Vulnerability Assesment Web Proposal Tugas Akhir Mahasiswa Menggunakan Acunetix dan NMAP

Vulnerability Assessment Web Proposal Student Final Project Using Acunetix and NMAP

1st Syailendra Alzana Putra
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
syailendraallen@student.telkomuniversity.ac.id

2nd Avon Budiono
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
avonbudi@telkomuniveristy.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

Abstrak-Teknologi berkembang pesat seiring berkembangnya zaman, salah satu contoh dari perkembangan teknologi yaitu dengan berkembangnya penggunaan website pada kegiatan sehari hari. Banyak institusi dan entitas yang telah memanfaatkan penggunaan website untuk mendukung proses bisnis yang dijalankan. Fakultas Rekayasa Industri sebagai salah satu fakultas dari Universitas Telkom telah menggunakan website yang bernama virtualfri untuk dapat membantu kegiatan administrasi. Salah satu website dari Fakultas Rekayasa Industri adalah website dahsboard proposal tugas akhir yang berisi plottingan pembimbing tugas akhir serta judul tugas akhir. Namun dengan berkembangnya suatu teknologi, maka perkembangan kerentanan atau serangan terhadap teknologi tersebut juga bertambah.. Oleh karena itu, perlu dilakukannya metode vulnerability assessment untuk dapat mengetahui kerentanan yang tedapat pada suatu website dan juga solusi yang dapat diterapkan untuk mengatasi kerentanan tersebut. Pada penelitian ini akan dilakukan vulnerability assessment pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri dengan menggunakan tools Nmap dan Acunetix. Hasil yang didapat setelah dilakukannya proses vulnerability assessment yaitu terdapat 12 kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri dengan Nmap mendeteksi 3 kerentanan beresiko menengah dan 1 kerentanan beresiko rendah sedangkan Acunetix berhasil mendeteksi 2 kerentanan beresiko menengah dan 6 kerentanan beresiko rendah.

Kata kunci - kerentanan, website, vulnerability assessment, acunetix, nmap.

Abstract-Technology is growing rapidly along with the times, one example of technological development is the development of the use of websites in daily activities. Many institutions and entities have taken advantage of the use of websites to support their business processes. The Faculty of Industrial Engineering as one of the faculties of Telkom University has used a website called virtualfri to be able to help with administrative activities. One of the websites of the Faculty of Industrial Engineering is the final project proposal dashboard website which contains the plotting of the final project supervisor and the title of the final project. However, with the development of a technology, the development of vulnerabilities or attacks against these technologies also increases. Therefore, it is necessary to do a vulnerability assessment method to be able to find out the vulnerabilities found on a website and also solutions that can be applied to overcome these vulnerabilities. In this study, a vulnerability assessment will be carried out on the website dashboard for the final project proposal of the Faculty of Industrial Engineering students using Nmap and Acunetix tools. The results obtained after the vulnerability assessment process was carried out were that there were 12 vulnerabilities on the website dashboard for the final project proposal of the Industrial Engineering Faculty students with Nmap detecting 3 medium risk vulnerabilities and 1 low risk vulnerability while Acunetix managed to detect 2 medium risk vulnerabilities and 6 low risk vulnerabilities.

Keywords- vulnerability, website, vulnerability assessment, acunetix, nmap.

I. PENDAHULUAN

Perkembangan teknologi informasi berkembang pesat seiring dengan pertumbuhan penggunanya. Contoh dari perkembangan teknologi adalah penggunaan website untuk mendukung kegiatan pembelajaran. Website merupakan kumpulan halaman web yang dapat diakses secara publik. Website dapat terdiri dari teks, gambar, video, dan media suara lainnya. Namun dengan berkembangnya suatu teknologi, maka perkembangan kerentanan atau serangan terhadap teknologi tersebut juga bertambah. Berdasarkan laporan tahunan monitoring keamanan siber tahun 2021 oleh Badan Siber dan Sandi Negara (BSSN), terdapat lebih dari 1,6 miliar serangan siber yang telah terjadi di Indonesia.

Fakultas Rekayasa Industri sebagai salah satu fakultas dari Universitas Telkom telah menggunakan website yang bernama virtualfri untuk dapat membantu kegiatan administrasi fakultas seperti administrasi kerja praktek, rekruitasi asisten laboratorium, dan administrasi peminatan. Salah satu website yang ada pada virtualfri adalah website dashboard proposal tugas akhir untuk mahasiswa Fakultas Rekayasa Industri.

