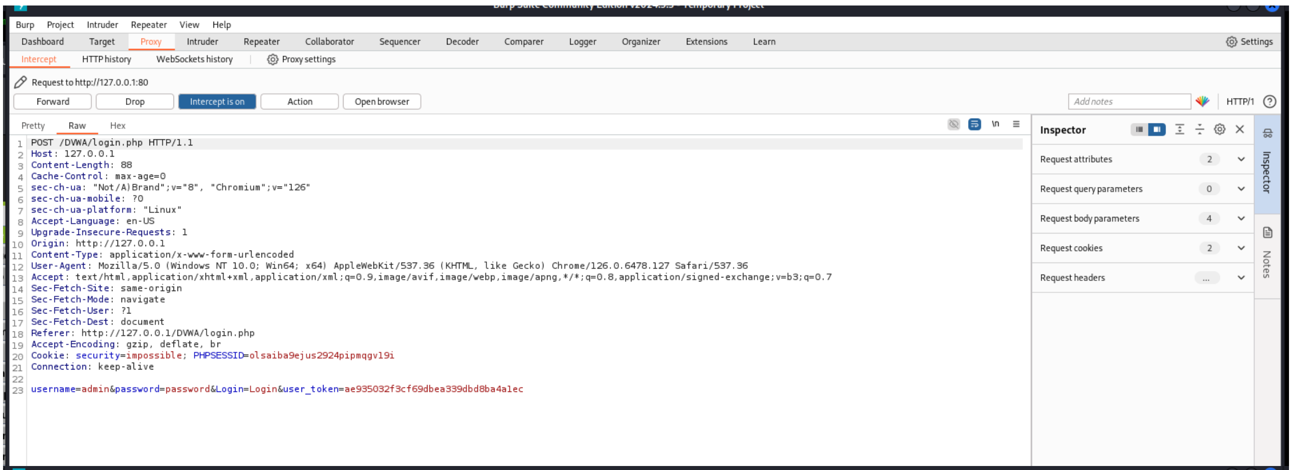
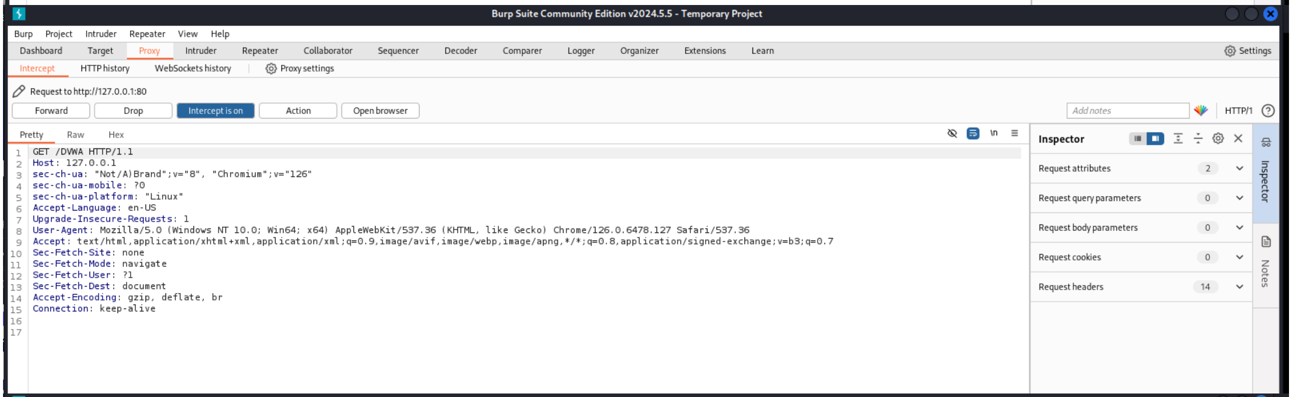
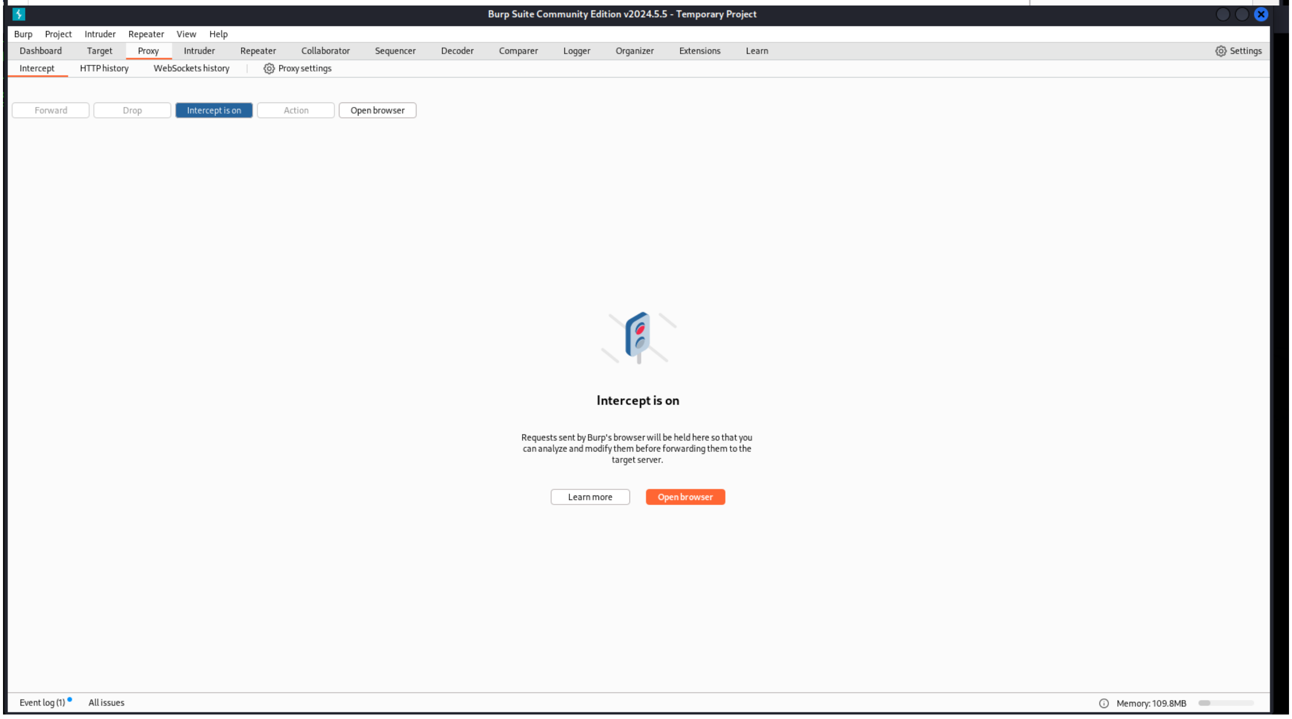

