability identification, and analysis. The analysis revealed varying vulnerability levels (Critical, High, Medium, Low, and Info) across the three websites. ftti.unjaya.ac.id, utilizing WordPress, exhibited no serious vulnerabilities. However, elearning.ftti.unjaya.ac.id and app.ftti.unjaya.ac.id showed Medium-level vulnerabilities according to the VPR Top Threats assessment. Among the scanned websites, ftti.unjaya.ac.id demonstrated the highest security level. Conversely, elearning.ftti.unjaya.ac.id and app.ftti.unjaya.ac.id presented several vulnerabilities with high or critical risk levels, as indicated by the scan results.

***Keywords* -** *vulnerability assessment, website, Nmap, Nessus, and WPScan*

Abstrak* - Di Indonesia, terdapat beberapa fenomena yang menunjukkan rendahnya tingkat keamanan digital. Pada tahun 2021, terdapat 5.940 kasus web defacement dari beberapa sektor yang menjadi sasaran. Salah satunya dari sektor akademik, yaitu perguruan tinggi dengan total 2.217 kasus, menjadikannya sektor dengan kasus terbanyak. Oleh karena itu, peneliti melakukan pemindaian pada ketiga website FTTI. Penelitian dilakukan dengan tujuan dapat menganalisis dan mengetahui tingkat keamanan serta bentuk-bentuk kerentanan pada website FTTI di Universitas Jenderal Achmad Yani Yogyakarta, yaitu ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id. Dengan hasil yang diperoleh dari analisis, peneliti harus melaporkan kepada Kepala Pusat Sistem Informasi (PUSI) FTTI. Menggunakan metode vulnerability assessment dengan beberapa alat seperti Nmap, Nessus, dan WPScan. Pada metode ini terdapat beberapa tahapan, seperti persiapan (instalasi alat dan pengumpulan data yang diperlukan), mengidentifikasi kerentanan, dan analisis. Hasil penelitian ini menunjukkan bahwa dari ketiga website, terdapat berbagai tingkat kerentanan seperti Critcal, High, Medium, Low, dan Info. Pada website ftti.unjaya.ac.id yang menggunakan WordPress, tidak terdapat kerentanan yang parah setelah dilakukan pemindaian menggunakan ketiga alat yang digunakan. Sementara itu, pada elearning.ftti.unjaya.ac.id dan app.ftti.unjaya.ac.id, menunjukkan hasil penilaian VPR Top Threats bahwa keduanya berada pada tingkat Medium. Pada ketiga website yang telah dipindai, ditemukan bahwa ftti.unjaya.ac.id adalah website dengan tingkat kerentanan paling aman. Menurut hasil pemindaian, website elearning.ftti.unjaya.ac.id maupun app.ftti.unjaya.ac.id memiliki beberapa kerentanan dengan tingkat risiko High bahkan Critical.

***Kata kunci* -** *vulnerability assessment, website, Nmap, Nessus, dan WPScan*

I. PENDAHULUAN

Perkembangan pesat *website* di Indonesia menjadi fenomena yang signifikan seiring meningkatnya pengguna layanan internet. Keberagaman *website*, termasuk jejaring sosial, *e-commerce*, forum, dan *port*al berita, menunjukkan pertumbuhan penggunaan internet yang masif. Namun, di balik kemudahan yang ditawarkan oleh berbagai layanan tersebut, terdapat masalah serius terkait keamanan, seperti *web defacement*, kebocoran informasi, dan serangan lainnya [1].

Dalam konteks ini, latar belakang permasalahan yang perlu diselesaikan adalah meningkatnya tingkat keamanan digital di Indonesia. Pada tahun 2021, terdapat 5.940 kasus *web defacement*, dengan sektor akademik, khususnya perguruan tinggi, menjadi sasaran terbanyak dengan 2.217 kasus [2]. Hal ini menunjukkan rendahnya tingkat keamanan digital di sektor pendidikan tinggi.

Beberapa isu terkait melibatkan celah keamanan pada *website*, termasuk *web defacement, information*

leakage, session management, authentication and authorization, SQL injection, cross-site scripting, dan CSRF. Risiko ini menyoroti perlunya melakukan analisis dan penilaian kerentanan secara berkala terhadap *website* guna memastikan keamanan dalam jangka panjang.