Dengan pentingnya keamanan data pada website dashboard tugas akhir tersebut, maka website dashboard tugas akhir tersebut perlu dijaga keamanannya dari kerentanan dan ancaman yang ada. Untuk menghadapi hal tersebut, pengelolaan keamanan informasi pada website dashboard tugas akhir perlu ditingkatkan. Salah satu cara untuk mendeteksi resiko kerentanan yang ada yaitu dengan melakukan vulnerability assessment. Mengidentifikasi ancaman yang ada sangat penting bagi seluruh jaringan komputer atau web untuk menggambarkan seberapa aman suatu perangkat dan web itu berdasarkan jumlah kerentanan yang diidentifikasi.

Pada tugas akhir ini akan dilakukan vulnerability assessment terhadap website dashboard tugas akhir yang dikelola oleh Fakultas Rekayasa Industri Universitas Telkom, Dalam proses vulnerability assessment tersebut, penulis menggunakan metode host-based scanning dan web app scanning dengan menggunakan Acunetix karena dapat mendeteksi sampai 7000 kerentanan, serta dapat memindai semua halaman dan web apps. Penulis juga menggunakan tools nmap karena tools ini terdokumentasi secara baik serta di update secara berkala sehingga dapat mendeteksi kerentanan terbaru, selain itu tools ini memiliki banyak fitur yang dapat digunakan untuk mencari kerentanan pada suatu website dan telah mendapatkan banyak penghargaan yang salah satunya adalah Information Security Product of the Year dari Linux Journal.

II. KAJIAN TEORI

A. Vulnerability

Vulnerability atau kerentanan adalah kerentanan pada sistem atau infrastrukturnya yang dapat dimanfaatkan pihak tidak berwenang untuk dapat mengeksploitasi suatu sistem [1]. Secara khusus, kerentanan dapat menjadi kelemahan pada sistem perangkat keras atau perangkat lunak, pada kebijakan dan prosedur yang digunakan didalam sistem, dan juga pada pengguna sistem itu sendiri[2].

B. Website

Website atau situs web adalah kumpulan halaman web yang ditautkan, dengan semua file yang ditautkan ke sana. Web terdiri dari satu atau lebih halaman dan kumpulan halaman yang disebut homepage / beranda. Halaman beranda berada di bagian atas dan halaman terkait ada di bagian bawah. Setiap halaman di bawah halaman beranda (halaman anak) biasanya berisi hyperlink ke halaman lain di web.

C. Keamanan Website

Keamanan website pada dasarnya yaitu melindungi situs web atau aplikasi web dari ancaman yang ada dengan mendeteksi, mencegah, dan merespon cyber threats. [3]

D. Nmap

Network Mapper atau nmap, merupakan program utilitas gratis dan open source yang berfungsi untuk network discovery dan audit keamanan. Nmap dapat membantu admin jaringan untuk melakukan berbagai hal seperti manajemen jaringan, memanajemen upgrade service, serta memonitoring host dan waktu uptime. [4]

Nmap menggunakan raw IP packet untuk menentukan host yang tersedia pada suatu jaringan, nama aplikasi dan versi yang digunakan oleh host tersebut, sistem operasi dan versi yang digunakan serta firewall yang digunakan [5]. Nmap dapat beroperasi pada berbagai sistem operasi seperti Linux, Windows, dan Mac OS X.

E. Acunetix

Acunetix Web Vulnerability Scanner adalah alat pengujian keamanan dari perushaan Invicti Security yang merupakan aplikasi web yang akan mengaudit aplikasi web dengan memeriksa kerentanan seperti SQL injection, cross-site scripting (XSS), dan kerentanan lain yang dapat dieksploitasi [6].

