International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume X, Issue III, March - 2023

Exploitation Of Remote Code Execution (RCE)

Rajkamal J
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
rajkamalj.ug20.cs@francisxavier.ac.in

Ebrahim Sickkander Nihal P
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
ebrahimsickkanderp.ug20.cs@francisxavier.ac.in

Praywin Samson E
Computer Science and Engineering
Cyber Forensics Applied Lab Student
Francis Xavier Engineering College
Tirunelveli
praywinsamsone.ug20.cs@francisxavier.ac.in

Winson R
Computer Science and Engineering
Francis Xavier Engineering College
Cyber Forensics Applied Lab Student
Tirunelveli
winsonr.ug20.cs@francisxavier.ac.in

Dr. R.ravi
Professor/Dept of Computer Science and Engineering
Francis Xavier Engineering College
Cyber Forensics Applied Lab In Charge
Tirunelveli
winsonr.ug20.cs@francisxavier.ac.in

***Abstract*—This journal paper presents an analysis of the Remote Code Execution (RCE) vulnerability discovered in the popular file management tool, Tiny File Manager. The paper presents several case studies of real-world attacks that have leveraged the Tiny File Manager RCE vulnerability to compromise web servers. Furthermore, the paper outlines the steps that can be taken to prevent this vulnerability and other similar vulnerabilities from being exploited. It emphasizes the importance of proper input validation and access control measures in web applications, as well as keeping software up-to-date with the latest security patches. This paper serves as a valuable resource for web developers and administrators who use Tiny File Manager and other similar web applications.**

***Keywords*— vulnerability, web, paper, file, applications, tiny, manager, rce, sensitive, exploited**

I. INTRODUCTION

Tiny File Manager is a popular file management tool that enables users to manage files and folders on a web server through a user-friendly web interface. However, this tool has recently been found to contain a critical Remote Code Execution (RCE) vulnerability that can allow attackers to execute arbitrary code on the server and potentially take over the system. The vulnerability affects versions 2.4.6 and earlier of Tiny File Manager, which are widely used by web developers and administrators.

The RCE vulnerability in Tiny File Manager is caused by improper input validation of user-supplied data, which can lead to the execution of malicious code on the server. Once the vulnerability is exploited, attackers can gain full control of the server and perform malicious actions, such as stealing sensitive data, deleting files, or installing backdoors.

Given the widespread use of Tiny File Manager and the severity of the vulnerability, web developers and administrators need to update their installations to the latest version and apply any available patches.

RCE :

Remote Code Execution (RCE) is a kind of safety weakness that permits aggressors to execute erratic code on an objective framework. This weakness can happen when an application neglects to appropriately approve client input, permitting an aggressor to infuse and execute malevolent code on the objective framework.[1]

An RCE weakness can have serious outcomes, including full framework split the difference, information burglary, and unapproved admittance to delicate data. A basic security issue requires quick consideration and relief to forestall possible assaults and safeguard the framework and its clients.

Netcat :

Netcat, otherwise called NC, is a strong systems administration utility that can be utilized to peruse and compose information across network associations utilizing TCP or UDP conventions. It can go about as a straightforward document move device or an investigating help for network investigating. Netcat has turned into a famous device for network chairmen and security experts because of its adaptability and flexibility.[2]

Netcat can be utilized to lay out different sorts of organization associations, including TCP or UDP, tuning in or associating modes, and port filtering. It can likewise be utilized to move records among frameworks and perform distant organization assignments. Furthermore, Netcat can be utilized for port sending, standard getting, and network list. Since it is a lightweight device with a little impression, Netcat is frequently utilized for entrance testing and double-dealing. Nonetheless, its power and adaptability likewise make it a potential security risk whenever utilized inappropriately.

Reverse shell:

A reverse shell is a type of shell in which the target system initiates a connection back to the attacker's system, rather than the other way around. This type of shell is typically used in network penetration testing and hacking to provide an attacker with remote access to a target system.

