



TCM
SECURITY

DemoCorp Security Assessment Findings Report

Date: March 26, 2025
Project: DemoCorp-2024-001
Version: 1.0

BUSINESS CONFIDENTIAL



Table of Contents

Table of Contents	2
Confidentiality Statement.....	4
Disclaimer.....	4
Contact Information.....	4
Assessment Overview.....	5
Assessment Components.....	6
External Penetration Test.....	6
Finding Severity Ratings	7
Risk Factors.....	7
Likelihood	7
Impact.....	7
Scope.....	8
Scope Exclusions	8
Client Allowances	8
Executive Summary	9
Scoping and Time Limitations.....	9
External Testing Summary.....	9
Key Strengths and Weaknesses	9
Vulnerability Summary & Report Card	11
External Penetration Test Findings	11
Technical Findings.....	13
External Penetration Test Findings	13
Finding EPT-001: Insufficient Authentication Controls – Multi-Factor Authentication (MFA) (High).....	13
Finding EPT-002: Insufficient Account Management – Cleartext Credentials in SharePoint (High).....	15
Finding EPT-003: Security Misconfiguration – Dangerous Ports are Externally Open (High).....	17
Finding EPT-004: Account Misconfiguration – Overly Permissive User Accounts (Moderate)	18
Finding EPT-005: Insufficient Encryption – HTTP (Moderate)	18
Finding EPT-006: Insufficient Patch Management – Software (Moderate).....	20
Finding EPT-007: Denial of Service – Wordpress wp-cron.php (Moderate)	22
Finding EPT-008: Server-Side Request Forgery (SSRF) – Wordpress xmlrpc.php (Moderate).....	24
Finding EPT-009: Security Misconfiguration – GraphQL Introspection Enabled (Moderate)	28
Finding EPT-010: Security Misconfiguration – phpinfo.php Information Disclosure (Moderate)	31
Finding EPT-011: Insufficient Patch Management – Wordpress Plugins (Moderate)	32
Finding EPT-012: Default Web Server Landing Page (Low).....	35
Finding EPT-013: Security Misconfiguration – Information Disclosure via HTTP Response Headers (Low)	37
Finding EPT-014: Security Misconfiguration – Wordpress Debug Log Information Disclosure (Low)	39
Finding EPT-015: Security Misconfiguration – Wordpress Login Page is Public (Low).....	40
Finding EPT-016: Outdated Wordpress Blog (Informational)	41



Additional Scans and Reports.....	42
-----------------------------------	----



Confidentiality Statement

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

DemoCorp 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
DemoCorp		
John Demo	Sr. Manager Cybersecurity	John@DemoCorp.com
TCM Security		
Ang Brown	Penetration Tester	abrown@tcm-sec.com
Jason Marcello	Principal Penetration Tester	jmarcello@tcm-sec.com

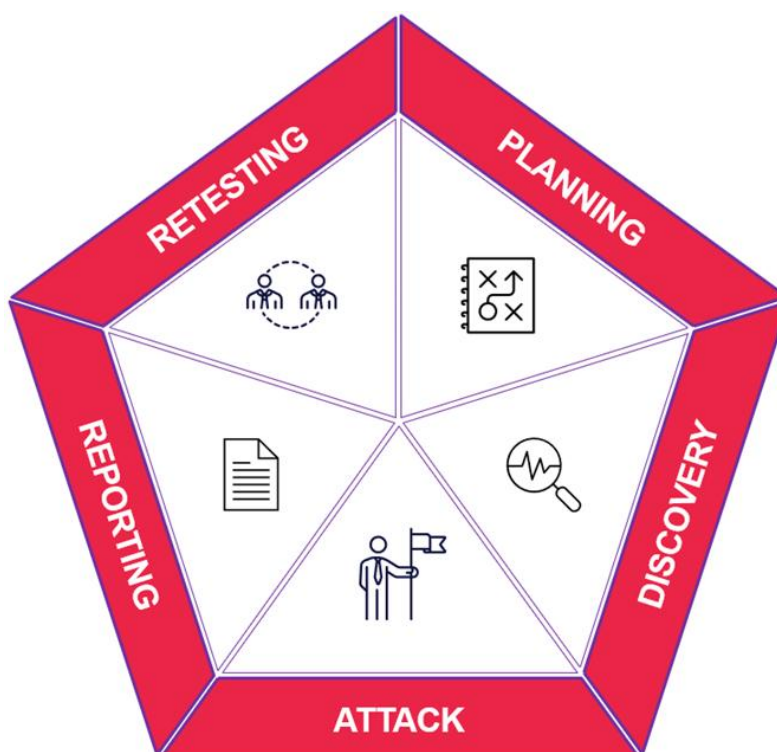


Assessment Overview

From December 9, 2024, to December 20, 2024, DemoCorp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included External penetration testing. 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 are 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.

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	Redacted

Scope Exclusions

Per client request, TCMS 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 DemoCorp.

Client Allowances

DemoCorp provided TCMS no allowances.



Executive Summary

TCMS evaluated DemoCorp's security posture through External penetration testing from December 9, 2024, to December 13, 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.

Testing was subject to time limitations, with external penetration testing permitted for five (5) business days. The TCMS team accounted for these constraints when assessing the overall risk and severity of the findings.

External Testing Summary

The External Penetration Test evaluated DemoCorp's external network security posture. From an external perspective, the TCMS team performed vulnerability scanning against the IP addresses provided by DemoCorp. The team also performed information gathering techniques to attempt to identify any sensitive information publicly listed on the web. This includes sensitive files, usernames, passwords, and any credentials from historical data breaches.

0365 multi-factor authentication (MFA) can be bypassed (see EPT-001). Cleartext credentials are stored in SharePoint (see EPT-002). RDP and SMB ports are open externally on a system (see EPT-003). 0365 accounts are overly permissive (see EPT-004). The unencrypted HTTP protocol is utilized on externally facing web servers (see EPT-005). Outdated software versions are utilized on externally facing systems (see EPT-006). The wp-cron.php file is exposed on Wordpress servers, which may lead to denial-of-service attacks (see EPT-007). GraphQL introspection is enabled on externally facing web servers (see EPT-008). Exposed xmlrpc.php files on Wordpress lead to SSRF (see EPT-009). The phpinfo.php file is exposed to unauthenticated users on a web server (see EPT-010). Wordpress plugins are out of date (see EPT-011). Default web server landing pages are used (see EPT-012). Information is disclosed via HTTP response headers (see EPT-013). A Wordpress debug log is exposed to unauthenticated users (see EPT-014). A Wordpress login page is publicly facing (see EPT-015). An outdated Wordpress blog was discovered (see EPT-016).

For further information on findings, please review the [Technical Findings](#) section of the report.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

- All 0365 password spraying attempts were unsuccessful
- External attack surface is small

The following identifies the key weaknesses identified during the assessment:



-
- 0365 multi-factor authentication (MFA) can be bypassed
 - Cleartext credentials are stored in SharePoint
 - 0365 accounts are overly permissive
 - RDP and SMB ports are open externally



Vulnerability Summary & Report Card

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

External Penetration Test Findings

0	3	8	4	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
EPT-001: Insufficient Authentication Controls – Multi-Factor Authentication (MFA)	High	Enforce MFA, conditional access policies, and disable inactive accounts.
EPT-002: Insufficient Account Management – Cleartext Credentials in SharePoint	High	Train users to store passwords in secured and encrypted locations.
EPT-003: Security Misconfiguration – Dangerous Ports are Externally Open	High	Close SMB and RDP from being externally accessible
EPT-004: Account Misconfiguration – Overly Permissive User Accounts	Moderate	Implement least privilege model within Microsoft 0365.
EPT-005: Insufficient Encryption – HTTP	Moderate	Enforce encrypted traffic channels for all externally facing web servers.
EPT-006: Insufficient Patch Management – Software	Moderate	Update software to the latest stable versions.
EPT-007: Denial of Service – Wordpress wp-cron.php	Moderate	Disable Wp-Cron and create a real cronjob inside the host.
EPT-008: Server-Side Request Forgery (SSRF) – Wordpress xmlrpc.php	Moderate	Turn off pingbacks globally.
EPT-009: Security Misconfiguration – GraphQL Introspection Enabled	Moderate	Disable introspection on the GraphQL Server.
EPT-010: Security Misconfiguration – phpinfo.php Information Disclosure	Moderate	Disable the phpinfo.php file.
EPT-011: Insufficient Patch Management – Wordpress Plugins	Moderate	Update plugins to the latest stable versions.
EPT-012: Default Web Server Landing Page	Low	Disable the default landing pages.
EPT-013: Security Misconfiguration – Information Disclosure via HTTP Response Headers	Low	Remove unnecessary information from HTTP response headers.