Penelitian-penelitian sebelumnya, menekankan pentingnya analisis kerentanan untuk meningkatkan keamanan aplikasi berbasis *website* [3]. Namun, wawancara dengan pengelola situs web FTTI Universitas Jenderal Achmad Yani Yogyakarta menunjukkan bahwa pengujian kerentanan belum pernah dilakukan.

Penelitian ini mengusung tujuan untuk menganalisis kerentanan pada beberapa *website* FTTI di Universitas Jenderal Achmad Yani Yogyakarta. FTTI, sebagai hasil perubahan bentuk dari STMIK Jenderal Achmad Yani, memiliki sejarah penting dalam perkembangan teknologi informasi di universitas tersebut.

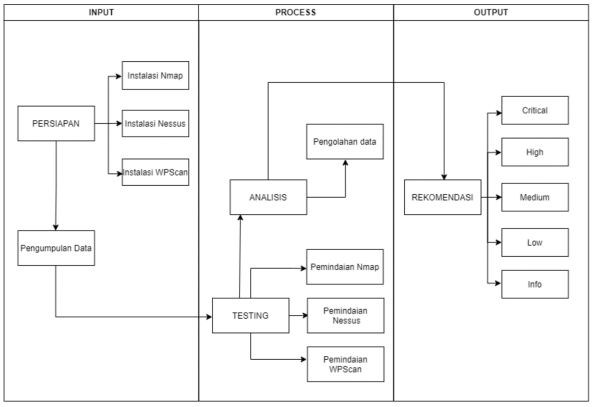
Penelitian ini menjadi penting karena memberikan pemahaman mendalam tentang tingkat keamanan *website* FTTI dan memberikan dasar bagi langkah-langkah pencegahan yang lebih efektif. Metode *vulnerability assessment*, sebagaimana dijelaskan oleh *GOV-CSIRT (Government Computer Security Incident Response Team)* [4], adalah tindakan mengidentifikasi kerentanan dari suatu aplikasi, sistem operasi, dan infrastruktur jaringan. *Vulnerability assessment* tidak melibatkan tindakan eksploitasi celah atau kelemahan dari suatu sistem, melainkan bertujuan untuk menemukan beragam *public vulnerability* pada seluruh sistem komputer dalam jaringan target. Dalam penelitian ini, alat-alat seperti *Nmap, Nessus*, dan *WPScan* digunakan sebagai pendekatan praktis untuk meningkatkan keamanan sistem informasi di lingkungan akademik. *Nmap*, yang bersifat *open source*, digunakan untuk eksplorasi dan audit keamanan jaringan, termasuk penemuan celah keamanan melalui teknik *port scanning* [5]. *Nessus*, sebagai salah satu *vulnerability scanner* jaringan, membantu mengevaluasi keamanan jaringan dan layanan berbasis sistem informasi[6]. *WPScan*, alat khusus untuk mendeteksi kerentanan keamanan pada situs web tipe *WordPress*, menjadi penting dalam mengamankan *website* yang menggunakan platform tersebut [7]. Dengan *WPScan*, pengguna dapat mengetahui kekuatan dan potensi kerentanan situs web target, tetapi juga perlu berhati-hati terhadap penyalahgunaan alat ini oleh pihak yang tidak bertanggung jawab [8]. *Zenmap*, sebagai antarmuka grafis untuk *Nmap*, memberikan kemudahan analisis hasil pemindaian *Nmap* [9]. *Nessus*, selain mencari kelemahan dalam jaringan target, juga membantu menentukan kelemahan yang ditemukan dari jaringan tersebut [10]. Dengan menggunakan alat-alat tersebut, penelitian ini diharapkan dapat memberikan kontribusi positif dalam memperkuat keamanan *website* FTTI Universitas Jenderal Achmad Yani Yogyakarta.