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers ...
Inspector
Notes

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=olsaiba9ejus2924pipmqgv19i
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=ae935032f3cf69dbea339dbd8ba4a1ec
```

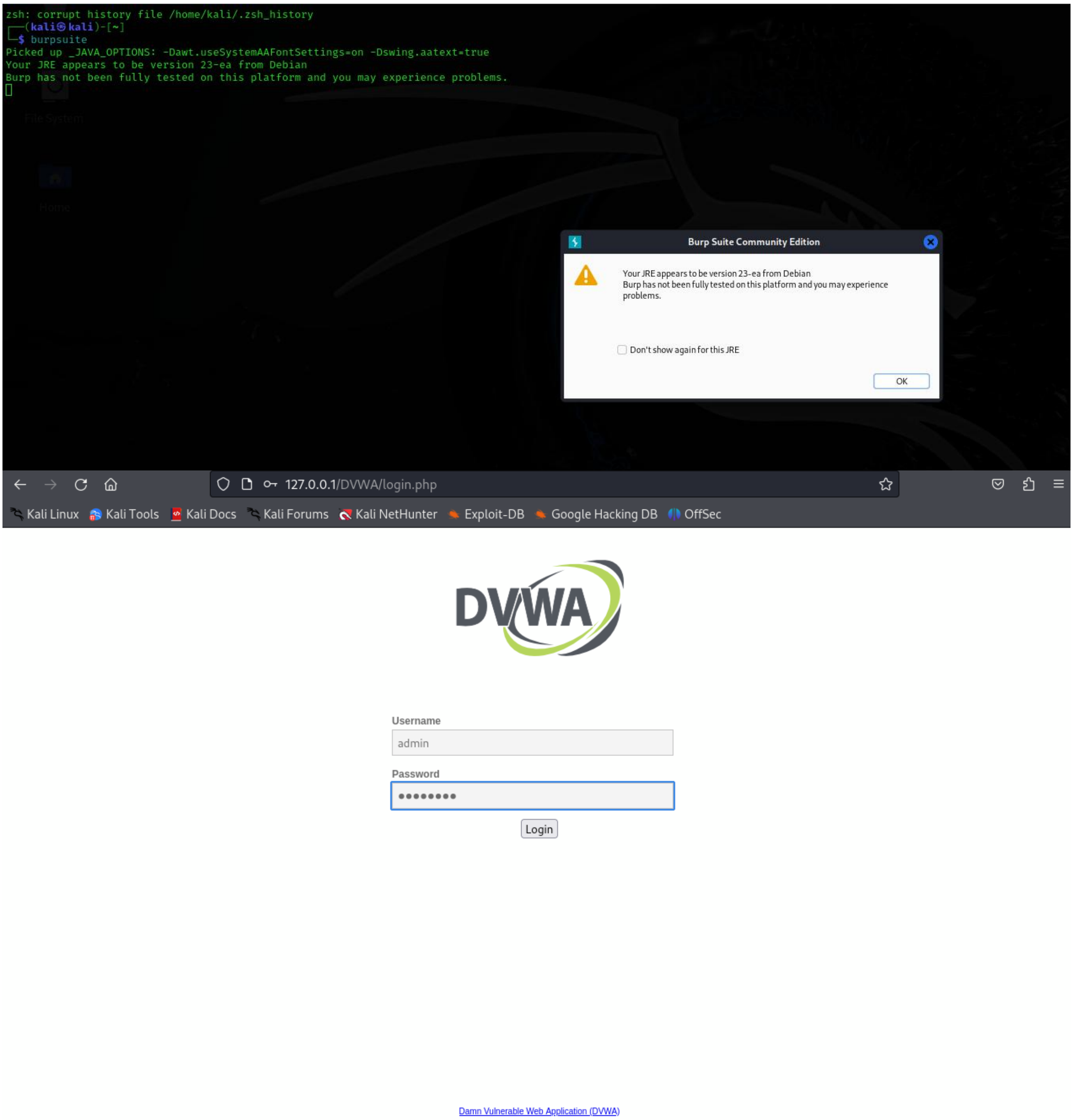

Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 14
Inspector
Notes

```
GET /DVWA HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Learn more
Open browser
Event log (1)
All issues
Memory: 109.8MB