Finding	Severity	Recommendation
EPT-014: Security Misconfiguration – Wordpress Debug Log Information Disclosure	Low	Restrict permissions on the debug.log file so that it is not publicly facing.
EPT-015: Security Misconfiguration – Wordpress Login Page is Public	Low	Add IP whitelisting to the wp-login.php page.
EPT-016: Outdated Wordpress Blog	Informational	Remove blog to reduce Wordpress attack surface.



Technical Findings

External Penetration Test Findings

Finding EPT-001: Insufficient Authentication Controls – Multi-Factor Authentication (MFA) (High)

Description:	TCMS successfully bypassed O365 multi-factor authentication through the following means: • The Microsoft Graph API • MacOS User-Agent Header • Android User-Agent Header • iPhone User-Agent Header • Windows Phone User-Agent Header Note: Risk reduced from “Critical” to “High” as no user credentials were successfully compromised during the engagement.
Risk:	Likelihood: High – Systems are available from the Internet. Exploitation requires a valid user account. Impact: Very High – If exploited, an attacker with valid credentials can successfully authenticate to the application without applying a second factor.
System(s):	Microsoft O365
Tools Used:	Manual Review
References:	NIST SP800-53r5 IA-5 – Authenticator Management CIS Password Policy Guide

Evidence

##### SINGLE FACTOR ACCESS RESULTS #####	
Microsoft Graph API	YES
Microsoft Service Management API	NO
M365 w/ Windows UA	NO
M365 w/ Linux UA	NO
M365 w/ MacOS UA	YES
M365 w/ Android UA	YES
M365 w/ iPhone UA	YES
M365 w/ Windows Phone UA	YES
Exchange Web Services (BASIC Auth)	NO
Active Sync (BASIC Auth)	NO

Figure 1 - MFASweep Output



```
PS C:\Users\jmarc\o365recon> .\o365recon.ps1 -azure
Connecting to Microsoft services:
    Checking for MsOnline Module ... DONE
    Checking for AzureAD Module ... DONE
    Connecting to AzureAD with Connect-AzureADWARNING: Install the latest
DONE
    Connecting to O365 ... DONE
Please enter a project name: Tricor_enum
    Retrieving Company Info ... DONE
-----
Overview
[REDACTED]
-----
Retrieving Domain Information:
    Retrieving O365 Domain Information ... DONE
    Retrieving AzureAD Domain Information ... DONE
-----
Retrieving User Information (this may take a while):
    Retrieving User List ... DONE
    Creating simple O365 user list ... DONE
    Creating Detailed O365 User List CSV ... DONE
    Creating user->ProxyAddresses list ... DONE
    Grabbing O365 LDAP style user data ... DONE
    Creating simple Azure AD user list ... DONE
-----
Retrieving Group Information:
    Retrieving O365 Group Names ... DONE
    Retrieving AzureAD Group Names ... DONE
    Creating Simple O365 Group List ... DONE
    Creating Simple AzureAD Group List ... DONE
    Retrieving Extended Group Information ... DONE
-----
```

Figure 2 - MFA Bypass through Microsoft Graph API

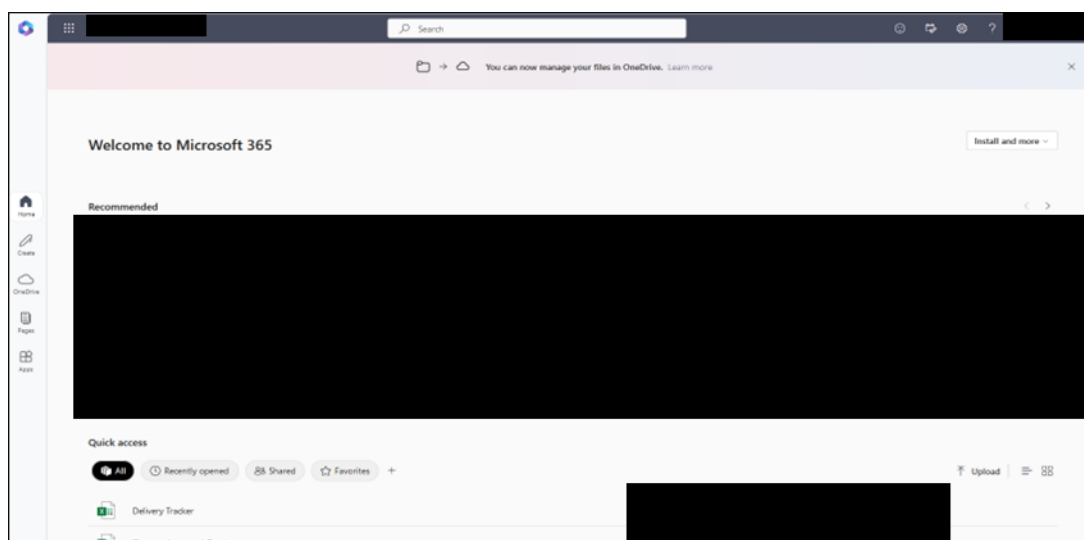


Figure 3 - MFA Bypass Through User-Agent String

Remediation

Enforce MFA and conditional access policies, disable inactive accounts.



Finding EPT-002: Insufficient Account Management – Cleartext Credentials in SharePoint (High)

Description:	Cleartext credentials are discoverable within documents stored on the DemoCorp SharePoint site. Note: Risk reduced from “Critical” to “High” as no user credentials were successfully compromised during the engagement.
Risk:	Likelihood: Moderate – Credentials need to be compromised in some manner, such as through a compromised email account. Impact: Very High – Compromised credentials can be used to access user accounts.
System(s):	DemoCorp Tenant
Tools Used:	GraphRunner
References:	NIST SP800-53r5 AC-6(3) – Least Privilege NIST SP800-53r5 SC-28(1) – Protection of Information at Rest

Evidence

```
PS C:\Users\jmarc\GraphRunner> Invoke-SearchSharePointAndOneDrive -Tokens $Tokens -SearchTerm 'password AND filetype:xlsx'
[*] Using the provided access tokens.
[*] Found 6 matches for search term password AND filetype:xlsx
Result [0]
File Name: [REDACTED]
Location: [REDACTED]
Created Date: [REDACTED]
Last Modified Date: 2014-11-17T18:59:28Z
Size: 19.51 KB
File Preview: [REDACTED]
DriveID & Item: [REDACTED]
Result [1]
File Name: [REDACTED]
Location: [REDACTED]
Created Date: [REDACTED]
Last Modified Date: [REDACTED]
Size: 16. [REDACTED]
File Preview: [REDACTED]
DriveID & Item: [REDACTED]
Result [2]
File Name: [REDACTED]
Location: [REDACTED]
Created Date: [REDACTED]
Last Modified Date: [REDACTED]
Size: 13.7 [REDACTED]
File Preview: [REDACTED]
DriveID & Item: [REDACTED]
Result [3]
File Name: [REDACTED]
Location: [REDACTED]
Created Date: [REDACTED]
Last Modified Date: [REDACTED]
Size: [REDACTED]
File Preview: [REDACTED]
DriveID & Item: [REDACTED]
```

Figure 4 - Searching for Sharepoint Files with Passwords via GraphRunner

	B	C	D	E
1	webaddress	username	password	
2	www.[REDACTED]	[REDACTED]	Den-Ridge	
3	http://[REDACTED]	[REDACTED]	Den-Ridge	
4	www.[REDACTED]	[REDACTED]	Den-Ridge	
5	www.[REDACTED]	[REDACTED]	Den-Ridge	
6	www.[REDACTED]	[REDACTED]	Den-Ridge	
7	www.[REDACTED]	[REDACTED]	Den-Ridge	
8	http://[REDACTED]	[REDACTED]	Den-Ridge	
9	http://[REDACTED]	[REDACTED]	Den-Ridge	
10	http://[REDACTED]	[REDACTED]	Den-Ridge	
11	www.[REDACTED]	[REDACTED]	Den-Ridge	
12				
13				
14				

Figure 5 - Cleartext Credentials Discovered in Excel File



A42 : X ✓ fx WHEW - YOU ARE DONE WITH THAT ONE.									
	A	B	C	D	E	F	G	H	
1	REI								
2									
3			.COM						
4									
5	PASSWORD AND SIGN ON:								
6									
7									
8									

Figure 6 - User Credentials Discovered in Excel File

Remediation

Train users to store passwords in secured and encrypted locations.