In [5] M. Chandru, S. Kasi Rajesh, S. Eeben, A. Mano Pandiyan, and R. Ravi used Netcat to understand how the reverse shell can be use by the network engineers .To establish a reverse shell, the attacker typically first compromises the target system and then injects a small script or program that initiates a connection to the attacker's system. Once the connection is established, the attacker can execute commands on the target system and access its resources as if they were physically present on the system.

Reverse shells are often used in network exploitation because they can help attackers evade detection by firewalls and other security measures.

II. INITIAL SETUP

Fig 1. Connecting to the Hackthebox network using the OpenVPN file

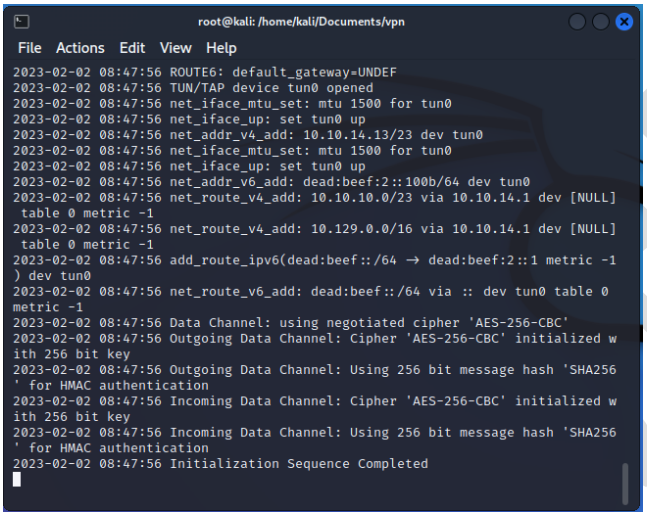


Fig 2. Joining the Machine and Getting the IP address of the Machine

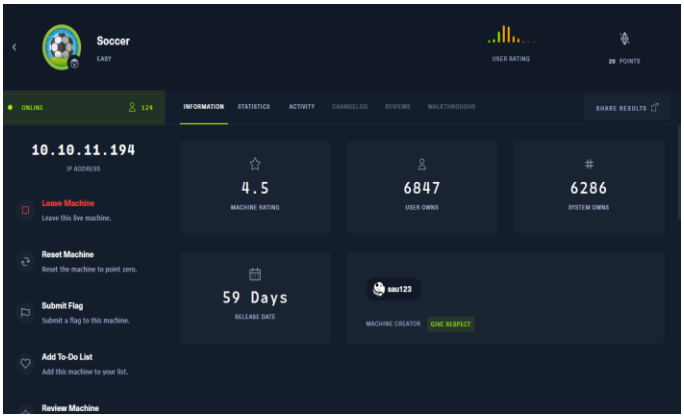
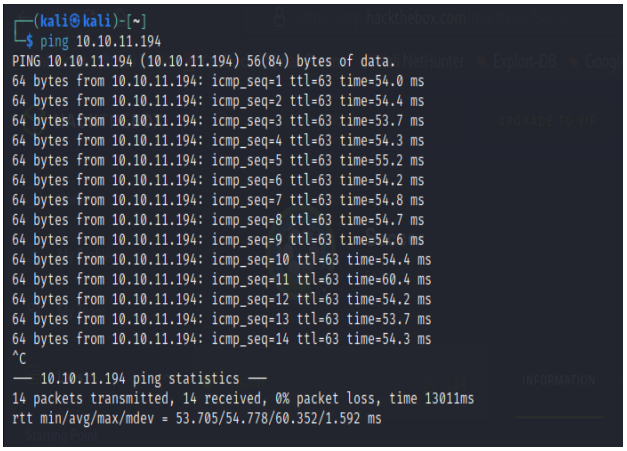
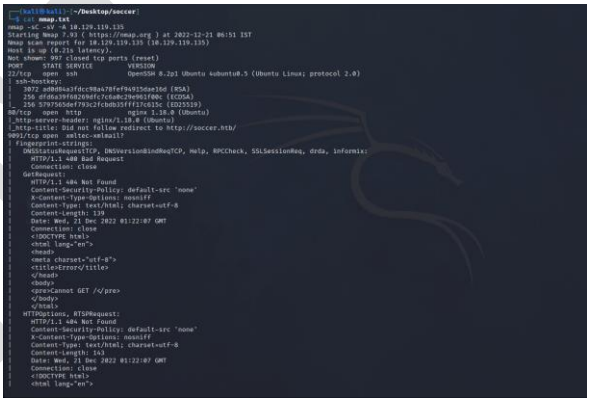


