
# Demo Company
# Security Assessment Findings Report

Business Confidential

*Date: May 28th, 2019*
*Project: 897-19*
*Version 1.0*

# Table of Contents

# Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

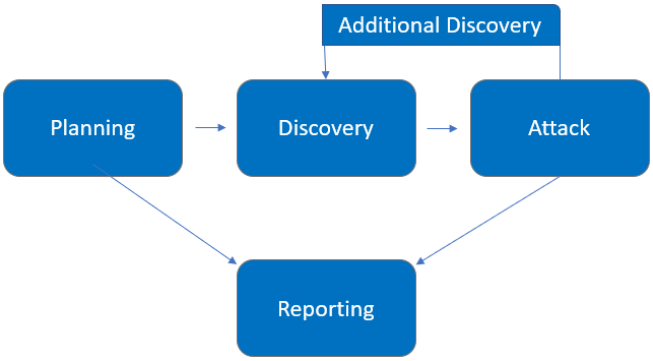
| Name | Title | Contact Information |
|---|---|---|
| **Demo Company** | | |
| John Smith | VP, Information Security (CISO) | Office: (555) 555-5555<br>Email: john.smith@demo.com |
| **TCM Security** | | |
| Dzaky Ahnaf | Lead Penetration Tester | Office: (555) 555-5555<br>Email: dzakyahnf@gmail.com |

# Assessment Overview

From October 4th, 2024 to October 7th, 2024, DC engaged TCMS 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 TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also 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. |
| 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. |

# Scope

| Assessment | Details |
|---|---|
| External Penetration Test | 10.15.42.245 |

## Scope Exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

## Client Allowances

A special wordlist for hashing/de-hashing purposes.

# Executive Summary

TCMS evaluated DC's external security posture through an external network penetration test from October 4th, 2024 to October 7th, 2024. By leveraging a series of attacks, TCMS found critical level vulnerabilities that allowed full internal network access to the DC headquarter office. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following table describes how TCMS gained internal network access, step by step:

| Step | Action | Recommendation |
|---|---|---|
| 1 | Obtained credentials of "ethack" through anonymous access enabled over FTP service. | Disable FTP service of anonymous will prevent unauthorized access of the FTP, which in turn also prevents unauthorized access of the SSH. |
| 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, will prevent unauthorized access via RCE. |

# Security Strengths

## SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

# Security Weaknesses

## Anonymous FTP Access

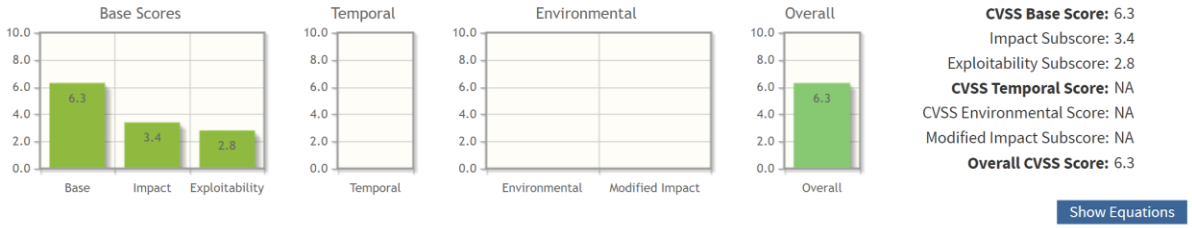
During the assessment, TCMS was able to obtain credentials for the "ethack" account through the anonymous access feature enabled on the FTP service. This vulnerability provided unauthorized access to sensitive files stored on the server. The ability to connect anonymously poses a significant risk as it can allow attackers to gather critical information without authentication.
**Recommendation:** It is recommended to disable anonymous FTP access entirely to prevent unauthorized users from accessing the system. Alternatively, restrict FTP access by using stronger authentication mechanisms and ensuring that sensitive files are not exposed.