II. METODE PENELITIAN

Penelitian ini mengadopsi metode *vulnerability assessment* untuk mengevaluasi kerentanan pada situs web yang menjadi target. *DNSDumpster*, yang merupakan alat penelitian domain, digunakan sebagai bagian dari persiapan dalam pengumpulan data dan pemeriksaan informasi DNS. *DNSDumpster*, yang dikelola oleh hackertarget.com, adalah sebuah sumber daya *online* yang dapat menemukan host yang terkait dengan domain tanpa menggunakan metode *brute force subdomain enumeration*. Sebagai alat terpercaya dalam pemindaian kerentanan keamanan pada *open source* dan intelijen jaringan, *DNSDumpster* menggunakan *open source intelligence resources* untuk meminta data yang relevan, yang kemudian dikompilasi menjadi sumber daya yang dapat ditindaklanjuti oleh penyerang maupun pembela sistem internet [11]. Proses analisis kerentanan pada situs web dalam penelitian ini terinci dari tahap persiapan hingga penilaian kerentanan sistem, melibatkan instalasi alat-alat seperti *Nmap*, *Nessus*, dan *WPScan*.

Dengan memanfaatkan alamat IP target, aplikasi *Zenmap* digunakan untuk melakukan pemindaian dan menentukan *host-host* aktif dalam jaringan. Selanjutnya, informasi sistem operasi, *port* terbuka, dan jenis *firewall* yang digunakan oleh target dianalisis. Pemindaian kerentanan pada target dilakukan menggunakan *Nessus*, yang hasilnya kemudian dianalisis untuk menilai tingkat kerentanan.

Alur pengujian terdiri dari tiga tahapan, yang menjelaskan jalannya penelitian sebagaimana



Gambar 1. Alur Pengujian

ditunjukkan pada Gambar 1. Pada tahap *input*, persiapan alat pemindaian dilakukan dengan instalasi terlebih dahulu, diikuti oleh pengumpulan data situs web yang akan dipindai kerentanannya. Data dikumpulkan dengan izin dari pusat sistem informasi, rekomendasi situs web FTTI, dan pemeriksaan DNS menggunakan alat *DNSDumpster* untuk mengidentifikasi *Headers* situs web yang akan dipindai.

Proses berlanjut pada tahap *process* yang dimulai dari testing. Sebelum melakukan pemindaian, pencarian *IP address* dilakukan menggunakan *Command Prompt* dengan perintah *ping* untuk mengetahui *IP address* situs web. Kemudian, pemindaian dilakukan dengan menggunakan ketiga alat pemindaian kerentanan. Hasil pemindaian tersebut memungkinkan analisis kerentanan masing-masing situs web, yang kemudian diolah untuk mencapai tahap *output*.

Pada tahap *output*, penulis merangkum rekomendasi perbaikan berdasarkan tingkat risiko kerentanan yang teridentifikasi dari setiap situs web.

A. Jalan Penelitian

Penelitian ini menempuh metode *Vulnerability Assessment* yang melibatkan pemindaian pada target, dipilih karena esensial untuk menganalisis kerentanan pada situs web FTTI. Situs web yang diizinkan untuk analisis meliputi ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id. Persiapan penelitian melibatkan penginstalan alat yang akan digunakan, dengan *Nmap* digunakan untuk mengidentifikasi *host* aktif dan *port* terbuka pada IP target. Selain itu, penilaian kerentanan pada IP target menggunakan *Nessus*, sementara *WPScan* digunakan khusus untuk situs web ftti.unjaya.ac.id yang menggunakan *WordPress*.

Proses pemindaian memerlukan waktu yang cukup lama karena analisis dilakukan secara komprehensif. Tahapan analisis penelitian terdiri dari empat langkah, melibatkan:

1. Tahap Persiapan: Instalasi alat dan aplikasi yang akan digunakan.
2. Permohonan Izin: Meminta izin kepada admin situs web FTTI.
3. Pengumpulan dan Pengolahan Data: Melibatkan identifikasi *Headers* dengan *DNSdumpster*, pemindaian dengan *Nmap* untuk menentukan *port* terbuka, pemindaian dengan *WPScan* untuk mengidentifikasi kerentanan pada situs web berbasis *WordPress*, pemindaian menggunakan *Nessus* untuk mengetahui kerentanan pada situs web target, dan analisis data hasil pemindaian.
4. Penulisan Laporan: Tahapan akhir penelitian ini.

B. Metode *Vulnerability Assessment*

Dalam penyusunan tugas akhir ini, penulis menerapkan metode *vulnerability assessment* yang mencakup topologi jaringan, testing, dan analisis sesuai dengan bidangnya. Beberapa alat digunakan untuk melakukan pemindaian kerentanan pada setiap situs web, sebagaimana tertera pada Tabel 1.