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

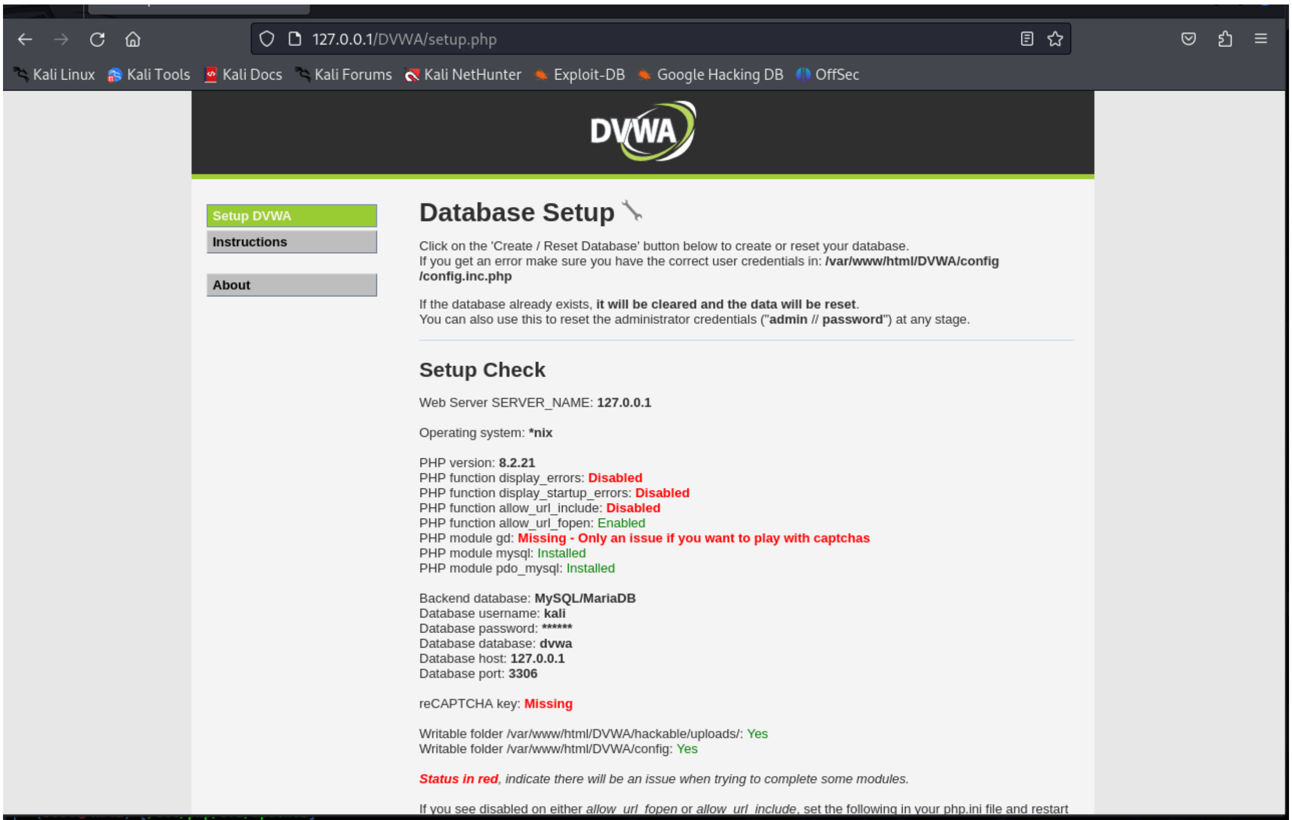
Burp Suite Community Edition

Your JRE appears to be version 23-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE

Username: admin

Password: ••••••••



## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config /config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