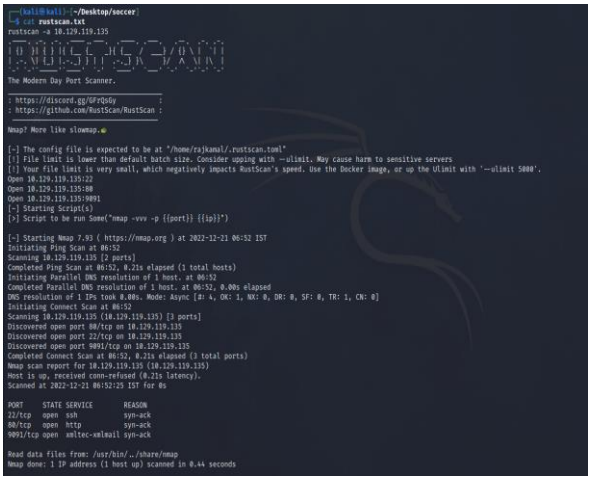
Fig 3. Let's ping the machine and check whether the machine is reachable



III. ENUMERATION OF PORTS

Let's check the open ports in the machine

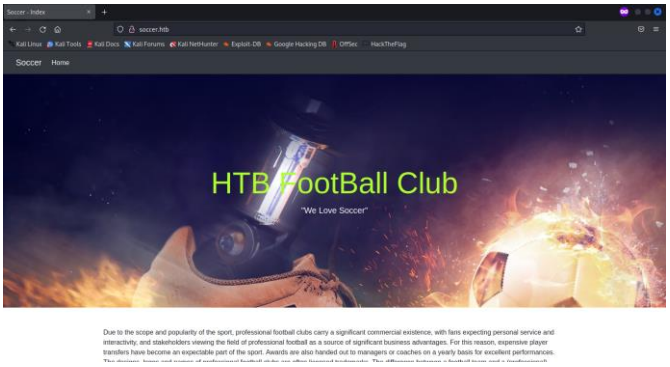




From the scan of nmap and rustscan we come to know that ports 80,22,9091 are open

- Port 80 - It is typically used for HTTP
- Port 22 - It is generally used for SSH
- Port 9091 - It is commonly used for the web user interface of BitTorrent clients

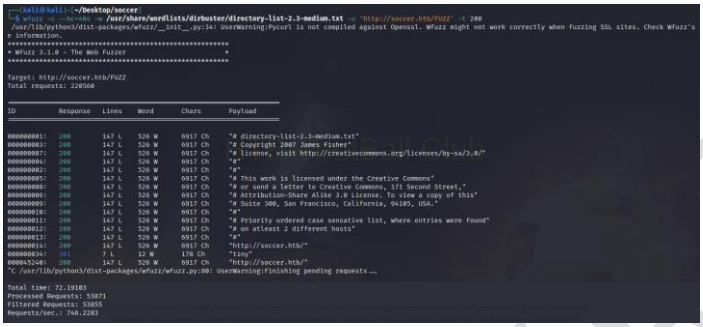
Let's see what's running on port 80 By using the web browser



The main page of the website looks like this. There is nothing significant in the source code as well.

