Jurnal Infosecure Vol.4 No.1, April 2023
p-ISSN: 2087-1023
MTI-UNLA

Pengujian Kerentanan Keamanan Layanan Daring pada Pemerintahan Kabupaten Menggunakan *Freeware Scanning*

Aisyah Nuraeni[1], Ali Ahmadi[2]

[1,2] *Teknik Informatika, Teknik, Universitas Langlangbuana*

[1]aisyahnuraeni20@gmail.com

[2]kang.aliahmadi@gmail.com

Abstrak—Pengujian kerentanan keamanan layanan daring memungkinkan penguji untuk memeriksa aspek fungsional dari suatu sistem bahwa seberapa banyak sistem itu rentan terhadap keamanan Jaringan, serangan intrusi, dan untuk lihat mekanisme pertahanannya untuk mengimbangi serangan ini. Pada pengujian ini akan menilai kerentanan keamanan di Pemerintahan Kabupaten dengan strategi Blind PEN Testing yang meliputi penelusuran celah keamanan pada sistem operasi, server aplikasi, sistem jaringan, dan juga kerentanan dari sisi aplikasi WEB. Alat yang digunakan adalah Shodan, Malgeto, Nmap, Nikto, Open-Vas, dan OWASP-Zap. Meliputi 5 tahapan yaitu information gathering, enumerasi, risk assessment, proof of Concept, dan rekomendasi. Dari 3 situs, yang diuji terdapat 58 logs dengan kategori aman untuk jaringan sedangkan terkait aplikasi dan web terdapat temuan kerentanan Zone Transfer Attack, ClickJacking Attack dan SQL Injection.

Kata kunci— Pengujian, kerentanan, layanan-daring, freeware-scanning

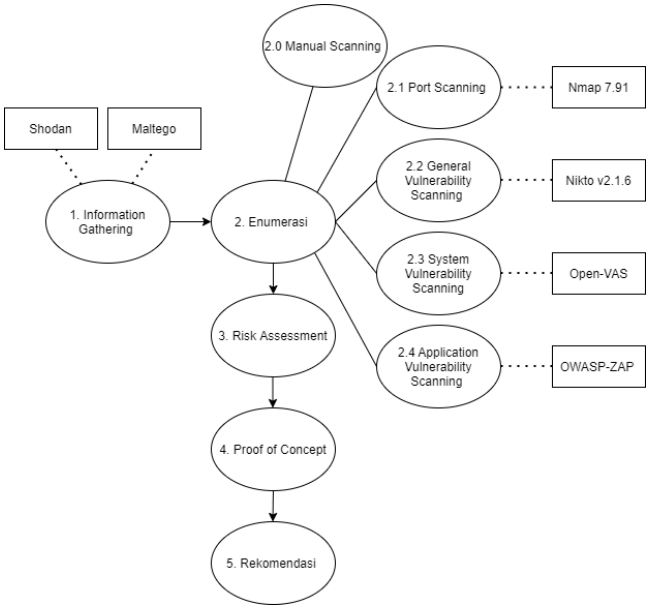
I. PENDAHULUAN

Pesatnya pertumbuhan internet dalam beberapa tahun terakhir telah membawa banyak keuntungan bagi masyarakat modern dalam hal komunikasi dan berbagi informasi. Selain itu, muncul isu-isu baru dan kompleks karena fleksibilitas jaringan, keterbukaan, dan integrasi sistem. Kerentanan sistem adalah dasar dari masalah ini. Sayangnya, kerentanan seperti itu di Internet dapat memengaruhi tidak hanya lingkungan virtual dengan cara yang terisolasi tetapi juga dapat menimbulkan dampak serius di dunia nyata. Itu sebabnya, mengidentifikasi kerentanan sistem merupakan informasi penting bagi pemilik sistem[1]. Pengujian kerentanan sistem umumnya juga melakukan penetrasi yaitu salah satu teknik yang digunakan untuk pengujian keamanan jaringan dan sistem. Dengan melibatkan upaya legal untuk masuk ke jaringan untuk memeriksa kerentanan dan eksploit system yang tersedia, mensimulasikan apa yang mungkin dilakukan oleh peretas. Hal tersebut dapat meningkatkan keamanan jaringan, ketika mencari eksploit dan kerentanan yang ada dalam sistem, maka adanya peluang menemukan cara untuk mengurangi risikonya [2]. Berbagai penelitian pengujian kerentanan pada syste banyak dilakukan seperti pada penelitian PEN Test di E-Government Libya yang menggunakan 3 alat scanner aplikasi web untuk melakukan evaluasi. Hasil dari penelitian adalah sebagian besar situs web pemerintah Libya memiliki kerentanan dan kelemahan keamanan berisiko tinggi, hal ini dapat membantu Pemerintah Libya dalam mengatasi kerentanan tersebut untuk meminimalisir resiko[3]. Studi literatur pada penelitian Vats menyampaikan bahwa PEN Test membantu dalam membingkai & membentuk aspek penting dari parameter keamanan informasi dengan mengidentifikasi kerentanan sistem pada keamanan jaringan secara akurat & efisien. Adapun ditinjau dari strategi PEN Test tedapat variasi yang yang dapat digunakan bergantung kepada spesifik tujuan test [4]. Selain strategi, peneliti Shebli,dkk memahami pentingnya factor-faktor dan komponen yang perlu dipertimbangkan dalam melaksanakan pengujian keamanan siber. Dengan melakukan survey terhadap prosedur, alat, peran penguji dan etika yang harus dimiliki dari tim sehingga dapat meningkatkan kualitas pengujian[5]. Menurut UU ITE, Pemerintah Kabupaten sebagai PSTE (Penyelenggara Sistem dan Transaksi Elektronik) wajib melindungi penggunanya dan masyarakat luas dari kerugian yang ditimbulkan terhadap layanan daring pemerintahan [6]. Akan tetapi, berdasarkan data Badan Siber dan Sandi Negara (BSSN) bahwa aduan tertinggi terkait keamanan siber ada pada sektor pemerintahan sebesar 51% tahun 2020 dan 48% pada tahun 2021 [7][8]. Hal ini yang mendorong pemerintah kabupaten untuk melakukan pengujian kerentanan terhadap sistem yang telah dibuat, sehingga diharapkan dapat mengantisipasi celah keamanan tersebut. Adapun freeware scanning dipilih sebagai alat bantu pengujian, alternatif untuk mengakomodir terbatasnya anggaran.

II. METODE

Metode yang digunakan dalam penelitian ini adalah metode kualitatif dengan melakukan observasi[9]. Mengacu pada spesifik tujuan maka strategi yang digunakan yaitu Blind PEN Testing dengan menggunakan lingkungan asli dari layanan daring pemerintahan kabupaten[4].

Terdiri dari 5 tahapan yaitu Information Gathering, Enumerasi, Pengujian resiko, Pembuktian temuan, serta rekomendasi untuk antisipasi dalam menutup kerentanan yang ada. Berikut adalah tahapan pengujian yang dilakukan



Gambar. 1 Tahapan pengujian

Berikut adalah penjelasan dari masing-masing tahapan.

1. Information Gathering terdiri dari foot printing dan pengintaian aktif. Footprinting (Reconnaissance pasif) adalah segala kegiatan mengumpulkan informasi target yang akan di-hack sistemnya, sebelum melakukan penguasaan sistem sesungguhnya. Pengintaian aktif, sebaliknya, melibatkan penggunaan teknologi dengan cara yang mungkin dideteksi oleh target.
   Setelah informasi berhasil dikumpulkan, maka memungkinkan untuk dibuat peta jaringan yang memetakan host yang sedang hidup, port UDP dan TCP yang terbuka (yang menjadi petunjuk untuk mengetahui jenis aplikasi yang berjalan pada host) dan sistem operasi pada tiap host tersebut. Informasi ini membentuk kerangka pemahaman untuk mengetahui jenis serangan apa yang akan diluncurkan.
2. Enumerasi adalah sebagai proses untuk melakukan koneksi aktif ke host target untuk menemukan potensi vektor-vektor serangan ke dalam sistem. Data yang diperoleh dapat digunakan untuk eksploitasi lebih lanjut terhadap sistem. Pada pengujian ini dilakukan enumerasi melalui empat jenis pengetesan, yaitu Portscanning, General Vulnerability Scanning, System Vulnerability Scanning dan Application Vulnerability Scanning serta Manual scanning.
3. Dari Hasil enumerasi akan diperoleh temuan yang kemudian akan diuji lebih lanjut sesuai dengan pengujian tingkat resiko yang diperoleh dari pada enumerasi. Umumnya pengujian resiko terdiri dari 4 level yaitu informational, low, medium, dan high. Urutan tingkat resiko yang semakin tinggi artinya memiliki potensi yang semakin tinggi dalam mengancam sistem dan jaringan sehingga akan menjadi prioritas.
4. Proof of Concept adalah membuktikan resiko-resiko yang diperoleh apakah sesuai dengan melakukan ekploitasi ke sistem dan jaringan yang dimaksud. Umumnya ada 2 status yaitu false positive artinya informasi kerentanan yang diperoleh dari hasil enumerasi tidak bisa dibuktikan sedangkan true positive berarti sebaliknya yaitu terbukti bahwa kerentanan tersebut dapat diexploit.
5. Rekomendasi adalah memberikan saran perbaikan terhadap kerentanan yang telah diuji tersebut. sehingga level keamanan pada sistem dan jaringan meningkat.

III. HASIL DAN PEMBAHASAN

Hasil dari pengujian kerentanan keamanan layanan daring di Pemerintahan Kabupaten adalah bahwa jaringan yang diuji masuk dalam kategori aman, sedangkan pada aplikasi ditemukan kerentanan yang benilai resiko medium, low, dan informational yang masing – masing sebanyak 6,7, dan 6 kerentanan. Kerentanan yang diperoleh dari alat scanning kemudian dibuktikan menggunakan teknik dan alat hacking dengan masuk ke sistem merujuk temuan kerentanan yang diperoleh sebelumnya. Berikut pembahasan dari setiap tahapan yang dilakukan

A. Information Gathering

Dalam melakukan pengumpulan informasi dilakukan pengintaian pasif dan pengintaian aktif. Pengintaian pasif dilakukan menggunakan shodan.io yang menghasilkan beberapa data penting terkait perangkat-perangkat yang digunakan oleh website target, misalnya sistem operasi yang digunakan, service yang aktif, dsb. Juga sejumlah data terkait potensi-potensi rawan pada target terkait dengan service-service yang digunakan. Sedangkan pada pengintaian aktif yaitu dengan melakukan DNS Zone Transfer dan DNS Lookup, ping sweep, traceroute, port scan, atau mengenali "sidik jari" sistem operasi.

B. Portscanning

Alat *port scanning* yang digunakan pada penelitian ini adalah Nmap 7.91 dengan hasil portscanning menunjukkan bahwa terdapat beberapa port terbuka namun hasilnya tidak dapat mendukung attack terhadap sistem.

C. General Vulnerability Scanning

Pendeteksian keamanan secara umum dilakukan dengan alat Nikto v2.1.6. Nikto adalah alat scanning aplikasi web

yang mencari kesalahan konfigurasi, direktori web diakses secara terbuka dan sejumlah kerentanan aplikasi web.

Hasil penelusuran dengan Nikto umumnya dimulai dengan mentarget alamat IP atau URL dari target, dan kemudian port http/https. Dari hasil scanning tersebut, ditemukan celah keamanan Berikut adalah penjelasan kerentanan pada web yang ditemukan:

1. Clickjacking Attack adalah sebuah kerentanan di mana situs target dapat menjadi umpan untuk memancing pengguna untuk mengklik sebuah link atau button yang seolah-olah berasal dari situs target, padahal sesungguhnya dia sedang menjalankan skrip lain yang bisa jadi berbahaya
2. Server rawan terhadap serangan Breach Attack yang memungkinan pada kondisi web server tertentu (biasanya terkait koding yang kurang aman) penyerang akan dapat mengambil informasi yang sensitif.
3. Beberapa file yang bila diakses terdapat kemungkinan untuk mengekspose data-data sensitif dari server

D. System Vulnerability Scanning

Penelusuran kerentanan keamanan jaringan ini menggunakan alat Open-VAS. Open-VAS selain menelusuri kerentanan dari sisi sistem, meliputi koneksi jaringan dan kerentanan terkait sistem operasi dan server aplikasinya. Resume penelusuran kerentanan keamanan yang diperoleh ditunjukkan gambar berikut.