Acunetix merupakan web security

scanner yang terus ditingkatkan sejak tahun 2005. Acunetix tersedia untuk berbagai sistem operasi seperti Windows, macOS, dan Linux. Selain itu, Acunetix juga dapat digunakan sebagai produk cloud sehingga dapat menghemat memori yang digunakan

III. METODE

Penulis menggunakan metode web application scan dan host-based scan dalam penelitian ini. Alasan penulis untuk memilih kedua metode tersebut adalah karena dua metode tersebut saling terhubung. Pada host-based scan berfokus pemindaian kerentanan pada tingkat jaringan. Sedangkan pada web application scan, berfungsi untuk memindai website pada tingkat aplikasi. Jadi penulis akan melakukan pemindaian pada dua tingkatan yang berbeda namun tetap saling berhubungan satu sama lainnya

Terdapat dua environment yang digunakan pada penelitian ini, yaitu hardware dan software. Berikut merupakan rincian detail dari tiap environment yang digunakan:

A. Hardware

Hardware yang digunakan dalam pelaksanaan vulnerability scanning yaitu sebagai berikut

TABEL 1.
SPESIFIKASI HARDWARE

Nama Perangkat	Spesifikasi	
Laptop (Main OS)	Model	Acer Nitro AN515-52
	Ram	16 GB
	Storage	1.5 TB
	Processor	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz 2.21 GHz
	System type	64-bit operating system, x64-based processor
	Operating System	Windows 10 Education
Laptop (Virtual OS)	RAM	1 GB
	Processor	1 CPU
	Storage	40 GB
	Operating system	Linux
	Version	Debian (64-bit)
Acunetix	RAM	2 GB
	Storage	1 GB
	Processor	64 bit processor
	Operating system	Windows
Router	Model	ZXHN F609
	Hardware Version	V5.3
	Software Version	V7.0.10P1N14

B. Software

Software yang digunakan untuk mendukung pelaksanaan vulnerability scanning yaitu sebagai berikut

TABEL 2.
SPESIFIKASI SOFTWARE

Nama	Spesifikasi	Versi	Fungsi
Windows 10 Education	Operating system	21H2	*Operating system* utama
Acunetix	Web Vulnerability Scanner	13.0.201126145	• Melakukan vulnerability scan • Mengenerate vulnerability scan report
Virtualbox	Virtual Machine	6.1.30	• Menjalankan virtual OS • Melakukan instalasi nmap
Nmap	Vulnerability scanner	7.91	Melakukan vulnerability scan

C. Target Pengujian

Target pengujian yang akan dilakukan pada penelitian ini yaitu website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University. Alasan penulis memilih website tersebut karena website tersebut merupakan website yang berisi

data data penting yang berupa judul tugas akhir, kelompok tugas akhir, dan juga pembimbing untuk tiap kelompok. Data tersebut wajib untuk diamankan karena bersifat penting dan tidak semua entitas dapat melihat serta mengubah tiap datanya.

IV. HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai hasil analisis mengenai kerentanan yang ada pada website proposal tugas akhir mahasiswa Fakultas Rekayasa Industri. Hasil yang akan dianalisis merupakan hasil vulnerability scanning dengan menggunakan tools nmap dan Acunetix. Pada akhir bab ini juga akan dijelaskan mengenai rekomendasi yang dapat dilakukan untuk mengatasi kerentanan yang ada pada website proposal tugas akhir mahasiswa Fakultas Rekayasa Industri

A. Hasil Vulnerability Scanning Menggunakan Nmap

Berdasarkan hasil vulnerability scanning dengan menggunakan nmap yang telah dilakukan, terdapat 9 port yang terbuka pada Virtual Private Server Fakultas Rekayasa Industri yaitu port 22, 80, 81, 82, 83, 84, 443, 8080, dan 8081.

Port 22 yang merupakan port yang digunakan untuk ssh atau secure shell yang berfungsi untuk melakukan login secara remote atau jarak jauh ke Virtual Private Server yang digunakan [7]. Pada port ini terdapat 4 kerentanan yang akan dijelaskan pada tabel berikut