Finding EPT-003: Security Misconfiguration – Dangerous Ports are Externally Open (High)

Description:	Externally facing hosts have SMB (port 445) and RDP (port 3389) open. These ports are often targeted by attackers to gain initial access to systems. If exploited, the attacker would be granted access to the internal network. Note: TCMS was unable to exploit these externally facing services during the engagement period.
Risk:	Likelihood: Moderate – Valid user credentials would need to be known/replayed to gain access to the system through these ports. Impact: Very High – Local access to one of these externally facing hosts would grant access to the internal network.
System(s):	DemoCorp.ca
Tools Used:	nessus; nmap
References:	How to Prevent Remote Ransomware Exposures

Evidence

```
(json json-laptop)-[~]
$ sudo nmap -p 3389 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 16:44 MST
Nmap scan report for [redacted].com ([redacted])
Host is up (0.070s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap scan report for [redacted].ca ([redacted])
Host is up (0.069s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.89 seconds
```

Figure 7 - RDP is Externally Open

Remediation

Close SMB and RDP from being externally accessible



Finding EPT-004: Account Misconfiguration – Overly Permissive User Accounts (Moderate)

Description:	TCMS observed several O365 groups that were not restricted, allowing for self-enrollment group membership. Note: Risk reduced from “High” to “Medium” as no user credentials were successfully compromised during the engagement.
Risk:	Likelihood: Moderate – Groups are unrestricted; however, authentication is required to access these settings. Impact: High – Adversaries can obtain sensitive information and can be leveraged for sophisticated social engineering attempts or privilege escalation attacks.
System(s):	Microsoft O365
Tools Used:	GraphRunner; Manual Review
References:	NIST SP800-53r5 AC-6(3) – Least Privilege

Evidence

```
PS C:\Users\jmarc\GraphRunner> Get-UpdateableGroups -Tokens $tokens
[*] Now gathering groups and checking if each one is updateable.
[*] Processing more groups...
[*] Processing more groups...
[+] Found updateable group: Fulfillment Leadership Committee: [REDACTED]
[*] Processing more groups...
[*] Processing more groups...
[*] Processing more groups...
[+] Found updateable group: Project - Concur: [REDACTED]
[*] Processing more groups...
[*] Processing more groups...
[+] Found updateable group: Sales Effectiveness Support: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: Working Parents: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: All Company: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: Treasury: [REDACTED]
[*] Processing more groups...
[*] Processing more groups...
[*] Processing more groups...
[*] Processing more groups...
[+] Found updateable group: [REDACTED]
[*] Processing more groups...
[*] Processing more groups...
[+] Found updateable group: Health & Wellness: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: Power BI User Community: [REDACTED]
[+] Found updateable group: Copilot & AI: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: Supply Chain Services (SCS): [REDACTED]
[+] Found updateable group: Town Hall Events: [REDACTED]
[+] Found updateable group: Data Governance Committee: [REDACTED]
[*] Processing more groups...
[+] Found updateable group: Happy Mother's Day: [REDACTED]
```

Figure 8 - Several Updateable Groups

Remediation

Implement a least privilege model within Microsoft O365 and audit access privileges regularly.

Finding EPT-005: Insufficient Encryption – HTTP (Moderate)



Description:	TCMS identified DemoCorp web servers that are being served without encryption via the HTTP protocol.
Risk:	Likelihood: Moderate – Communications to the web servers will be transferred in cleartext when visited on port 80 by any user. However, a man-in-the-middle position is required to intercept traffic. Impact: High – If exploited, adversaries may intercept user credentials or use them in other attacks.
System(s):	Redacted
Tools Used:	Manual Review
References:	CWE-319: Cleartext Transmission of Sensitive Information NIST SP800-53r5 SC-8 – Cryptographic Protection

Evidence

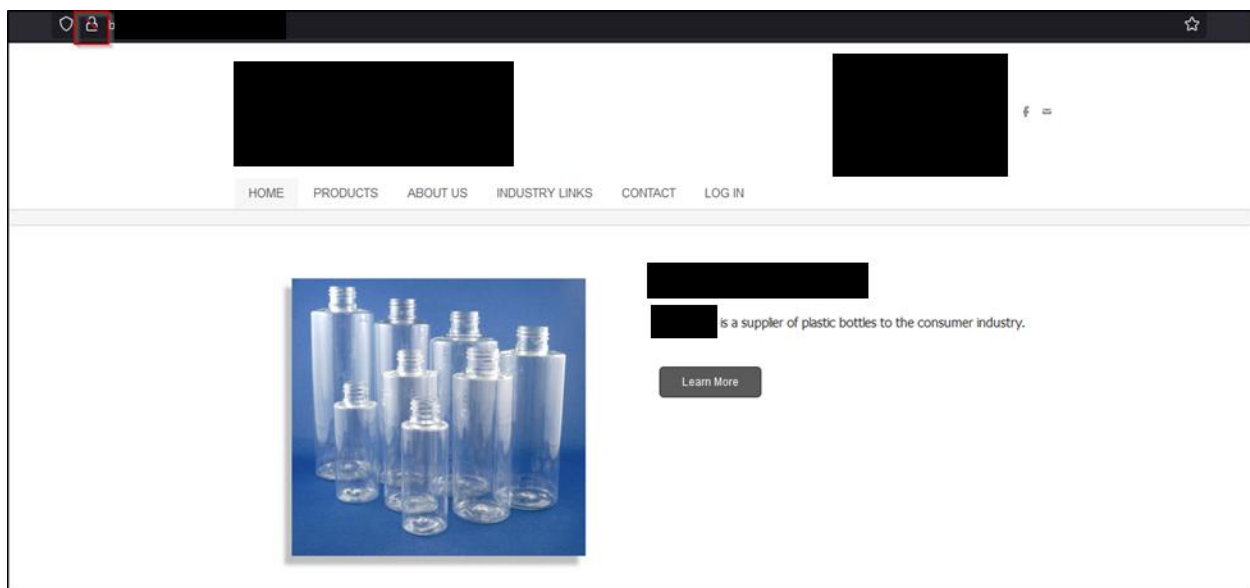


Figure 9 - Redacted Uses HTTP Protocol

Remediation

Enforce encrypted traffic channels for all externally facing web servers.



Finding EPT-006: Insufficient Patch Management – Software (Moderate)

Description:	DemoCorp deploys deprecated software on externally facing web servers. This software includes the following software versions: • PHP 7.4.10 • PHP 7.4 • PHP 7.4.33 • Joomla 3.10.5 Note: TCMS was not able to verify all vulnerable services within the testing window. It is recommended that DemoCorp review and audit the software identified to determine if it is vulnerable.
Risk:	Likelihood: High – Attackers frequently target vulnerable software, especially when it no longer receives support and may have unpatched vulnerabilities. Impact: High – Should attackers gain access to vulnerable software; they can exploit these vulnerabilities to conduct further enumeration within the network and potentially achieve privilege escalation. This can lead to unauthorized access to sensitive data, system compromise, and further exploitation of the network's resources.
System(s):	Redacted
Tools Used:	Burp Suite; Manual Review
References:	NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Evidence

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 18:53:31 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 0
5 Connection: keep-alive
6 Server: Apache
7 X-Powered-By: PHP/7.4.10
8 X-DS-Version: 1714677663
9 Age: 3
```

Figure 10 - End of Life Version of PHP



This XML file does not appear to have any style information associated with it. The document tree is shown