## Remote Code Execution in WordPress wpDiscuz Plugin

A remote code execution vulnerability was identified in the wpDiscuz plugin, specifically versions 7.0 through 7.0.4. This flaw allows attackers to execute arbitrary code on the server by exploiting improper input handling in the comment feature. With this vulnerability, attackers could potentially gain control of the entire WordPress site, compromising both user data and site integrity.
**Recommendation:** Update the wpDiscuz plugin to the latest version immediately. Regularly check for updates and patches for all installed plugins to ensure vulnerabilities like this are promptly addressed.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:




**CVSS Base Score:** 6.3
Impact Subscore: 3.4
Exploitability Subscore: 2.8
**CVSS Temporal Score:** NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
**Overall CVSS Score:** 6.3

Show Equations

**CVSS v3.1 Vector**
AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

## Base Score Metrics

### Exploitability Metrics

**Attack Vector (AV)***
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

**Attack Complexity (AC)***
Low (AC:L) | High (AC:H)

**Privileges Required (PR)***
None (PR:N) | Low (PR:L) | High (PR:H)

**User Interaction (UI)***
None (UI:N) | Required (UI:R)

**Scope (S)***
Unchanged (S:U) | Changed (S:C)

### Impact Metrics

**Confidentiality Impact (C)***
None (C:N) | Low (C:L) | High (C:H)

**Integrity Impact (I)***
None (I:N) | Low (I:L) | High (I:H)

**Availability Impact (A)***
None (A:N) | Low (A:L) | High (A:H)

## External Penetration Test Findings

### Insufficient Lockout Policy – Outlook Web App (Critical)

| | |
|---|---|
| **Description:** | DC enabled anonymous access over FTP service. This configuration allowed TCMS to gain credentials of username “ethack” through its database. |
| **Impact:** | Medium (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L \| Score: 6.3) |
| **System:** | 10.15.42.245 |
| **References:** | https://medium.com/nerd-for-tech/tryhackme-anonymous-989fb5c0edde - Enabled FTP access |

### Exploitation Proof of Concept

TCMS gathered information through network scan using NMAP. The network scan output shows enabled access of anonymous over FTP service.

```
jeky@LAPTOP-NPPB6LFN:~$ sudo nmap 10.15.42.245 -sS -sC -sV -A -T4 -p-
[sudo] password for jeky:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-07 08:45 WIB
Nmap scan report for 10.15.42.245
Host is up (0.050s latency).
Not shown: 65532 closed ports
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:10.33.13.116
|      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 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
487/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-generator: WordPress 6.6.2
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Suka-Suka Zidan
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Cam
1 - 3.2 (89%), Linux 3.2 - 4.9 (89%), Linux 3.7 - 3.10 (89%), Linux 3.8 (89%), Synology DiskStation Manag
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

*Figure 1: Sample output of scanning*

TCMS connected to the FTP service, which needs credentials to login. Using the common anonymous login, S3rv4nt0fGod can logged in and discovered a file that stored certain credentials by listing the directory

