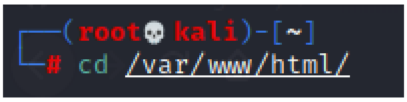
Aryaman Mishra

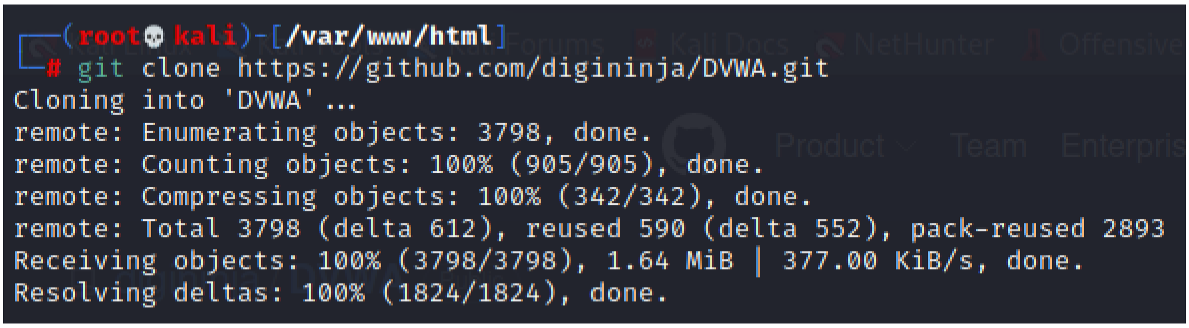
19BCE1027

DVWA is made with PHP and MySQL for security professionals or aspiring security professionals to discover as many issues as possible and exploit some of the most commons vulnerabilities of web platforms like **SQL injection**, **Cross Site Scripting** (*XSS*), **Cross Site Request Forgery** (*CSRF*), and more.

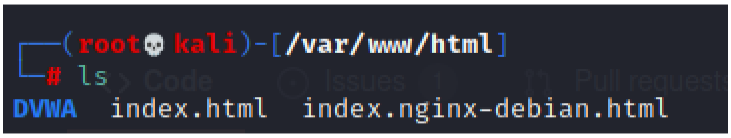
https://github.com/digininja/DVWA.git



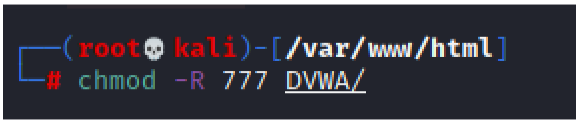
```
┌──(root💀kali)-[~]
└─# cd /var/www/html/
```



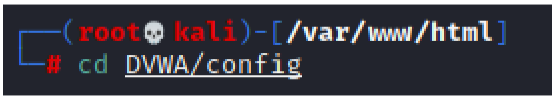
```
┌──(root💀kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 3798, done.
remote: Counting objects: 100% (905/905), done.
remote: Compressing objects: 100% (342/342), done.
remote: Total 3798 (delta 612), reused 590 (delta 552), pack-reused 2893
Receiving objects: 100% (3798/3798), 1.64 MiB | 377.00 KiB/s, done.
Resolving deltas: 100% (1824/1824), done.
```



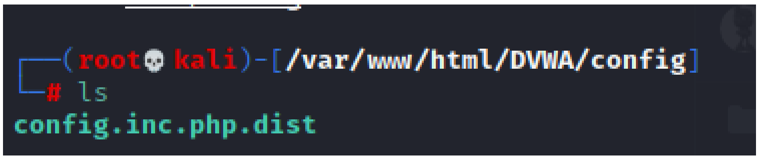
```
┌──(root💀kali)-[/var/www/html]
└─# ls
DVWA  index.html  index.nginx-debian.html
```



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



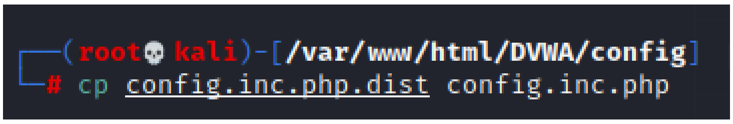
```
┌──(root💀kali)-[/var/www/html]
└─# cd DVWA/config
```



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

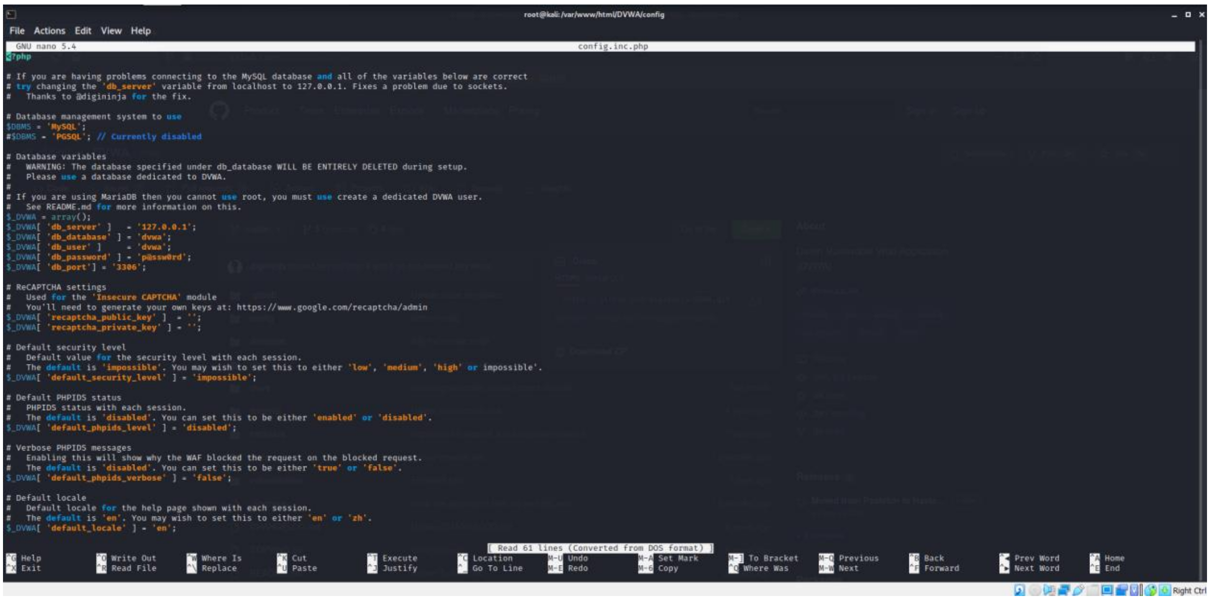
We will use the text editor to edit the configuration typing the following command:

sudo vim /var/www/html/dvwa/config/config.inc.php.dist



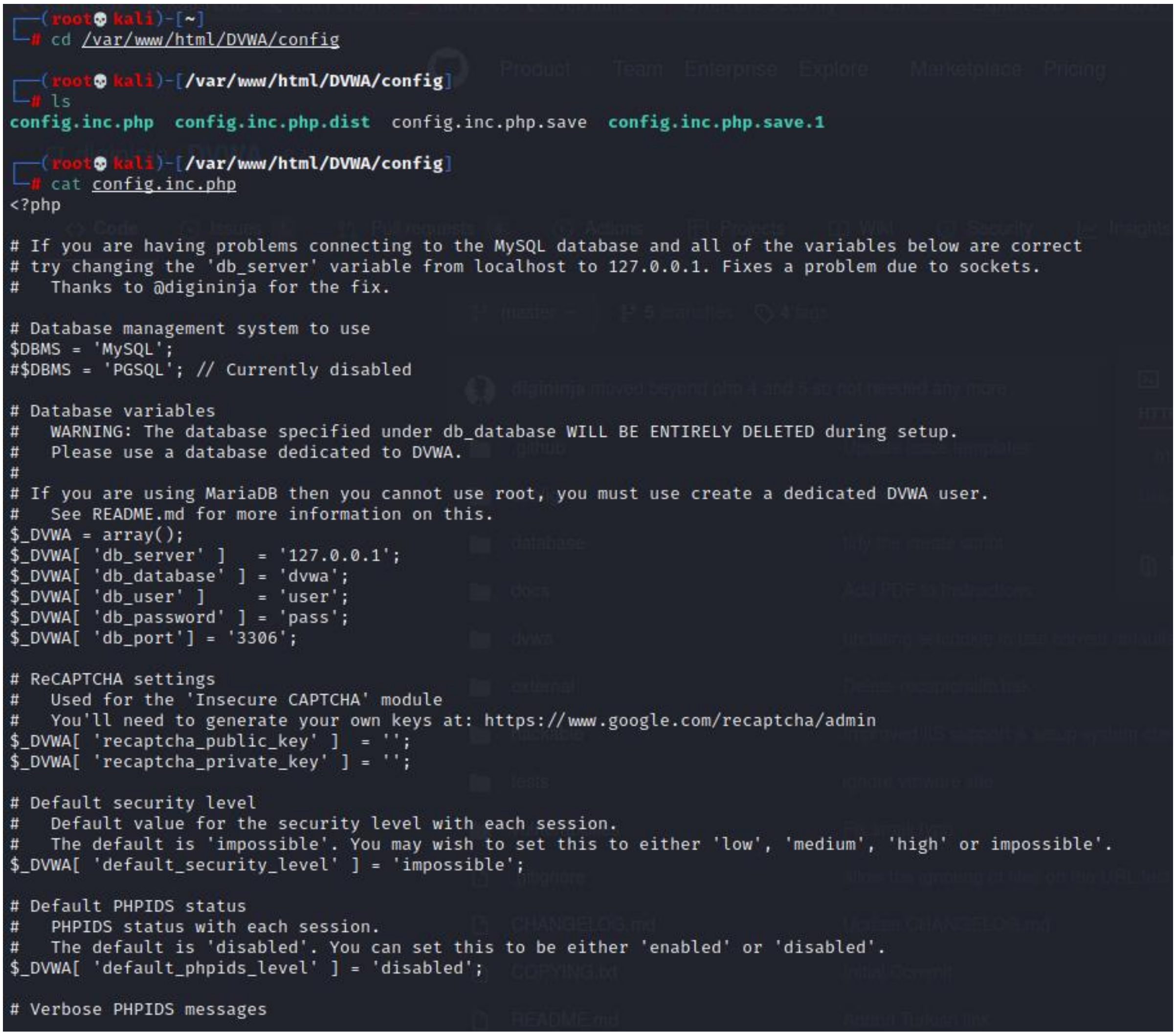
```
┌──(root💀 kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
```

Change username and password as required by you.

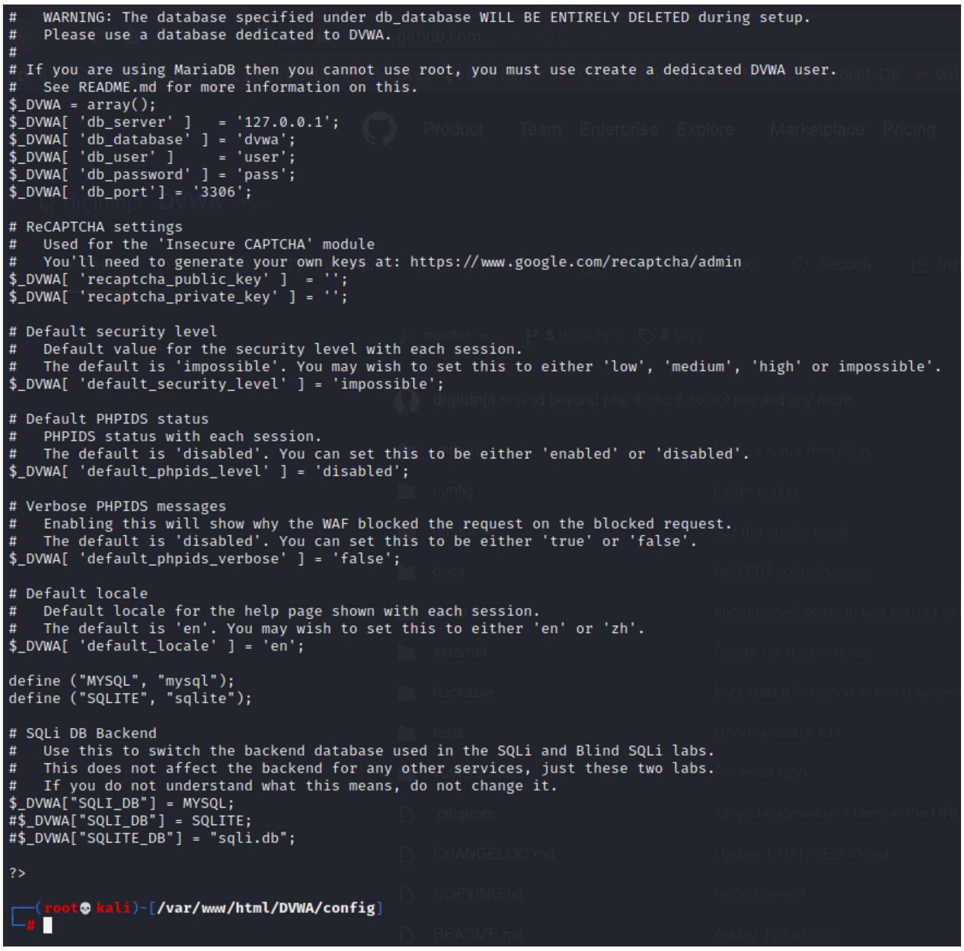


File Actions Edit View Help
root@kali: /var/www/html/DVWA/config
GNU nano 5.4
config.inc.php
[Read 61 lines (Converted from DOS format)]
^G Help ^X Exit
^O Write Out ^R Read File
^W Where Is ^\ Replace
^K Cut ^U Paste
^T Execute ^J Justify
^C Location ^_ Go To Line
M-U Undo M-E Redo
M-A Set Mark M-6 Copy
M-] To Bracket ^Q Where Was
M-Q Previous M-W Next
^B Back ^F Forward
^◀ Prev Word ^▶ Next Word
^A Home ^E End
Right Ctrl

```
<?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
$DBMS = 'MySQL';
#$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' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ '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' ]  = '';
$_DVWA[ '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' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
#   Enabling this will show why the WAF blocked the request on the blocked request.
#   The default is 'disabled'. You can set this to be either 'true' or 'false'.
$_DVWA[ 'default_phpids_verbose' ] = 'false';

# 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' ] = 'en';
```

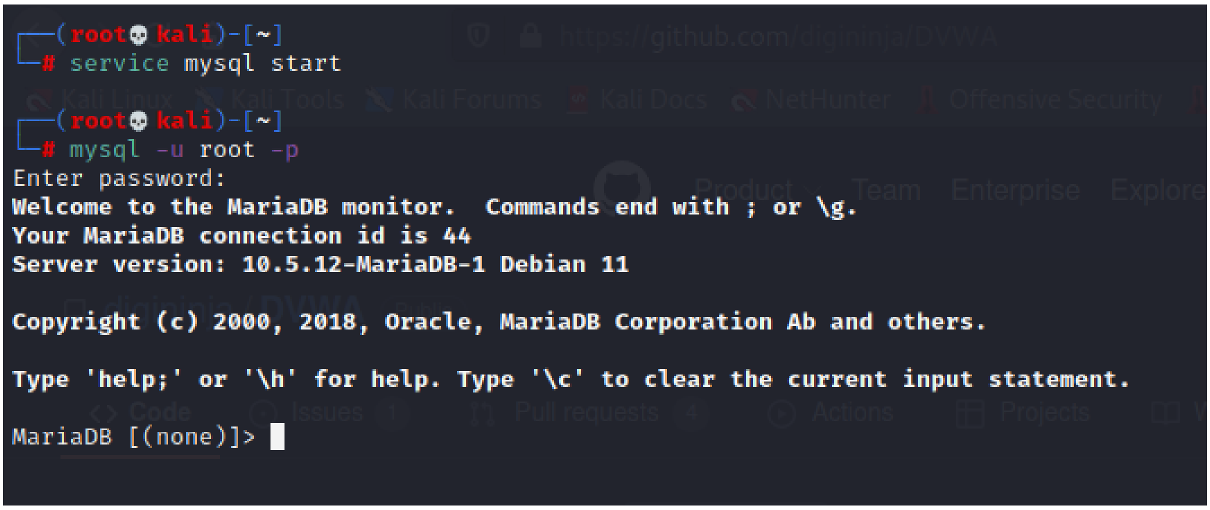


```
┌──(root💀 kali)-[~]
└─# cd /var/www/html/DVWA/config

┌──(root💀 kali)-[/var/www/html/DVWA/config]
└─# ls
config.inc.php  config.inc.php.dist  config.inc.php.save  config.inc.php.save.1

┌──(root💀 kali)-[/var/www/html/DVWA/config]
└─# cat 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
$DBMS = 'MySQL';
#$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' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ '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' ]  = '';
$_DVWA[ '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' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
```