Host Summary

Host	High	Medium	Low	Log	False Positive
43.249.142.70 (xxx.go.id)		1	1	58	0

Gambar. 21 Resume kerentanan keamanan jaringan dengan Open-Vas

Port yang memiliki ancaman keamanan pada level medium adalah port 443/TCP dengan CVSS: 6.4 dan sumber NVT: SSL/TLS: Missing ‘secure` Cookie Attribute. Dapat disimpulkan bahwa celah medium hanya berkaitan dengan konfigurasi SSL untuk penanganan cookie.

E. Application Vulnerability Scanning

Penelusuran kerentanan terkait aplikasi ini menggunakan alat OWASP-ZAP. Resume penelusuran kerentanan keamanan yang diperoleh ditunjukkan gambar berikut.

Host	High	Medium	Low	Informational	False Positive
43.249.142.70	0	6	7	6	0

Gambar. 3 Resume kerentanan keamanan jaringan dengan OWASP-ZAP

Adapun resiko ancaman yang dihadapi dapat dilihat pada gambar berikut.

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	7
Proxy Disclosure	Medium	14
Reverse Tabnabbing	Medium	2
Sub Resource Integrity Attribute Missing	Medium	4
Vulnerable JS Library	Medium	2
X-Frame-Options Header Not Set	Medium	3
Cookie Slack Detector	Low	14
Cross-Domain JavaScript Source File Inclusion	Low	4
Dangerous JS Functions	Low	1
Feature Policy Header Not Set	Low	9
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	3
Strict-Transport-Security Header Not Set	Low	21
X-Content-Type-Options Header Missing	Low	17
Base64 Disclosure	Informational	2
Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	1
Non-Storable Content	Informational	7
Storable and Cacheable Content	Informational	18
User Agent Fuzzer	Informational	28

Gambar. 4 Resiko/ancaman

Dari hasil scan terhadap kerentanan keamanan, peneliti focus pada level resiko bernilai medium sebanyak 6 kerentanan, berikut adalah detail url (dalam bentuk alias) yang ditunjukkan pada table berikut.

TABEL I
TABEL URL KERENTANAN DENGAN TINGKAT RESIKO MEDIUM

Medium (High)	Content Security Policy (CSP) Header Not Set
URL	https://xxx.go.id/index.php/assets/images/group.png
	https://xxx.go.id/index.php
	https://xxx.go.id/sitemap.xml
	https://xxx.go.id/robots.txt
	https://xxx.go.id/index.php/login/offline
	https://xxx.go.id/index.php/index.php/portal/antrian
	https://xxx.go.id/index.php/
Medium (Medium)	Proxy Disclosure
URL	https://xxx.go.id/index.php/assets/images
	https://xxx.go.id/index.php/portal
	https://xxx.go.id/index.php/mobile
	https://xxx.go.id/index.php/portal/antrian
	https://xxx.go.id/index.php/index.php/portal
	https://xxx.go.id/index.php/index.php
	https://xxx.go.id/index.php/login/offline
	https://xxx.go.id/index.php/portal/pilih
	https://xxx.go.id/index.php/index.php/portal/antrian
	https://xxx.go.id/index.php/login
	https://xxx.go.id/index.php/
	https://xxx.go.id/index.php/assets/images/group.png
	https://xxx.go.id/index.php/assets
	https://xxx.go.id/index.php
Medium (Medium)	Reverse Tab nabbing
URL	https://xxx.go.id/index.php/
	https://xxx.go.id/index.php

Medium (High)	Sub Resource Integrity Attribute Missing
URL	https://xxx.go.id/index.php
	https://xxx.go.id/index.php
	https://xxx.go.id/index.php/
Medium (Medium)	Vulnerable JS Library
URL	https://xxx.go.id/assets/plugins/bootstrap/js/bootstrap.min.js
	https://xxx.go.id/assets/js/vendor-all.min.js
Medium (Medium)	X-Frame-Options Header Not Set
URL	https://xxx.go.id/index.php
	https://xxx.go.id/index.php/
	https://xxx.go.id/index.php/login/offline

Berikut adalah penjelasan dari setiap kerentanan.

1) *Content Security Policy (CSP) Header Not Set*

Content Security Policy (CSP) adalah lapisan keamanan tambahan yang membantu mendeteksi dan mengurangi jenis serangan tertentu, termasuk Cross Site Scripting (XSS) dan serangan injeksi data. Serangan ini digunakan untuk segala hal mulai dari pencurian data hingga perusakan situs atau penyebaran malware. CSP menyediakan sekumpulan header HTTP standar yang memungkinkan pemilik situs web untuk menyatakan sumber konten yang disetujui yang boleh dimuat oleh browser pada halaman tersebut - jenis yang tercakup adalah JavaScript, CSS, bingkai HTML, font, gambar, dan objek yang dapat disematkan seperti applet Java, ActiveX, file audio dan video.

2) *Proxy Disclosure*

Proxy Disclosure adalah kondisi dimana informasi penggunaan proxy dapat diketahui pihak tidak berkepentingan. Dengan adanya mis konfigurasi pada proxy yaitu mengaktifkan metode trace pada server (umumnya metode ini digunakan untuk mencari debug), hal ini memungunkinkan terjadi penelusuran oleh penyerang, misalnya list aplikasi yang pengguna gunakan sehingga membantu penyerang dalam menentukan strategi/metode penyerangan yang akan dilakukan.

3) *Reverse Tabnabbing*

Reverse tabnabbing adalah serangan di mana halaman yang ditautkan dari halaman target dapat menulis ulang halaman tersebut, misalnya untuk menggantinya dengan situs phishing. Karena pengguna pada awalnya berada di halaman yang benar, mereka cenderung tidak menyadari bahwa itu telah diubah menjadi situs phishing, terutama jika situs tersebut terlihat sama dengan target. Jika pengguna mengautentikasi ke halaman baru ini, kredensial mereka (atau data sensitif lainnya) dikirim ke situs phishing, bukan ke situs yang sah.

4) *Sub Resource Integrity Attribute Missing*

Integrity Attribute tidak ada pada skrip atau tag tautan yang disajikan oleh server eksternal. Tag integritas mencegah penyerang yang telah memperoleh akses ke server ini menginjeksi konten berbahaya.

5) *Vulnerable JS Library*

Library yang teridentifikasi berikut: ExampleLibrary, pada versi yang digunakan mengandung kerentanan.

6) *X-Frame-Options Header Not Set*

Clickjacking, juga dikenal sebagai "serangan UI", adalah saat penyerang menggunakan beberapa lapisan transparan atau buram untuk mengelabui pengguna agar mengklik tombol atau link di halaman lain saat user bermaksud mengklik halaman terluar. Karenanya, penyerang "membajak" klik halaman sebenarrnya yang dimaksudkan dan merutekannya ke halaman lain, kemungkinan besar dimiliki oleh aplikasi, domain, atau keduanya.

F. Manual Technique Scanning

Selain dengan menggunakan tools untuk melakukan scanning terhadap kerentanan, penguji juga melakukan penelusuran secara manual dan menemukan kerentanan yang sangat tinggi yaitu SQL Injection.

1) SQL Injection

SQL Injection merupakan teknik eksploitasi dengan cara memodifikasi perintah sql pada form input aplikasi yang memungkinkan penyerang untuk dapat mengirimkan sintaks ke database aplikasi. SQL Injection juga dapat didefinisikan sebagai teknik eksploitasi celah keamanan pada layer database untuk mendapatkan query data pada sebuah aplikasi.

2) Dashboard Admin Dapat di Akses Tanpa Login

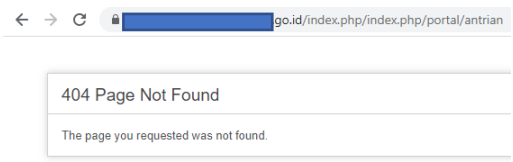
Awal mula didapatkannya celah SQL Injection adalah dapat diaksesnya dashboard admin tanpa harus login terlebih dahulu melalui tautan https://xxx.go.id/index.php/pengguna/operator dan mendapatkan error message “A PHP Error was encountered” pada halaman operator.

G. Proof of Concept

Dalam membuktikan temuan kerentanan yang diperoleh dari alat yang digunakan, maka dilakukan ekploitasi terhadap masing-masing kerentanan yang memiliki nilai resiko Medium, yaitu sebagai berikut.