Metode tersebut menggunakan tiga alat, yakni *Nmap*, *Nessus*, dan *WPScan*. Tabel 1 menunjukkan bahwa *WPScan* hanya digunakan pada ftti.unjaya.ac.id karena app.ftti.unjaya.ac.id dan elearning.ftti.unjaya.ac.id tidak menggunakan *WordPress*, seperti hasil pencarian pada *DNSDumpster*. Oleh karena itu, *WPScan* tidak digunakan untuk pemindaian pada kedua situs web tersebut.

III. Hasil dan Pembahasan

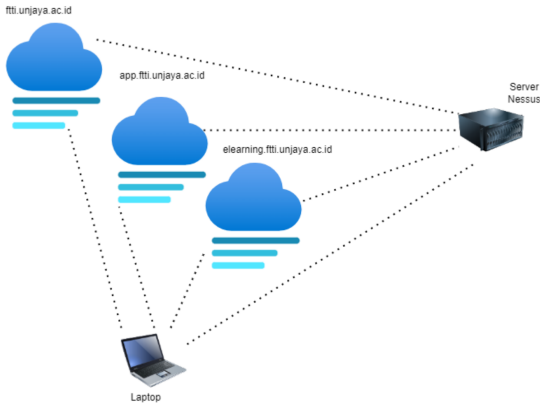
Tabel 1. Alat Pemindaian

ALAT	ftti.unjaya.ac.id	app.ftti.unjaya.ac.id	elearning.ftti.unjaya.ac.id
Nmap	Ya	Ya	Ya
Nessus	Ya	Ya	Ya
WPScan	Ya	Tidak	Tidak

A. Arsitektur Sistem

Penelitian ini memanfaatkan aplikasi *Nmap* dan *WPScan* yang diinstal pada laptop, sedangkan *Nessus* menggunakan web server untuk pemindaian dan memerlukan persiapan paket *Nessus* yang sudah terpasang di laptop. Topologi jaringan yang digunakan dalam penelitian ini dapat dilihat pada Gambar 2.

C. Testing



Gambar 2. Topologi Jaringan

Pada tahap ini, peneliti melakukan pemindaian pada ketiga situs web untuk mendapatkan hasil. Hasil pemindaian melibatkan beberapa langkah, termasuk identifikasi *Headers* menggunakan *DNSdumpster*, pemindaian pada IP target menggunakan *Nmap*, pemindaian kerentanan menggunakan *WPScan*, dan pemindaian kerentanan menggunakan *Nessus*. Berikut adalah rincian hasil pemindaian:

1. Identifikasi *Headers* menggunakan *DNSdumpster*

Sebelum melakukan pemindaian dengan *WPScan*, peneliti memeriksa DNS pada ketiga situs web menggunakan *DNSDumpster*. Hasil identifikasi *headers* pada ftti.unjaya.ac.id menunjukkan penggunaan *WordPress*, sementara app.ftti.unjaya.ac.id dan elearning.ftti.unjaya.ac.id tidak menggunakan *WordPress*.

2. Pemindaian pada IP target menggunakan *Nmap*

Tabel 2. Daftar fungsi *port* yang terbuka menggunakan *Nmap*

No	Port	Terbuka	Fungsi
1	21	Ya	FTP (File Transfer Protocol)
2	22	Ya	SSH (Secure Shell)
3	25	Ya	SMTP (Simple Mail Transfer Protocol)
...	...	...	...
15	10000	Ya	HTTP untuk layanan pengelolaan berbasis web (Webmin)

Tabel 3. Analisis hasil pemindaian ftti.unjaya.ac.id menggunakan *WPScan*

No	Hasil Pemindaian	Keterangan	Kerentanan
1	Header	Menggunakan server Litespeed	-
2	Versi WordPress	Versi 5.9.3	-
3	WordPress theme	Menggunakan Onepress dengan versi terbaru	-
4	Plugin *Jetpack*	Versi 11.1.2 (sudah kadaluwarsa)	Versinya sudah kadaluwarsa dan versi terbarunya adalah 11.2
5	*WordPress-seo*	Versi 19.3 (sudah kadaluwarsa)	Versinya sudah kadaluwarsa dan versi terbarunya adalah 19.5.1

Pemindaian menggunakan *Nmap* menghasilkan informasi *port* yang terbuka pada setiap situs web. Pada ftti.unjaya.ac.id terdapat 12 *port* terbuka, elearning.ftti.unjaya.ac.id memiliki 5 *port* terbuka, dan app.ftti.unjaya.ac.id memiliki 14 *port* dengan 1 *port* tertutup.