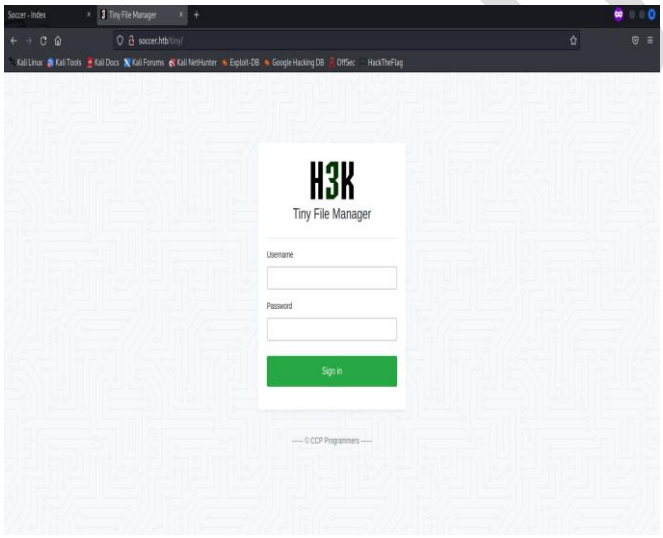
IV. SCANNING FOR ENTRY

So let's try to get the directory of the website using 'wfuzz'[4]



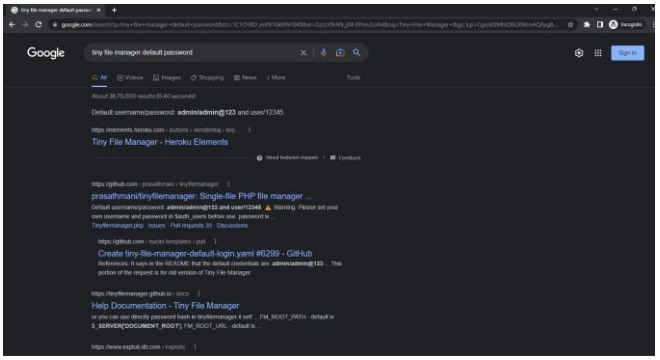
There is a directory called 'tiny'

Let's see what is there in that directory

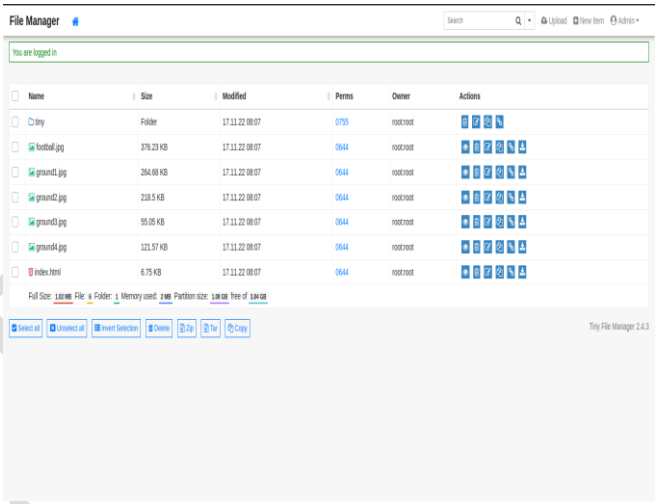


Tiny File Manager is a free web application that allows you to easily manage and edit files and folders on your server through a web browser

Let's find the username of the Tiny File Manager by googling



By trying the default username and password



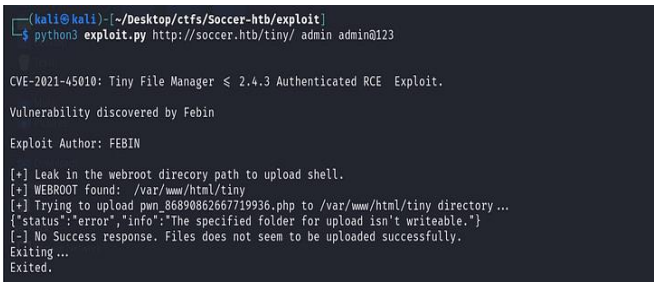
After some googling about the tiny file manager exploit

I came to know that there is a Remote Code Execution in the Tiny File Manager

Exploit-Link

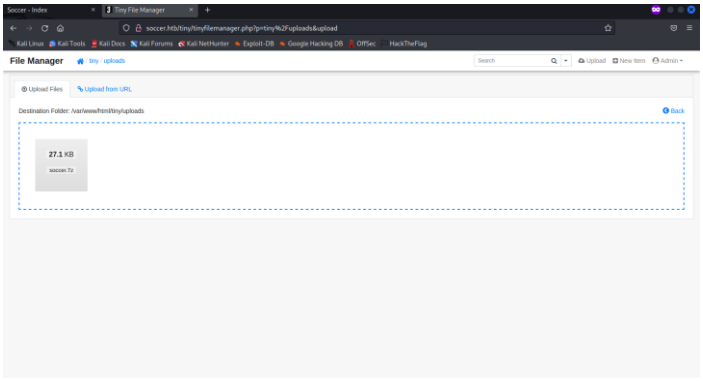
V. EXPLOITING CVE 2021-45010, 2021-40964