### Setup Check

Web Server SERVER_NAME: **127.0.0.1**

Operating system: ***nix**

PHP version: **8.2.21**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

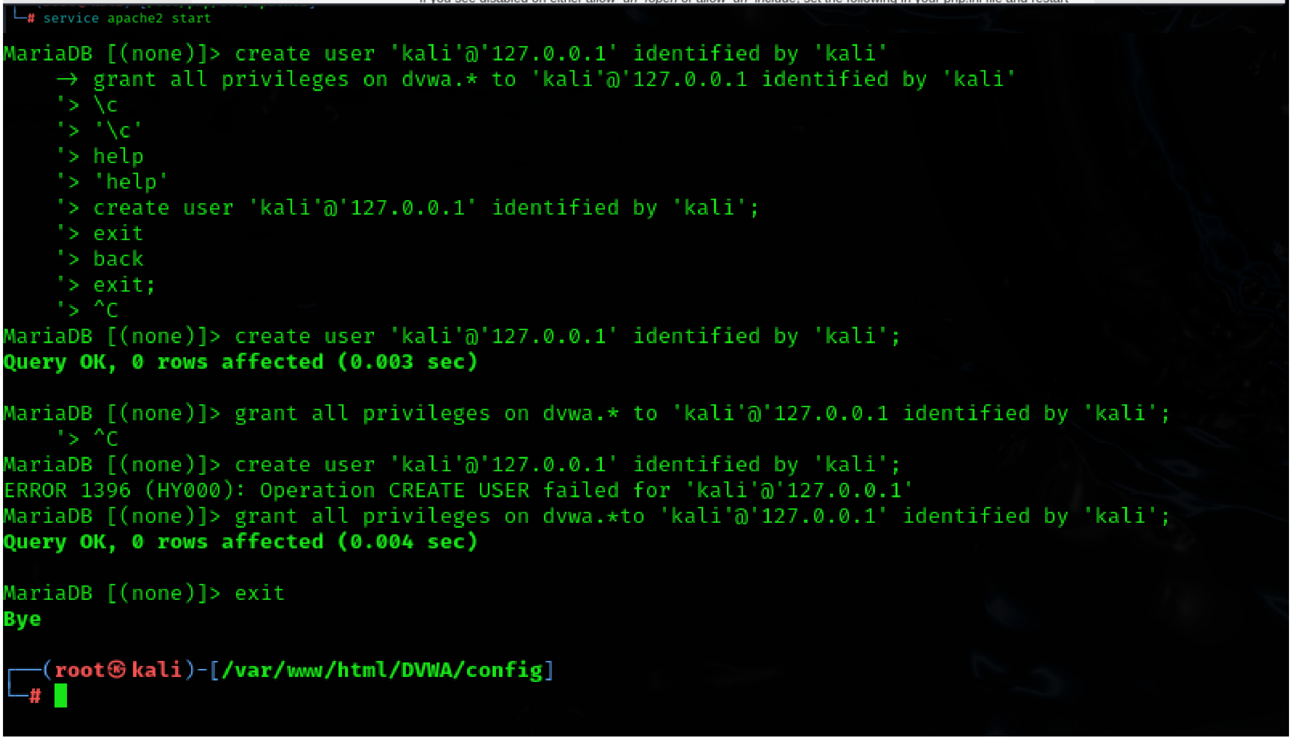
Backend database: **MySQL/MariaDB**
Database username: **kali**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

