

Индивидуальный проект этап №2

Основы информационной безопасности

Павлюченков С.В.

07 сентября 25

Российский университет дружбы народов, Москва, Россия

- Павлюченков Сергей Витальевич
- Студент ФФМиЕН
- Российский университет дружбы народов
- 1132237372@pfur.ru
- <https://serapshi.github.io/svpavliuchenkov.github.io/>



Подготовить специально предназначенном для поиска уязвимостей веб приложении под названием Damn Vulnerable Web Application (DVWA).

Установите DVWA в гостевую систему к Kali Linux.

Выполнение лабораторной работы

```
(svpavliuchenkov@svpavliuchenkov)-[~]  
$ cd /var/www/html  
  
(svpavliuchenkov@svpavliuchenkov)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 5373, done.  
Receiving objects: 40% (2150/5373), 1.38 MiB | 303.00 KiB/s
```

Рис. 1: Клонирование DVWA

Установка имени пользователя и пароля для базы данных

```
svpavliuchenkov@svpavliuchenkov: /var/www/html/dvwa/config
File Actions Edit View Help
GNU nano 8.4 config.inc.php *
<?php
# If you are having problems connecting to the MySQL database and a
# try changing the 'db_server' variable from localhost to 127.0.0.1
# 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
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use c
# 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') ?: 'svpavliuchenkov';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'pass';
$_DVWA['db_port'] = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Exec
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Just
```

```
svpavliuchenkov@svpavliuchenkov: /var/www/html/dvwa/config
File Actions Edit View Help
config.inc.php config.inc.php.dist

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

(svpavliuchenkov@svpavliuchenkov)-[/var/www/html/dvwa/config]
$ sudo apt install default-mysql-server
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: 977

(svpavliuchenkov@svpavliuchenkov)-[/var/www/html/dvwa/config]
$ sudo service mysql start

(svpavliuchenkov@svpavliuchenkov)-[/var/www/html/dvwa/config]
$ sudo service status mysql
status: unrecognized service

(svpavliuchenkov@svpavliuchenkov)-[/var/www/html/dvwa/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.8.1 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-09-14 08:04:34 EDT; 53s ago
     Invocation: 805143c870c248fd8560d8a82efecc3d
       Docs: man:mariadb(8)
            https://mariadb.com/kb/en/library/systemd/
   Process: 47453 ExecStartPre=/usr/bin/install -m 755 -o mysql -g
```



```
MariaDB [(none)]> grant all privileges on dvwa.* to 'svpavliuchenkov'@'127.0.0.1' identified by 'pass'  
→ ;  
Query OK, 0 rows affected (0.024 sec)  
  
MariaDB [(none)]> █
```

Рис. 4: Изменение прав в MySQL

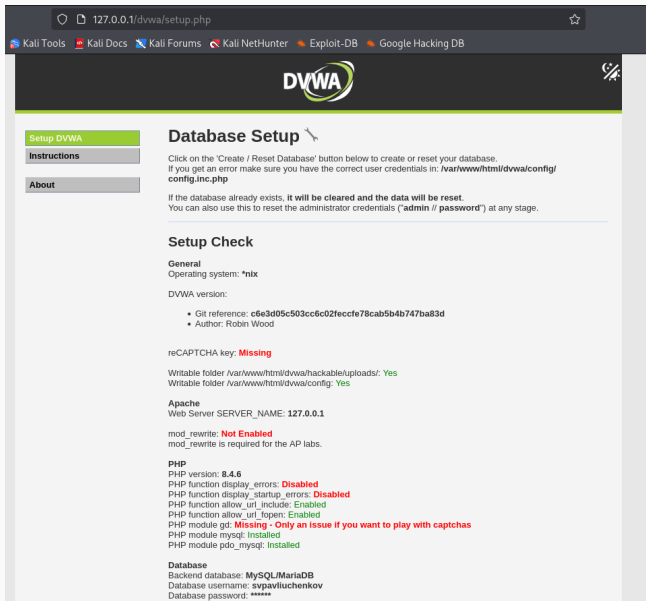
```
(svpavliuchenkov@svpavliuchenkov)-[/etc/php/8.4/apache2]
$ sudo nano php.ini

(svpavliuchenkov@svpavliuchenkov)-[/etc/php/8.4/apache2]
$ sudo service apache2 start

(svpavliuchenkov@svpavliuchenkov)-[/etc/php/8.4/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 Sun 2025-09-14 08:26:39 EDT; 18s ago
     Invocation: 6f8bec7203c14813aedbcd563a5c76ba
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 58561 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 58590 (apache2)
      Tasks: 6 (limit: 12607)
```

Рис. 5: Запуск Apache

Открытие DVWA в браузере



127.0.0.1/dvwa/setup.php

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DVWA

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

General

Operating system: `*nix`

DVWA version:

- Git reference: `c6e3d05c503cc6c02fcccfe78cab5b4b747ba83d`
- Author: Robin Wood

reCAPTCHA key: **Missing**

Writable folder `/var/www/html/dvwa/hackable/uploads/`: **Yes**
Writable folder `/var/www/html/dvwa/config/`: **Yes**

Apache

Web Server `SERVER_NAME`: `127.0.0.1`

`mod_rewrite`: **Not Enabled**
`mod_rewrite` is required for the AP labs.

PHP

PHP version: `8.4.6`
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**

Database

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

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

Please [login](#).

На этом этапе я подготовил веб интерфейс для работы и тестирования по в следующих этапах