Pentest report - 192.99.54.66

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **192.99.54.66** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.
The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.
Date: 2024-05-15 15:15
Target : 192.99.54.66
Type: vulnerability scanner

II. DNS Request

Check your domain name or the API website (https://networkcalc.com/api/)

III. Data about HTTP/HTTPS certificate

Error. Check your domain name or the API website (https://networkcalc.com/api/)

IV. Subdirectories Found

Subdirectories

V. NMAP scan

Port	Service	Version
22	ssh	7.2p2 Ubuntu 4ubuntu2.10
80	http	2.4.18
2222	ssh	7.2p2 Ubuntu 4ubuntu2.10
8080	http-proxy	

VI. Nikto scan

Web server : Apache/2.4.18 (Ubuntu)
The server supports compression.
Version of software might be found in the following header Server : 2.4.18
Target URL don't use any redirection
Target URL isn't protected by a basic HTTP authentication
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined.
The X-Content-Type-Options header is not set.

VII. Potential vulnerabilities

CVE ID	Description	Score
CVE-2015-8325	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.	7.8
CVE-2016-6515	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.	7.5
CVE-2016-8858	The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party	7.5

CVE ID	Description	Score
	reports that "OpenSSH upstream does not consider this as a security issue."	
CVE-2016-1000	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-0999.	8.8
CVE-2023-3578	A vulnerability classified as critical was found in DedeCMS 5.7.109. Affected by this vulnerability is an unknown functionality of the file co_do.php. The manipulation of the argument rssurl leads to server-side request forgery. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-233371.	9.8
CVE-2016-1001	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors.	8.8
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call	9.8

CVE ID	Description	Score
	ap_hook_process_connection() during an HTTP request to an HTTPS port.	
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.	7.8
CVE-2022-2394	Puppet Bolt prior to version 3.24.0 will print sensitive parameters when planning a run resulting in them potentially being logged when run programmatically, such as via Puppet Enterprise.	3.5
CVE-2022-3181	Failed to fetch CVE details	
CVE-2017-7679	Failed to fetch CVE details	
CVE-2022-2272	This vulnerability allows remote attackers to bypass authentication on affected installations of Sante PACS Server 3.0.4. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of calls to the login endpoint. When parsing the username element, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17331.	9.8
CVE-2023-2569	Failed to fetch CVE details	
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the	9.8

CVE ID	Description	Score
	ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	
CVE-2021-3927	Failed to fetch CVE details	
CVE-2015-8325	Failed to fetch CVE details	
CVE-2016-6515	Failed to fetch CVE details	
CVE-2016-8858	Failed to fetch CVE details	
CVE-2016-1000	Failed to fetch CVE details	
CVE-2023-3578	Failed to fetch CVE details	
CVE-2016-1001	Failed to fetch CVE details	

VIII. Exploit find

Exploits found for CVE-CVE-2019-0211:

Exploit Title	Path
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privil	linux/local/46676.php

Exploits found for CVE-CVE-2016-6515:

Exploit Title	Path
OpenSSH 7.2 - Denial of Service	linux/dos/40888.py

Exploits found for CVE-CVE-2021-4479:

Exploit Title	Path
Apache 2.4.x - Buffer Overflow	multiple/webapps/51193.py

Exploits found for CVE-CVE-2016-1000:

Exploit Title	Path
Adobe Flash - Sprite Creation Use-After-Free	windows/dos/39610.txt
Joomla! Component Huge-IT Portfolio Gallery Plugin 1.0.6 - SQL Injectio	php/webapps/42597.txt
Joomla! Component Huge-IT Portfolio Gallery Plugin 1.0.7 - SQL Injectio	php/webapps/42598.txt
Joomla! Component Huge-IT Video Gallery 1.0.9 - SQL Injection	php/webapps/42596.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt

Exploits found for CVE-CVE-2022-3181:

Exploit Title	Path
pfBlockerNG 2.1.4_26 - Remote Code Execution (RCE)	php/webapps/51032.py

Exploits found for CVE-CVE-2016-1001:

Exploit Title	Path
Adobe Flash - Zlib Codec Heap Overflow	windows/dos/39609.txt
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain	linux/local/40962.txt

IX. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.
We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.
By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.