

CyberShield

Security Assessment Findings Report

Business Confidential

Date: May 08th, 2024
Report Prepared By: CyberShield
Version 1.0

Table of Contents

Table of Contents	2
Pernyataan Kerahasiaan	3
Penafian	3
Ikhtisar Penilaian.....	4
Komponen Penilaian	4
Uji Penetrasi Eksternal	4
Penemuan Tingkat Keparahan.....	5
Jangkauan	6
Pengecualiaan Lingkup	6
Tunjangan Klien.....	6
Ringkasan Singkat.....	7
Ringkasan Serangan	7
Temuan Uji Penetrasi Eksternal	9

Pernyataan Kerahasiaan

Dokumen ini adalah properti eksklusif dari FortifyTech dan CyberShield. Dokumen ini mengandung informasi properti dan rahasia. Penggandaan, redistribusi, atau penggunaan, baik secara keseluruhan maupun sebagian, dalam bentuk apapun, memerlukan persetujuan dari kedua FortifyTech dan CyberShield.

CyberShield dapat membagikan dokumen ini kepada pihak auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan kebutuhan uji penetrasi.

Penafian

Uji penetrasi dianggap sebagai gambaran pada suatu waktu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

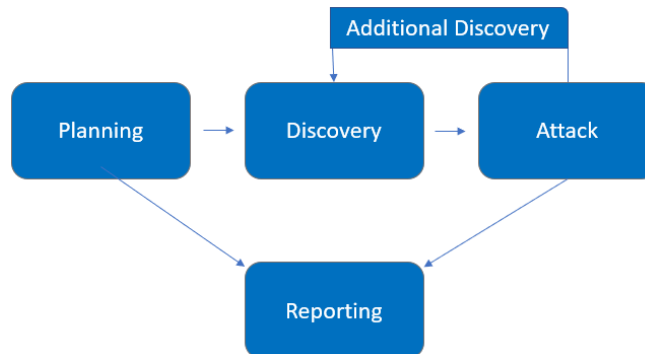
Keterlibatan yang terbatas waktu tidak memungkinkan untuk evaluasi penuh dari semua kontrol keamanan. CyberShield memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan yang paling lemah yang akan dieksploitasi oleh penyerang. CyberShield merekomendasikan untuk melakukan penilaian serupa secara tahunan oleh penilai internal atau pihak ketiga untuk memastikan kesuksesan berkelanjutan dari kontrol-kontrol tersebut.

Ikhtisar Penilaian

Mulai dari 05 Mei 2024 hingga 08 Mei 2024, FortifyTech melibatkan CyberShield untuk mengevaluasi posisi keamanan infrastrukturnya. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis terbaik untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka pengujian yang disesuaikan.

Fase-fase kegiatan uji penetrasi meliputi hal-hal berikut:

- Perencanaan – Tujuan pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Discovery – Melakukan pemindaian dan enumerasi untuk mengidentifikasi kerentanan potensial, area yang lemah, dan eksploitasi.
- Serangan – Mengonfirmasi kerentanan potensial melalui eksploitasi dan melakukan discovery tambahan saat akses baru diperoleh.
- Pelaporan – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, percobaan gagal, serta kekuatan dan kelemahan perusahaan.



Komponen Penilaian

Uji Penetrasi Eksternal

Uji penetrasi eksternal mensimulasikan peran seorang penyerang yang berusaha untuk mendapatkan akses ke jaringan internal tanpa sumber daya internal atau pengetahuan internal. Seorang dari tim CyberShield berusaha untuk mengumpulkan informasi sensitif melalui intelijen sumber terbuka (OSINT), termasuk informasi username/email, kata sandi yang rentan dan dapat dimanfaatkan untuk mendapatkan akses jaringan internal.

Penemuan Tingkat Keparahan

Tabel berikut menentukan tingkat keparahan dan rentang skor CVSS yang digunakan dalam dokumen ini untuk menilai kerentanan dan dampak risiko.

Keparahan	CVSS V3 Score Range	Definisi
Critical	9.0-10.0	Pemanfaatan mudah dilakukan dan biasanya mengakibatkan kompromi tingkat sistem. Disarankan untuk membentuk rencana tindakan dan memperbarui segera.
High	7.0-8.9	Pemanfaatan lebih sulit namun dapat menyebabkan hak istimewa yang ditingkatkan dan potensial kehilangan data atau waktu henti. Disarankan untuk membentuk rencana tindakan dan memperbarui sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah tambahan seperti rekayasa sosial. Disarankan untuk membentuk rencana tindakan dan memperbarui setelah masalah prioritas tinggi telah diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membentuk rencana tindakan dan memperbarui selama jendela pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan yang ada. Informasi tambahan disediakan mengenai item yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Jangkauan

Assessment	Details
External Penetration Test	10.15.42.36, 10.15.42.7

Pengecualiaan Lingkup

Sesuai permintaan klien, CyberShield tidak melakukan serangan Denial of Service selama pengujian.

