

Презентация по второму этапу индивидуального проекта

Установка DVWA

Неустроева И.Н.

30 февраля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов
- <https://inneustroeva.github.io/ru/>

Вводная часть

DVWA (Damn Vulnerable Web Application) — это веб-приложение, которое уязвимо. Его главная цель-помочь веб-разработчикам лучше понять процесс безопасности веб-приложений и помочь студентам в изучении безопасности веб-приложений в контролируемой среде.

Установить DVWA в гостевую систему Kali Linux

Основная часть

Клонирование репозитория

Запустили терминал и перешли в каталог `/var/www/html`, это место где хранятся файлы локального хостинга. Далее мы клонируем репозиторий DVWA с GitHub в каталог `/html`.

```
(inneustroeva@inneustroeva)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
Клонирование в «DVWA» ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Получение объектов: 100% (5105/5105), 2.49 МиБ | 1.65 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.

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


Назначение разрешения папке на чтение запись и выполнение. Просмотр Директории

Папке DVWA назначаем разрешение на чтение, запись и выполнение. Далее переходим в каталог config и просмотрели ее содержание, там оказался файл, который содержит конфигурацию DVWA по умолчанию.

```
(inneustroeva@inneustroeva)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(inneustroeva@inneustroeva)-[/var/www/html]
$ cd DVWA/config

(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist

(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$
```

Создаем копию файла с именем config.inc.php, командой ls проверяем создание копии.

```
(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist
```

Далее открываем этот файл в редакторе nano, командой `sudo nano config.inc.php`, чтобы произвести необходимые настройки. Меняем значения `db_user` to `userDVWA` and `db_password` to `dvwa`.

```
$_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' ) ?: 'userDVWA';  
$_DVWA[ 'db_password' ] = getenv( 'DB_PASSWORD' ) ?: 'dvwa';
```

Запуск службы mysql

Запускаем службу mysql и проверяем ее запуск

```
(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disap>
   Active: active (running) since Wed 2025-03-19 22:21:45 MSK; 8s ago
 Invocation: 8cd7fa20d02343168c201b729230a121
    Docs: man:mariabdb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 18405 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/>
   Process: 18415 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_P>
   Process: 18417 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] 86 VAR=>
   Process: 18498 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START>
   Process: 18501 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCE>
 Main PID: 18478 (mariabdb)
   Status: "Taking your SQL requests now..."
    Tasks: 13 (limit: 14652)
  Memory: 242M (peak: 246.2M)
     CPU: 1.744s
   CGroup: /system.slice/mariadb.service
           └─18478 /usr/sbin/mariabdb

map 19 22:21:44 inneustroeva mariabdb[18478]: 2025-03-19 22:21:44 0 [Note] Plugin 'FE>
map 19 22:21:44 inneustroeva mariabdb[18478]: 2025-03-19 22:21:44 0 [Note] Plugin 'ws>
map 19 22:21:44 inneustroeva mariabdb[18478]: 2025-03-19 22:21:44 0 [Note] InnoDB: Lo>
map 19 22:21:44 inneustroeva mariabdb[18478]: 2025-03-19 22:21:44 0 [Note] InnoDB: Bu>
map 19 22:21:45 inneustroeva mariabdb[18478]: 2025-03-19 22:21:45 0 [Note] Server soc>
map 19 22:21:45 inneustroeva mariabdb[18478]: 2025-03-19 22:21:45 0 [Note] mariabdb:>
map 19 22:21:45 inneustroeva mariabdb[18478]: 2025-03-19 22:21:45 0 [Note] /usr/sbin/>
```

Создание нового пользователя в базе данных и предоставление ему всех прав доступа.

Входим в базу данных от имени суперпользователя root, далее система просит ввести пароль. Сначала мы создадим нового пользователя, используя учетные данные, которые мы создавали в файле config.inc.php. Далее предоставляем этому пользователю все права доступа к базе данных DVWA.

```
(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.4.3-MariaDB-1 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 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0,008 sec)
```

Веб-сервер Apache установлен по умолчанию, нам не нужно устанавливать дополнительные пакеты. Переходим в каталог `/etc/php/8.2/apache2`.

```
(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ ls /etc/php
8.2

(inneustroeva@inneustroeva)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2
```

Открываем файл `php.ini` в редакторе `nano` и меняем значение `allow_url_fopen` с `off` на `on`

```
; 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
```

Запуск службы веб-сервера

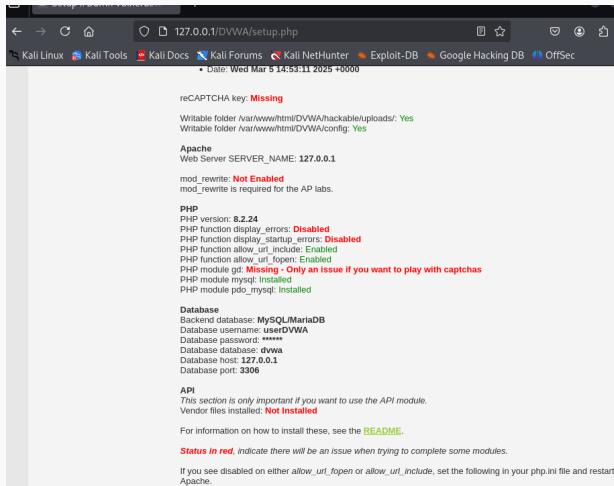
Переходим к запуску службы веб-сервера Apache, и проверяем запуск.

```
(inneustroeva@inneustroeva)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(inneustroeva@inneustroeva)-[/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 Wed 2025-03-19 22:56:02 MSK; 11s ago
 Invocation: fabba2eaffce4f4ab1739d03a20f7155
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 35169 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 35185 (apache2)
    Tasks: 6 (limit: 2220)
   Memory: 20.2M (peak: 20.4M)
      CPU: 81ms
   CGroup: /system.slice/apache2.service
           └─35185 /usr/sbin/apache2 -k start
           └─35188 /usr/sbin/apache2 -k start
           └─35189 /usr/sbin/apache2 -k start
           └─35190 /usr/sbin/apache2 -k start
           └─35191 /usr/sbin/apache2 -k start
           └─35192 /usr/sbin/apache2 -k start
```


Переход на страницу DVWA, через браузер

Переходим к запуску приложения DVWA. