Ethical Hacking
Penetration Testing Report

Oleh:
Marselinus Krisnawan Riandika
5027221056

Table of Contents

Assessment Overview **3**
Scope **3**
Scope Exclusions 4
Client Allowances 4
Executive Summary **5**
Attack Summary 5
Additional Reports and Scans (Informational) 10

Assessment Overview

Pengerjaan Pentesting ini dilakukan dari tanggal 5 Mei 2024 hingga 8 Mei 2024. Pentesting ini dilakukan guna mengevaluasi keamanan sistem dan jaringan dari ip yang telah diberikan menggunakan teknik penetration testing untuk mengidentifikasi potensi kerentanan dan mendapatkan pemahaman yang komprehensif tentang tingkat keamanan.

Terdapat beberapa fase yang akan dilakukan yaitu :

1. **Planning:** Tahap ini melibatkan pembuatan rencana penilaian yang mencakup penetapan sasaran, tujuan, dan metode yang akan digunakan selama penilaian.
2. **Discovery:** Pada fase ini, dilakukan pencarian dan pengumpulan informasi tentang target yang akan dievaluasi.
3. **Attack:** Tahap ini merupakan implementasi dari serangan terhadap sistem dan jaringan dengan tujuan untuk menguji keamanan dan mencari potensi kerentanan yang dapat dieksploitasi.
4. **Reporting:** Setelah tahap penilaian selesai, hasilnya akan didokumentasikan dalam laporan yang mencakup temuan kerentanan, rekomendasi perbaikan, dan kesimpulan dari penilaian tersebut.

Scope

Terdapat beberapa ip yang akan dicoba untuk dilakukan pentesting :

- 10.15.42.36
- 10.15.42.7

Scope Exclusion

Untuk pengecualian, kegiatan pentesting ini tidak akan melakukan hal yang akan mengubah atau merusak susnan atau bentuk dari tampilan asli dari ip tersebut.

Scope Allowances

Tidak dijelaskan secara detail tentang hal hal yang diperkenankan untuk dilakukan pada tes ini

Executive Summary

Berdasarkan dari percobaan yang telah dilakukan dari tanggal 5 Mei 2024 hingga 8 Mei 2024, didapatkan beberapa informasi yang diperoleh

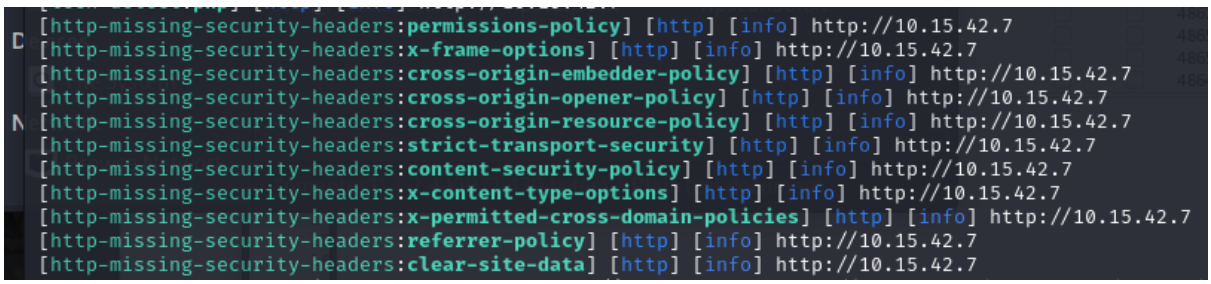
Attack Summary

Tabel dibawah akan menjelaskan apa saja yang telah dilakukan selama Pentesting

No	Tindakan	Detail
1	Melakukan Reconnaissance	1. Menggunakan NMAP untuk melihat port dan sebagainya 2. Menggunakan dirb untuk melihat direktori
2	Vulnerabilities Assessment	1. Menggunakan Nuclei untuk melihat vulnerabilities 2. Menggunakan WPScan untuk melihat vulnerabilities pada
3	Mencoba login	1. mencoba login ke website dengan menggunakan burp suite

Test Findings

1. **Missing security Header**



Terdapat beberapa 'http missing security Headers', beberapa security headers ini dapat membuat aplikasi rentan terhadap beberapa jenis serangan dan ancaman keamanan seperti:

1. **Masalah Cross-Origin Resource Sharing (CORS)**: Ketidakadaan kebijakan sumber daya Cross-Origin (CORP) dan kebijakan embedder Cross-Origin (COEP) yang tepat dapat menyebabkan serangan Cross-Origin, di mana skrip jahat dari asal lain dapat mengakses data sensitif atau melakukan tindakan yang tidak sah atas nama pengguna.
2. **Kerentanan Clickjacking**: Tanpa header X-Frame-Options, situs web menjadi rentan terhadap serangan clickjacking, di mana penyerang dapat menyematkan situs dalam bingkai pada halaman berbahaya, menipu pengguna untuk melakukan tindakan yang tidak diinginkan.
3. **Serangan Cross-Site Scripting (XSS)**: Kebijakan Keamanan Konten (CSP) sangat penting untuk memitigasi serangan XSS dengan menentukan serangkaian sumber konten yang harus dipercayai oleh peramban. Tanpanya, penyerang dapat menyisipkan skrip jahat ke dalam aplikasi web, yang dapat menyebabkan pencurian data, perampasan sesi, atau perusakan tampilan.
4. **Serangan Man-in-the-Middle**: Ketidakadaan Strict Transport Security (HSTS) memungkinkan penyerang untuk mencegat komunikasi antara pengguna dan server, yang berpotensi menyebabkan penyadapan data, pemalsuan, atau perwakilan.
5. **Pengungkapan Informasi**: Ketidakhadiran header keamanan seperti Referrer-Policy dan Clear-Site-Data dapat menyebabkan kebocoran informasi, di mana data sensitif seperti URL, informasi pengarah, atau data situs terbuka kepada pihak yang tidak berwenang, membantu penyerang dalam rekognisi atau serangan yang ditargetkan.
6. **Sniffing Tipe Konten**: Ketidakadaan header X-Content-Type-Options dapat menyebabkan serangan sniffing tipe konten, di mana peramban menimpa tipe konten yang dideklarasikan dan menginterpretasikan konten berdasarkan algoritma mereka sendiri, yang berpotensi menyebabkan kerentanan keamanan.

2. **Exposed User**

```
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
```

command tersebut menunjukkan bahwa sebuah alamat IP (10.15.42.7) memiliki endpoint untuk mengambil daftar pengguna WordPress (usernames) yang terdaftar di situs WordPress pada alamat tersebut. Dalam contoh ini, hanya satu pengguna ("admin") yang terdaftar.

Ini bisa menjadi masalah keamanan karena memberikan informasi sensitif kepada penyerang potensial. Dengan mengetahui username dari pengguna yang ada, penyerang dapat mencoba metode serangan seperti serangan brute-force untuk mencoba menebak kata sandi pengguna tersebut. Oleh karena itu, penting untuk meminimalkan informasi sensitif yang terpapar, termasuk daftar pengguna yang terdaftar.

3. **CVE-2023-48795**

```
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
```

Command tersebut menyiratkan bahwa alamat IP 10.15.42.7 dengan port 22 rentan terhadap CVE-2023-48795, yang dikenal dengan nama "Terrapin". Dalam konteks ini, "Terrapin" mungkin merujuk pada jenis serangan atau celah keamanan tertentu yang dieksploitasi dengan memanfaatkan CVE tersebut.

4. **WP-Cron**

```
[+] The external WP-Cron seems to be enabled: http://10.15.42.7/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

Aktivasi WP-Cron yang eksternal dapat memiliki beberapa implikasi keamanan dan kinerja:

1. Potensi untuk Penyerangan: Penyerang dapat menyalahgunakan WP-Cron yang eksternal untuk meluncurkan serangan penolakan layanan (DoS) dengan membebani server dengan permintaan cron yang berlebihan atau dengan mengirimkan permintaan cron palsu yang memicu tugas yang tidak diinginkan atau berat.
2. Ketergantungan pada Sumber Eksternal: Mengandalkan WP-Cron yang eksternal berarti bahwa keterandalan dan kinerja tugas terjadwal tergantung pada ketersediaan dan kinerja sumber eksternal. Jika ada gangguan pada sumber eksternal atau jaringan, tugas-tugas terjadwal mungkin gagal atau terlambat.
3. Potensi Kerentanan: Jika ada celah keamanan dalam implementasi WP-Cron atau di server yang menjalankannya, WP-Cron yang eksternal dapat menjadi sasaran eksploitasi, memberikan penyerang akses atau kendali yang tidak sah.

5. **XML-RPC**

```
[+] XML-RPC seems to be enabled: http://10.15.42.7/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

Aktivasi XML-RPC dapat memiliki beberapa implikasi keamanan:

- Potensi untuk Serangan Brute-Force: Penyerang dapat menggunakan XML-RPC untuk melakukan serangan brute-force pada akun pengguna WordPress dengan mencoba berbagai kombinasi nama pengguna dan kata sandi.
- Potensi untuk Serangan DoS: XML-RPC dapat disalahgunakan untuk meluncurkan serangan penolakan layanan (DoS) dengan mengirimkan permintaan yang berlebihan dan membebani server.

- Potensi untuk Eksploitasi: Jika ada kerentanan keamanan dalam implementasi XML-RPC atau plugin yang menggunakannya, penyerang dapat memanfaatkannya untuk mendapatkan akses tidak sah atau mengambil alih situs WordPress.

Additional Reports and Scans (Informational)

Beberapa Hasil dari pengetesan telah dilampirkan pada github

Last Page