

Индивидуальный проект этап 2

Информационная безопасность

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

- Научиться основным способам тестирования веб приложений
- Установить и настроить DVWA на Kali linux

1. Клонировал DVWA с <https://github.com/digininja/DVWA>

```
(ksudzuki@KSudzuki)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 185), reused 266 (delta 139), pack-reused 4450 (from 1
)
Receiving objects: 100% (4784/4784), 2.36 MiB | 387.00 KiB/s, done.
Resolving deltas: 100% (2296/2296), done.
```

2. Переименовал директорию DVWA на dvwa

```
(ksudzuki@KSudzuki)-[/var/www/html]  
$ sudo mv DVWA dvwa
```

3. Задал права пользователя для директории

```
(ksudzuki@KSudzuki)-[/var/www/html]  
$ sudo chmod -R 777 dvwa/
```

4. Зашел в директорию dvwa/config

```
(ksudzuki@KSudzuki)-[/var/www/html]  
$ cd dvwa/config
```

5. Проверил что в ней есть

```
(ksudzuki@KSudzuki)-[/var/www/html/dvwa/config]  
$ ls  
config.inc.php  config.inc.php.dist
```

6. Открыл файл config.inc.php

```
(ksudzuki@KSudzuki)-[/var/www/html/dvwa/config]  
$ sudo nano config.inc.php
```


7. Файл config.inc.php

```
GNU nano 8.1
<?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' ] = getenv( 'DB_SERVER' ) ? '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'user';
$_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';
```

8. Заменял в нем db_user и db_password на user и pass

```
GNU nano 8.1
<?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.

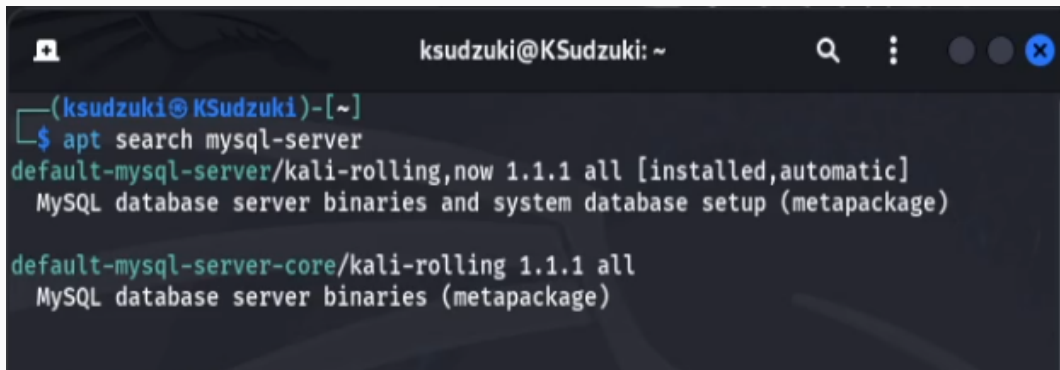
# Database management system to use
$dbms = 'MySQL';
#$dbms = 'PGSQL'; // Currently disabled

# 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' ] = getenv('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';
```

9. Посмотрел мой mysql-server

A terminal window with a dark background. The title bar shows 'ksudzuki@KSudzuki: ~' and standard window controls. The terminal text shows a user prompt, a command to search for 'mysql-server', and two search results for 'default-mysql-server' and 'default-mysql-server-core' from the 'kali-rolling' repository, both version 1.1.1. The results indicate they are installed and are metapackages for MySQL database server binaries and system setup.

```
(ksudzuki@KSudzuki)-[~]  
$ apt search mysql-server  
default-mysql-server/kali-rolling,now 1.1.1 all [installed,automatic]  
  MySQL database server binaries and system database setup (metapackage)  
  
default-mysql-server-core/kali-rolling 1.1.1 all  
  MySQL database server binaries (metapackage)
```

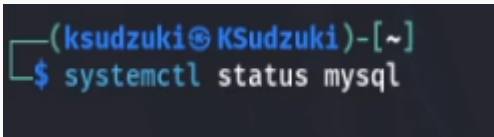
10. Установил mysql-server

```
(ksudzuki@KSudzuki)-[~]  
$ sudo apt install default-mysql-server  
[sudo] password for ksudzuki:  
default-mysql-server is already the newest version (1.1.1).  
default-mysql-server set to manually installed.  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 484
```

