FortifyTech

Security Assessment Findings Report

Date: May 8th, 2024

Assessment Overview

Client: FortifyTech

Assessment Date: 5 - 8 May 2024

Assessment Team: Mutiara Nurhaliza

Objective: The objective of this security assessment is to identify and analyze potential vulnerabilities within FortifyTech's infrastructure, with a focus on the specified IP addresses: 10.15.42.36 and 10.15.42.7. By conducting a series of ethical hacking techniques and penetration testing, the goal is to uncover weaknesses that could pose a risk to the confidentiality, integrity, and availability of FortifyTech's systems and data.

Scope:

- 10.15.42.36
- 10.15.42.7

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Executive Summary

The objective of the security assessment conducted for FortifyTech was to identify and evaluate potential vulnerabilities within their infrastructure, focusing on the specified IP addresses: 10.15.42.36 and 10.15.42.7. Through ethical hacking techniques and penetration testing, our goal was to assess the security posture of FortifyTech's systems and provide actionable recommendations for improvement.

Attack Summary

Key Finding: Discovery of Vulnerabilities in FortifyTech's Web Application

1. Login Page Discovery:
    - During the reconnaissance phase, a login page was identified on the FortifyTech web application following Nmap scanning. The presence of this login page indicates a potential access point for authenticated users to access sensitive information or perform actions within the application.
2. Failed Credential Acquisition:
    - Despite the identification of the login page, attempts to obtain login credentials were unsuccessful. This highlights a potential weakness in the authentication mechanism, as it did not allow for unauthorized access via default or weak credentials.
3. Web Application Enumeration:
    - Enumeration of the web application revealed the presence of an XML sitemap and robots.txt file. These resources provide insight into the structure and content of the web application, potentially aiding attackers in identifying additional attack vectors or sensitive areas.
4. Outdated WordPress Plugin:
    - Analysis of the web application also uncovered the presence of the WordPress Forminator plugin, version 1.24.6. This version is known to be outdated, posing security risks such as vulnerabilities and exploits that could be leveraged by attackers to compromise the integrity and confidentiality of the application.

Recommendations:

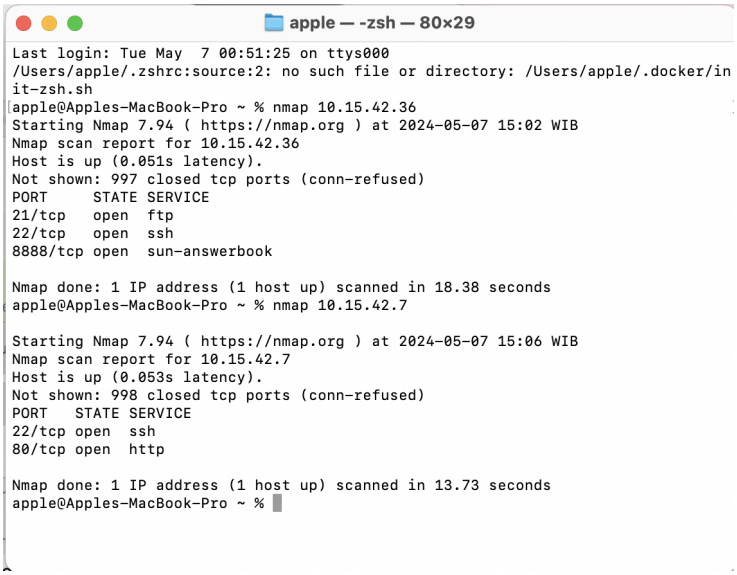
1. Credential Management:
    - FortifyTech should review and strengthen its authentication mechanisms to prevent unauthorized access. This includes implementing secure password policies, multi-factor authentication, and regular password audits to mitigate the risk of credential-based attacks.
2. Web Application Security Updates:
    - Immediate action should be taken to update the WordPress Forminator plugin to the latest version or consider alternative solutions if support for the current

version is discontinued. Regularly monitoring for plugin updates and applying patches promptly is crucial to mitigate known vulnerabilities.

3. Enhanced Web Application Security:
    - Conduct regular security assessments, including vulnerability scanning and penetration testing, to identify and remediate potential weaknesses in the web application. This proactive approach will help fortify the application against emerging threats and ensure robust security posture.

Additional Reports and Scans (Informational)

1. nmap scan



2. Wordpress scan

```
 | 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_ghos
t_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_d
os/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlr
pc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ping
back_access/

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

[+] 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

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</gen
erator>
 |  - http://10.15.42.7/comments/feed/, <generator>https://wordpress.org/?v=6
.5.2</generator>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
```

```
[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and
applicable to any website. Its collecti ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match:
'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02 <> (100 / 137) 72.99%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (101 / 137) 73.72%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (105 / 137) 76.64%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (106 / 137) 77.37%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (110 / 137) 80.29%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (111 / 137) 81.02%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (114 / 137) 83.21%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (116 / 137) 84.67%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (118 / 137) 86.13%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:02 <> (119 / 137) 86.86%  ETA: 00:00:0
```

3. Nuclei scan

```
┌──(mutiara㉿kali)-[~]
└─$ nuclei -u 10.15.42.36:8888 -o result.txt

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.1.10

                projectdiscovery.io

[INF] Current nuclei version: v3.1.10 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7947 signed templates from projectdiscovery/nuclei-templates
[WRN] Executing 55 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1479 (Reduced 1399 Requests)
[INF] Using Interactsh Server: oast.online
[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:strict-transport-security] [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-content-type-options] [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:permissions-policy] [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:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888/
```

4. Nikto scan

```
┌──(mutiara㉿kali)-[~]
└─$ nikto -h 10.15.42.36:8888
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.15.42.36
+ Target Hostname:    10.15.42.36
+ Target Port:        8888
+ Start Time:         2024-05-07 12:11:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cau
se false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-05-07 12:26:02 (GMT-4) (898 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```