1) Content Security Policy (CSP) Header Not Set

Hasil percobaan ekploitasi dari url yang terpindai beresiko adalah “page not found” menunjukkan bahwa temuan kerentanan ini hanya *false positive*, seperti yang ditunjukkan gambar berikut.



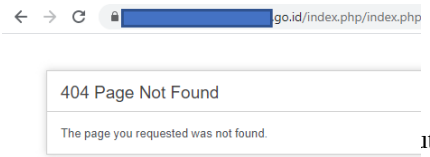
2) Proxy Disclosure

Hasil percobaan ekploitasi dari url yang terpindai beresiko adalah “no cache” menunjukkan bahwa temuan kerentanan ini hanya *false positive*, seperti yang ditunjukkan gambar berikut.

```
HTTP/1.1 200 OK
Date: Tue, 11 May 2021 17:23:04 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=5227u1qbdrff66kortjkt1obfs8n85g0;
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
```

3) Reverse Tabnabbing

Hasil percobaan ekploitasi dari url yang terpindai beresiko adalah “page not found” menunjukkan bahwa temuan kerentanan ini hanya *false positive*, seperti yang ditunjukkan gambar berikut.



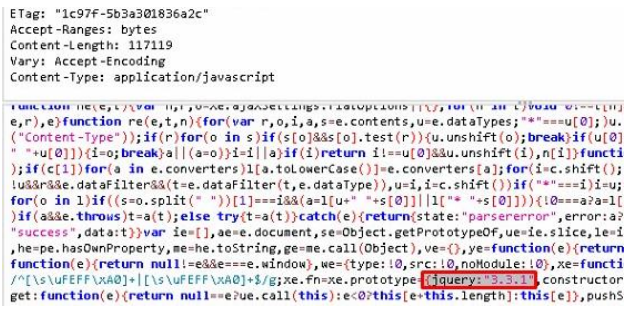
ıte Missing

Hasil percobaan ekploitasi dari url yang terpindai beresiko menunjukkan bahwa kerentanan ini hanya *false positive*, dimana scanner owasp mendeteksi adanya sumber link, seperti yang terlihat pada gambar dibawah ini.

Gambar

5) Vulnerable JS Library

Hasil percobaan ekploitasi dari url yang terpindai beresiko menunjukkan bahwa kerentanan ini hanya *false positive*, dimana scanner owasp mendeteksi adanya versi javascript yang tidak update, seperti yang terlihat pada gambar dibawah ini.



6) Clickjacking Attack

Percobaan Clickjacking dilakukan dengan membuat skrip HTML sebagai berikut:

```
Clickjacking
</tittle>
<style type="text/css">
<!--
body {background: #D7E7F5 no-repeat fixed center;}
-->
</style>
<center>
        <h4> POC Clickjacking<br>
                Untuk melanjutkan layanan kami, anda perlu persetujuan account bank
anda<br>
                1. Pastikan anda login dengan account Bank anda<br>
                2. CLICK DOWNLOAD<br>
                ANDA AKAN MENDAPAT File YANG ANDA INGINKAN<br>
        </h4>
        </h2>
                CATATAN: KOLOM SUDAH DIPROVACY HARAP PASTEKAN DENGAN HATI-HATI !
        </h2>
</center>
<form action=http://localhost:4000/">
<input align="left" style="position:absolute;top:230px;left:660px"
        name="Rekening" value=""><br>
```

Gambar

Ketika dijalankan, maka akan muncul halaman yang menampakkan situs layanan daring pemerintah kabupaten sebagai background, sehingga user dapat beranggapan bahwa halaman tersebut asli.

7) SQL Injection

Eksploitasi teknik sql injection dilakukan dengan bantuan alat BurpSuites dan SQLmap. Dari proses tersebut penguji mendapatkan data dari database yang terdapat pada situs pemerintah kabupaten. Tahapan eksploitasi database diawali dari Daftar Database kemudian ke Daftar Tabel selanjutnya membuka Struktur Tabel tb_user, dan terakhir tabel user: admin passwordnya. Berikut hasil ekploitasi dari database table admin.

Dari data tersebut didapatkan informasi username administrator yaitu admin@gmail.com dengan password yang telah dihash menggunakan MD5. Password MD5 tersebut dapat di-"decrypt" oleh penguji dengan bantuan website penyedia decryptor untuk hash MD5. Setelah didekripsi penguji mendapatkan password administrator adalah "admin" seperti dapat dilihat pada gambar berikut.