```
<extension version="3.6" type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
  <copyright>(C) 2019 Open Source Matters, Inc.</copyright>
  <license>
    GNU General Public License version 2 or later; see LICENSE.txt
  </license>
  <version>3.10.5</version>
  <creationDate>January 2022</creationDate>
  <description>FILES_JOOMLA_XML_DESCRIPTION</description>
  <scriptfile>administrator/components/com_admin/script.php</scriptfile>
  <update>
    <schemas>
      +<schemapath type="mysql"></schemapath>
      -<schemapath type="sqlsrv">
        administrator/components/com_admin/sql/updates/sqlazure
```

Figure 11 - Outdated Joomla Version

Remediation

Update to the latest versions of software in accordance with vendor instructions.



Finding EPT-007: Denial of Service – Wordpress wp-cron.php (Moderate)

Description:	Publicly facing Wordpress sites permit any unauthenticated user to view the wp-cron.php file. When this file is viewed, a heavy MySQL query is performed on the backend. Attackers can attempt to exhaust system resources by sending extraneous requests to this endpoint. Note: TCMS did not perform denial of service testing during the engagement. However, this is a well-known file that threat actors use to exhaust system resources.
Risk:	Likelihood: High – The wp-cron.php file is publicly facing and is a well known Denial of Service attack vector for threat actors. Impact: Moderate – This attack can result in site denial of service. Impact has been reduced from “High” to “Moderate” since TCMS did not prove out the vulnerability through denial of service testing.
System(s):	redacted.com/wp-cron.php
Tools Used:	Manual Review
References:	CWE-770: Allocation of Resources Without Limits or Throttling Tenable WordPress Cron Enabled

Evidence

Request	Response
<pre>1 GET /wp-cron.php HTTP/2 2 3 4 5 6 7 8 Upgrade-Insecure-Requests: 1 9 Sec-Fetch-Dest: document 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-Site: none 12 Sec-Fetch-User: ?1 13 Priority: u=0, i 14 Te: trailers</pre>	<pre>1 HTTP/2 200 OK 2 Server: openresty 3 Date: Fri, 13 Dec 2024 21:27:26 GMT 4 Content-Length: 0 5 X-Backend: varnish_ssl 6 Strict-Transport-Security: max-age=31536000; includeSubDomains 7 8</pre>

Figure 12 - wp-cron.php Publicly Accessible



Request
Pretty Raw Hex

1 GET /wp/wp-cron.php HTTP/2

0 Sec-Fetch-Mode: navigate

1 Sec-Fetch-Site: none

2 Sec-Fetch-User: ?1

3 Priority: u=0, i

4 Te: trailers

Response
Pretty Raw Hex Render

1 HTTP/2 200 OK

2 X-Powered-By: PHP/7.4.33

3 X-Litespeed-Cache-Control: no-cache

4 Content-Type: text/html; charset=UTF-8

5 Content-Length: 0

6 Date: Fri, 13 Dec 2024 21:27:01 GMT

7 Server: LiteSpeed

8 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

9

10

Figure 13 - wp-cron.php Publicly Accessible

Remediation

Disable Wp-Cron and create a real cronjob inside the host to perform the needed actions.



Finding EPT-008: Server-Side Request Forgery (SSRF) – Wordpress xmlrpc.php (Moderate)

Description:	DemoCorp has externally facing Wordpress sites with the “xmlrpc.php” file exposed. This PHP file is susceptible to Server-Side Request Forgery (SSRF). This allows an attacker to initiate GET requests to arbitrary domains and systems, including internally facing assets. TCMS was unable to exploit any internally facing assets due to the blind nature of the server-side request as well as being limited to only the http and https protocols. However, TCMS was able to successfully receive an out-of-band callback to a Burp collaborator domain, proving that the server makes a GET request to the arbitrary user supplied input. Additionally, this out-of-band request to the Burp collaborator URL reveals the public IP address and Wordpress version number.
Risk:	Likelihood: Moderate – Any unauthenticated user can access the xmlrpc.php file. Since the attacker is unable to see the response of the server-side request, it is unlikely that further enumeration and/or exploitation of internally facing systems will occur. Impact: Moderate – An attacker can make requests to arbitrary and potentially malicious domains. Additionally, the public IP address of the host is revealed as well as the full Wordpress version number through the User-Agent string.
System(s):	redacted.com/xmlrpc.php redacted.org/wp/xmlrpc.php
Tools Used:	Burp Suite
References:	CWE-918: Server-Side Request Forgery (SSRF) PortSwigger Wordpress SSRF

Evidence



redacted.com SSRF Request

```
POST /xmlrpc.php HTTP/2
Host: [....TRUNCATED....]
Cookie: [....TRUNCATED....]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
X-Forwarded-For: 127.0.0.1
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Content-Type: application/xml
Content-Length: 287

<methodCall>
<methodName>pingback.ping</methodName>
<params><param>
<value><string>[....TARGET URL....]</string></value>
</param><param><value><string>[....TRUNCATED....]string>
</value></param></params>
</methodCall>
```



redacted.org SSRF Request

```
POST /wp/xmlrpc.php HTTP/1.1
Host: redacted.org
Cookie: [....TRUNCATED....]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
Gecko/20100101 Firefox/133.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Content-Type: application/xml
Content-Length: 269

