

Sample Penetration Test Report Apache HTTP Server

Date: 08 July 2024  
 Version 1.0

# Introduction

This is a pentesting report for Apache HTTP Server vulnerabilities. The vulnerabilities addressed in this report include Path Traversal and Remote Code Execution. The impact of these vulnerabilities includes unauthorized access to the server, data theft, and potential network compromise. It is crucial to address these vulnerabilities promptly to protect the security and integrity of the network infrastructure.

# Findings

## Nmap Scan Results

889/tcp open http Apache httpd 2.4.50 ((Unix))

## Vulnerability Exploitation Results

http://152.42.212.132:889 is vulnerable to Path Traversal Attack (CVE-2021-42013)  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

# Recommendation

To mitigate the identified vulnerabilities (CVE-2021-42013 and CVE-2021-41773), it is recommended to take the following steps:  
1. Update Apache HTTP Server:  
 - Upgrade to the latest version of Apache HTTP Server where these vulnerabilities have been patched.  
 - Regularly apply updates and patches from the Apache Software Foundation.  
2. Configure the Server Securely:  
 - Disable the use of vulnerable modules such as mod\_cgi, unless absolutely necessary.  
 - Restrict access to the server by configuring the `Directory` settings correctly. For example, use `Options -Indexes` and `Require all denied` to restrict unauthorized access.  
3. Employ Web Application Firewalls (WAF):  
 - Use a WAF to detect and block malicious requests that may exploit path traversal and RCE vulnerabilities.  
4. Regular Security Audits:  
 - Conduct regular security audits and vulnerability assessments to identify and address potential security issues.  
5. Logging and Monitoring:  
 - Enable detailed logging and regularly monitor logs for suspicious activity.  
 - Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and protect against exploits.  
6. Access Controls:  
 - Implement strong access controls to limit who can modify the server configuration and execute scripts.  
7. Input Validation:  
 - Implement strict input validation to ensure that user input is sanitized and validated before processing.  
By following these recommendations, the risk associated with CVE-2021-42013 and CVE-2021-41773 can be significantly reduced, helping to ensure the security and integrity of the Apache HTTP Server.