Let's try the exploit



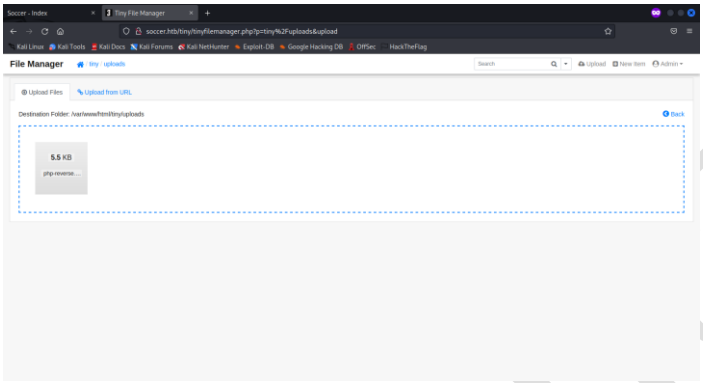
Due to insufficient permissions, we are unable to upload the shell to the webroot.

Let's find the directory where we can upload files.

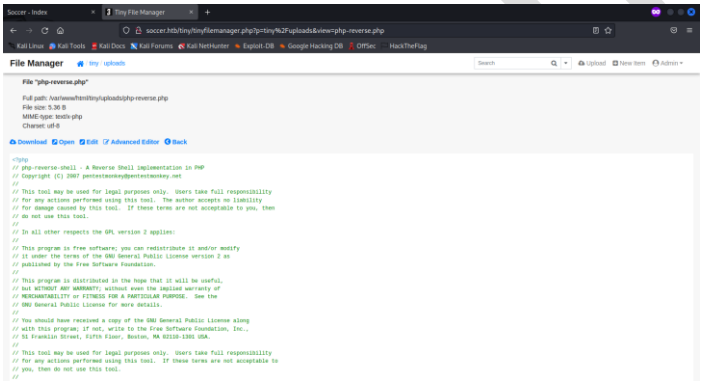


Here we can upload a .7z file

Now let's create a PHP reverse shell and upload it to the folder[3]



Let's open the reverse shell php file



Let the Netcat listen in the port we given in the reverse shell

Now we got the shell of the machine

REFERENCES

[1] Sayar, Imen & Bartel, Alexandre & Bodden, Eric & Le Traon, Yves. (2022). An In-depth Study of Java Deserialization Remote-Code Execution Exploits and Vulnerabilities. ACM Transactions on Software Engineering and Methodology. 32. 10.1145/3554732.

[2] Kostaras, Ioannis & Drabo, Constantin & Juneau, Josh & Reimers, Sven & Schröder, Mario & Wielenga, Geertjan. (2020). The NetCAT Program on Testing. 10.1007/978-1-4842-5370-0_14.

[3] Li, Yu & Huang, Jin & Ikusan, Ademola & Mitchell, Milliken & Zhang, Junjie & Dai, Rui. (2019). ShellBreaker: Automatically Detecting PHP-Based Malicious Web Shells. Computers & Security. 87. 101595. 10.1016/j.cose.2019.101595.

[4] Utama, I & Putri, Kadek & Wirayuda, Anak & Herlambang, Varelly & Listartha, I Made Edy & Saskara, Gede. (2022). Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA. Informatik : Jurnal Ilmu Komputer. 18. 278. 10.52958/iftk.v18i3.5256.

[5] According to M. Chandru, S. Kasi Rajesh, S. Eeben, A. Mano Pandiyan, and R. Ravi (2021) utilize the basic troubleshooting commands to determine the state of the router. Configure the communication server. Use the Cisco Discovery Protocol (formerly known as CDP) to learn the fundamentals of a network's topology