11. Запустил mysql

```
(ksudzuki@KSudzuki)-[~]  
$ sudo service mysql start
```

12. Посмотрел статус mysql



```
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 20:42:55 MSK; 37s ago
 Invocation: 0f9e52dd8a9a4a189dc2d3be25d0db47
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
 Process: 3041 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
 Process: 3043 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 3046 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=/usr/bin/galera_recovery; [ $? -eq 0 ] && systemctl set-environment _WSREP_START_POSITION=$VAR || exit 1 (code=exited, statu>
 Process: 3119 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 3121 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 3105 (mariadb)
   Status: "Taking your SQL requests now..."
     Tasks: 14 (limit: 30401)
    Memory: 241.5M (peak: 246.1M)
       CPU: 1.170s
    CGroup: /system.slice/mariadb.service
            └─3105 /usr/sbin/mariadb

Sep 21 20:42:54 KSudzuki mariadb[3105]: 2024-09-21 20:42:54 0 [Note] Plugin 'wsrep-provider' is disabled.
Sep 21 20:42:54 KSudzuki mariadb[3105]: 2024-09-21 20:42:54 0 [Note] InnoDB: Buffer pool(s) load completed at 240921 20:42:54
Sep 21 20:42:55 KSudzuki mariadb[3105]: 2024-09-21 20:42:55 0 [Note] Server socket created on IP: '127.0.0.1'.
Sep 21 20:42:55 KSudzuki mariadb[3105]: 2024-09-21 20:42:55 0 [Note] mariadb: Event Scheduler: Loaded 0 events
Sep 21 20:42:55 KSudzuki mariadb[3105]: 2024-09-21 20:42:55 0 [Note] /usr/sbin/mariadb: ready for connections.
Sep 21 20:42:55 KSudzuki mariadb[3105]: Version: '11.4.2-MariaDB-4' socket: '/run/mysqld/mysqld.sock' port: 3306 Debian n/a
Sep 21 20:42:55 KSudzuki systemd[1]: Started mariadb.service - MariaDB 11.4.2 database server.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3124]: Upgrading MariaDB tables if necessary.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3136]: Checking for insecure root accounts.
Sep 21 20:42:55 KSudzuki /etc/mysql/debian-start[3140]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables
```

13. Зашел в mysql

```
(ksudzuki@KSudzuki)-[~] 11.4.2 database server
$ sudo mysql -u root -p lib/systemd/system/mariadb.service; disabled; preset: d
[sudo] password for ksudzuki: since Sat 2024-09-21 20:42:55 MSK; 37s ago
Enter password: e52ddb8944a189dc2d3be25d0db47
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31 lib/en/library/systemd/
Server version: 11.4.2-MariaDB-4 Debian n/a
Process: 3043 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Process: 3119 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START
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)]>
```

14. Создал пользователя и дал ему все права

```
(ksudzuki@KSudzuki)-[~]
$ sudo mysql -u root -p
[sudo] password for ksudzuki:
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

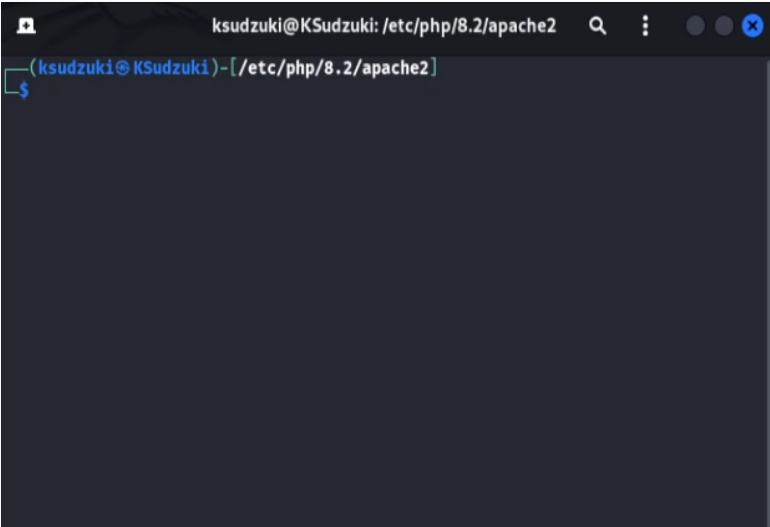
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.002 sec)

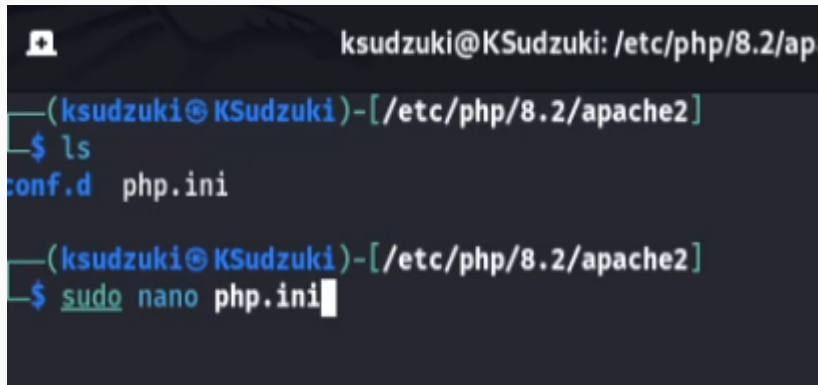
MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
```