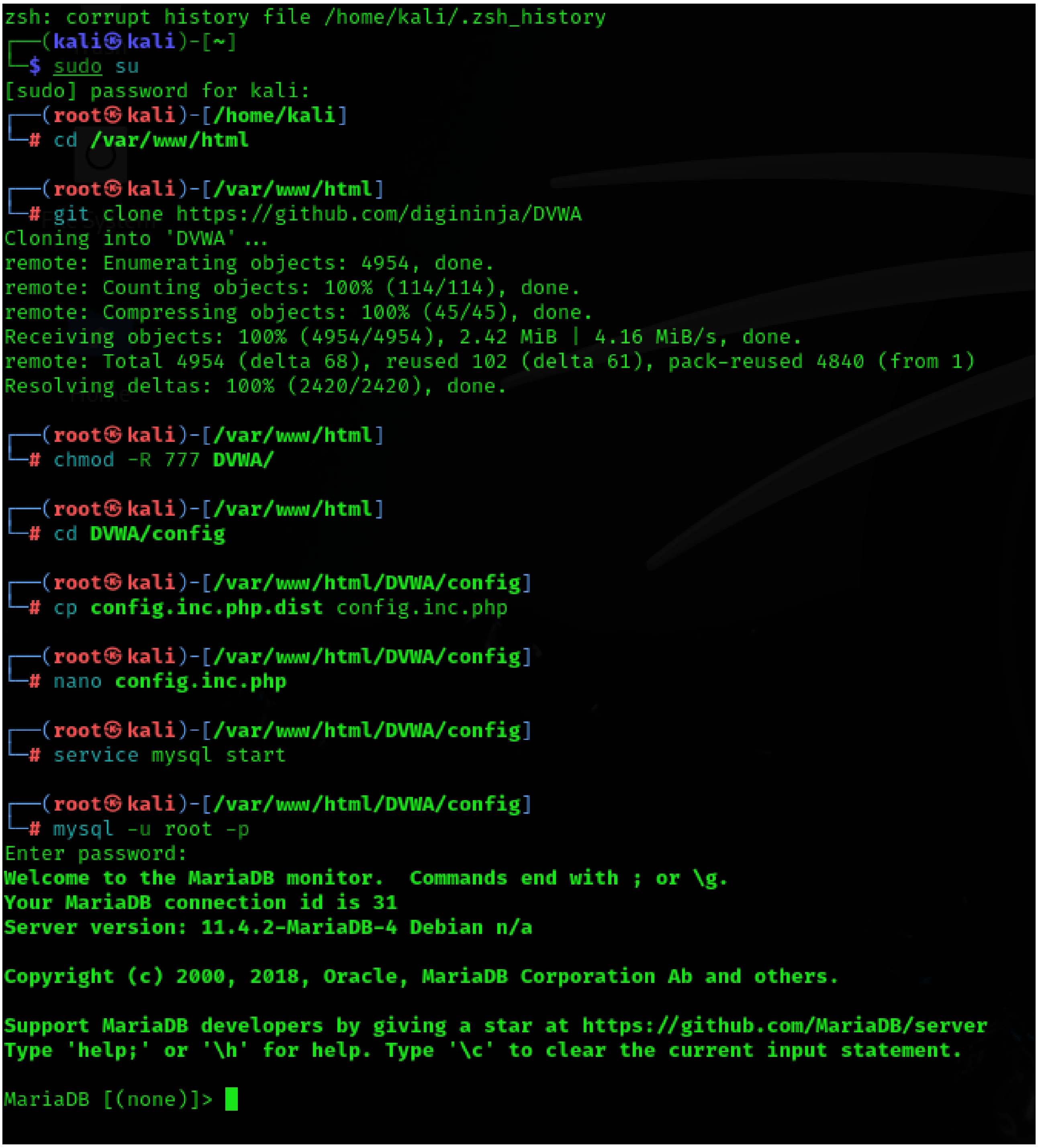
Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