Tunjangan Klien

FortifyTech tidak memberikan tunjangan apa pun untuk membantu pengujian.

Ringkasan Singkat

Selama periode penilaian, CyberShield melakukan uji penetrasi eksternal pada infrastruktur FortifyTech. Penilaian bertujuan untuk mengidentifikasi kerentanan dalam lingkup yang disediakan. Temuan yang disajikan dalam laporan ini menguraikan risiko keamanan potensial dan rekomendasi untuk penanganan.

Ringkasan Serangan

Step	Aksi	Rekomendasi
1	<ul style="list-style-type: none">- Menggunakan nmap -Pn 10.15.42.36 untuk memindai target.- Menemukan port terbuka 21, 8888 di 10.15.42.36.- Mengidentifikasi halaman login pada port 8888.- Mencoba akses FTP ke 10.15.42.36 dengan kredensial anonim.- Menggunakan github.com/3ndG4me/KaliLists untuk menghasilkan daftar kata untuk gobuster.- Mengungkapkan endpoint /server-status, yang tidak dapat diakses karena akses terlarang.	Manajemen Pembaruan: Terapkan pembaruan secara teratur untuk mengatasi kerentanan dalam perangkat lunak dan layanan.
2	<ul style="list-style-type: none">- Menggunakan gobuster untuk menemukan /server-status.- Menggunakan nuclei untuk pemindaian kerentanan yang lebih dalam pada port 10.15.42.36.	Kontrol Akses: Tinjau dan batasi izin akses ke endpoint sensitif seperti /server-status.

3	<ul style="list-style-type: none"> - Menemukan instalasi WordPress pada port 10.15.42.36. - Mengidentifikasi endpoint /wp-admin/ melalui robots.txt. - Prompt login WordPress memerlukan kredensial yang valid. 	<p>Keamanan WordPress:</p> <ul style="list-style-type: none"> - Pastikan instalasi WordPress tetap diperbarui dengan pembaruan keamanan terbaru. - Terapkan kebijakan kata sandi yang kuat dan pertimbangkan otentikasi dua faktor untuk login WordPress. <p>Segmentasi Jaringan:</p> <p>Terapkan segmentasi jaringan yang tepat untuk membatasi akses tidak sah ke sistem kritis.</p>
---	--	--

Temuan Uji Penetrasi Eksternal

IP: 10.15.42.36

Reconnaissance

1. Pemindaian dengan Nmap

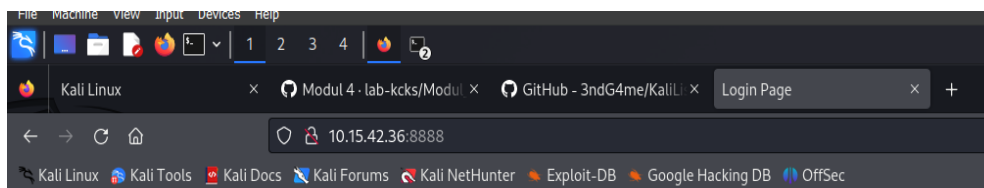
Dilakukan pemindaian menggunakan perangkat lunak nmap tanpa ping (-Pn) pada alamat IP target 10.15.42.36.

```
(root@kali)-[/home]
# nmap -Pn 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 11:49 EDT
Nmap scan report for 10.15.42.36
Host is up (0.060s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
8888/tcp   open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
```

2. Analisis Port

Ditemukan bahwa port 21 dan 8888 terbuka pada alamat IP 10.15.42.36. Pada port 8888, ditemukan sebuah halaman login.



Login

Username:

Password:

3. Percobaan FTP

Dilakukan percobaan akses FTP ke alamat IP 10.15.42.36 dengan menggunakan kredensial anonim.

```
or 221 Goodbye. Memory Storage Accessibility
(root@kali)-[/home]
# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4. Eksploitasi GitHub:

Percobaan untuk mengkloning repository dari GitHub (github.com/3ndG4me/KaliLists) guna mendapatkan daftar kata untuk penggunaan selanjutnya dengan perangkat gobuster.