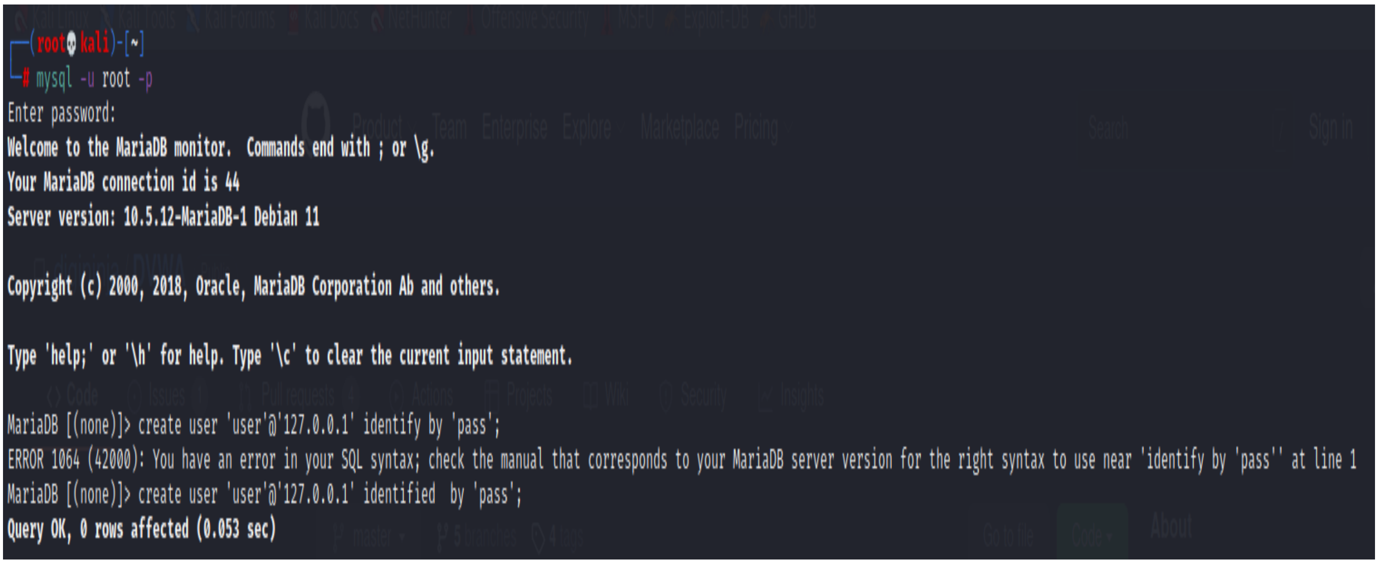
```
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'user';
$_DVWA[ 'db_password' ] = 'pass';
$_DVWA[ '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' ]  = '';
$_DVWA[ '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' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
#   Enabling this will show why the WAF blocked the request on the blocked request.
#   The default is 'disabled'. You can set this to be either 'true' or 'false'.
$_DVWA[ 'default_phpids_verbose' ] = 'false';

# 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' ] = 'en';

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

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
#   This does not affect the backend for any other services, just these two labs.
#   If you do not understand what this means, do not change it.
$_DVWA["SQLI_DB"] = MYSQL;
#$_DVWA["SQLI_DB"] = SQLITE;
#$_DVWA["SQLITE_DB"] = "sqli.db";

?>

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

Start Mysql server.

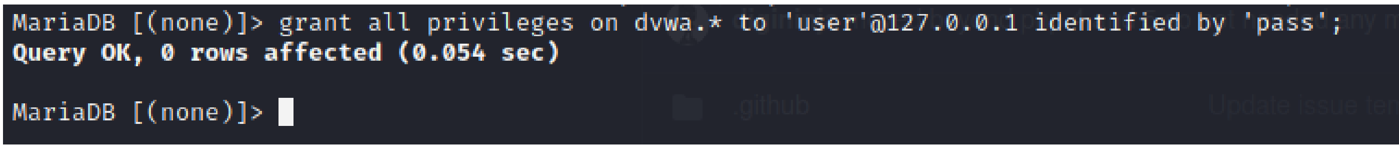


```
┌──(root💀kali)-[~]
└─# service mysql start

┌──(root💀kali)-[~]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.5.12-MariaDB-1 Debian 11

