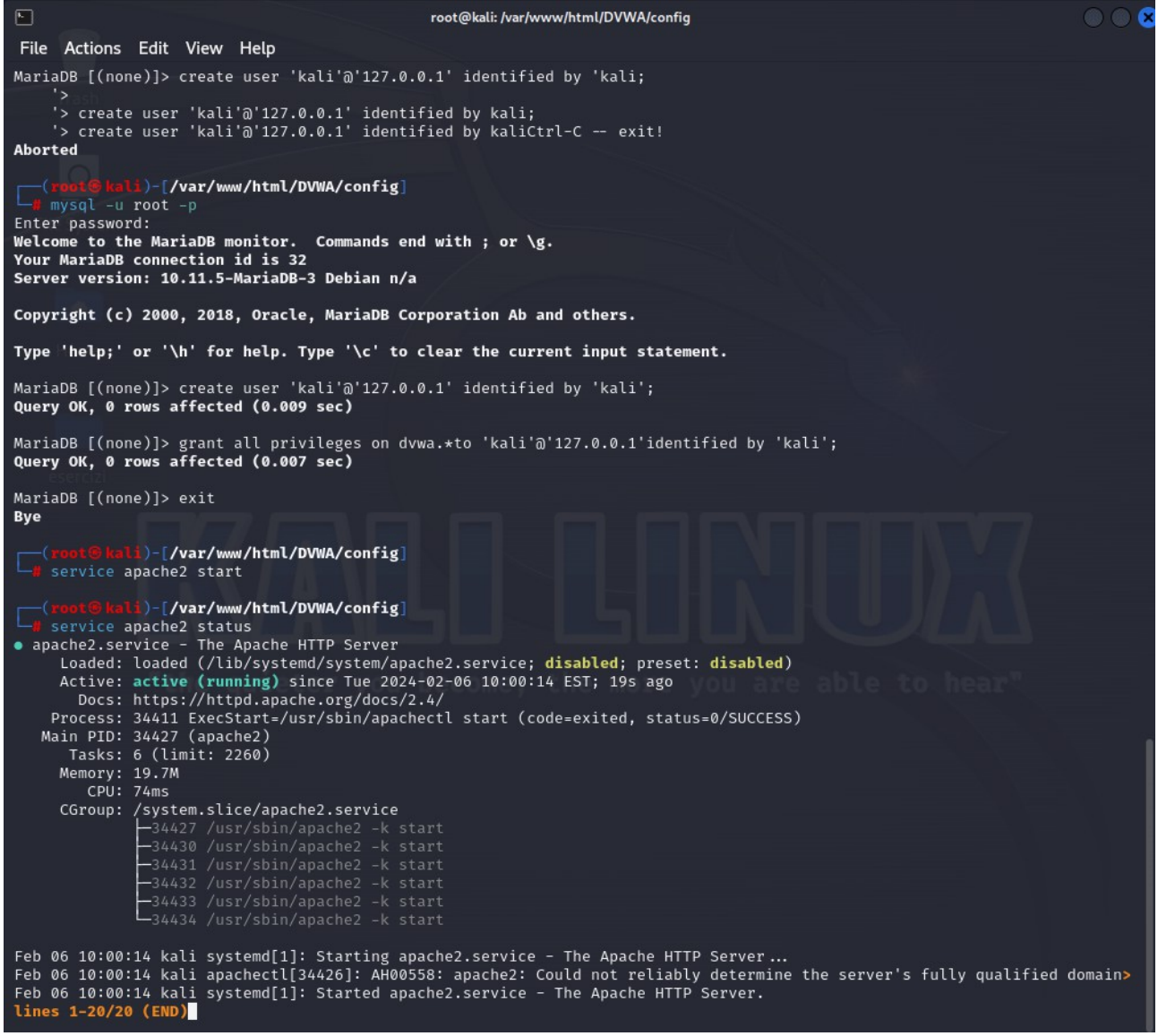
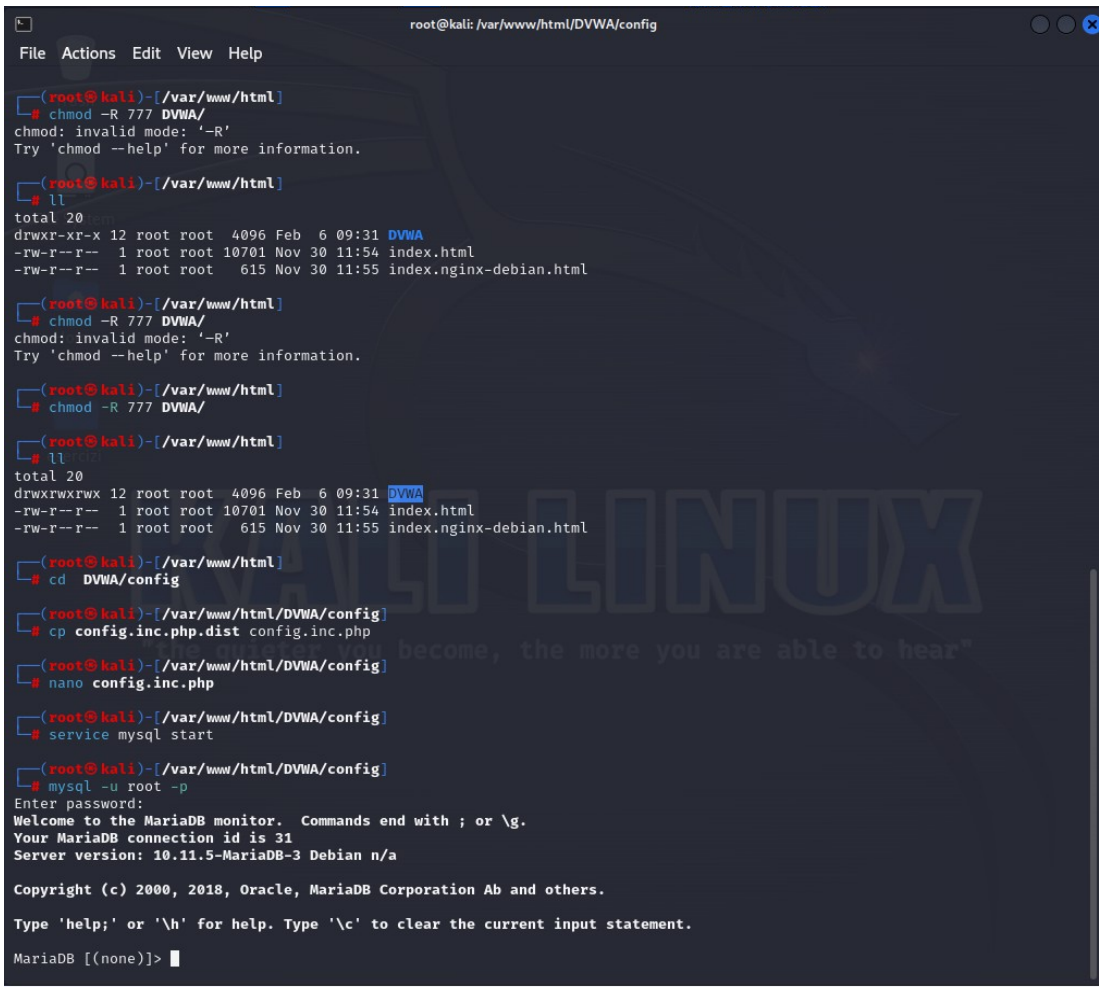
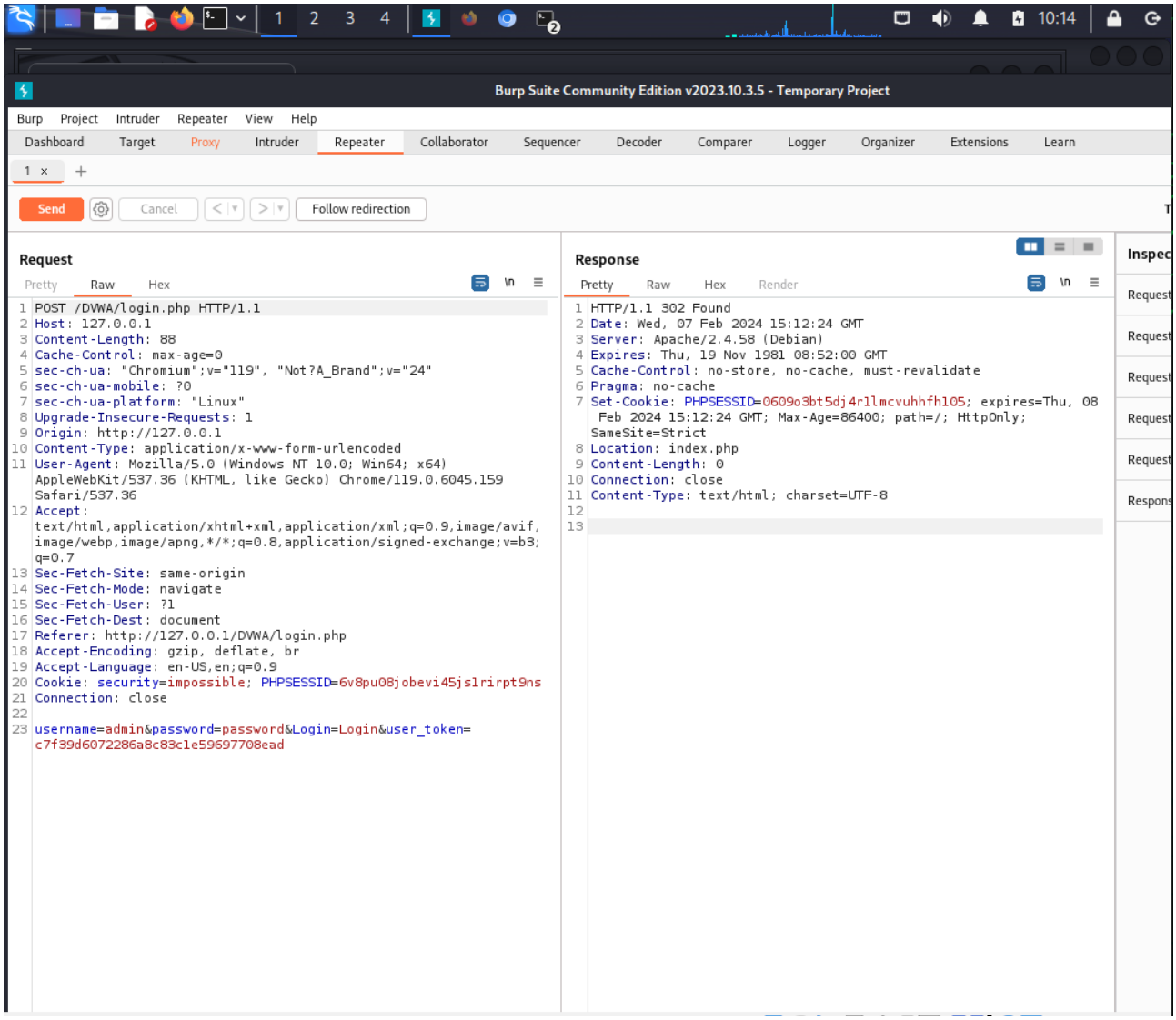
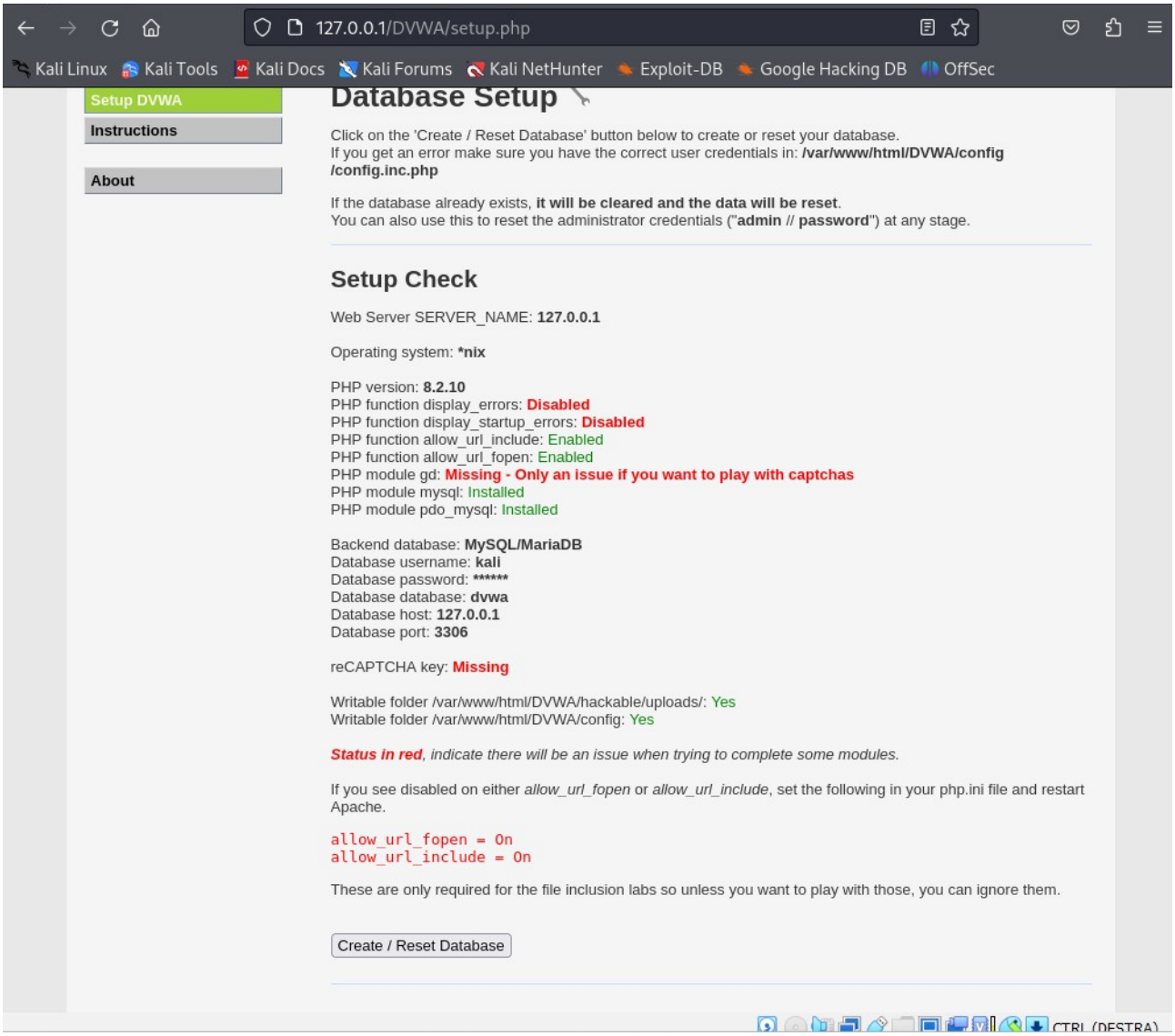

root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali;
'>
'> create user 'kali'@'127.0.0.1' identified by kali;
'> create user 'kali'@'127.0.0.1' identified by kaliCtrl-C -- exit!
Aborted
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.5-MariaDB-3 Debian n/a
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)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.009 sec)
MariaDB [(none)]> grant all privileges on dvwa.*to 'kali'@'127.0.0.1'identified by 'kali';
Query OK, 0 rows affected (0.007 sec)
MariaDB [(none)]> exit
Bye
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 start