```
jeky@LAPTOP-NPPB6LFN:~$ ftp 10.15.42.245
Connected to 10.15.42.245.
220 (vsFTPd 3.0.5)
Name (10.15.42.245:jeky): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -a
229 Entering Extended Passive Mode (|||46785|)
150 Here comes the directory listing.
drwxr-xr-x    2 1002     1002         4096 Oct 04 19:41 .
drwxr-xr-x    2 1002     1002         4096 Oct 04 19:41 ..
-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> get list.xyz
local: list.xyz remote: list.xyz
229 Entering Extended Passive Mode (|||36945|)
150 Opening BINARY mode data connection for list.xyz (142834 bytes).
100% |*****************************************************************************|
226 Transfer complete.
142834 bytes received in 00:00 (1.63 MiB/s)
ftp> get readme.txt
local: readme.txt remote: readme.txt
229 Entering Extended Passive Mode (|||64180|)
150 Opening BINARY mode data connection for readme.txt (701 bytes).
100% |*****************************************************************************|
226 Transfer complete.
701 bytes received in 00:00 (103.61 KiB/s)
ftp> exit
221 Goodbye.
```

*Figure 2: FTP Service*

TCMS found some credentials that suspiciously be the admin,

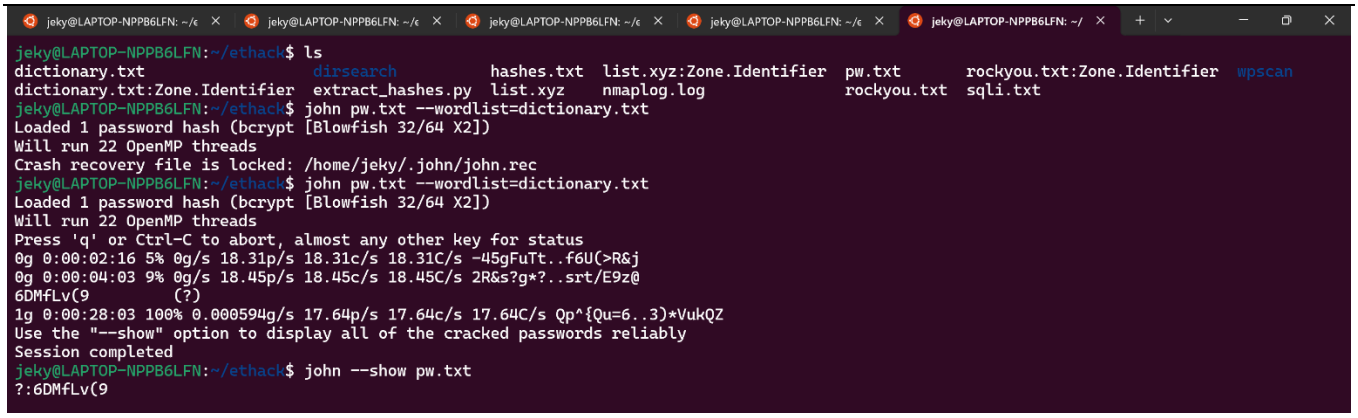



*Figure 3: Admin Credentials Cracked*

TCMS decrypt the password using some txt file and successfully decrypted it. S3rv4nt0fGod used the credentials and successfully logged in to the machine

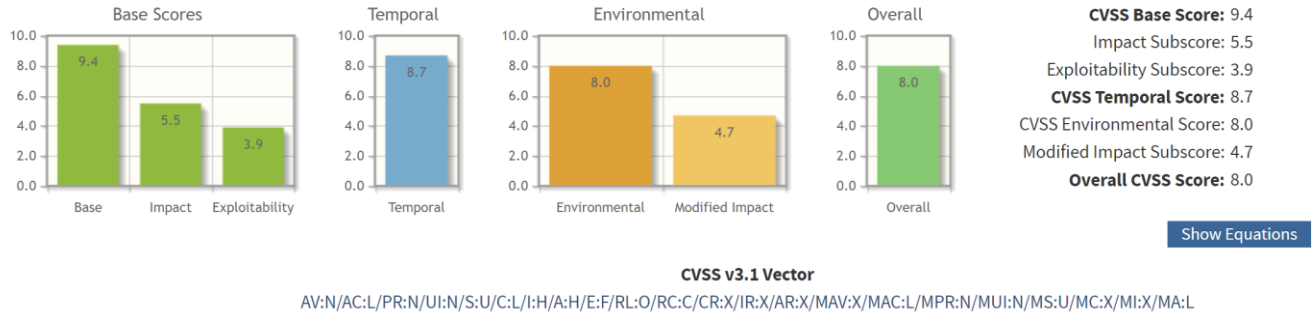
## Remediation

| | |
|---|---|
| **Who:** | IT Team |
| **Vector:** | Remote |
| **Action:** | Disable Anonymous FTP Access, Use FTPS or SFTP service and Implementing Strong Authentication. |

WordPress wpDiscuz 7.0.4 - Remote Code Execution (High)

| | |
|---|---|
| **Description:** | Remote Code Execution which allows unauthenticated users to upload any type of file, including PHP files via the wmuUploadFiles AJAX action. |
| **Impact:** | High (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:F/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:L/MPR:N/MUI:N/MS:U/MC:X/MI:X/MA:L \| Score: 8.0) |
| **System:** | 10.15.42.245 |
| **References:** | hev0x/CVE-2020-24186-wpDiscuz-7.0.4-RCE: wpDiscuz 7.0.4 Remote Code Execution (github.com) |

## CVSS Score




## Exploitation Proof of Concept

TCMS gathered information about WordPress plugin called wpDiscuz and its version by scanning the WordPress security using wpscan