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)]>
```

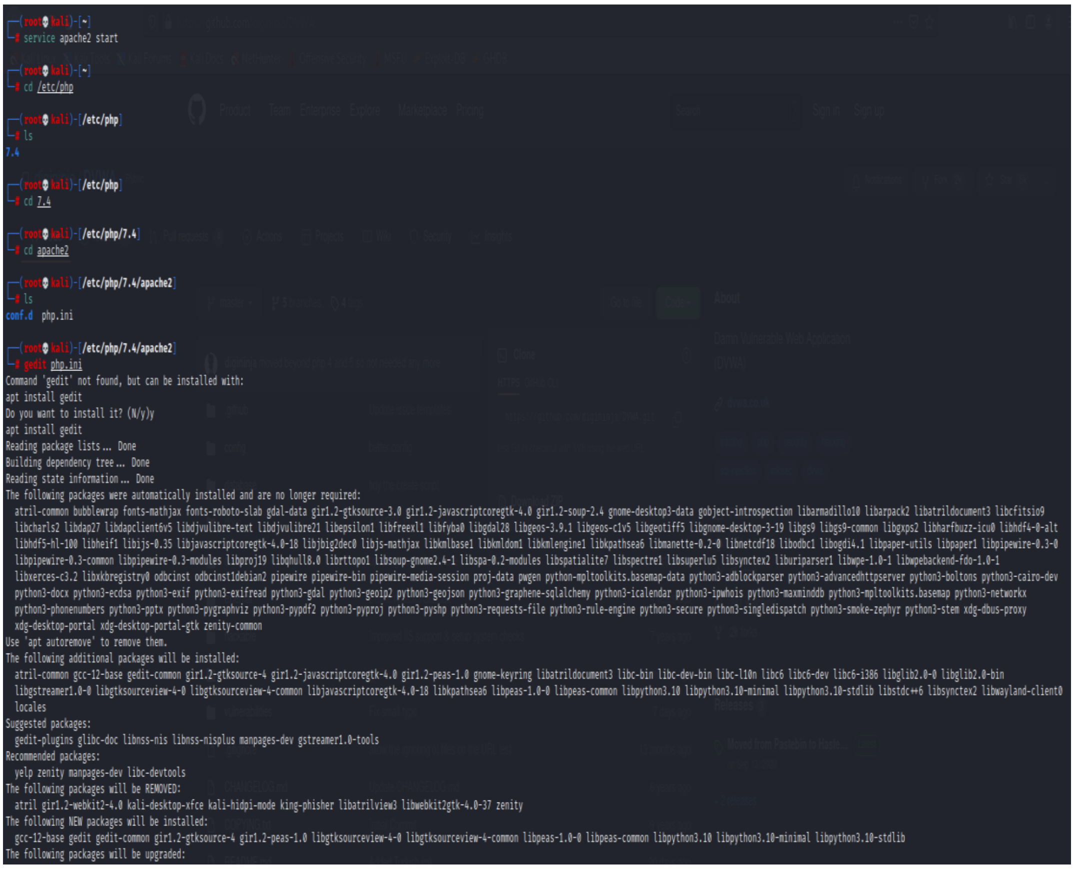
Create a user in MariaBD and grant all priviledges to ‘user’@127.0.0.1



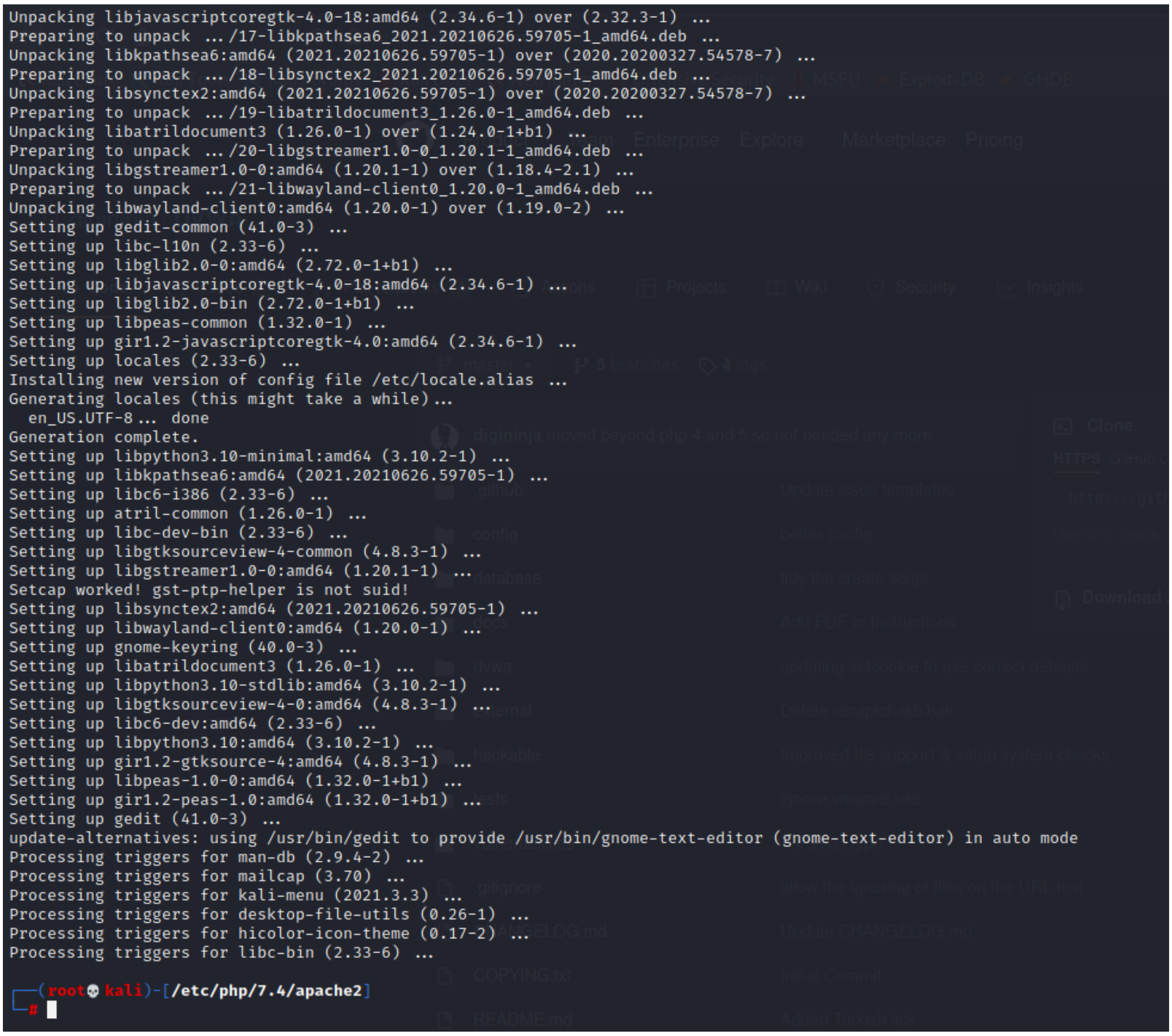
```
┌──(root💀kali)-[~]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 44
Server version: 10.5.12-MariaDB-1 Debian 11

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 'user'@'127.0.0.1' identify by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'identify by 'pass'' at line 1
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified  by 'pass';
Query OK, 0 rows affected (0.053 sec)
```



```
MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@127.0.0.1 identified by 'pass';
Query OK, 0 rows affected (0.054 sec)