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Tue 2024-02-06 10:00:14 EST; 19s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 34411 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 34427 (apache2)
Tasks: 6 (limit: 2260)
Memory: 19.7M
CPU: 74ms
CGroup: /system.slice/apache2.service
├─34427 /usr/sbin/apache2 -k start
├─34430 /usr/sbin/apache2 -k start
├─34431 /usr/sbin/apache2 -k start
├─34432 /usr/sbin/apache2 -k start
├─34433 /usr/sbin/apache2 -k start
└─34434 /usr/sbin/apache2 -k start
Feb 06 10:00:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Feb 06 10:00:14 kali apachectl[34426]: AH00558: apache2: Could not reliably determine the server's fully qualified domain>
Feb 06 10:00:14 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)


root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
chmod: invalid mode: '-R'
Try 'chmod --help' for more information.
┌──(root㉿kali)-[/var/www/html]
└─# ll
total 20
drwxr-xr-x 12 root root 4096 Feb 6 09:31 DVWA
-rw-r--r-- 1 root root 10701 Nov 30 11:54 index.html
-rw-r--r-- 1 root root 615 Nov 30 11:55 index.nginx-debian.html
┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
chmod: invalid mode: '-R'
Try 'chmod --help' for more information.
┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
┌──(root㉿kali)-[/var/www/html]
└─# ll
total 20
drwxrwxrwx 12 root root 4096 Feb 6 09:31 DVWA
-rw-r--r-- 1 root root 10701 Nov 30 11:54 index.html
-rw-r--r-- 1 root root 615 Nov 30 11:55 index.nginx-debian.html
┌──(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: 10.11.5-MariaDB-3 Debian n/a
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)]>


Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection
Request
Pretty Raw Hex
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
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/119.0.6045.159 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
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=6v8pu08jobevi45js1rirpt9ns
Connection: close
username=admin&password=password&Login=Login&user_token=c7f39d6072286a8c83c1e59697708ead
Response
Pretty Raw Hex Render
HTTP/1.1 302 Found
Date: Wed, 07 Feb 2024 15:12:24 GMT
Server: Apache/2.4.58 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=0609o3bt5dj4r1lmcvuhhfh105; expires=Thu, 08 Feb 2024 15:12:24 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


127.0.0.1/DVWA/setup.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Setup DVWA
Instructions
About
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: 8.2.10
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Enabled
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 Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database