15. Зашёл в папку `/etc/php/8.2/apache2`



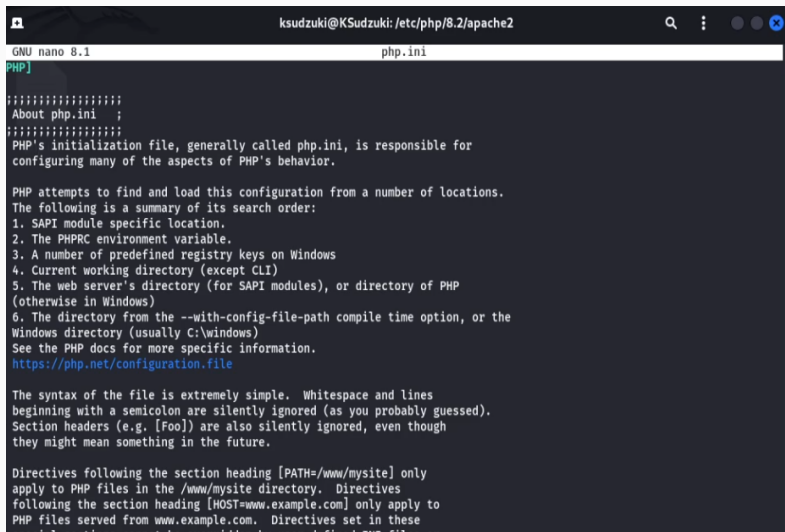
```
ksudzuki@KSudzuki: /etc/php/8.2/apache2
(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]
$
```

16. Посмотрел что в ней есть и открыл файл php.ini

A terminal window with a dark background. The title bar shows a window icon and the text 'ksudzuki@KSudzuki: /etc/php/8.2/ap'. The terminal content shows a prompt '(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]' followed by the command '\$ ls' and the output 'conf.d php.ini'. A second prompt shows the command '\$ sudo nano php.ini' with a cursor at the end.

```
ksudzuki@KSudzuki: /etc/php/8.2/ap  
—(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]  
$ ls  
conf.d  php.ini  
  
—(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]  
$ sudo nano php.ini
```