MariaDB [(none)]> █
```



```
┌──(root💀kali)-[~]
└─# service apache2 start

┌──(root💀kali)-[~]
└─# cd /etc/php

┌──(root💀kali)-[/etc/php]
└─# ls
7.4

┌──(root💀kali)-[/etc/php]
└─# cd 7.4

┌──(root💀kali)-[/etc/php/7.4]
└─# cd apache2

┌──(root💀kali)-[/etc/php/7.4/apache2]
└─# ls
conf.d  php.ini

┌──(root💀kali)-[/etc/php/7.4/apache2]
└─# gedit php.ini
Command 'gedit' not found, but can be installed with:
apt install gedit
Do you want to install it? (N/y)y
apt install gedit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  atril-common bubblewrap fonts-mathjax fonts-roboto-slab gdal-data gir1.2-gtksource-3.0 gir1.2-javascriptcoregtk-4.0 gir1.2-soup-2.4 gnome-desktop3-data gobject-introspection libarmadillo10 libarpack2 libatrildocument3 libcfitsio9
  libcharls2 libdap27 libdapclient6v5 libdjvulibre-text libdjvulibre21 libepsilon1 libfreexl1 libfyba0 libgdal28 libgeos-3.9.1 libgeos-c1v5 libgeotiff5 libgnome-desktop-3-19 libgs9 libgs9-common libgxps2 libharfbuzz-icu0 libhdf4-0-alt
  libhdf5-hl-100 libheif1 libijs-0.35 libjavascriptcoregtk-4.0-18 libjbig2dec0 libjs-mathjax libkmlbase1 libkmldom1 libkmlengine1 libkpathsea6 libmanette-0.2-0 libnetcdf18 libodbc1 libogdi4.1 libpaper-utils libpaper1 libpipewire-0.3-0
  libpipewire-0.3-common libpipewire-0.3-modules libproj19 libqhull8.0 librttopo1 libsoup-gnome2.4-1 libspa-0.2-modules libspatialite7 libspectre1 libsuperlu5 libsynctex2 liburiparser1 libwpe-1.0-1 libwpebackend-fdo-1.0-1
  libxerces-c3.2 libxkbregistry0 odbcinst odbcinst1debian2 pipewire pipewire-bin pipewire-media-session proj-data pwgen python-mpltoolkits.basemap-data python3-adblockparser python3-advancedhttpserver python3-boltons python3-cairo-dev
  python3-docx python3-ecdsa python3-exif python3-exifread python3-gdal python3-geoip2 python3-geojson python3-graphene-sqlalchemy python3-icalendar python3-ipwhois python3-maxminddb python3-mpltoolkits.basemap python3-networkx
  python3-phonenumbers python3-pptx python3-pygraphviz python3-pypdf2 python3-pyproj python3-pyshp python3-requests-file python3-rule-engine python3-secure python3-singledispatch python3-smoke-zephyr python3-stem xdg-dbus-proxy
  xdg-desktop-portal xdg-desktop-portal-gtk zenity-common
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  atril-common gcc-12-base gedit-common gir1.2-gtksource-4 gir1.2-javascriptcoregtk-4.0 gir1.2-peas-1.0 gnome-keyring libatrildocument3 libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libglib2.0-0 libglib2.0-bin
  libgstreamer1.0-0 libgtksourceview-4-0 libgtksourceview-4-common libjavascriptcoregtk-4.0-18 libkpathsea6 libpeas-1.0-0 libpeas-common libpython3.10 libpython3.10-minimal libpython3.10-stdlib libstdc++6 libsynctex2 libwayland-client0
  locales
Suggested packages:
  gedit-plugins glibc-doc libnss-nis libnss-nisplus manpages-dev gstreamer1.0-tools
Recommended packages:
  yelp zenity manpages-dev libc-devtools
The following packages will be REMOVED:
  atril gir1.2-webkit2-4.0 kali-desktop-xfce kali-hidpi-mode king-phisher libatrilview3 libwebkit2gtk-4.0-37 zenity
The following NEW packages will be installed:
  gcc-12-base gedit gedit-common gir1.2-gtksource-4 gir1.2-peas-1.0 libgtksourceview-4-0 libgtksourceview-4-common libpeas-1.0-0 libpeas-common libpython3.10 libpython3.10-minimal libpython3.10-stdlib
The following packages will be upgraded:
```



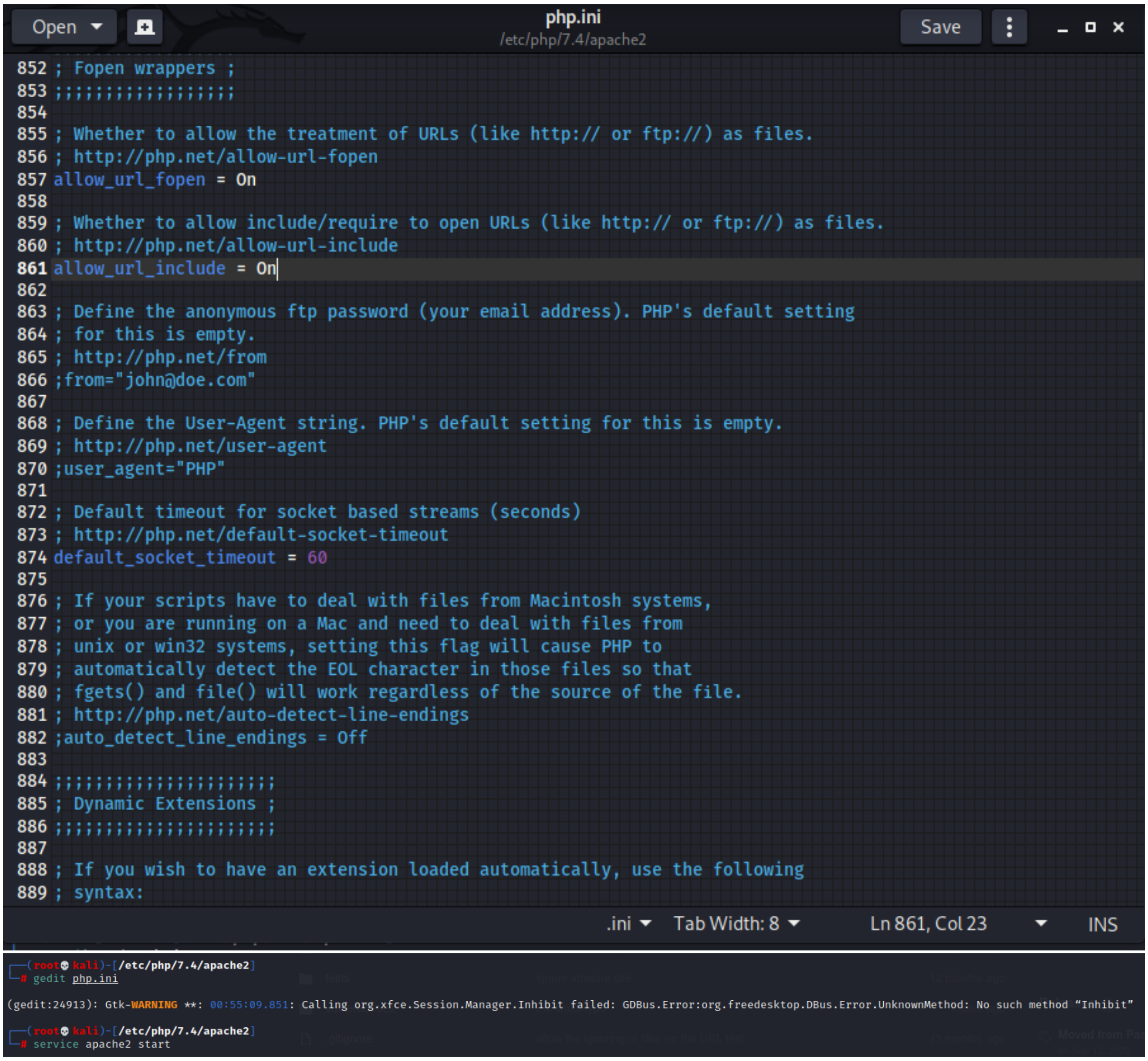
```
Unpacking libjavascriptcoregtk-4.0-18:amd64 (2.34.6-1) over (2.32.3-1) ...
Preparing to unpack .../17-libkpathsea6_2021.20210626.59705-1_amd64.deb ...
Unpacking libkpathsea6:amd64 (2021.20210626.59705-1) over (2020.20200327.54578-7) ...
Preparing to unpack .../18-libsynctex2_2021.20210626.59705-1_amd64.deb ...
Unpacking libsynctex2:amd64 (2021.20210626.59705-1) over (2020.20200327.54578-7) ...
Preparing to unpack .../19-libatrildocument3_1.26.0-1_amd64.deb ...
Unpacking libatrildocument3 (1.26.0-1) over (1.24.0-1+b1) ...
Preparing to unpack .../20-libgstreamer1.0-0_1.20.1-1_amd64.deb ...
Unpacking libgstreamer1.0-0:amd64 (1.20.1-1) over (1.18.4-2.1) ...
Preparing to unpack .../21-libwayland-client0_1.20.0-1_amd64.deb ...
Unpacking libwayland-client0:amd64 (1.20.0-1) over (1.19.0-2) ...
Setting up gedit-common (41.0-3) ...
Setting up libc-l10n (2.33-6) ...
Setting up libglib2.0-0:amd64 (2.72.0-1+b1) ...
Setting up libjavascriptcoregtk-4.0-18:amd64 (2.34.6-1) ...
Setting up libglib2.0-bin (2.72.0-1+b1) ...
Setting up libpeas-common (1.32.0-1) ...
Setting up gir1.2-javascriptcoregtk-4.0:amd64 (2.34.6-1) ...
Setting up locales (2.33-6) ...
Installing new version of config file /etc/locale.alias ...
Generating locales (this might take a while)...
  en_US.UTF-8... done
Generation complete.
Setting up libpython3.10-minimal:amd64 (3.10.2-1) ...
Setting up libkpathsea6:amd64 (2021.20210626.59705-1) ...
Setting up libc6-i386 (2.33-6) ...
Setting up atril-common (1.26.0-1) ...
Setting up libc-dev-bin (2.33-6) ...
Setting up libgtksourceview-4-common (4.8.3-1) ...
Setting up libgstreamer1.0-0:amd64 (1.20.1-1) ...
Setcap worked! gst-ptp-helper is not suid!
Setting up libsynctex2:amd64 (2021.20210626.59705-1) ...
Setting up libwayland-client0:amd64 (1.20.0-1) ...
Setting up gnome-keyring (40.0-3) ...
Setting up libatrildocument3 (1.26.0-1) ...
Setting up libpython3.10-stdlib:amd64 (3.10.2-1) ...
Setting up libgtksourceview-4-0:amd64 (4.8.3-1) ...
Setting up libc6-dev:amd64 (2.33-6) ...
Setting up libpython3.10:amd64 (3.10.2-1) ...
Setting up gir1.2-gtksource-4:amd64 (4.8.3-1) ...
Setting up libpeas-1.0-0:amd64 (1.32.0-1+b1) ...
Setting up gir1.2-peas-1.0:amd64 (1.32.0-1+b1) ...
Setting up gedit (41.0-3) ...
update-alternatives: using /usr/bin/gedit to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for mailcap (3.70) ...
Processing triggers for kali-menu (2021.3.3) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.33-6) ...