TABEL 3.
HASIL SCANNIG MENGGUNAKAN NMAP

No	Model Kerentanan	Nilai Kerentanan	Deskripsi
22.1	CVE-2020-15778	6.8	Penyerang yang memiliki kemampuan untuk melakukan scp file ke remote server dapat menjalankan perintah di remote server dengan memasukkan perintah sebagai bagian dari nama file yang sedang disalin pada server.
22.2	CVE-2021-28041	4.6	Ssh-agent pada OpenSSH dibawah versi 8.5 mempunyai kerentanan double free memory corruption yang memungkinkan attacker yang mempunyai akses ke socket agent untuk meneruskan agen ke akun yang dibagikan dengan pengguna ilegal atau ke host yang dikendalikan oleh attacker.
22.3	CVE-2020-14145	4.3	Pada sisi klien di OpenSSH versi 5.7 sampai 8.4 terjadi Observable Discrepancy dan menyebabkan kebocoran informasi dalam algorithm negotiation. Kerentanan ini memungkinkan attacker untuk melakukan aksi man-in-the-middle untuk menargetkan upaya koneksi awal yang mana tidak ada host key untuk server yang telah di-cache oleh klien.
22.4	CVE-2021-36368	2.6	Pada OpenSSH dibawah versi 8.9, jika klien menggunakan autentikasi public key dengan agent forwarding namun tidak menggunakan –oLogLevel=verbose, dan attacker telah diam diam mengubah server untuk mendukung opsi tanpa autentikasi, maka user tidak dapat menentukan bahwa autentikasi FIDO akan mengkonfirmasi user tersebut untuk terhubung ke server itu atau user ingin mengizinkan server tersebut terhubung ke server lain atas nama pengguna tersebut.

Port 80 merupakan HTTP port server / web server yang umum digunakan. Port ini berfungsi untuk mengakses internet. Port ini digunakan unutk mengubungkan web server dengan client [8]. Pada Virtual Private Server Fakultas Rekayasa Industri Telkom University, web server yang digunakan adalah nginx dengan versi 1.18.0 dan nmap tidak mendeteksi adanya kerentanan pada port ini.

Port 81-84 Pada port 81-84 merupakan port yang digunakan untuk port alternatif web server. Pada pengaturan bawaan dari Virtual Private Server Fakultas Rekayasa Industri Telkom University, port 81-84 digunakan untuk service Apache HTTP Server, namun Apache tersebut tidak terinstall pada Virtual Private Server Fakultas Rekayasa Industri Telkom University. Tools nmap yang digunakan pada penelitian ini menganggap bahwa port 81-84 benar benar menggunakan Apache HTTP Server pada port tersebut sehingga mendeteksi kerentanan berdasarkan versinya yaitu versi 2.4.51 untuk port 81 dan 2.4.10 untuk port 82-84. Total kerentanan yang tidak terverifikasi ini berjumlah 49 kerentanan.

Port 443. Pada port 443 merupakan port dengan protokol HTTPS yang berfungsi untuk mengatur komunikasi client dan web serever secara terenkripsi dan dilindungi oleh serifikat Secure Sockets Layer (SSL) [9]. Ketika port 443 terbuka, maka terdapat perangkat lunak dari server yang berjalan yang berarti bahwa web server sedang menunggu koneksi dari web browser. Tools nmap tidak mendeteksi adanya kerentanan pada port

ini.

Port 8080. Port 8080 merupakan port yang digunanan untuk port server proxy web. yang digunakan oleh web server untuk membuat koneksi TCP jika port 80 sedang sibuk. Tools nmap tidak mendeteksi adanya kerentanan pada port ini.

Port 8081. Port 8081 merupakan port yang berfungsi untuk port alternatif Hyper Text Transfer Protocol (HTTP) yang digunakan untuk lalu lintas jaringan website. Tools nmap tidak mendeteksi adanya kerentanan pada port ini.

B. Hasil Vulnerability Scanning Menggunakan Acunetix

Berdasarkan hasil vulnerability scanning dengan menggunakan acunetix yang telah dilakukan, terdapat 8 kerentanan yang ada pada website proposal tugas akhir mahasiswa Fakultas Rekayasa Industri. Penjelasan mengenai tiap kerentanan yang ditemukan dengan menggunakan software acunetix akan dijelaskan pada tabel berikut