17. Файл php.ini



```
ksudzuki@KSudzuki: /etc/php/8.2/apache2
GNU nano 8.1 php.ini
PHP]

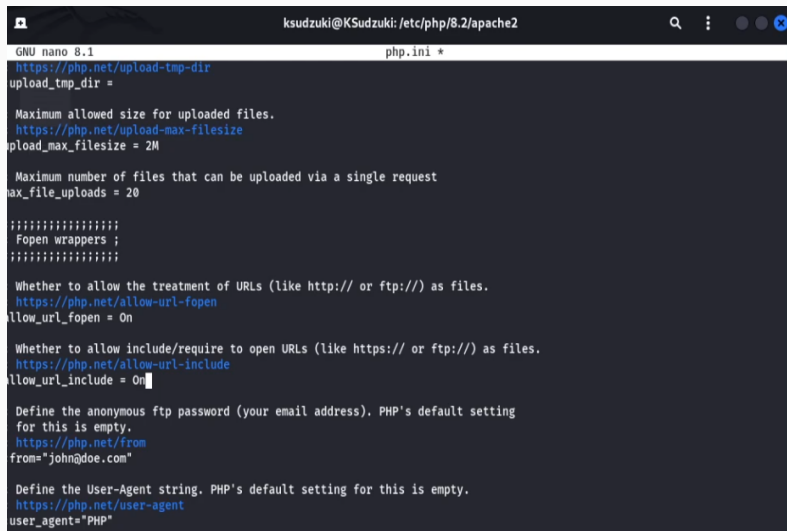
;;;;;;;;;;;;;
About php.ini ;
;;;;;;;;;;;;;
PHP's initialization file, generally called php.ini, is responsible for
configuring many of the aspects of PHP's behavior.

PHP attempts to find and load this configuration from a number of locations.
The following is a summary of its search order:
1. SAPI module specific location.
2. The PHPRC environment variable.
3. A number of predefined registry keys on Windows
4. Current working directory (except CLI)
5. The web server's directory (for SAPI modules), or directory of PHP
   (otherwise in Windows)
6. The directory from the --with-config-file-path compile time option, or the
   Windows directory (usually C:\windows)
See the PHP docs for more specific information.
https://php.net/configuration.file

The syntax of the file is extremely simple. Whitespace and lines
beginning with a semicolon are silently ignored (as you probably guessed).
Section headers (e.g. [Foo]) are also silently ignored, even though
they might mean something in the future.

Directives following the section heading [PATH=/www/mysite] only
apply to PHP files in the /www/mysite directory. Directives
following the section heading [HOST=www.example.com] only apply to
PHP files served from www.example.com. Directives set in these
```

18. Нашел в нем `allow_url_fopen` и `allow_url_include` и поменял на "On"



```
ksudzuki@KSudzuki: /etc/php/8.2/apache2
GNU nano 8.1 php.ini *
https://php.net/upload-tmp-dir
upload_tmp_dir =

Maximum allowed size for uploaded files.
https://php.net/upload-max-filesize
upload_max_filesize = 2M

Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;
Fopen wrappers ;
;;;;;;;;;;;;;

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

Whether to allow include/require to open URLs (like https:// or ftp://) as files.
https://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.
https://php.net/from
from="john@doe.com"

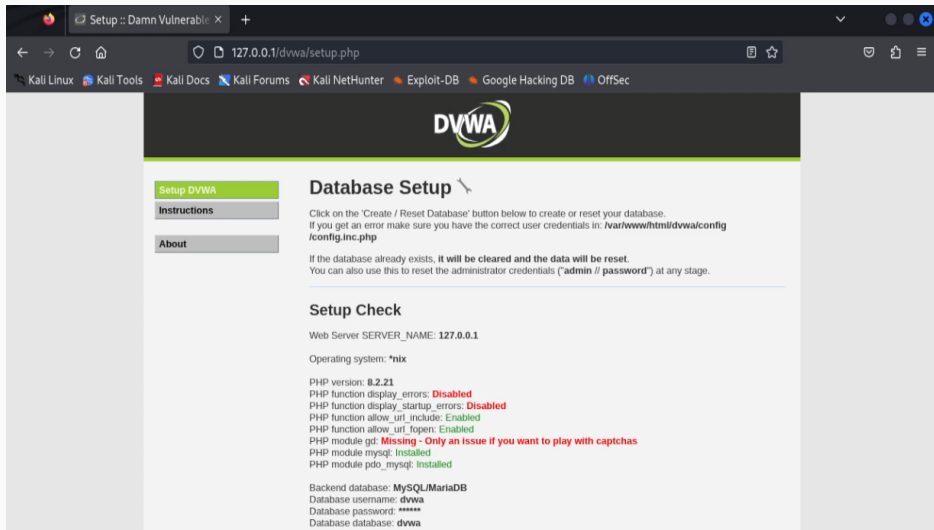
Define the User-Agent string. PHP's default setting for this is empty.
https://php.net/user-agent
user_agent="PHP"
```

19. Запустил apache2 и проверил его статус

```
(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]
$ sudo service apache2 start

(ksudzuki@KSudzuki)-[/etc/php/8.2/apache2]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 20:57:53 MSK; 23s ago
 Invocation: 5f655a8aea7a4b71abaa62f1b5143ac1
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 3545 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 3561 (apache2)
   Tasks: 7 (limit: 4606)
  Memory: 20.6M (peak: 21.5M)
     CPU: 33ms
  CGroup: /system.slice/apache2.service
          └─3561 /usr/sbin/apache2 -k start
            └─3564 /usr/sbin/apache2 -k start
              └─3565 /usr/sbin/apache2 -k start
                └─3566 /usr/sbin/apache2 -k start
                  └─3567 /usr/sbin/apache2 -k start
                    └─3568 /usr/sbin/apache2 -k start
                      └─3569 /usr/sbin/apache2 -k start
```

