FortifyTech

Security Assessment Findings

Report/

Business Confidential

Date: Oct 5th,
2024 Version 1.0

Table of Contents

Table of Contents 2
Confidentiality Statement 3
Disclaimer 3
Contact Information 3
Assessment Overview 4
Assessment Components 4
External Penetration Test 4
Finding Severity Ratings 5
Scope 6
Scope Exclusions 6
Client Allowances 6
Executive Summary 7
Attack Summary 7
Security Strengths Error! Bookmark not defined.
SIEM alerts of vulnerability scans **Error! Bookmark not defined.**
Security Weaknesses Error! Bookmark not defined.
Missing Multi-Factor Authentication **Error! Bookmark not defined.**
Weak Password Policy **Error! Bookmark not defined.**
Unrestricted Logon Attempts **Error! Bookmark not defined.**
Vulnerabilities by Impact 8
External Penetration Test Findings 9
Insufficient Lockout Policy – Outlook Web App (Critical) **Error! Bookmark not defined.**
Additional Reports and Scans (Informational) 12

Confidentiality Statement

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

TCMS 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

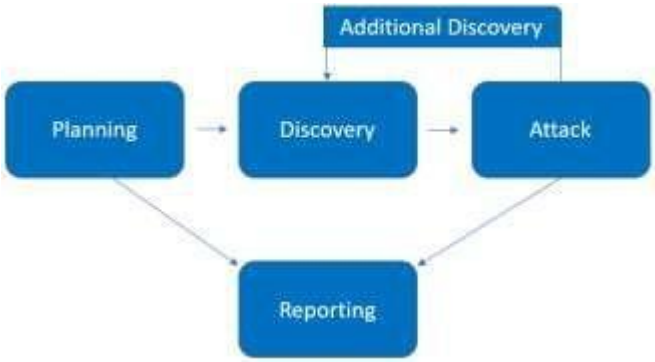
Name	Title	Contact Information
FortifyTech		
U5ELESS	Information Security Consultant	Office: (555) 555-5555 Email: u5eless@fortifytech.com
VulnCore		
Trentz	Penetration Tester	Office: (555) 555-5555 Email: trentz@vulncore.com

Assessment Overview

From Oct 5th, 2024 to Oct 7th, 2024, FortifyTech engaged CyberShield to evaluate the security posture of its infrastructure compared to current industry best practices that included an external 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

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A CyberShield engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

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.
Medium	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.

Scope

Assessment	Details
External Penetration Test	10.15.42.245

Scope Exclusions

FortifyTech did not give any limitations.

Client Allowances

FortifyTech did not provide any allowances to assist the testing.

Executive Summary

VulnCore conducted an external network penetration test on **FortifyTech** from **Oct 5th** to **Oct 7th**. The primary goal of this assessment was to evaluate the security posture of the external network and identify potential vulnerabilities that could be exploited by malicious actors.
During the engagement, VulnCore identified several vulnerabilities, including one medium-severity issue that allowed us to obtain the admin password through relatively simple attack techniques. These vulnerabilities were found during standard reconnaissance and required minimal effort to exploit, indicating potential risks to the organization if left unaddressed.

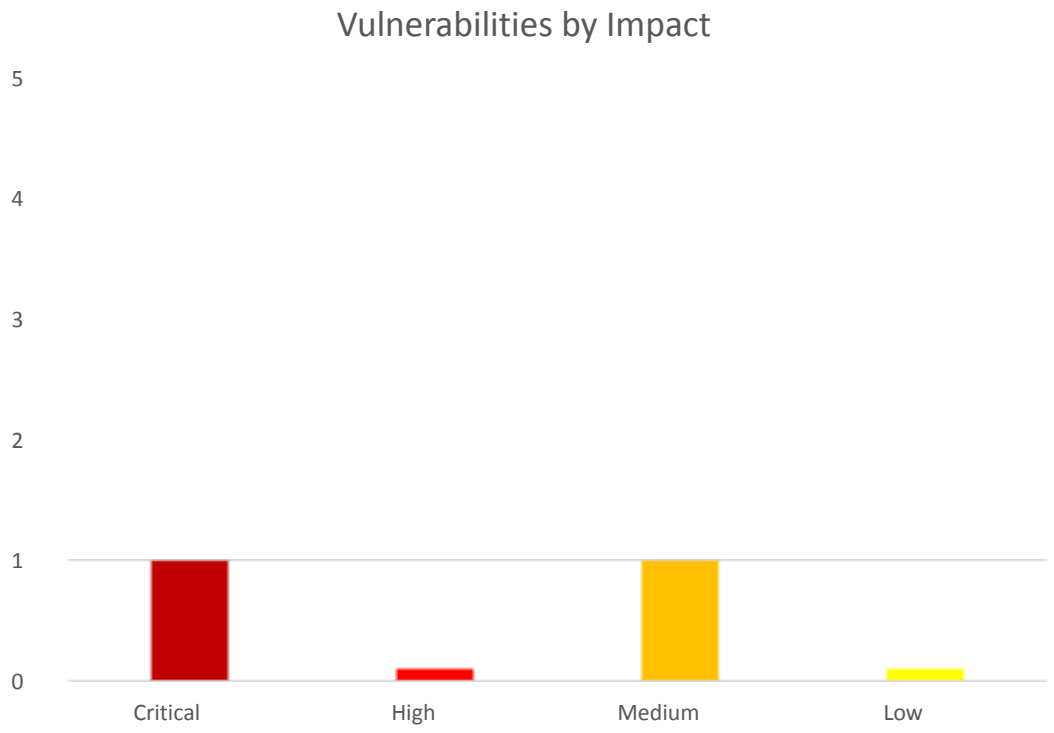
Attack Summary

The following table describes how VulnCore gained user credentials, step by step:

Step	Action	Recommendation
1	Obtained credentials of “ethack” through anonymous access enabled over FTP service.	Disable FTP service of anonymous.
2	A Remote Code Execution vulnerability exists in the gVectors wpDiscuz plugin 7.0 through 7.0.4 for WordPress	Update to the latest version of wpDiscuz plugin.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



External Penetration Test Findings

Enabled Access Over FTP Service – Login (Medium)

Description:	FortifyTech enabled anonymous access over FTP service. This configuration allowed VulnCore to gain credentials of username "ethack" through its database.
Impact:	Medium (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N | Score: 5.3)
System:	10.15.42.245
References:	https://medium.com/nerd-for-tech/tryhackme-anonymous-989fb5c0edde - Enabled FTP access

Exploitation Proof of Concept

VulnCore gathered information through network scan. The network scan output shows enabled access of anonymous over FTP service (**Note:** A full list of the network scan can be found in "**Additionals**" Folder.).

```
# Nmap 7.94SVN scan initiated Sun Oct  6 04:39:25 2024 as: /usr/lib/nmap/nmap -sS -sV -sC -A -T2 -p1-1000 -v -oN nmapscan2.log 10.15.42.245
Nmap scan report for 10.15.42.245
Host is up (0.15s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0          142834 Oct 04 19:41 list.xyz
|_-rw-r--r--    1 0        0             701 Oct 03 17:41 readme.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.33.13.67
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 1800
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
```

Figure 1: Sample output of nmap network scan

VulnCore used the gathered information to connect to the FTP service which requires no password. By listing the directory, VulnCore found two **files**

```
Connected to 10.15.42.245.
220 (vsFTPd 3.0.5)
Name (10.15.42.245:trentz): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||34683|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0          142834 Oct 04 19:41 list.xyz
-rw-r--r--    1 0        0             701 Oct 03 17:41 readme.txt
226 Directory send OK.
ftp>
```

Figure 2: Snippet of directory listing

After conducting a directory listing on the target, **VulnCore** discovered two files: `list.xyz` and `readme.txt`. We proceeded to download and inspect these files. Upon review, we found that the contents included credentials, and in the `readme.txt`, the word 'ethack' appeared four times. Based on this, we decided to search for a username 'ethack' in the `list.xyz` file, which contained a list of usernames and hashes. We successfully identified the hash corresponding to 'ethack' and proceeded to crack the hash using hashcat and successfully crack the hash

```
Last login: Sun Oct  6 12:09:27 2024 from 10.33.13.131
-bash: readme.txt: Permission denied
ethack@eth2024:~$ ls
readme.txt
ethack@eth2024:~$ cat readme.txt
Selamat, Kamu Berhasil!
Kalian kira ini sampai disini? eits, dilanjut yaa masih ada lhoo
ethack@eth2024:~$ pwd
/home/ethack
```

Figure 3: ssh to ethack with credentials

After successfully SSH-ing into the `ethack` account, **VulnCore** discovered another `readme.txt` file, which indicated that the task was not yet complete. Following this clue, we proceeded to investigate further and turned our attention to a WordPress instance hosted at IP 487, as the next logical step in our penetration test.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Configure FTP service by disabling anonymous access.

Additional Reports and Scans (Informational)

VulnCore provides all clients with all report information gathered during testing. This includes vulnerability scans. For more information, please see the following documents:

- **nmapscan2.log**

WordPress Plugin wpDiscuz-7.0.4 - Unauthenticated Remote Command Execution

Description:	Unauthenticated Remote Command Execution
Impact:	Critical (**CVSS Vector** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
System:	10.15.42.245
References:	https://nvd.nist.gov/vuln/detail/CVE-2020-24186 https://github.com/hev0x/CVE-2020-24186-wpDiscuz-7.0.4-RCE

Exploitation Proof of Concept

VulnCore found information about wordpress plugin called wpDiscuz and its version by viewing source of http://10.15.42.245:487/2024/10/03/trial/.

wpdiscuz-combo....n.js?ver=7.0.4

```
1   /* Cookie */
2   (function(factory) {
-       var registeredInModuleLoader = false;
-       if (typeof define === 'function' && define.amd) {
-           define(factory);
-           registeredInModuleLoader = true
-       }
-       if (typeof exports === 'object') {
-           module.exports = factory();
-           registeredInModuleLoader = true
-       }
-       if (!registeredInModuleLoader) {
-           var OldCookies = window.Cookies;
-           var api = window.Cookies = factory();
-           api.noConflict = function() {
-               window.Cookies = OldCookies;
-               return api
-           }
-       }
```

Figure 4: Inspect Element of wpdizcus js

After inspecting the 'Trial' page on the WordPress instance, **VulnCore** discovered a vulnerable plugin called `wpDiscuz`, which was authored by `ZidanAPik`. By inspecting the element, we identified that the plugin had a known vulnerability, specifically **CVE-2020-24186**. Referring to the exploit details provided on GitHub, we leveraged this vulnerability to execute Remote Code Execution (RCE), successfully gaining system access.

Remediation

Who:	IT Team
Vector:	Remote
Action:	Update to the latest version of wpDiscuz.

Last Page