TABEL 4.
HASIL SCANNING MENGGUNAKAN ACUNETIX

No	Kerentanan	Level	Deskripsi
1	Cross-site scripting (content-sniffing)	Medium	Terdapat script yang mungkin rentan terhadap serangan cross-site scripting (XSS). Cross-site scripting merupakan kerentanan yang memungkinkan attacker untuk mengirim kode berbahaya yang biasanya dalam bentuk javascript ke pengguna lain. Hal tersebut dapat terjadi karena browser tidak dapat mengetahui apakah skrip tersebut harus dipercaya atau tidak, maka browser akan mengeksekusi skrip dalam konteks pengguna yang memungkinkan attacker dapat mengakses cookie atau session token apapun yang disimpan oleh browser.
2	Penggunaan library JavaScript yang rentan	Medium	Pada website proposal tugas akhir mahasiswa FRI menggunakan jQuery versi 3.3.1 yang merupakan library JavaScript yang rentan.
3	Clickjacking : X-Frame-Options header missing	Low	Server tidak mengembalikan header X-Frame-Options yang berarti bahwa situs web ini berisiko terkena serangan clickjacking. Header respons X-Frame-Options merupakan header respons yang dapat digunakan untuk menunjukan apakah browser harus diizinkan untuk merender halaman didalam frame atau iframe. Halaman web dapat menggunakan ini untuk menghindari serangan clickjacking dengan memastikan bahwa konten mereka tidak disematkan ke situs lain dengan tanpa izin.
4	Cookies dengan kekurangan atribut atau properti.	Low	Terdapat cookies yang tidak memiliki atribut SameSite. Ini dapat mengarah kepada perilaku tak terduga oleh aplikasi yang nantinya dapat menyebabkan masalah keamanan sekunder.
5	Cookies tanpa adanya flag HttpOnly	Low	Terdapat beberapa cookie yang tidak memiliki flag HttpOnly. Ketika cookie disetel dengan flag HttpOnly, itu menginstruksikan browser supaya cookie hanya dapat diakses oleh server dan bukan oleh client-side scripts, ini merupakan perlindungan keamanan yang penting untuk session cookies.
6	Cookies tanpa adanya flag Secure.	Low	Terdapat beberapa cookie yang tidak memiliki Secure flag. Saat cookie di setel dengan secure flag, itu menginstruksikan browser bahwa cookie hanya dapat diakses melalui channel SSL/TLS yang aman. Ini merupakan perlindungan keamanan yang penting untuk session cookies.
7	Tidak mengimplementasikan HTTP Strict Transport Security (HSTS)	Low	HTTP Strict Transport Security (HSTS) memberitahu browser bahwa situs web ini hana dapat diakses menggunakan HTTPS. Aplikasi web TA1 tersebut tidak mengimplementasikan HTTP Strict Transport Secutity (HSTS) karena header Strict Transport Security tidak terdapat pada respons.
8	Halaman sensitif beresiko untuk di-cache	Low	Terdapat halaman yang berisi informasi sensitif seperti parameter kata sandi dan berpotensi di-cache bahkan pada channel SSL yang aman. Data sensitif tersebut dapat disimpan oleh intermediary proxy / proxy perantara dan terminator SSL.

C. Rekomendasi Solusi

Dari kerentanan yang didapatkan melalui scanning dengan menggunakan nmap dan acunetix, penulis dapat menyimpulkan menjadi rekomendasi solusi akhir yang dapat mencakup semua kerentanan yang ada dengan solusi sebagai berikut

1. Melakukan upgrade OpenSSH ke versi 9.0

   Pada Virtual Private Server Fakultas Rekayasa Industri menggunakan OpenSSH versi 8.2p1. Pada versi OpenSSH tersebut, terdapat kerentanan yang sudah diperbaiki pada versi barunya, untuk itu penulis menyarankan untuk melakukan upgrade versi OpenSSH setidaknya ke versi 9.0
2. Membuat script yang digunakan agar dapat memfilter metacharacter dari hasil input yang dimasukkan oleh user

   Terdapat dua cara yang dapat digunakan untuk memfilter hasil input yang dimasukkan oleh user yaitu dengan menggunakan validasi input black-list dan juga white-list. Pada validasi input black-list bekerja dengan

membuat list mengenai nilai yang tidak diizinkan pada hasil input user, jika terdapat nilai yang tidak diizinkan maka request tersebut akan diblokir. Sedangkan pada validasi input white-list bekerja dengan membuat list nilai yang boleh diinputkan oleh user, jika terdapat nilai yang tidak terdapat pada daftar, maka request akan diblokir