***Status in red***, *indicate there will be an issue when trying to complete some modules.*

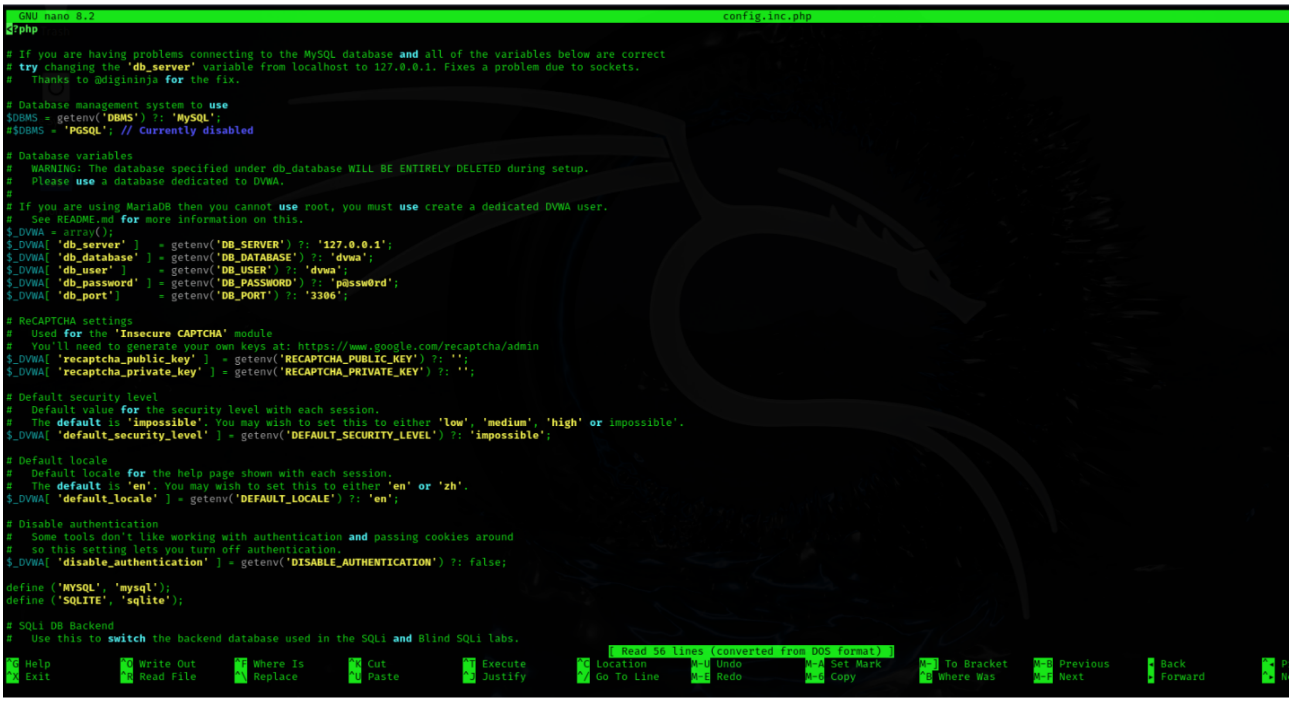
If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart



```
└─# service apache2 start
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali'
    → grant all privileges on dvwa.* to 'kali'@'127.0.0.1 identified by 'kali'
    '> \c
    '> '\c'
    '> help
    '> 'help'
    '> create user 'kali'@'127.0.0.1' identified by 'kali';
    '> exit
    '> back
    '> exit;
    '> ^C
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1 identified by 'kali';
    '> ^C
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
ERROR 1396 (HY000): Operation CREATE USER failed for 'kali'@'127.0.0.1'
MariaDB [(none)]> grant all privileges on dvwa.*to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# 
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
Receiving objects: 100% (4954/4954), 2.42 MiB | 4.16 MiB/s, done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Resolving deltas: 100% (2420/2420), done.

┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/

┌──(root㉿kali)-[/var/www/html]
└─# cd DVWA/config

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service mysql start

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.2-MariaDB-4 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```



```
  GNU nano 8.2                                                                   config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'impossible';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = getenv('DEFAULT_LOCALE') ?: 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = getenv('DISABLE_AUTHENTICATION') ?: false;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
                                                                 [ Read 56 lines (converted from DOS format) ]
^G Help         ^O Write Out    ^F Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set Mark    M-] To Bracket  M-B Previous    ◂ Back          ^◂ P
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo        M-6 Copy        ^B Where Was    M-F Next        ▸ Forward       ^▸ N
```