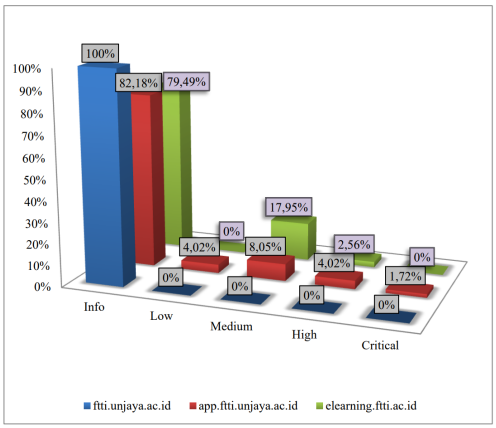
3. Pemindaian kerentanan menggunakan *WPScan*

Pada pemindaian dengan *WPScan*, hanya ftti.unjaya.ac.id yang menggunakan *WordPress*. Hasil pemindaian menunjukkan bahwa situs ini memiliki tingkat kerentanan yang rendah.

4. Pemindaian kerentanan menggunakan *Nessus*

Pemindaian kerentanan menggunakan *Nessus* menghasilkan beberapa kerentanan. Untuk ftti.unjaya.ac.id, tidak terdapat kerentanan yang signifikan. Pada app.ftti.unjaya.ac.id, terdapat tingkat ancaman Medium, dan pada elearning.ftti.unjaya.ac.id terdapat tingkat ancaman Medium.

Grafik perbandingan kerentanan pada ketiga situs web menunjukkan tingkat kerentanan tertinggi pada level Info, dengan ftti.unjaya.ac.id mencapai 100%, app.ftti.unjaya.ac.id 82,18%, dan elearning.ftti.unjaya.ac.id 79,49%. Tingkat kerentanan terendah terdapat pada level *Critical*, dengan persentase 1,72% hanya pada situs web app.ftti.unjaya.ac.id.



Gambar 3. Grafik Perbandingan Kerentanan

D. Analisis

Analisis dilakukan dengan mengumpulkan informasi mengenai kerentanan yang telah dipindai. Analisis data ini menjadi kunci untuk meningkatkan keamanan situs web dari potensi serangan pihak yang tidak bertanggung jawab.

1. Analisis hasil pemindaian menggunakan *Nmap*

Hasil pemindaian menggunakan *Nmap* memberikan informasi tentang beberapa *port* yang terbuka pada ketiga situs web. Fungsi dari setiap *port* tersebut dirangkum dalam Tabel 2.

Analisis menunjukkan bahwa setiap *port* yang terbuka pada masing-masing situs web memiliki fungsi yang berbeda. Terdapat catatan pada pemindaian *Nmap* pada elearning.ftti.unjaya.ac.id bahwa hanya terdapat 5 *port* terbuka, mengakibatkan *port* yang tertutup tidak dapat menjalankan tugasnya.

2. Analisis hasil pemindaian menggunakan *WPScan*

Analisis hasil pemindaian menggunakan *WPScan* pada ftti.unjaya.ac.id ditampilkan dalam Tabel 3.

Hasil pemindaian menunjukkan bahwa situs web ftti.unjaya.ac.id tidak memiliki kerentanan yang signifikan. Namun, terdapat peringatan terkait versi yang sudah kadaluwarsa pada *plugin Jetpack* dan *WordPress-seo*.

3. Analisis hasil pemindaian menggunakan *Nessus*

Analisis hasil pemindaian menggunakan *Nessus* diringkas dalam Tabel 4 dengan penilaian menggunakan *CVSS* versi 3.0.