<methodCall>
<methodName>pingback.ping</methodName>
<params><param>
<value><string>[....TARGET URL....]</string></value>
</param><param><value><string>https://redacted.org/wp/?p=1</string>
</value></param></params>
</methodCall>
```

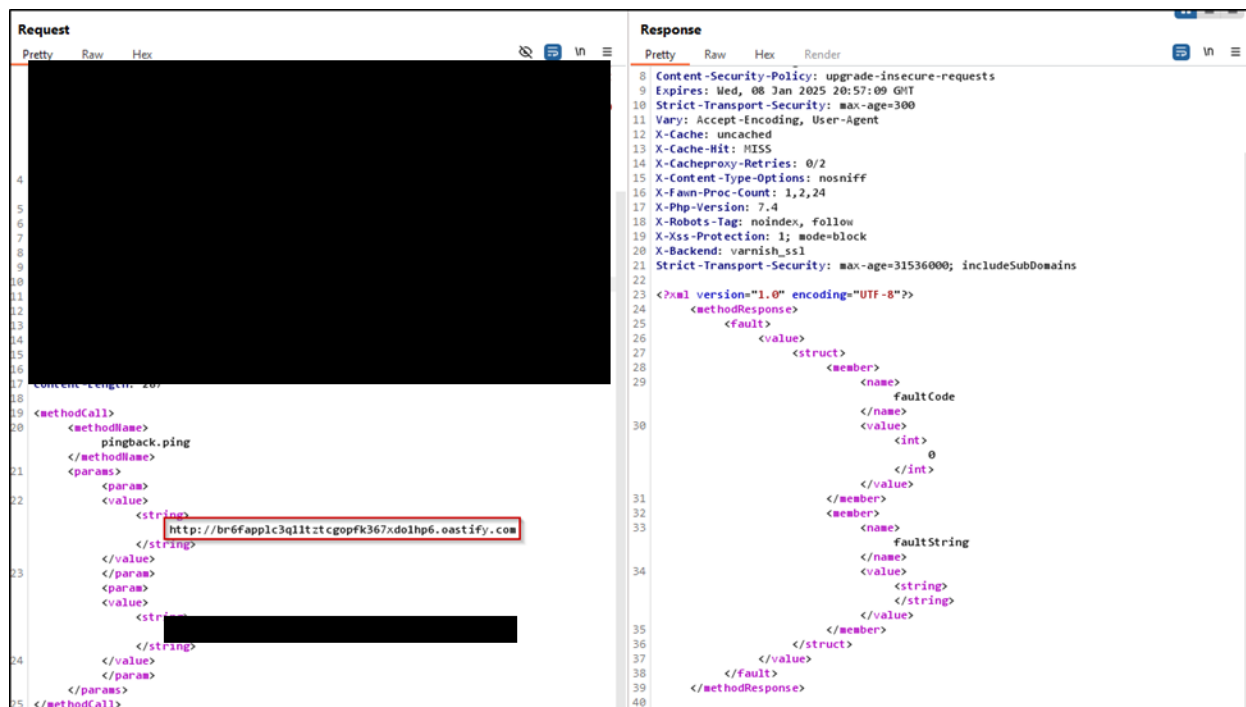


Figure 14 - SSRF Request

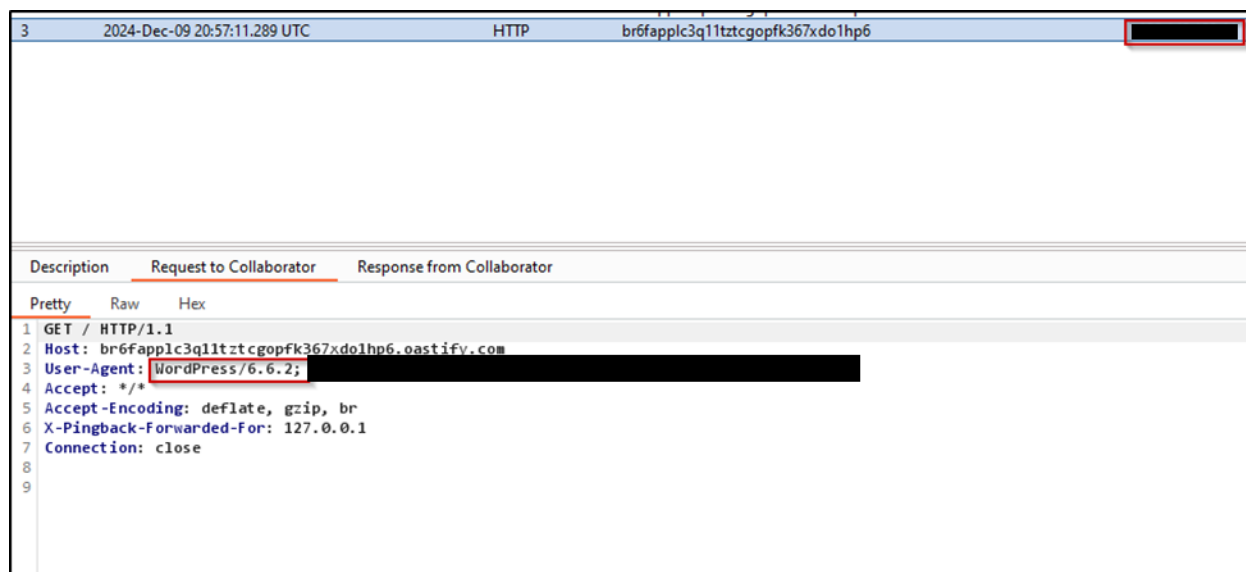


Figure 15 - SSRF Callback

Remediation

Turn off pingbacks globally.



Finding EPT-009: Security Misconfiguration – GraphQL Introspection Enabled (Moderate)

Description:	DemoCorp has externally facing web applications with GraphQL Introspection enabled. This allows an attacker to view the full GraphQL schema which can aid them in discovering what operations are available. Note: TCMS did not discover any vulnerabilities related to GraphQL operations, However, not all operations were audited due to time/scope restraints. All GraphQL operations should be reviewed to ensure malicious actions can not be performed.
Risk:	Likelihood: High – The GraphQL endpoints are publicly facing and available to any unauthenticated user. Impact: Moderate – An attacker can view the whole GraphQL schema and potentially discover vulnerable operations.
System(s):	www.DemoCorp.com/graphql/graphql DemoCorp.com/graphql/graphql
Tools Used:	Burp Suite
References:	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor PortSwigger GraphQL OWASP GraphQL Cheat Sheet

Evidence

The screenshot displays the Burp Suite interface with a GraphQL introspection request and response. The request is a GET to `/graphql/graphql?query={__schema{types{name,fields{name,args{name,description,type{name,kind,ofType{name,kind}}}}}} HTTP/2`. The response is a 200 OK with a JSON body containing the GraphQL schema. A red box highlights the schema details, including the 'Query' type and its fields: 'availableStores' and 'useCurrentGroup'.

Figure 16 - GraphQL Introspection Enabled

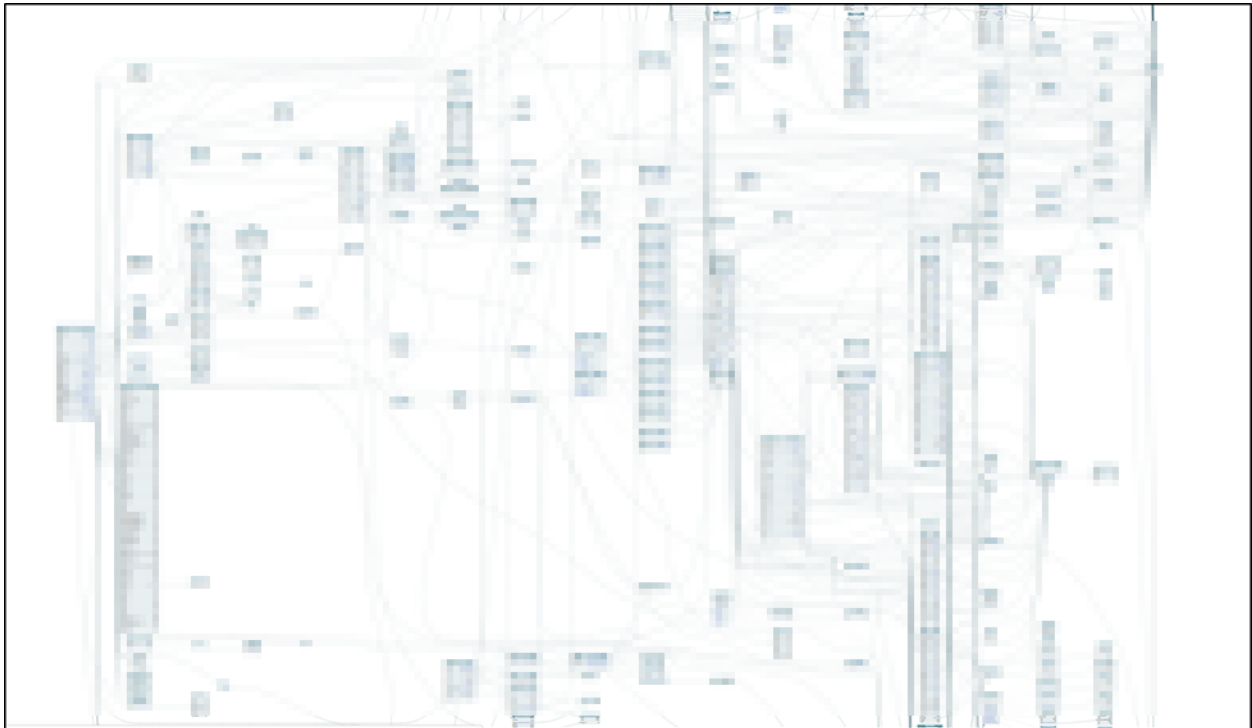


Figure 17 - GraphQL Full Schema

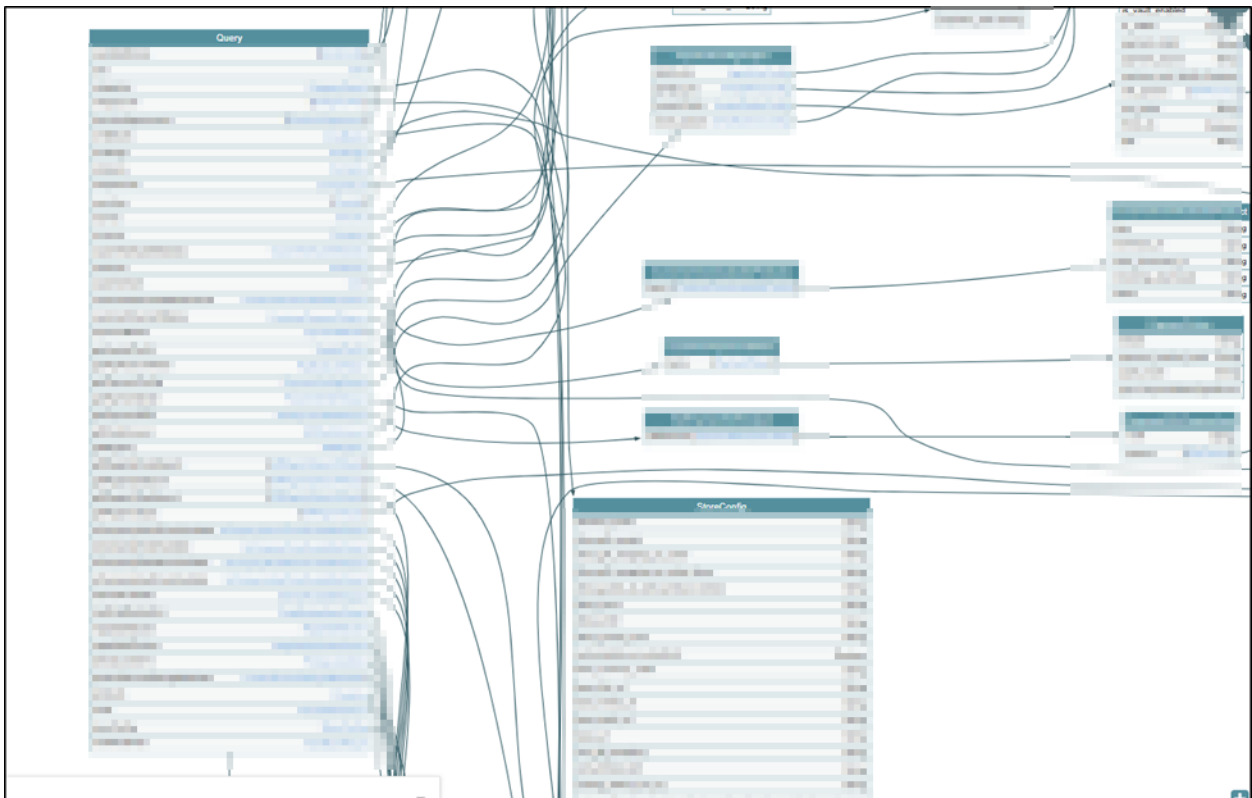


Figure 18 - GraphQL Zoomed in Schema



Request

PrettyRawHexGraphQL

Query

