

Индивидуальный проект. Этап 2. Установка DVWA

Информационная безопасность

Фаик Карим

Содержание

Цель работы	1
Ход работы.....	2
Вывод.....	5

Цель работы

Этап 2. Установка DVWA Установите DVWA в гостевую систему к Kali Linux.
Репозиторий: <https://github.com/digininja/DVWA>. Некоторые из уязвимостей веб приложений, который содержит DVWA: Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений. Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение. SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение. Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер. Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS. Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие. DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях. Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу. Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб

приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

Ход работы

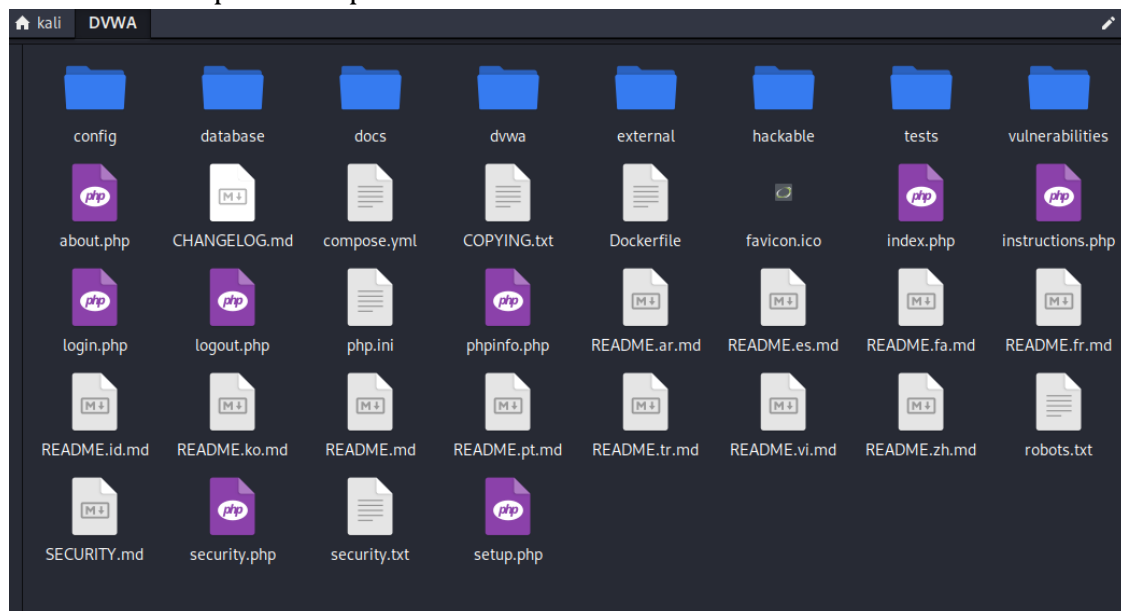
1. Клон репозитория DVWA.

```
(kali㉿kali)-[~]  
$ git clone https://github.com/digininja/DVWA.git  
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 184), reused 267 (delta 139), pack-reused 4450 (from 1)  
Receiving objects: 100% (4784/4784), 2.39 MiB | 628.00 KiB/s, done.  
Resolving deltas: 100% (2279/2279), done.
```

изображение 1

изображение 1

2. Файлы репозитория DVWA.



изображение 2

изображение 2

3. DVWA installer.

```
(kali㉿kali)-[~]  
$ sudo bash -c "$(curl --fail --show-error --silent --location https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh)"  
[sudo] password for kali:  
  
DVWA  
INSTALLER
```

изображение 3

изображение 3

4. Успешное выполнение DVWA installer.

```
DVWA has been installed successfully. Access http://localhost/DVWA to get started.  
Credentials:  
Username: admin  
Password: password
```

изображение 4

изображение 4

5. Успешный запуск DVWA локально.



Username

admin

Password


••••••••

Login

изображение 5

изображение 5

6. Вход в 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

Web Server SERVER_NAME: **localhost**

Operating system: ***nix**

PHP version: **8.2.23**
PHP function display_errors: **Enabled**
PHP function display_startup_errors: **Enabled**
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**

изображение 6

изображение 6

Вывод

Было установлинно DVWA в дистрибутиве Kali Linux в виртуальной машине.