Tabel 4. Tabel ringkasan pengujian menggunakan *Nessus*

No	Level	Situs web	Kerentanan
1	*Critical*	ftti.unjaya.ac.id	Tidak ada kerentanan yang terdeteksi
		app.ftti.unjaya.ac.id	*PHP unsupported version detection*
		elearning.ftti.unjaya.ac.id	-
2	*High*	ftti.unjaya.ac.id	-
		app.ftti.unjaya.ac.id	Versi PHP yang berjalan pada web server
			jarak jauh adalah sebelum 7.3.24
		elearning.ftti.unjaya.ac.id	*Remote* web server menghosting satu atau lebih skrip CGI
			yang gagal membersihkan *request strings* secara memadai
			dan tampaknya rentan terhadap serangan 'injeksi SSI'
3	*Medium*	ftti.unjaya.ac.id	-
		app.ftti.unjaya.ac.id	Versi *JQuery* yang di *hosting* pada *remote* web server sebelum
			3.5.0. *Web application* berpotensi rentan terhadap *Clickjacking*
			Metode *HTTP TRACE* / *TRACK* diizinkan.
		elearning.ftti.unjaya.ac.id	Direktori pada web server yang dapat dijelajahi. Web
			application berpotensi rentan terhadap *clickjacking*.
			HTTP TRACE / *TRACK methods allowed*.
4	*Low*	ftti.unjaya.ac.id	-
		app.ftti.unjaya.ac.id	Web server mentransmisikan *cleartext credentials*.
			Web server mengizinkan *password auto-completion*.
		elearning.ftti.unjaya.ac.id	-
5	Info	ftti.unjaya.ac.id	*Cookie web application* sudah kedaluwarsa.
		app.ftti.unjaya.ac.id	*Plugin* pada ftti.unjaya.ac.id menampilkan untuk setiap *host*
			yang diuji. *Plugin* ftti.unjaya.ac.id mencoba untuk menentukan
			jenis dan versi *remote* web server.
		elearning.ftti.unjaya.ac.id	Trans*port*asi properti *HTTP cookie* '*secure*' tidak cocok.
			Header respons HTTP X-FrameOptions tidak ada atau permisif.
			Versi server *HTTP Apache*

Pemindaian menggunakan *Nessus* menunjukkan bahwa setiap situs web memiliki kerentanan pada berbagai tingkatan, termasuk tingkat *Critical*, *High*, Medium, Low, dan Info. Beberapa kerentanan yang perlu mendapat perhatian lebih lanjut adalah seperti versi PHP yang sudah kadaluwarsa, kerentanan terhadap serangan 'injeksi SSI', serta potensi rentan terhadap *clickjacking* dan akses ke direktori pada web server.

E. Pembahasan

Penelitian ini berhasil memperoleh hasil dari pemindaian ketiga situs web, masing-masing dengan tingkat risiko yang berbeda. Fungsi dari ketiga alat pemindai—*Nmap* untuk mengetahui *port* terbuka, *Nessus* sebagai pemindaian celah kerentanan, dan *WPScan* untuk memindai kerentanan pada situs web *WordPress*—telah memberikan kontribusi penting dalam analisis keamanan situs web.

Rekomendasi perbaikan celah diambil dari hasil pemindaian dan dirangkum dalam Tabel 5. Penilaian kerentanan menggunakan skor dan tingkatan kerentanan yang dinilai menggunakan *CVSS* pada *Nessus*.

Tabel tersebut memberikan gambaran komprehensif tentang kerentanan, tingkat risiko, dan rekomendasi perbaikan yang dihasilkan dari pemindaian. Rekomendasi ini akan membantu PUSI untuk meningkatkan keamanan situs web FTTI dari potensi serangan pihak yang tidak bertanggung jawab.