```
1 query availableStores($useCurrentGroup:Boolean){
2   availableStores(useCurrentGroup: $useCurrentGroup){
3     store_name
4   }
5 }
```

Variables

```
1 {
2   "useCurrentGroup":false
3 }
```

Response

PrettyRawHexRender

```
1 HTTP/2 200 OK
2 Expires: Tue, 12 Dec 2023 21:00:50 GMT
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23 Content-Length: 59
24
25 {
  "data":{
    "availableStores":[
      {
        [REDACTED]
      }
    ]
  }
}
```

Figure 19 - GraphQL Querying the Available Stores

Remediation

Disable introspection on the GraphQL Server.



Finding EPT-010: Security Misconfiguration – phpinfo.php Information Disclosure (Moderate)

Description:	The phpinfo.php file is readable by any unauthenticated user. This file contains system information that includes system paths, software versions, etc.
Risk:	Likelihood: High – The phpinfo.php file is viewable by any unauthenticated user and is included in many directory fuzzing wordlists. Impact: Moderate – This file contains system information that includes system paths, software versions, etc. This information is not directly exploitable, but can aid a malicious actor in future attacks.
System(s):	Redacted.com/phpinfo.php
Tools Used:	dirsearch; Manual Review
References:	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Evidence

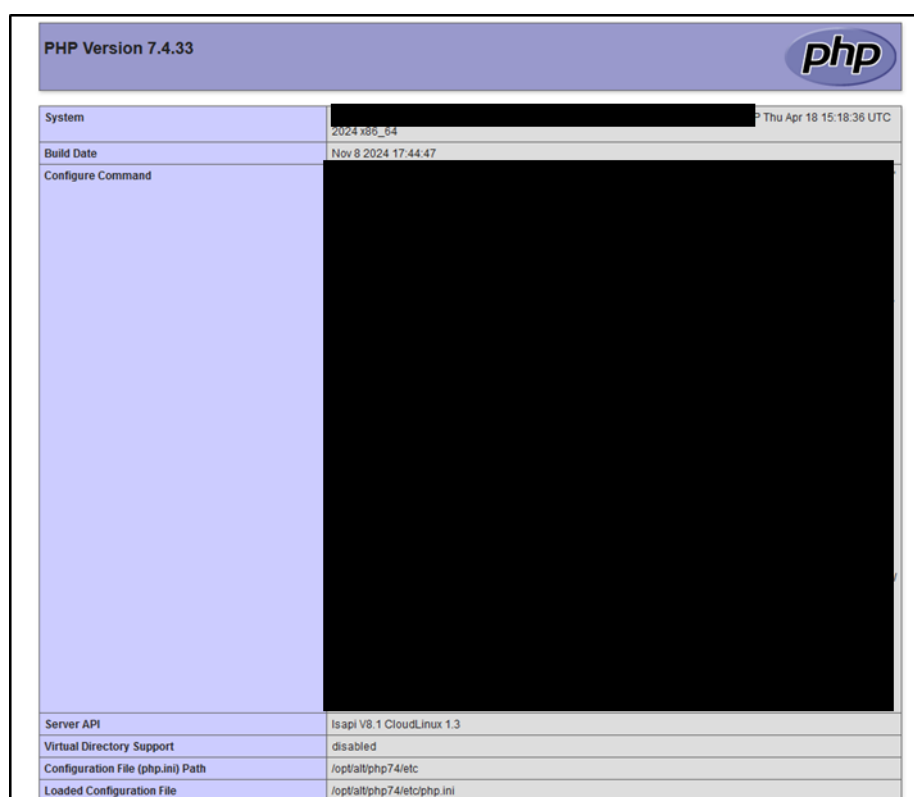


Figure 20 - phpinfo.php File is Publicly Accessible

Remediation

Disable the phpinfo.php file so that it is not viewable by unauthenticated users.



Finding EPT-011: Insufficient Patch Management – Wordpress Plugins (Moderate)

Description:	An externally facing Wordpress webserver has several outdated plugins that have known vulnerabilities. The outdated plugins are the following: • revslider 5.4.1 • js_composer 4.11.2 • jet-elements – Version could not be determined • ckeditor-for-wordpress – Version could not be determined • wp-config-file-editor – Version could not be determined Note: TCMS was unable to develop a successful exploit for any of the vulnerabilities during the engagement period.
Risk:	Likelihood: High – Out of date Wordpress plugins can be discovered by unauthenticated users using tools such as wpscan. Impact: Moderate – The majority of the vulnerabilities discovered require authenticated access to the Wordpress site in order to exploit.
System(s):	redacted.com
Tools Used:	wpscan
References:	NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Evidence

```
[+] revslider
| Location: [REDACTED]
| Last Updated: 2024-11-21T01:20:52.000Z
| [!] The version is out of date, the latest version is 6.7.23
|
| Found By: Comment (Passive Detection)
| Confirmed By:
|   Div Data Version (Passive Detection)
|   Meta Generator (Passive Detection)
|
| [!] 12 vulnerabilities identified:
|
| [!] Title: Revolution Slider <= 6.6.12 - Author+ Remote Code Execution
| Fixed in: 6.6.13
| References:
|   - https://wpscan.com/vulnerability/a8350890-e6d4-4b04-a158-2b0ee3748e65
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2359
|
| [!] Title: Slider Revolution < 6.6.15 - Authenticated (Contributor+) Stored Cross-Site Scripting
| Fixed in: 6.6.15
| References:
|   - https://wpscan.com/vulnerability/3cde24f3-aaad-4eb3-b6ba-a518afe66f6e
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47772
|   - https://www.wordfence.com/threat-intel/vulnerabilities/id/772e843b-00ea-45f5-b730-c9a793d4c2d
|
| [!] Title: Slider Revolution < 6.6.16 - Authenticated (Author+) Arbitrary File Upload
| Fixed in: 6.6.16
| References:
|   - https://wpscan.com/vulnerability/1b841a64-fb0a-434f-b7b4-0777f0480c87
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47784
|   - https://www.wordfence.com/threat-intel/vulnerabilities/id/e2d29afd-06e8-461a-918f-38228441a51
|
| [!] Title: Slider Revolution < 6.6.19 - Author+ Insecure Deserialization leading to RCE
| Fixed in: 6.6.19
| References:
|   - https://wpscan.com/vulnerability/36ced447-84ea-4162-80d2-6df226cb53cb
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6528
|
| [!] Title: Revslider < 6.7.0 - Authenticated (Author+) Stored Cross-Site Scripting
| Fixed in: 6.7.0
```

Figure 21 - revslider Outdated Wordpress Plugin



```
[!] 1 vulnerability identified:

[!] Title: WP Config File Editor <= 1.7.1 - Authenticated Stored Cross-Site Scripting (XSS)
References:
- https://wpscan.com/vulnerability/f35b7c8f-cfb6-42b6-8a3a-8c07cd1e9da0
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24367
```

Figure 22 - wp-config-file-editor Outdated Wordpress Plugin

```
[+] js_composer
Location: [REDACTED]
Last Update: [REDACTED]
[!] The version is out of date, the latest version is 8.0.1

Found By: Urls In Homepage (Passive Detection)
Confirmed By:
Meta Generator (Passive Detection)
Body Tag (Passive Detection)

[!] 9 vulnerabilities identified:

[!] Title: WPBakery Page Builder < 6.4.1 - Authenticated Stored Cross-Site Scripting (XSS)
Fixed in: 6.4.1
References:
- https://wpscan.com/vulnerability/11285589-1b22-4ec0-adfc-f2add70dbd4d7
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28650
- https://www.wordfence.com/blog/2020/10/vulnerability-exposes-over-4-million-sites-using-wpbakery/

[!] Title: WPBakery Page Builder < 6.13.0 - Contributor+ Stored XSS
Fixed in: 6.13.0
References:
- https://wpscan.com/vulnerability/ee99521d-be25-41ef-8988-5cfd66e9c5ca
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-31213

[!] Title: WPBakery Visual Composer < 7.6 - Authenticated (Contributor+) Stored Cross-Site Scripting via Post Title tag attribute
Fixed in: 7.6
References:
- https://wpscan.com/vulnerability/787a71f8-1179-4442-9441-87f8e83a7e67
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1841
- https://www.wordfence.com/threat-intel/vulnerabilities/id/34d21418-4faf-40bf-a960-79482a592722

[!] Title: WPBakery Visual Composer < 7.6 - Authenticated (Contributor+) Stored Cross-Site Scripting via Custom Heading tag attribute
Fixed in: 7.6
References:
- https://wpscan.com/vulnerability/8ebfad34-7b46-4783-9fad-c96ab4f4c737
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1842
- https://www.wordfence.com/threat-intel/vulnerabilities/id/674e6722-d293-4572-80bf-984e74c3e33f