┌──(root💀kali)-[/etc/php/7.4/apache2]
└─#
```

Once done, we need to edit the main config (***php.ini***) file for apache2, which is not correctly overridden for **DVWA** by default.

sudo vim /etc/php5/apache2/php.ini

- Enable Allow_url_fopen
- Enable Allow_url_include

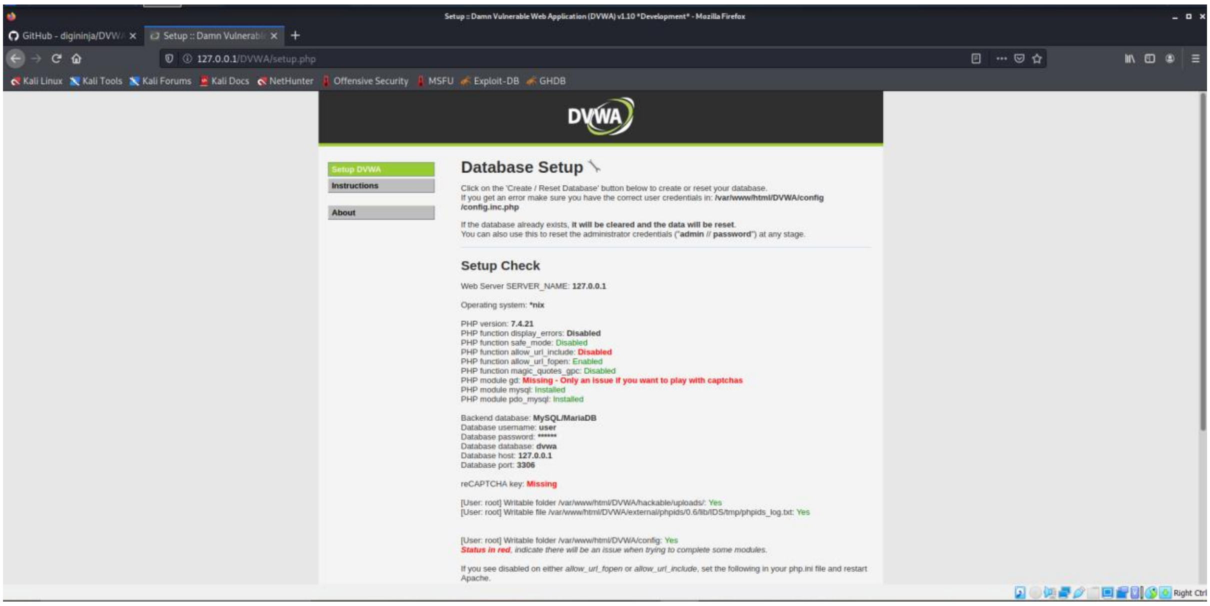
This is necessary to exploit the file upload vulnerability. Here's a screenshot for ***php.ini*** after making changes.



```
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; http://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; http://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; http://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to
; automatically detect the EOL character in those files so that
; fgets() and file() will work regardless of the source of the file.
; http://php.net/auto-detect-line-endings
;auto_detect_line_endings = Off

;;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;;

; If you wish to have an extension loaded automatically, use the following
; syntax:
```

```
┌──(root💀kali)-[/etc/php/7.4/apache2]
└─# gedit php.ini

(gedit:24913): Gtk-WARNING **: 00:55:09.851: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: No such method “Inhibit”