Tabel 5. Tabel Rekomendasi perbaikan celah

No	Kerentanan	Skor/Level	Rekomendasi Perbaikan Celah
1	*PHP unsupported version detection*	10.0/*Critical*	Disarankan untuk meningkatkan ke versi *PHP* yang terbaru.
2	Versi *PHP* yang berjalan pada *remote web server* adalah sebelum 7.3.24	7.5/*High*	Disarankan untuk meningkatkan *PHP* versi 7.3.24 atau yang lebih baru.
3	Versi *PHP* yang berjalan pada *remote web server* adalah 7.2.x atau 7.3.x sebelum 7.3.21	7.5/*High*	Disarankan untuk meningkatkan *PHP* versi 7.3.22 atau yang lebih baru.
4	*CGI generic SQL injection (blind)*	7.5/*High*	Disarankan untuk mengubah skrip *CGI* yang terpengaruh.
5	*Remote web server* menghosting satu atau lebih skrip *CGI* yang gagal membersihkan *request strings* secara memadai dan tampaknya rentan terhadap serangan 'injeksi SSI'.	7.5/*High*	*Disable server-side* walaupun tidak dijalankan, atau batasi akses ke aplikasi yang rentan.
...	...	...	...
16	*HSTS* hilang dari *server HTTPS*	Info	Konfigurasikan *remote web server* untuk menggunakan *HSTS*.
17	Pengungkapan Informasi robots.txt web server	Info	Tinjau file robots.txt, gunakan *tag META Robots* sebagai ganti entri dalam file robots.txt, dan sesuaikan kontrol akses web server.
18	Versi *server HTTP Apache*	Info	Konfigurasi *remote host* untuk menggunakan *server HTTP Apache*.

IV. KESIMPULAN

Dari hasil penelitian ini, dapat disimpulkan bahwa situs web ftti.unjaya.ac.id memiliki tingkat kerentanan yang lebih aman dibandingkan dengan app.ftti.unjaya.ac.id dan elearning.ftti.unjaya.ac.id. Situs web app.ftti.unjaya.ac.id memiliki tingkat kerentanan paling parah, yakni *Critical*, sementara elearning.ftti.unjaya.ac.id memiliki tingkat kerentanan tertinggi pada tingkat *High*. Rekomendasi perbaikan telah dijabarkan dalam Tabel rekomendasi perbaikan celah, yang sebaiknya diimplementasikan oleh Pusat Sistem Informasi FTTI Universitas Jenderal Achmad Yani Yogyakarta untuk memperkuat keamanan situs web mereka. Saran peneliti melibatkan implementasi rekomendasi untuk mencegah potensi serangan dan menyarankan agar pihak Pusat Sistem Informasi FTTI secara rutin memperbaharui keamanan situs web, terutama saat melakukan pembaharuan fitur atau tampilan, dengan melakukan pengujian celah kerentanan.

DAFTAR PUSTAKA

[1] N. Junaedi, F. M. Hidayat, M. Rizqi, and I. W. P. Agung, "Membangun Startup ARSpira Sebuah Platform E-Counseling Berbasis Website Untuk Pelajar SMA," *Jurnal Ilmu Komputer dan Bisnis*, vol. 12, no. 2a, pp. 48–58.

[2] ID-SIRTII/CC, "Laporan tahunan monitoring keamanan siber," vol. 238, pp. 60–71, 2021.

[3] F. Yudha and A. M. Panji, "Perancangan aplikasi pengujian celah keamanan pada aplikasi berbasis web," *Cyber Security Dan Forensik Digital*, vol. 1, no. 1, pp. 1–6, 2018.

[4] Afifah, "Pembangunan Sistem It Assessment Center Pelabuhan Indonesia," pp. 1–7, 2018.

[5] D. Sudirman and A. N. Yaqin, "Network Penetration dan Security Audit Menggunakan *Nmap*," *SATIN-Sains dan Teknologi Informasi*, vol. 7, no. 1, pp. 32–44, 2021.

[6] T. Tan and B. Soewito, "Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity," *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research)*, vol. 6, no. 2, pp. 411–422, 2022.

[7] A. P. Dewanto and others, "Penetration Testing pada Domain uii. ac. id Menggunakan OWASP 10," 2018.

[8] R. Azis and S. Yazid, "Pengujian Kerentanan Website *WordPress* Dengan Menggunakan Penetration Testing Untuk Menghasilkan Website Yang Aman," *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, vol. 3, no. 3, pp. 93–105, 2021.

[9] A. Ahmad Aji Guntur Saputra, "Scanning Website menggunakan Zenmap," *Scanning Website menggunakan Zenmap*.

[10] D. Juardi, “Kajian Vulnerability Keamanan Jaringan Internet Menggunakan *Nessus*,” *Syntax Jurnal Informatika*, vol. 6, no. 1, pp. 11–19, 2017.
[11] Hackertarget, “Map an organizations attack surface with a virtual dumpster dive of the DNS records associated with the target organization.”