

Индивидуальный проект. Этап 2

Установка DVWA

Парфенова Е. Е.

20 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньевна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

- Необходимость установки пакета DVWA для дальнейшего выполнения проекта
- Важность практикования умения работать с ресурсом GitHub

Цель: Установка DVWA в гостевую систему к Kali Linux.

Теоретическое введение

Damn Vulnerable Web Application (DVWA) — это веб-приложение на PHP/MySQL, которое очень сильно уязвимо. Его главная цель — помочь профессионалам по безопасности протестировать их навыки и инструменты в легальном окружении, помочь веб-разработчикам лучше понять процесс безопасности веб-приложений и помочь и студентам и учителям в изучении безопасности веб-приложений в контролируемом окружении аудитории.

Некоторые из уязвимостей веб приложений, который содержит DVWA:

- Брутфорс
- Исполнение (внедрение) команд
- Межсайтовая подделка запроса (CSRF)
- SQL внедрение
- небезопасная выгрузка файлов
- Межсайтовый скриптинг (XSS)
- Пасхальные яйца

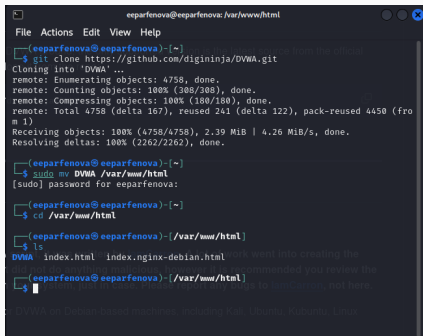
DVWA имеет несколько уровней безопасности:

- Невозможный
- Высокий
- Средний
- Низкий

Выполнение второго этапа проекта

Клонирование репозитория

1. Клонирование репозитория DVWA



```
eeparfenova@eeparfenova: /var/www/html
File Actions Edit View Help
(eeparfenova@eeparfenova)-[~]
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from the origin)
Receiving objects: 100% (4758/4758), 2.39 MiB | 4.26 MiB/s, done.
Resolving deltas: 100% (2262/2262), done.
(eeparfenova@eeparfenova)-[~]
$ sudo mv DVWA /var/www/html
[sudo] password for eeparfenova:
(eeparfenova@eeparfenova)-[~]
$ cd /var/www/html
(eeparfenova@eeparfenova)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html
work went into creating the
did not do anything malicious, however it is recommended you review the
(eeparfenova@eeparfenova)-[/var/www/html]
$
```

Рис. 1: Клонирование репозитория DVWA

Запуск сервера apache2

Адрес: `http://localhost`

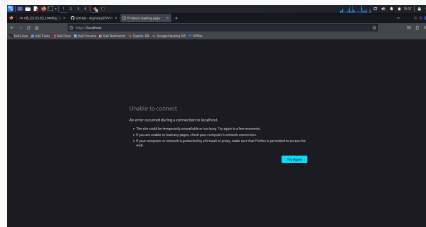
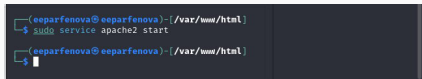


Рис. 2: Неудачная попытка входа

2. Запускаем стандартный сервер apache2

A terminal window with a dark background. The prompt is '(eeeparfenova@eeeparfenova)-[/var/www/html]'. The command 'sudo service apache2 start' is entered and executed. The prompt is shown again below the command.

```
(eeeparfenova@eeeparfenova)-[/var/www/html]  
$ sudo service apache2 start  
  
(eeeparfenova@eeeparfenova)-[/var/www/html]  
$
```

Рис. 3: Запуск сервера apache2

Запуск сервера apache2

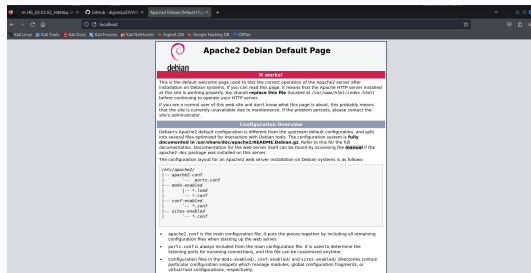


Рис. 4: Удачное открытие страницы

Адрес: `http://localhost/DVWA/`

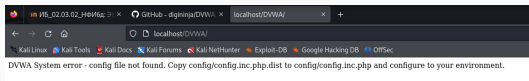


Рис. 5: Неудачная попытка открытия DVWA

3. Копируем дист-версию конфигурационного файла в файл config.inc.php

```
(eeparfenova@eeparfenova)-[/var/www/html]
$ cd DVWA
(eeparfenova@eeparfenova)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.ko.md  compose.yml  index.php  README.md  security.txt  README.rst  README.tr.md  README.vi.md  README.zh.md  SECURITY.md  about.php  config.inc.php.dist  config.inc.php
COPYING.txt  README.md  config  instructions.php  setup.php  tests
Dockerfile  README.pt.md  database  login.php
README.ar.md  README.tr.md  docs  logout.php  vulnerabilities
README.es.md  README.vi.md  dvwa  php.ini  robots.txt
README.fa.md  README.zh.md  external  phpinfo.php
README.fr.md  SECURITY.md  favicon.ico  robots.txt
README.id.md  about.php  hackable  security.php
(eeparfenova@eeparfenova)-[/var/www/html/DVWA]
$ ls config
config.inc.php.dist
(eeparfenova@eeparfenova)-[/var/www/html/DVWA]
$ cp config/config.inc.php.dist config/config.inc.php
```

Рис. 6: Копирование конфигурационного файла

4. Читаем файла config.inc.php

```
[separfenova@separfenova]~/var/www/html/DVWA$ cat config/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 = 'MySQL'; // 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 de
# dicated 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'] = 'password';
$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/recaptch
a/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', 'm
# edium', 'high' or 'impossible'.
$DVWA['default_security_level'] = 'impossible';

# 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';

# Disable authentication
# Some tools don't like working with authentication and passing cookies are
# und
# so this setting lets you turn off authentication.
$DVWA['disable_authentication'] = false;
```

Рис. 7: Прочтение конфигурационного файла

Адрес: <http://localhost/DVWA/setup.php>

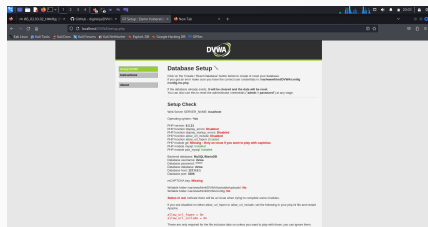
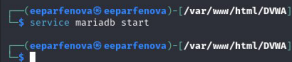


Рис. 8: Открытие страницы <http://localhost/DVWA/setup.php>

5. Запускаем стандартную базу данных mariadb



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

(eeparfenova@eeparfenova)-[/var/www/html/DVWA]
$ █
```

Рис. 9: Запуск базы данных

6. Создаем нового пользователя dvwa базы данных

```
(eeeparfenova@eeeparfenova)-[~]  
$ sudo su -  
root@eeeparfenova)-[~]  
$ mysql  
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/ser  
ver  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement  
.  
MariaDB [(none)]> create database dvwa  
→ ^C  
MariaDB [(none)]> create database dvwa;  
Query OK, 1 row affected (0.001 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';  
Query OK, 0 rows affected (0.016 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)]> █
```

Рис. 10: Создание нового пользователя базы данных (dvwa)

```
(eeparfenova@eeparfenova)-[~]  
$ mysql -u dvwa -pp@ssw0rd  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 32  
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)]> █
```

Рис. 11: Проверка создания нового пользователя

Вывод

Мы установили DVWA в гостевую систему к Kali Linux.