┌──(root💀kali)-[/etc/php/7.4/apache2]
└─# service apache2 start
```

Access localhost/DVWA and work with DVWA Application.



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: **7.4.21**
PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
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: **user**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

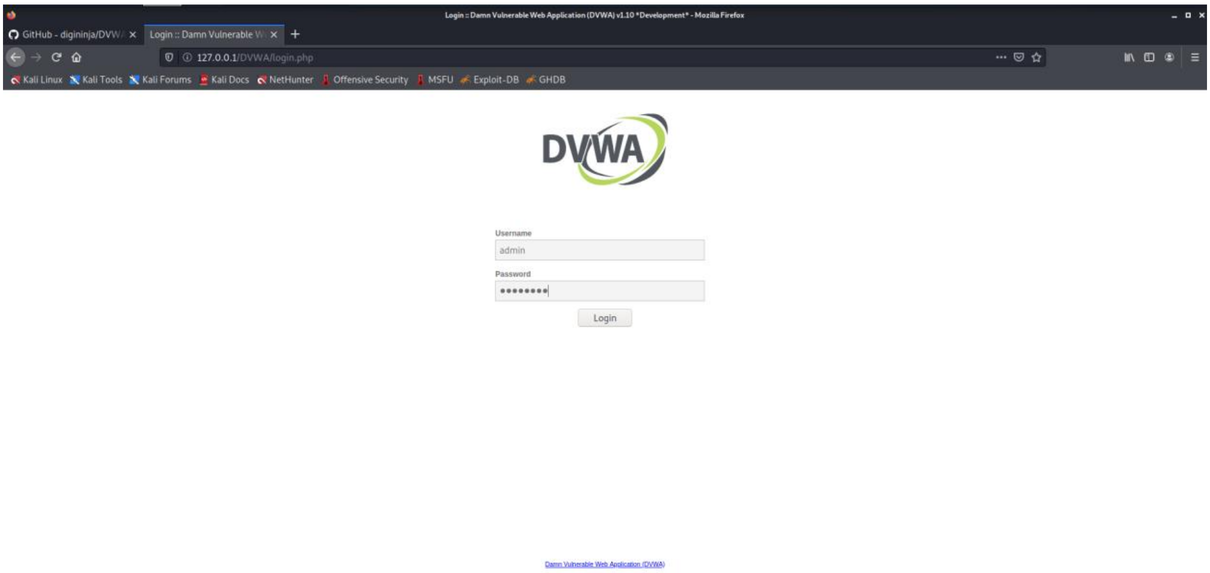
reCAPTCHA key: **Missing**

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

[User: root] 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.

Scroll and click ‘recreate database’ option and you will be redirected to login page.

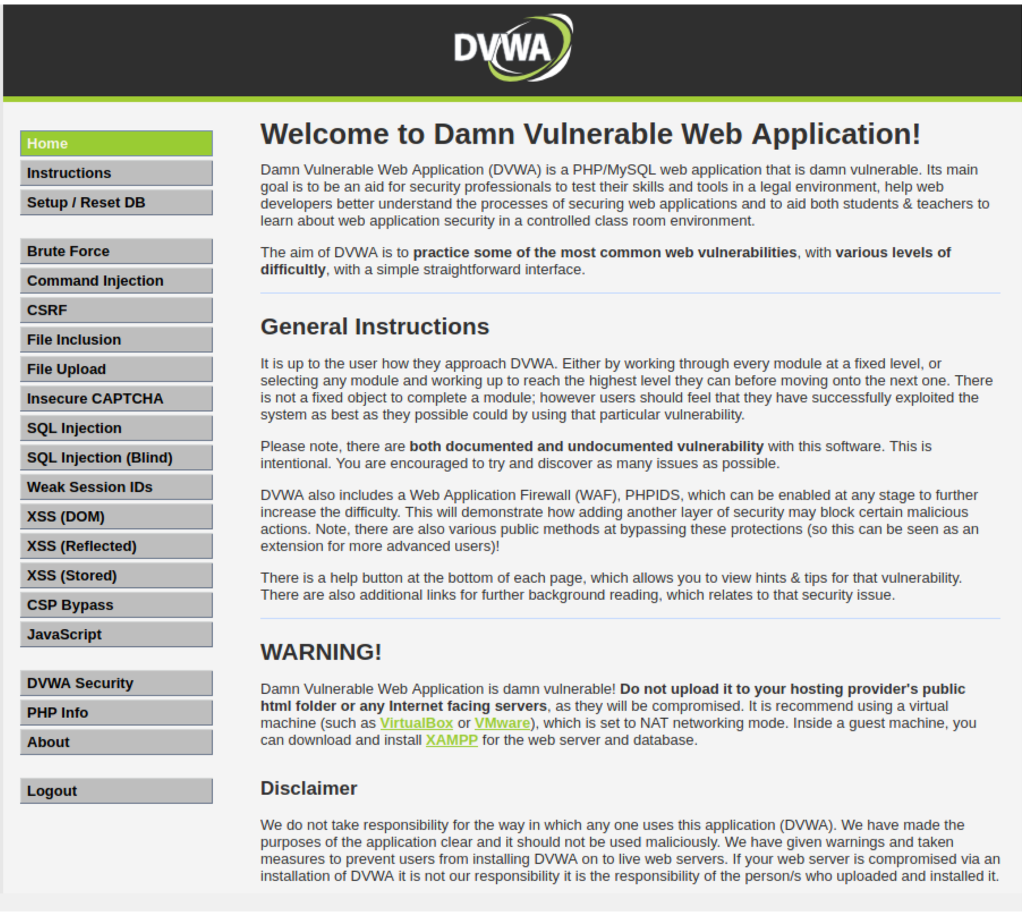

Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox
GitHub - digininja/DVWA
Login :: Damn Vulnerable W
127.0.0.1/DVWA/login.php
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
DVWA
Login
Damn Vulnerable Web Application (DVWA)

Username
admin

Password
••••••••

Username:**admin**

Password:**password**



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

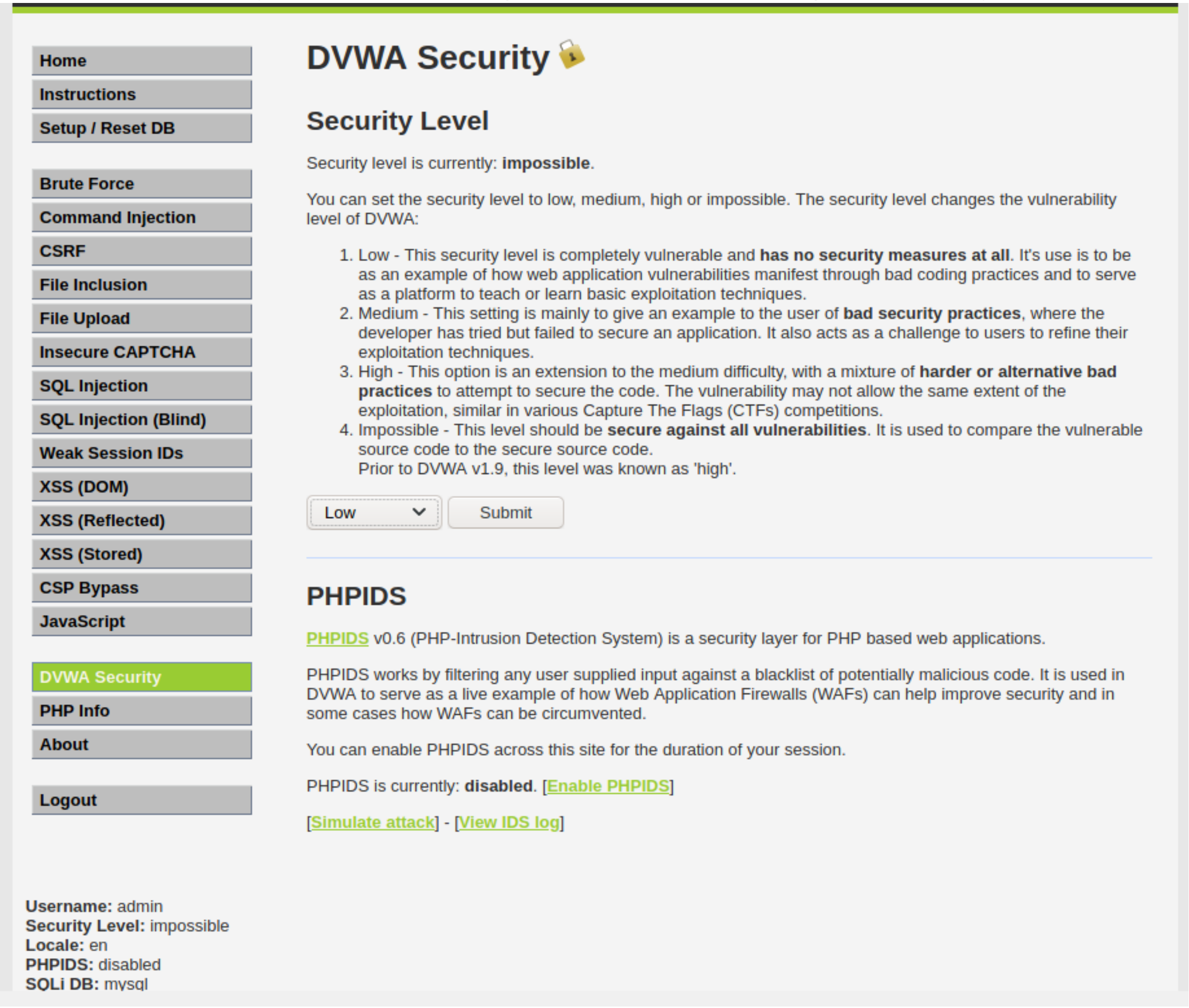
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

Now, login to change the strength of vulnerabilities by clicking on “DVWA Security”.

Low Level: Low-Level Security gives you the freedom to exploit all known vulnerabilities means there will be no security in a given framework and hence you can try all attacks if you are using it first Time.

Medium Level: Medium security will have all entry-level validations and filtration which can stop any script kiddie to get the benefit of available vulnerabilities.

High Level: High Level is kind of Zero Day environment and if you can breach it then that means you are on the right track to becoming a VAPT Expert.



DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

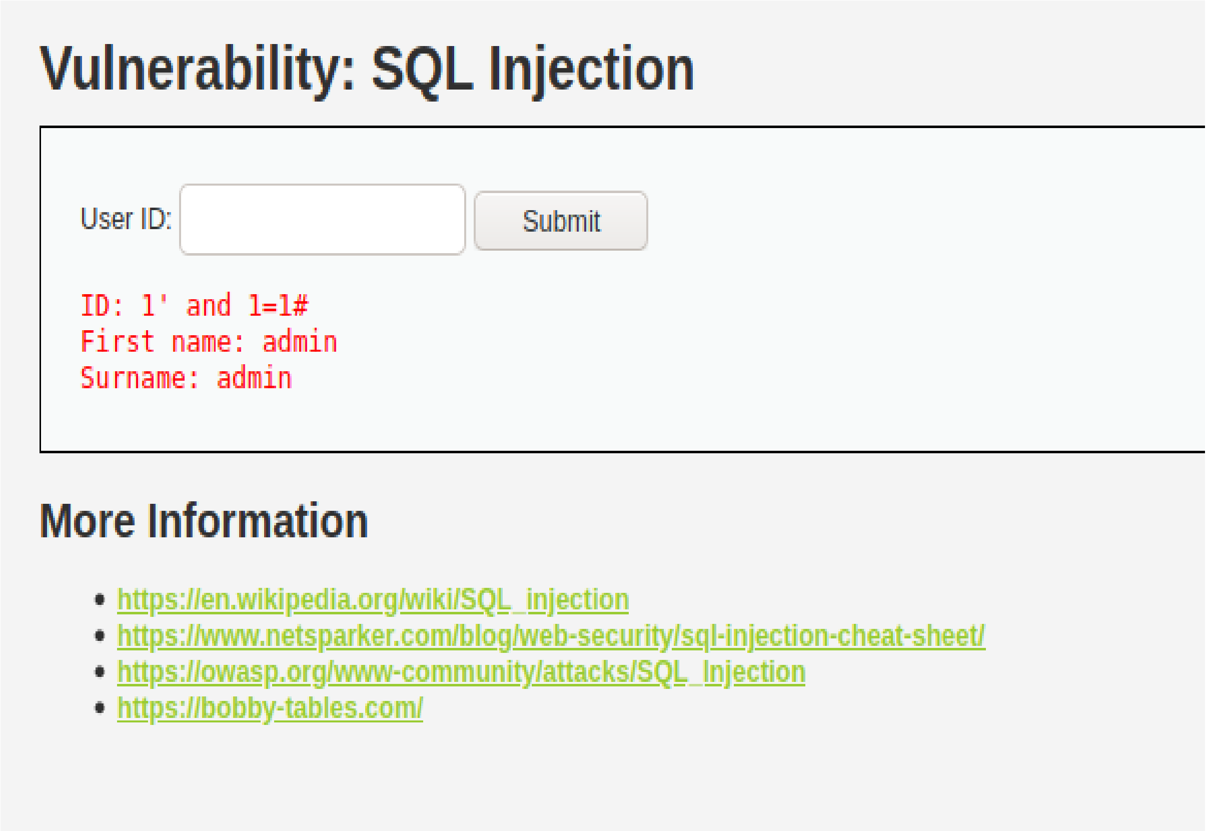
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin
Security Level: impossible
Locale: en
PHPIDS: disabled
SQLi DB: mysql

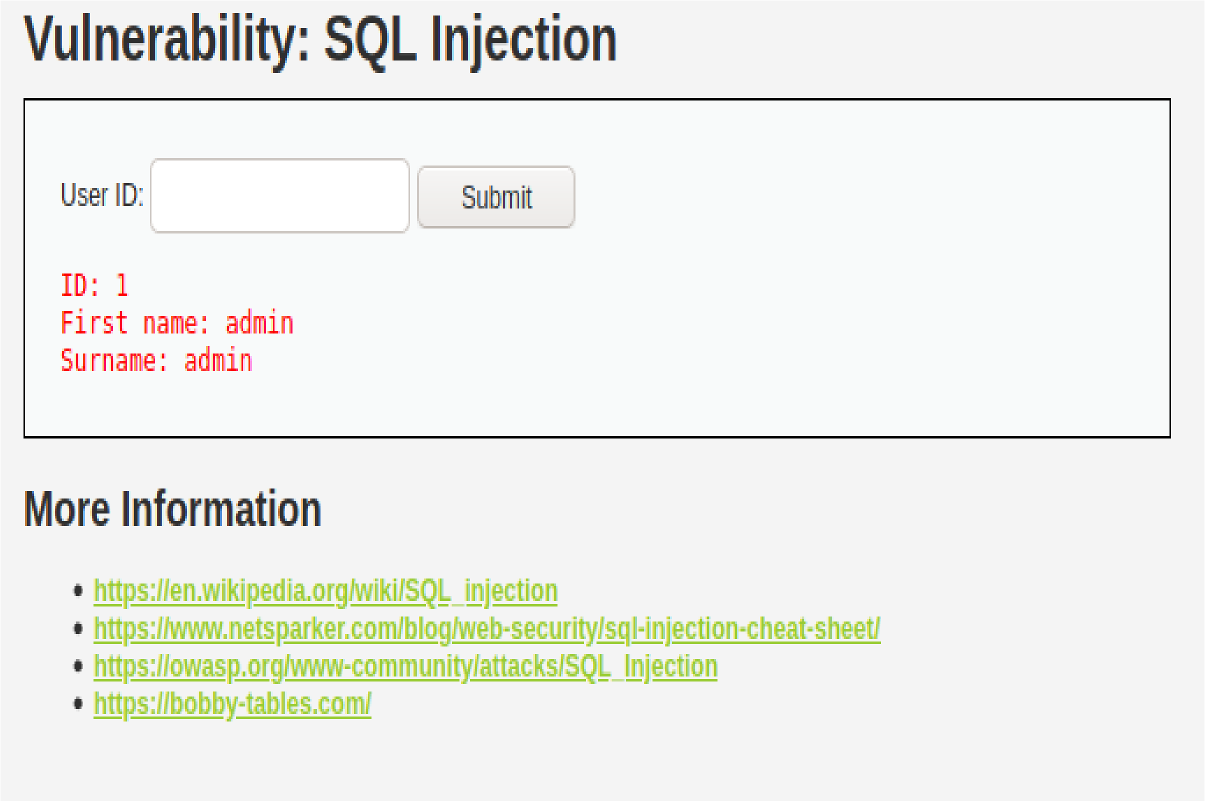


Vulnerability: SQL Injection