```
root@kali: /home/kali/Documents/KaliLists/dirbuster
File Actions Edit View Help
Error: error on running gobuster: unable to connect to http://10.15.42.36:8888/: Get "http://10.15.42.36:8888/": dial tcp 10.15.42.36:8888: connect: connection refused
(root@kali)-[/home/kali/Documents/KaliLists/dirbuster]
# gobuster dir -u http://10.15.42.36:8888/ -w /home/kali/Documents/KaliLists/dirbuster/directory-list-2.3-medium.txt -o /home/kali/Documents/Output.log

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.15.42.36:8888/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/Documents/KaliLists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

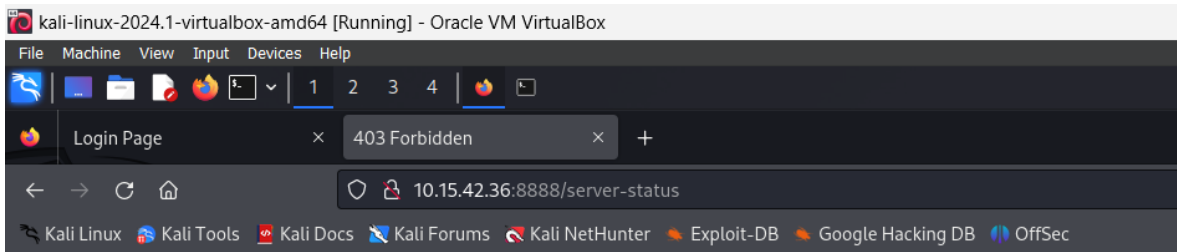
Progress: 20957 / 220561 (9.50%) [ERROR] Get "http://10.15.42.36:8888/7631": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.15.42.36:8888/7437": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.15.42.36:8888/Driver": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/server-status (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)