3. Mengupgrade library jQuery ke versi 3.6.0
   JQuery merupakan library JavaScript lintas platform yang dapat melakukan event handling dan hal lainnya. Tujuan dari jQuery yaitu untuk mempermudah penggunaan javascript pada suatu website dengan cara membungkus kode javascript menjadi method yang dapat dipanggil dengan satu baris kode saja.
   Versi dari library jQuery yang digunakan untuk website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University adalah versi 3.3.1 yang merupakan versi yang memiliki kerentanan cross-site Scripting (XSS) dan prototype pollution sehingga direkomendasikan untuk mengupgrade library jQuery ke versi 3.6.0.
4. Mengkonfigurasikan web server untuk memasukkan X-Frame-Options header dan CSP header dengan menggunakan directive frame-ancestors
   X-Frame-Options dan directive frame-ancestor dapat memungkinkan anda untuk menentukan URL parent mana yang dapat membingkai (frame) resource saat ini. Dengan menggunakan direktif CSP frame-ancestor, kita dapat memblokir atau mengizinkan halaman ditempatkan di dalam bingkai atau iframe sehingga dapat mencegah terjadinya clickjacking.
5. Mengatur atribut Samesite pada cookie yang ada
   Pada website dashboard proposal tugas akhir mahasiswa FRI, cookie tidak terdapat atribut SameSite. Atribut SameSite pada cookie merupakan atribut yang memungkinkan anda untuk mendeklarasikan apakah cookie anda dapat diterima saat request baru datang dari third-party. Atribut samesite dapat berisi tiga value yaitu Strict, Lax, dan None. Jika cookie di setel pada nilai atribut SameSite ke Strict, maka cookie hanya akan dikirim jika situs untuk cookie cocok dengan situs yang saat ini ditampilkan di URL bar pada browser. Namun jika cookie di setel dengan nilai atribut SameSite ke Lax, browser akan mengizinkan sebagian besar cross-domain cookie-sharing selama berasal dari top-level GET request.
6. Mengatur flag HttpOnly pada cookie yang ada
   HttpOnly merupakan atribut pada cookie yang dapat membantu mengurangi resiko skrip pada sisis klien untuk mengakses cookie yang dilindungi dengan membuat gerbang yang mencegah cookie yang dilindungi diakses oleh siapapun selain server yang membuatnya menjadi lebih aman. Atribut ini perlu untuk diatur agar cookie tidak dapat diakses pada client-side.
7. Mengatur flag Secure untuk cookie yang ada
   Atribut secure pada suatu cookie merupakan opsi yang dapat diatur oleh server aplikasi saat mengirim cookie baru ke pengguna dalam suatu HTTP response. Tujuan dari atribut ini yaitu untuk mencegah cookie diamati atau dilihat oleh pihak yang tidak berwenang karena pengiriman dari cookie tersebut dilakukan dengan cleartext. Dengan menyetel atribut secure, browser yang mensupport penggunaan atribut secure hanya akan mengirim cookie dengan atribut secure saat terdapat request menuju halaman HTTPS. Dengan kata lain, browser tidak akan mengirim cookie yang menggunakan atribut secure melalui request HTTP yang tidak terenkripsi
8. Mengimplementasikan HTTP Strict Transport Security (HSTS)
   Jika situs web menerima koneksi melalui HTTP kemudian meredirect ke HTTPS, pengunjung web masih dapat berkomunikasi dengan situs web yang tidak terenkripsi sesaat sebelum dialihkan. Redirect terebut dapat dieksploitasi untuk mengarahkan pengunjung website lain yang dibuat oleh penyerang.

Header HTTP Strict Transport Security memberitahu browser bahwa tidak boleh memuat situs menggunakan HTTP dan secara otomatis mengkonversi semua upaya untuk mengakses situs yang tadinya menggunakan HTTP menjadi HTTPS.

9. Menambahkan "Cache Control: No-store" dan "Pragma: no-cache" pada respons header HTTP

   Cache-control merupakan header HTTP yang berfungsi untuk menentukan kebijakan cache browser dalam request dari klien dan respons dari server. Direktif no-store berarti browser tidak diizinkan untuk melakukan cache respons dan harus menariknya dari server setiap kali di request. Pengaturan ini biasanya digunakan untuk data yang bersifat sensitif.