[!] Title: WPBakery Visual Composer < 7.6 - Authenticated (Contributor+) Stored Cross-Site Scripting via Button onclick attribute
Fixed in: 7.6
References:
- https://wpscan.com/vulnerability/b87926cd-0fe0-49df-8c61-9df1363a67a8
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1805
```

Figure 23 - js_composer Outdated Wordpress Plugin



```
[!] 3 vulnerabilities identified:

[!] Title: JetElements For Elementor < 2.6.13.1 - Missing Authorization to Unauthenticated Arbitrary Attachment Download
Fixed in: 2.6.13.1
References:
- https://wpscan.com/vulnerability/cf9c4f4f-d7ba-41c5-b817-61f5879119f8
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48759
- https://www.wordfence.com/threat-intel/vulnerabilities/id/d199e597-64ed-4dcc-a153-b5c8e4e9e93d

[!] Title: JetElements < 2.6.20.1 - Authenticated (Contributor+) Arbitrary Local File Inclusion
Fixed in: 2.6.20.1
References:
- https://wpscan.com/vulnerability/b662edc4-80d7-4a4e-a4d3-31bc94257cf2
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-7145
- https://www.wordfence.com/threat-intel/vulnerabilities/id/793f27ec-a3bb-4273-a41c-cc5b04c8e8fc

[!] Title: JetElements < 2.6.20.1 - Authenticated (Contributor+) Stored Cross-Site Scripting
Fixed in: 2.6.20.1
References:
- https://wpscan.com/vulnerability/c8adfc30-3ad4-4514-b50a-1c3f04a9299a
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-7144
- https://www.wordfence.com/threat-intel/vulnerabilities/id/c5e64adf-49b3-4e85-8dc1-918f7e92965b

The version could not be determined.
```

Figure 24 - jet-elements Outdated Wordpress Plugin

```
[!] 1 vulnerability identified:

[!] Title: CKEditor for WordPress <= 4.5.3 - Authenticated Reflected Cross-Site Scripting (XSS)
Fixed in: 4.5.3.1
References:
- https://wpscan.com/vulnerability/d6076ee4-02cd-41f4-9b81-0eae36c70dd7
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9349
- http://cinu.pl/research/wp-plugins/mail_671ea8cb1c6d71f59599643c90f2573c.html
- http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html

The version could not be determined.
```

Figure 25 - ckeditor-for-wordpress Outdated Wordpress Plugin

Remediation

Update to the latest versions of software in accordance with vendor instructions.



Finding EPT-012: Default Web Server Landing Page (Low)

Description:	DemoCorp deploys Microsoft IIS and Plesk with default landing pages. Default web server landing pages provide an attacker with information about the underlying web server.
Risk:	Likelihood: High – Adversaries will discover this information with open-source tools. Impact: Low – Adversaries can use this information to focus attacks. With publication of new vulnerabilities, adversaries can target known instances of vulnerable software
System(s):	Redacted
Tools Used:	Manual Review
References:	NIST SP 800-53r5 CM-7 – Least Functionality

Evidence

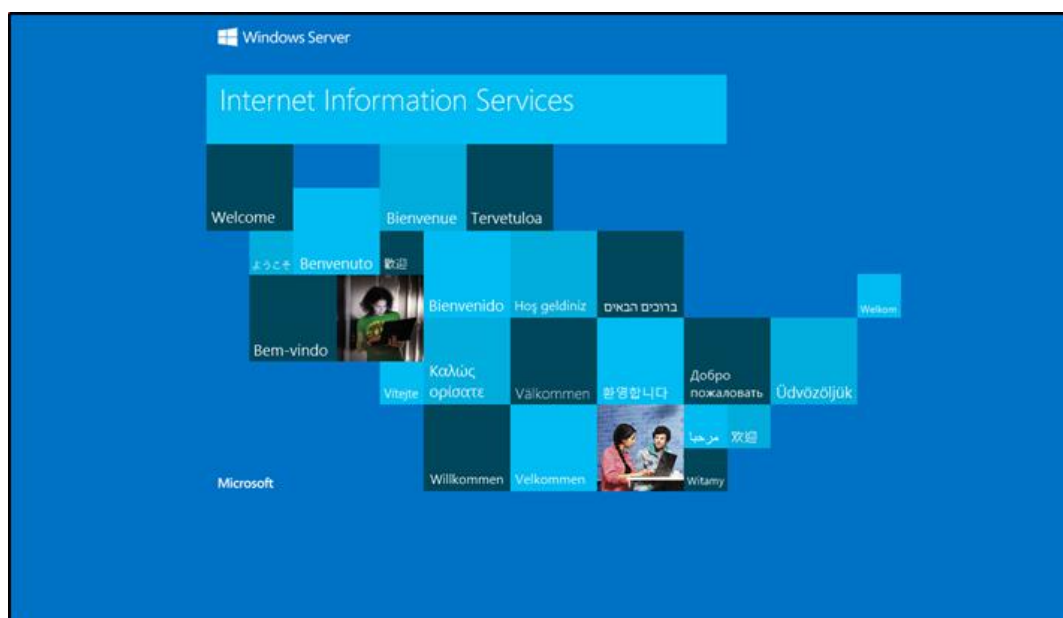


Figure 26 - Microsoft IIS Default Landing Page

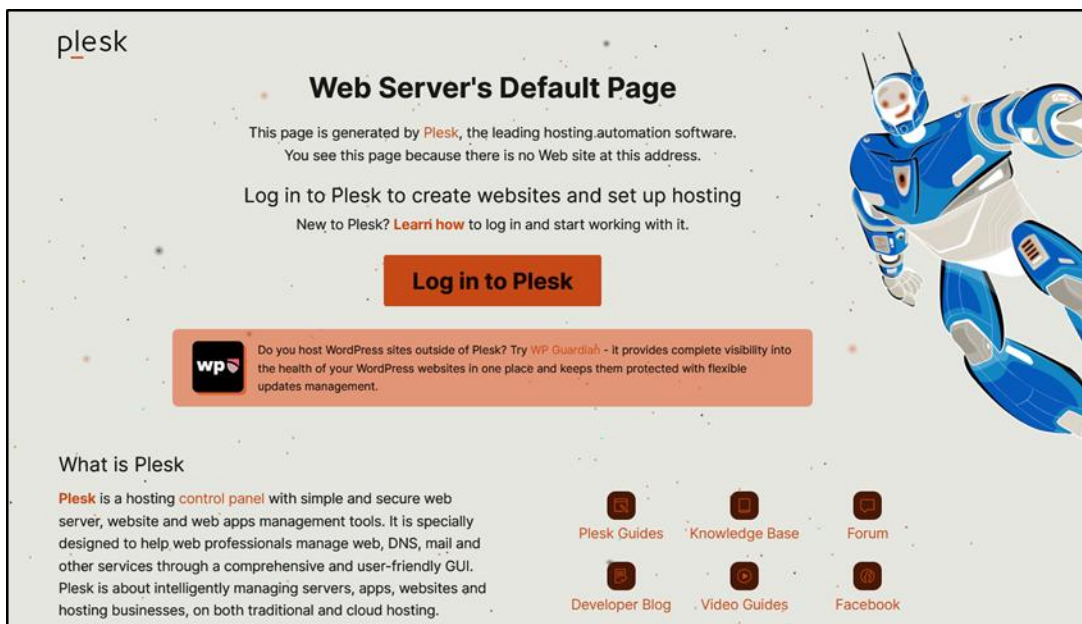


Figure 27 - Plesk Default Landing Page

Remediation

Disable the default landing pages.



Finding EPT-013: Security Misconfiguration – Information Disclosure via HTTP Response Headers (Low)

Description:	The DemoCorp application discloses web server version information through HTTP response headers.
Risk:	Likelihood: High – This information can be discovered by observing the HTTP response headers of web traffic to the impacted sites. Impact: Low – This information could allow an attacker to fingerprint these web servers to better target future exploit attempts.
System(s):	redacted.com
Tools Used:	Burp Suite
References:	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere OWASP – Security Headers Project

Evidence

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 18:53:31 GMT
3 Content-Type: text/html; charset=UTF-8
4 Content-Length: 0
5 Connection: keep-alive
6 Server: Apache
7 X-Powered-By: PHP/7.4.10
8 X-DS-Version: 1714677663
9 Age: 3
10
11
```

Figure 28 - redacted Leaks PHP Version

```
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Fri, 13 Dec 2024 17:43:48 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 447500
6 X-Powered-By: PHP/8.3.14
7 Server-Timing:
8 Strict-Transport-Security: max-age=31536000; includeSubDomains
9 X-Frame-Options: SAMEORIGIN
```

