Pentest report - 192.99.54.66

Summary

I. Overview

II. DNS Request

III. Data about HTTP/HTTPS certificate

IV. NMAP scan

V. Nikto scan

VI. Potential vulnerabilities

VII. Exploit find

VIII. Recommendations

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: 2024-05-09 08:40
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. 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	

V. 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.

VI. Potential vulnerabilities

CVE ID	Description	Score
CVE-2012-1577	lib/libc/stdlib/random.c in OpenBSD returns 0 when seeded with 0.	9.8
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-2016-1000	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-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	8.8

CVE ID	Description	Score
	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.	
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 reports that "OpenSSH upstream does not consider this as a security issue."	7.5
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 ap_hook_process_connection() during an HTTP request to an HTTPS port.	9.8
CVE-2021-3927	vim is vulnerable to Heap-based Buffer Overflow	7.8
CVE-2022-2272	Failed to fetch CVE details	

CVE ID	Description	Score
CVE-2023-2569	Failed to fetch CVE details	
CVE-2021-4479	Failed to fetch CVE details	
CVE-2017-7679	Failed to fetch CVE details	
CVE-2022-3181	Failed to fetch CVE details	
CVE-2017-3167	Failed to fetch CVE details	
CVE-2019-0211	Failed to fetch CVE details	
CVE-2022-2394	Failed to fetch CVE details	
CVE-2012-1577	Failed to fetch CVE details	
CVE-2023-3578	Failed to fetch CVE details	
CVE-2016-1000	Failed to fetch CVE details	
CVE-2016-1001	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	

VII. Exploit find

Exploits found for CVE-2019-0211:

Exploit Title	Path
Exploit Title	Path
Apache	linux/local/46676.php

Exploits found for CVE-2016-1000:

Exploit Title	Path
Exploit Title	Path
Adobe F	windows/dos/39610.txt
Joomla!	php/webapps/42596.txt
Joomla!	php/webapps/42597.txt
Joomla!	php/webapps/42598.txt
OpenSSH	linux/remote/40963.txt

Exploits found for CVE-2016-1001:

Exploit Title	Path
Exploit Title	Path
Adobe F	windows/dos/39609.txt
OpenSSH	linux/local/40962.txt

Exploits found for CVE-2021-4479:

Exploit Title	Path
Exploit Title	Path
Apache	multiple/webapps/51193.py

Exploits found for CVE-2022-3181:

Exploit Title	Path
Exploit Title	Path
pfBlock	php/webapps/51032.py

Exploits found for CVE-2016-6515:

Exploit Title	Path
Exploit Title	Path
OpenSSH	linux/dos/40888.py

VIII. 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.