

Второй этап индивидуального проекта

Установка DVWA

Ибатулина Д.Э.

14 марта 2024

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Информация

- Ибатулина Дарья Эдуардовна
- студентка группы НКАбд-01-22
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- deibatulina.github.io
- <https://github.com/deibatulina>

Вводная часть

DVWA - это веб-приложение на PHP/MySQL, основная цель которого - стать помощником для профессионалов в области безопасности, чтобы проверить свои навыки и инструменты в легальной среде. Мы постарались сделать развертывание DVWA максимально простым и создали надстройку, которую можно легко применить к балансировщику нагрузки edgeNEXUS ALB-X. Для специалиста по информационной безопасности данное приложение - это отличная возможность попрактиковаться и прокачать свои навыки в защите информации (при этом, совершенно легально!).

Установить утилиту DVWA на Kali Linux.

Основная часть

Клонирую репозиторий на гитхабе через терминал. Качается архив с приложением.

```
(deibatulina@deibatulina)-[~]  
$ git clone https://github.com/digininja/DVWA.git  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4500, done.  
remote: Counting objects: 100% (50/50), done.  
remote: Compressing objects: 100% (39/39), done.  
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450  
Receiving objects: 100% (4500/4500), 2.30 MiB | 2.55 MiB/s, done.  
Resolving deltas: 100% (2112/2112), done.
```

```
(deibatulina@deibatulina)-[~]  
$
```


Запускаю сервис apache2.

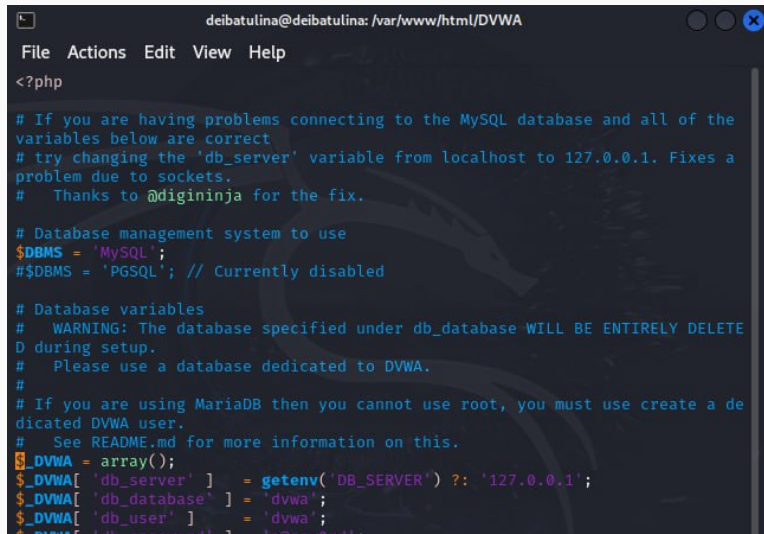
```
deibatulina@deibatulina:~/var/www/html$ sudo service apache2 start
```

9.1k stars

293 watching

Редактирование конфигурационного файла

Задаю нужные параметры в конфиг-файле.



```
deibatulina@deibatulina: /var/www/html/DVWA
File Actions Edit View Help
<?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' ] = 'dvwa';
$_DVWA[ 'db_password' ] = '12345678';
```

Запуск сервиса mariadb

Запускаю сервис mariadb.

```
(deibatulina@deibatulina)-[/var/www/html/DVWA]  
$ service mariadb start  
  
(deibatulina@deibatulina)-[/var/www/html/DVWA]  
$
```

Создаю и настраиваю базу данных, пользователя и права доступа к ней.

```
MariaDB [(none)]> create database dvwa;  
Query OK, 1 row affected (0.000 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';  
ERROR 1396 (HY000): Operation CREATE USER failed for 'dvwa'@'localhost'  
MariaDB [(none)]> drop user 'dvwa';  
ERROR 1396 (HY000): Operation DROP USER failed for 'dvwa'@'%'  
MariaDB [(none)]> drop user 'dvwa'@'localhost';  
Query OK, 0 rows affected (0.009 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';  
Query OK, 0 rows affected (0.046 sec)  
  
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;  
Query OK, 0 rows affected (0.007 sec)  
  
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.001 sec)  
  
MariaDB [(none)]> █
```

Проверка выставленных параметров

Проверяю выставленные параметры.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

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: **localhost**

Operating system: ***nix**

PHP version: **8.2.12**
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: **Installed**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

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

Заключительная часть

- установила DVWA;
- произвела его первичную настройку.