Figure 29 - redacted Leaks PHP Version

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Server: openresty
3 Date: Thu, 12 Dec 2024 17:37:04 GMT
4 Content-Type: text/xml; charset=UTF-8
5 Age: 0
6 Cache-Control: max-age=2592000
7 Content-Security-Policy: upgrade-insecure-requests
8 Expires: Sat, 11 Jan 2025 17:37:01 GMT
9 Strict-Transport-Security: max-age=300
10 Vary: Accept-Encoding, User-Agent
11 X-Cache: uncached
12 X-Cache-Hit: MISS
13 X-Cacheproxy-Retries: 0/2
14 X-Content-Type-Options: nosniff
15 X-Fawn-Proc-Count: 1,1,24
16 X-Php-Version: 7.4
17 X-Robots-tag: noindex, follow
```

Figure 30 - Leaks PHP Version



```
Response
Pretty Raw Hex Render
1 HTTP/2 405 Method Not Allowed
2 Allow: GET, HEAD, OPTIONS, TRACE
3 Content-Type: text/html
4 Server: Microsoft-IIS/10.0
5 Date: Mon, 09 Dec 2024 21:54:05 GMT
6 Content-Length: 1293
7
```

Figure 31 - DemoCorp.ca Leaks IIS Version

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 X-Powered-By: PHP/7.4.33
3 X-Frame-Options: SAMEORIGIN
4 Permissions-Policy: interest-cohort=()
5 Content-Type: text/html; charset=utf-8
6 Expires: Wed, 17 Aug 2005 00:00:00 GMT
7 Last-Modified: Wed, 11 Dec 2024 21:34:55 GMT
8 Cache-Control: no-store, no-cache, must-revalidate,
9 Pragma: no-cache
10 Vary: Accept-Encoding
11 Date: Wed, 11 Dec 2024 21:34:55 GMT
12 Server: LiteSpeed
```

Figure 32 - Redacted Leaks PHP Version

Remediation

Remove unnecessary information from HTTP response headers. Consult vendor documentation for instructions and best practices.



Finding EPT-014: Security Misconfiguration – Wordpress Debug Log Information Disclosure (Low)

Description:	The Wordpress debug.log file is readable by any unauthenticated user. This file contains debug information that includes system paths, source code snippets, etc.
Risk:	Likelihood: High – The debug.log file is viewable by any unauthenticated user and is included in many directory fuzzing wordlists. Impact: Low – This file contains debug information that includes system paths, source code snippets, etc. This information is not directly exploitable but can aid a malicious actor in future attacks.
System(s):	redacted.com/wp-content/debug.log
Tools Used:	dirsearch; Manual Review
References:	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Evidence

```
19-Sep-2022 16:41:32 UTC] PHP Deprecated: Function create_function() is deprecated in /var/www/wp-content/plugins/rev-slider/includes/framework/functions-wordpress.class.php on line 258
19-Sep-2022 16:41:32 UTC] PHP Deprecated: Function create_function() is deprecated in /var/www/wp-content/themes/cosmetro/cherry-framework/setup.php on line 14
19-Sep-2022 16:41:32 UTC] PHP Deprecated: The each() function is deprecated. This message will be suppressed on further calls in /var/www/wp-content/plugins/js_composer/include/classes/core/class-vc-mapper.php on line 111
19-Sep-2022 16:41:38 UTC] PHP Deprecated: Function create_function() is deprecated in /var/www/wp-content/plugins/rev-slider/includes/framework/functions-wordpress.class.php on line 258
19-Sep-2022 16:41:38 UTC] PHP Deprecated: Function create_function() is deprecated in /var/www/wp-content/themes/cosmetro/cherry-framework/setup.php on line 14
19-Sep-2022 16:41:38 UTC] PHP Deprecated: The each() function is deprecated. This message will be suppressed on further calls in /var/www/wp-content/plugins/js_composer/include/classes/core/class-vc-mapper.php on line 111
```

Figure 33 - Wordpress debug.log File

Remediation

Restrict permissions on the debug.log file so that it is not publicly facing



Finding EPT-015: Security Misconfiguration – Wordpress Login Page is Public (Low)

Description:	There is an externally facing Wordpress login page available. These pages are often targeted by attackers with password spraying/or credential brute forcing attacks.
Risk:	Likelihood: Low – TCMS was unable to successfully guess valid credentials. IP addresses are also blocked after several failed attempts. Impact: High – If credentials were successfully guessed, an attacker would gain access to the Wordpress admin portal which could result in remote code execution, site defacement, etc.
System(s):	redacted.com/wp-login.php
Tools Used:	Manual Review
References:	How to Limit Access by IP to Your wp-login.php file in WordPress

Evidence

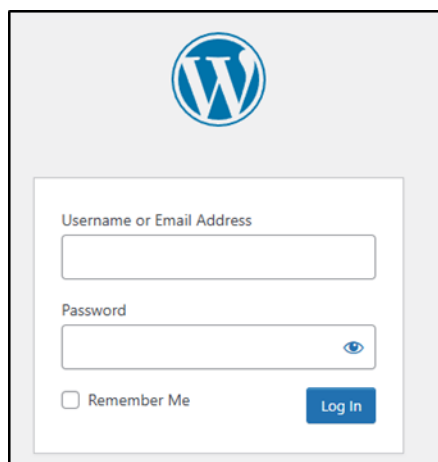


Figure 34 - wp-login.php is Externally Accessible

Remediation

Add IP whitelisting to the wp-login.php page.



Finding EPT-016: Outdated Wordpress Blog (Informational)

Description:	There is an externally facing Wordpress blog that has a welcome post dating back to September 26th, 2014. The blog appears to not be in use.
Risk:	Likelihood: Very High – This blog page is trivial to discover as Wordpress URIs are commonly fuzzed by attackers. Impact: Low – The blog itself is not directly exploitable.
System(s):	redacted.com/wp
Tools Used:	Manual Review
References:	OWASP A06:2021 – Vulnerable and Outdated Components

Evidence

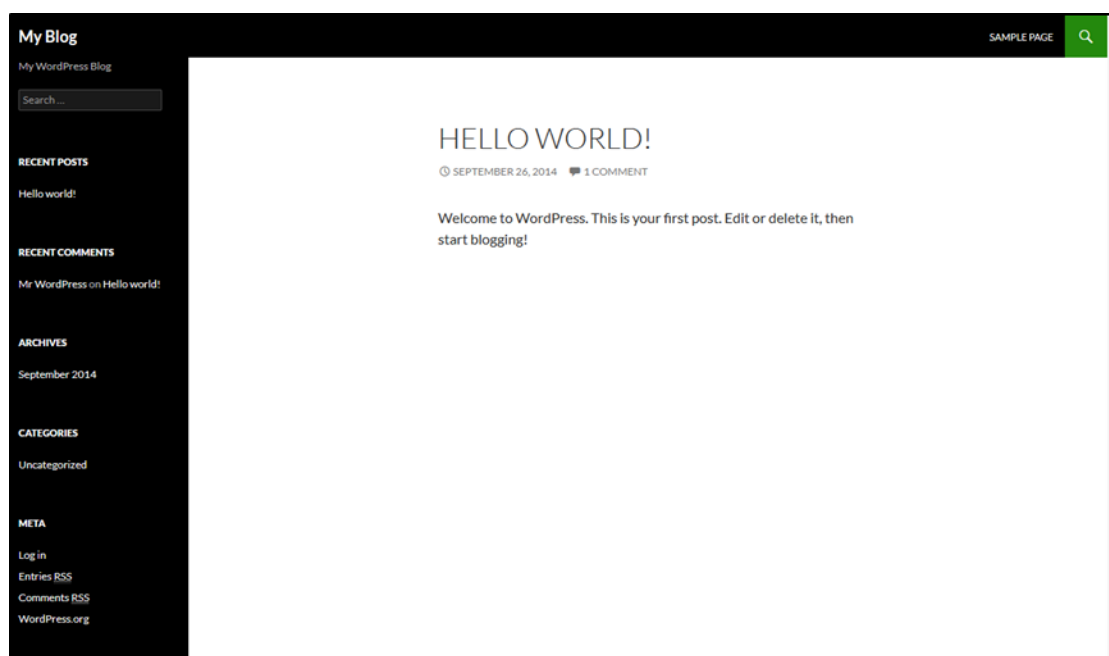


Figure 35 - Outdated Wordpress Blog

Remediation

If not in use, remove the blog page to reduce Wordpress attack surface.



Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.



Last Page