FortifyTech
Ethical Hacking 2nd Lab Work

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of CyberShield and FortifyTech. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CyberShield and FortifyTech

CyberShield may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberShield prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberShield recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

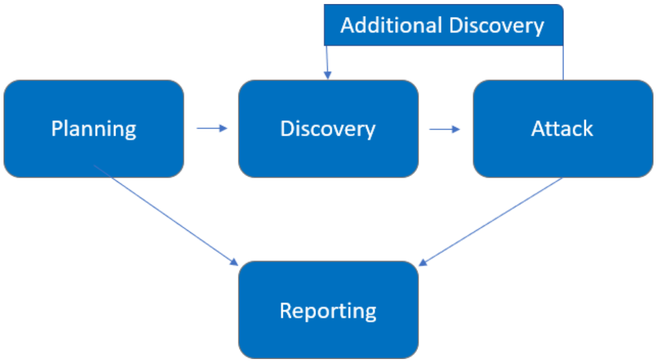
Name	Title	Contact Information
ITS Information Technology Student		
Sighra Attariq	Student	Email: sighraattariq@gmail.com

Assessment Overview

From May 5th, 2024 to May 8th, 2024, CyberShield engaged FortifyTech to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

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.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

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.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	• 10.15.42.36 • 10.15.42.7

Scope Exclusions

Per client request, CyberShield did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by FortifyTech.

Client Allowances

FortifyTech provided CyberShield the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

CyberShield evaluated FortifyTech's internal security posture through penetration testing from May 5th, 2024 to May 8th, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for four (4) business days.

Testing Summary

The network assessment evaluated FortifyTech's internal network security posture. From an internal perspective, the CyberShield team performed vulnerability scanning against the two IPs provided by FortifyTech to evaluate the overall patching health of the network. Beyond vulnerability scanning, the CyberShield evaluated other potential risks.

CyberShield team discovered that there are vulnerabilities inside the IP address 10.15.42.7 (Hello World Wordpress Website). Vulnerability scanning has shown that there are multiple security headers missing. Scans have also shown that there exist vulnerabilities to Terrapin within the website (CVE-2023-48795).

Ultimately, these vulnerabilities have not been exploited and examined properly since the team did not succeed in proving the authenticity of risks that could be caused by the vulnerabilities found in scans

Tester Notes and Recommendations

Testing results of the FortifyTech network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are caused by missing security headers. These security headers allow hackers and other unethical parties to exploit cross-site scripting (XSS).

During testing in the IP address 10.15.42.7, there was also possible exploitation method in the SSH Server found in CVE-2023-48795. This exposes the website to the vulnerability of Terrapin attacks.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

0	0	0	0	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Missing Security Headers	Informational	Review action and remediation steps.
CVE-2023-48795	Informational	Review action and remediation steps.

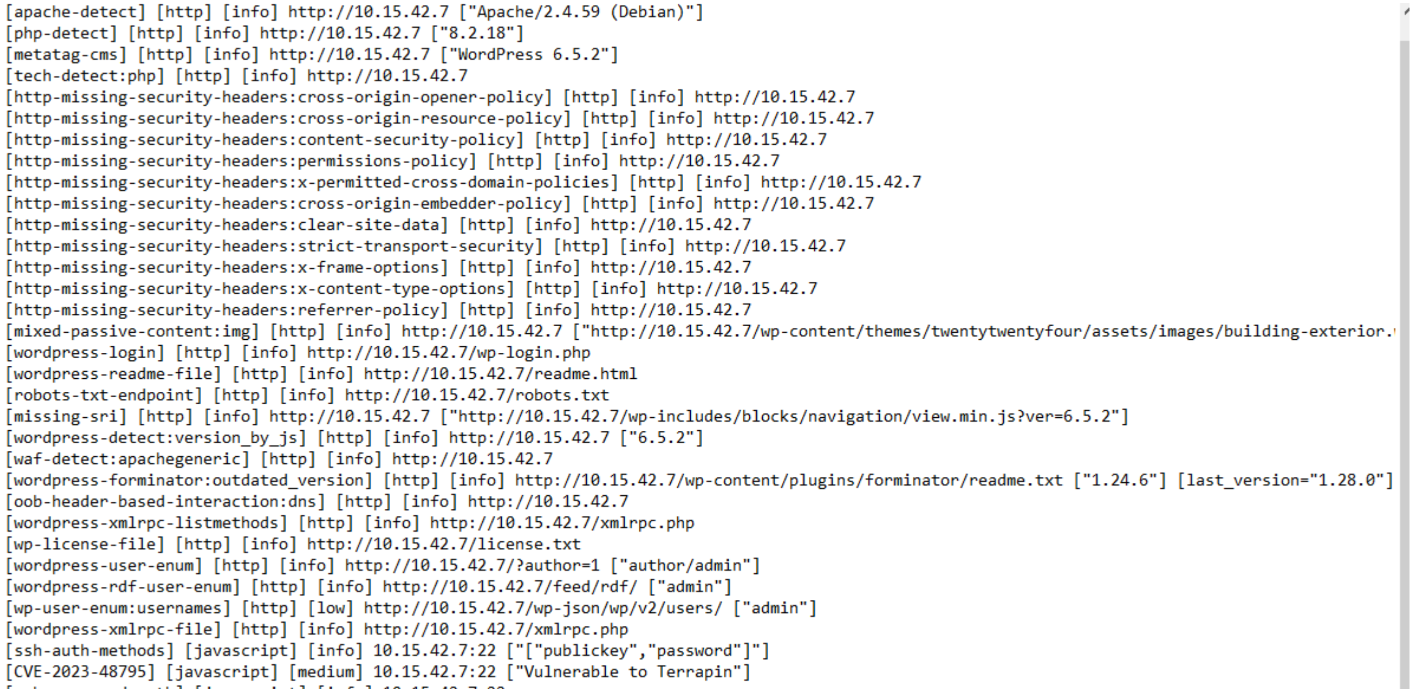
Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Insufficient LLMNR Configuration (Critical)

Description:	There are missing security headers Found CVE-2023-48795
Risk:	Likelihood: High – This attack is effective in environments allowing multicast name resolution. Impact: Unknown
System:	All
Tools Used:	Responder, Hashcat
References:	

Evidence



```
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7
[mixed-passive-content:img] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exterior.
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-sri] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
```