```
jeky@LAPTOP-NPPB6LFN:~$ wpscan --url http://10.15.42.245:487/2024/10/03/trial/ --wp-content-dir wp-content
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.15.42.245:487/2024/10/03/trial/ [10.15.42.245]
[+] Started: Mon Oct  7 08:43:05 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: nginx/1.18.0 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.15.42.245:487/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | 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 version 6.6.2 identified (Latest, released on 2024-09-10).
 | Found By: Rss Generator (Passive Detection)
```

*Figure 1: Founded WordPress wpDiscuz plugins*

Based on the version of the wpDiscuz, it can be exploited by executing PoC script that available at this link (https://github.com/hev0x/CVE-2020-24186-wpDiscuz-7.0.4-RCE)

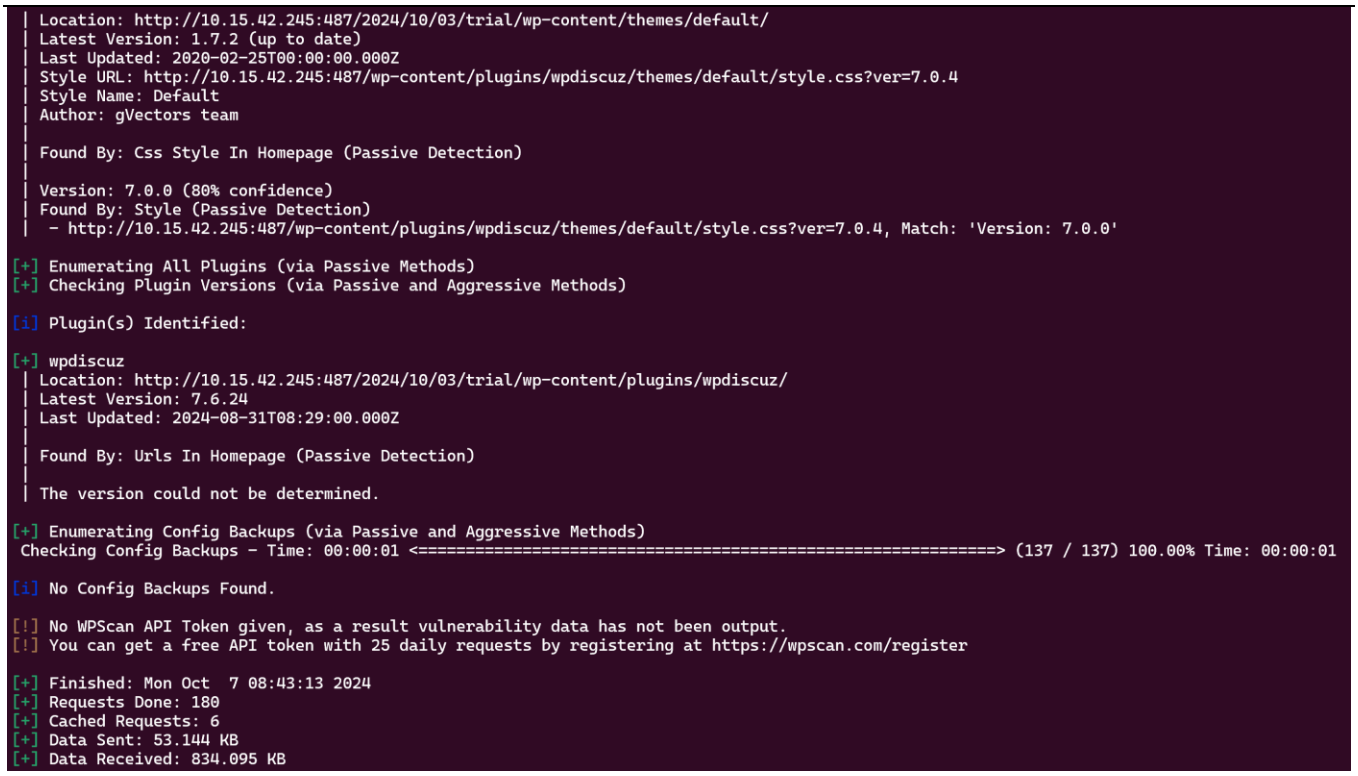



*Figure 2: Web Server Credentials Login*

The programs work by uploading PHP files via the wmuUploadFiles AJAX action.

## Remediation

| | |
|---|---|
| **Who:** | IT Team |
| **Vector:** | Remote |
| **Action:** | Update to the latest version of wpDiscuz plugins. |


# Last Page