```
ID: 1' and 1=1#
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

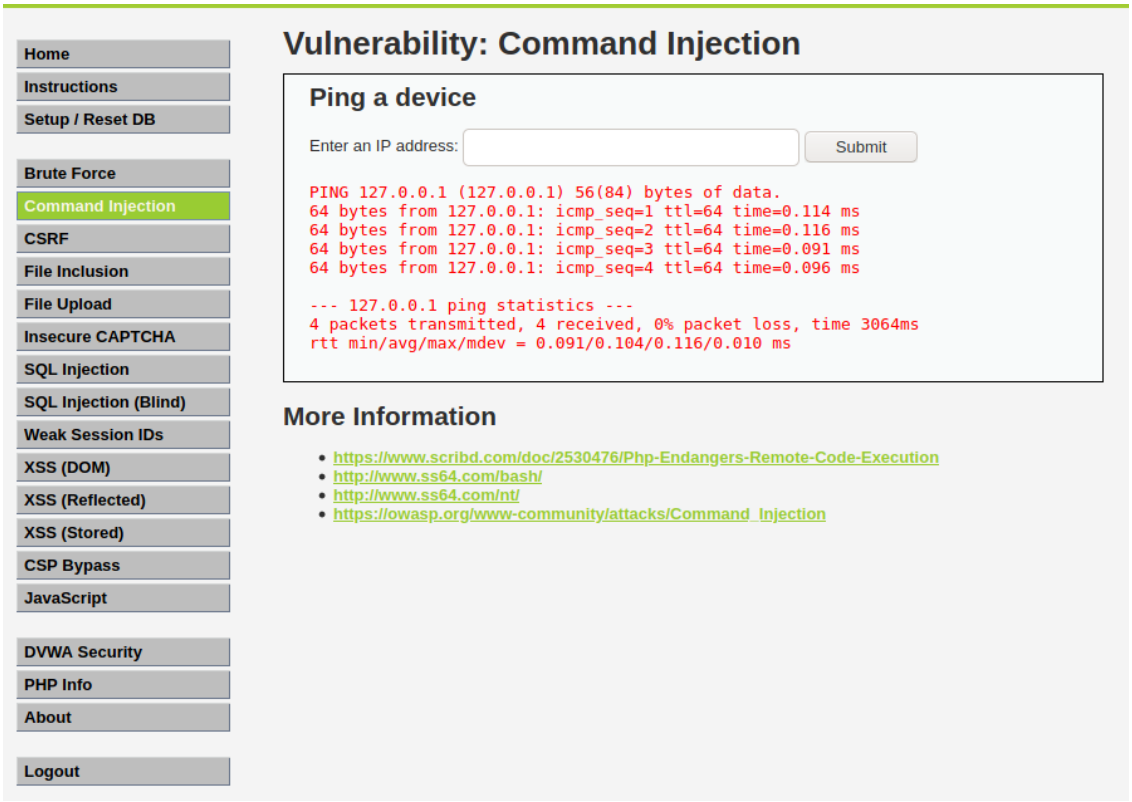


Vulnerability: SQL Injection

```
ID: 1
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/



Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.116 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.096 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3064ms
rtt min/avg/max/mdev = 0.091/0.104/0.116/0.010 ms
```

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

Conclusion:DVWA has been successfully configured and SQL and Command Injection can be implemented using the web tool.