20. Зашёл на Localhost 127.0.0.1/dvwa/setup.php



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/dvwa/setup.php`. The browser's tab is labeled "Setup :: Damn Vulnerable". The page features the DVWA logo at the top. On the left side, there is a navigation menu with three items: "Setup DVWA" (highlighted in green), "Instructions", and "About". The main content area is titled "Database Setup" and includes instructions on how to create or reset the database, mentioning the file `/var/www/html/dvwa/config/config.inc.php`. It also states that if the database already exists, it will be cleared and the data will be reset. Below this, there is a "Setup Check" section that displays various system and configuration details, including the web server name, operating system, PHP version, and database settings.

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

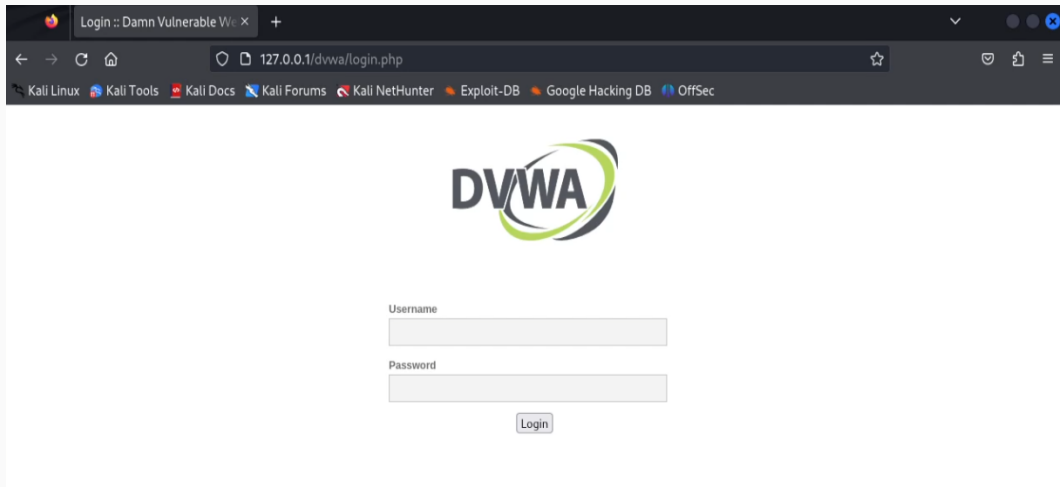
Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

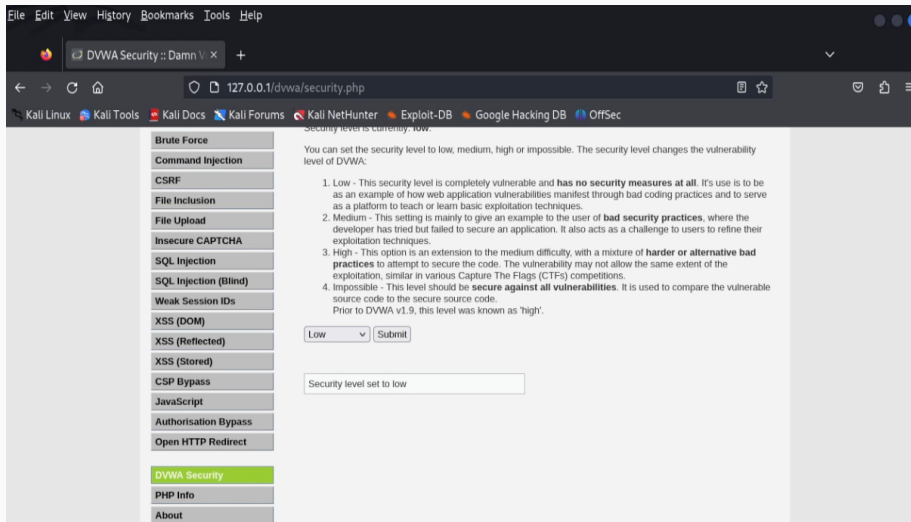
PHP version: 8.2.21
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysqli: Installed
PHP module pdo_mysql: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

Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa

21. Ввёл логин и пароль admin password



22. Поменял защиту на low



- Установил и настроил DVWA на Kali linux