H. Recommendation

Dari 7 kerentanan yang dibuktikan untuk memastikan hasil scanning, ditemukan 2 kerentanan bernilai positif yaitu clikjacking dan SQL Injection. Berikut adalah rekomendasi dalam upaya antisipasi terhadap kerentanan tersebut.

1. Antisipasi terhadap kerentanan ClickJacking Attack dapat dilakukan dengan 2 strategi, yaitu mengatur Content Security Policy: frame-ancestors dan mengatur header X-Frame Respose
2. Antisipasi terhadap kerentanan SQL Injection adalah dengan memperbaiki code dan pembatasan akses tanpa login

IV. SIMPULAN

Dalam rangka meningkatkan keamanan sistem layanan daring di Pemerintahan Kabupaten, dilakukan pengujian kerentanan dengan strategi Blind PEN Testing. Pengujian ini melibatkan serangkaian alat *freeware* seperti Shodan, Malgeto, Nmap, Nikto, Open-Vas, dan OWASP-Zap. Proses pengujian meliputi lima tahapan utama: pengumpulan informasi, enumerasi, penilaian risiko, bukti konsep, dan rekomendasi. Dari hasil pengujian, terdapat temuan kerentanan khususnya pada sisi aplikasi dan web, termasuk serangan Zone Transfer, ClickJacking, dan SQL Injection. Temuan ini menekankan pentingnya pengujian keamanan, khususnya di sektor pemerintahan, untuk mengidentifikasi dan mengatasi potensi risiko.

Dalam konteks yang lebih luas, pesatnya pertumbuhan internet telah meningkatkan kompleksitas isu-isu keamanan. Meskipun ada manfaat yang signifikan dari konektivitas online, ada juga risiko keamanan yang harus diperhatikan. Oleh karena itu, pengujian seperti ini adalah langkah penting untuk memastikan bahwa sistem yang rentan dapat ditemukan dan diperbaiki sebelum mereka dieksploitasi oleh pihak yang tidak berwenang.

UCAPAN TERIMA KASIH / ACKNOWLEDGMENT

Peneliti mengucapkan terima kasih kepada pihak-pihak yang membantu dalam pengembangan penelitian ini.

REFERENSI

[1] Andrea Tundis, Wojciech Mazurczyk, and Max Mühlhäuser. 2018. A review of network vulnerabilities scanning tools: types, capabilities and functioning. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). Association for Computing Machinery, New York, NY, USA, Article 65, 1–10. https://doi.org/10.1145/3230833.3233287.

[2] Kumar, R., Tlhagadikgora, K. (2019). Internal Network Penetration Testing Using Free/OpenSource Tools: Network and System Administration Approach. In: Luhach, A., Singh, D., Hsiung, PA., Hawari, K., Lingras, P., Singh, P. (eds) Advanced Informatics for Computing Research. ICAICR 2018. Communications in Computer and Information Science, vol 956. Springer, Singapore. https://doi.org/10.1007/978-981-13-3143-5_22

[3] Masoud, Rabia & Mohd Alwi, Najwa. (2013). Penetration testing for libyan government website.

[4] Vats, P., Mandot, M., & Gosain, A. (2020, June). A comprehensive literature review of penetration testing & its applications. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 674-680). IEEE.

[5] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018, pp. 1-7, doi: 10.1109/LISAT.2018.8378035.

[6] Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik Pasal 31.

[7] Badan Siber dan Sandi Negara, Laporan Tahunan Monitoring Keamanan Siber Tahun 2020, https://www.bssn.go.id/laporan-tahunan-monitoring-keamanan-siber-tahun-2020/ diakses 22 Mei 2023, pk 12.06.

[8] Badan Siber dan Sandi Negara, Laporan Tahunan Monitoring Keamanan Siber Tahun 2021, https://www.bssn.go.id/laporan-tahunan-monitoring-keamanan-siber-tahun-2021/ diakses 22 Mei 2023, pk 02.44.

[9] Creswell, J. W. (2010). Research design: pendekatan kualitatif, kuantitatif, dan mixed. Yogjakarta: PT Pustaka Pelajar.