   Pragma HTTP/1.0 general header merupakan header khusus implementasi yang memiliki efek pada request-response chain [10]. Pragma: no-cache berfungsi untuk memaksa cache untuk mengirimkan request ke server asal untuk dilakukan validasi sebelum salinan cache dirilis

D. Hasil Pemindaian dan Karakteristik Tools Nmap dan Acunetix

Setelah dilakukannya scanning menggunakan tiap tools, penulis dapat mendeskripsikan hasil dan karakteristik tools Nmap dan Acunetix. Nmap dan Acunetix merupakan dua tools yang berfokus pada pemindaian kerentanan di lapisan yang berbeda sehingga tidak dapat dibandingkan secara langsung. Nmap merupakan aplikasi yang berfokus untuk melakukan pemindaian kerentanan pada lapisan jaringan dengan menggunakan metode host-based scan sedangkan Acunetix merupakan aplikasi yang berfokus untuk melakukan pemindaian kerentanan pada lapisan aplikasi dengan menggunakan metode web application scan. Penjelasan mengenai hasil pemindaian dan karakteristik pada tiap tools akan dijelaskan pada tabel 5 dan tabel 6 berikut.

TABEL 5.
HASIL PEMINDAIAN DAN KARAKTERISTIK NMAP

Indikator	nmap
Metode	Host-based scan
Jenis aplikasi	Aplikasi berbasis command line
Jumlah kerentanan yang terdeteksi	53
Kerentanan yang sesuai	4 (13.25%)
Terdapat informasi detail tiap kerentanan	Tidak
Pricing	Gratis

TABEL 6.
HASIL PEMINDAIAN DAN KARAKTERISTIK NMAP

Indikator	Deskripsi
Metode	Web application scan
Jenis aplikasi	Aplikasi berbasis web based
Jumlah kerentanan yang terdeteksi	8
Kerentanan yang sesuai	8 (100%)
Terdapat informasi detail tiap kerentanan	Ya
Pricing	Komersil

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat diambil kesimpulan yaitu sebagai berikut:

A. Terdapat 12 kerentanan yang terdeteksi pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University dengan 5 kerentanan beresiko sedang, dan 7 kerentanan beresiko rendah.

B. Solusi yang direkomendasikan untuk mengatasi kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University yaitu dengan mengupgade versi ssh dan jQuery serta mengkonfigurasi cookie dengan atribut yang lengkap.

C. Tools Nmap yang berfokus melakukan pemindaian pada lapisan

jaringan dapat mendeteksi 53 kerentanan dengan akurasi 13.25% sedangkan tools Acunetix yang berfokus melakukan pemindaian pada lapisan aplikasi dapat mendeteksi 8 kerentanan dengan akurasi 100%.

REFERENSI

[1] J. Goel and B. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology", Procedia Computer Science, vol. 57, pp. 710-715, 2015.

[2] M. Abomhara and G. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.

[3] A. Zirwan, "Pengujian Dan Analisis Kemanan website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, 2022. pp. 70–75.

[4] I. Malinich, V. Mesyura and I. Arseniuk, "Analysis of Traffic Usage by Scanning Computer Networks with Different Versions of Nmap", Visnyk of Vinnytsia Politechnical Institute, vol. 155, no. 2, pp. 92-97, 2021. Available: 10.31649/1997-9266-2021-155-2-92-97

[5] S. Jetty, Network Scanning Cookbook: Practical network security using Nmap and Nessus 7. Birmingham, United Kingdom: Packt Publishing, 2018..

[6] R. Mayasari, A. Ali Ridha, D. Juardi and K. Ahmad Baihaqi, "Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability", SYSTEMATICS, vol. 2, no. 1, pp. 33-38, 2020. Available: 10.35706/sys.v2i1.3450

[7] A. Slameto and L. Lukman, "Penerapan Openssh dan Bash Script Untuk Simultaneos Remote Access Client Pada Laboratorium STMIK Amikom Yogyakarta", Respati, vol. 9, no. 27, pp. 23-32, 2017. Available: 10.35842/jtir.v9i27.79

[8] J. Wang and Z. Kai, "Performance Analysis and Optimization of Nginx-based Web Server", Journal of Physics: Conference Series, vol. 1955, no. 1, p. 012033, 2021. Available: 10.1088/1742-6596/1955/1/012033

[9] M. Arman, "Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer", JURNAL INTEGRASI, vol. 9, no. 1, pp. 16-23, 2017. Available: 10.30871/ji.v9i1.272

[10] G. Gou, Q. Bai, G. Xiong and Z. Li, "Discovering abnormal behaviors via HTTP header fields measurement", Concurrency and Computation: Practice and Experience, vol. 29, no. 20, p. e3926, 2016. Available: 10.1002/cpe.3926