Finished

(root@kali)-[/home/kali/Documents/KaliLists/dirbuster]
```

5. Penemuan Endpoint /server-status:

Ditemukan adanya endpoint /server-status, namun akses ke endpoint tersebut ditolak (forbidden).



Forbidden

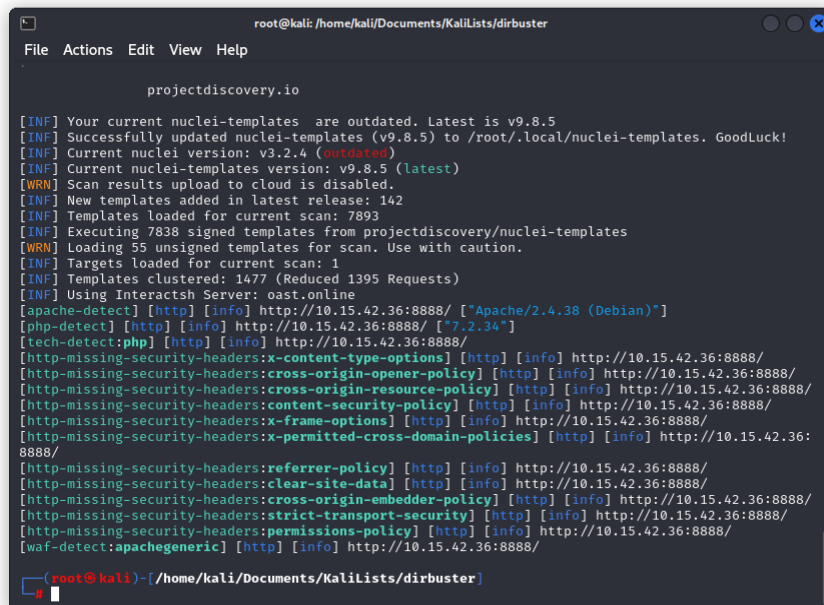
You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 10.15.42.36 Port 8888

Ketika didapatkan **port 10.15.42.36/server-status**, didapatkan forbidden, yang dimana tidak punya akses untuk mengakses endpoints tersebut

6. Penggunaan Gobuster dan Nuclei:

Dilakukan penggunaan perangkat Gobuster dan Nuclei untuk mendalami kerentanan yang mungkin ada pada port 10.15.42.36.



7. Analisis Log

Dari hasil Gobuster dan Nuclei, diperoleh log yang mencerminkan potensi kerentanan dan informasi terkait.

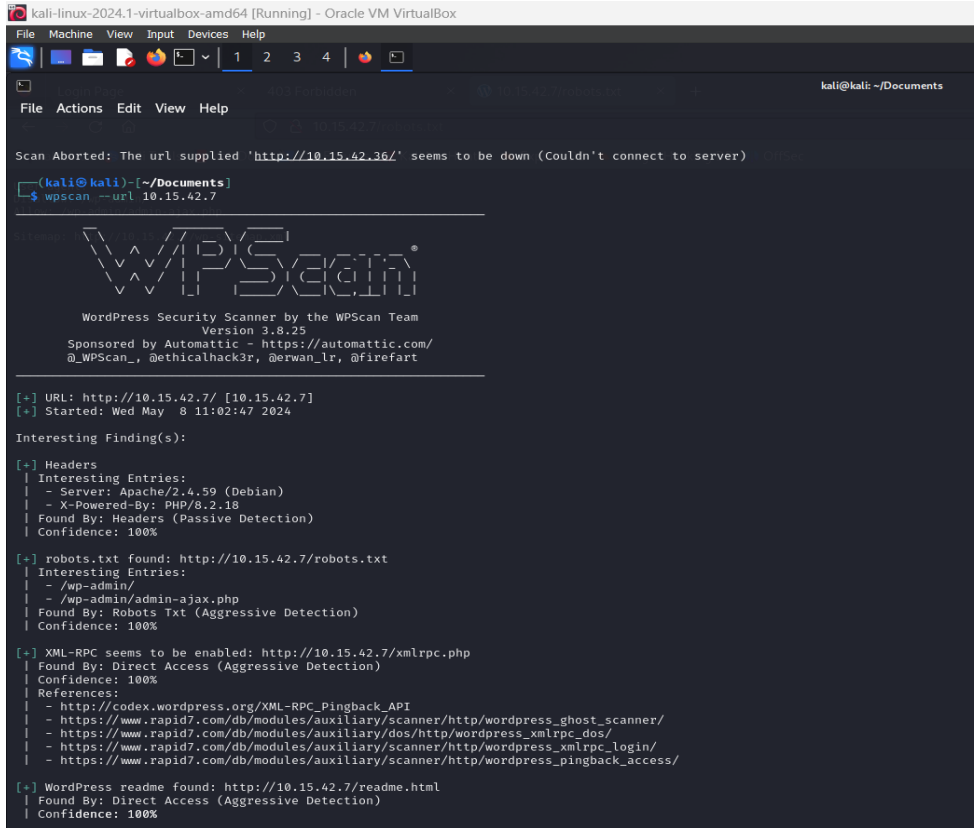
```
(kali㉿kali)-[~/Documents]
$ cat dataLog.txt
[apache-detect] [http] [info] http://10.15.42.36:8888/ ["Apache/2.4.38 (Debian)"]
[php-detect] [http] [info] http://10.15.42.36:8888/ ["7.2.34"]
[tech-detect:php] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888/
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888/
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888/

(kali㉿kali)-[~/Documents]
$ cat Output.log
/server-status (Status: 403) [Size: 278]
```

8. Percobaan WPScan

Dilakukan percobaan WPScan untuk mengidentifikasi potensi kerentanan pada sistem.

Ditemukan instalasi WordPress pada port 10.15.42.36 dengan adanya robots.txt yang merujuk ke endpoint /wp-admin/.



```
kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/Documents
File Actions Edit View Help

Scan Aborted: The url supplied 'http://10.15.42.36/' seems to be down (Couldn't connect to server)

(kali@kali) - [~/Documents]
$ wpscan --url 10.15.42.7

  W P S C A N
  W O R D P R E S S
  S E C U R I T Y

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://10.15.42.7/ [10.15.42.7]
[+] Started: Wed May  8 11:02:47 2024

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.59 (Debian)
| - X-Powered-By: PHP/8.2.18
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://10.15.42.7/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] 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/

[+] WordPress readme found: http://10.15.42.7/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

Kesimpulan:

Pada pencarian kerentanan mengidentifikasi beberapa kerentanan dalam infrastruktur FortifyTech, termasuk port terbuka, masalah kontrol akses, dan kekhawatiran keamanan WordPress. Sangat penting bagi FortifyTech untuk segera mengambil tindakan untuk menangani temuan ini guna melindungi infrastruktur FortifyTech dari potensi pelanggaran keamanan. CyberShield tersedia untuk memberikan bantuan dan panduan lebih lanjut dalam menerapkan langkah-langkah keamanan yang direkomendasikan.

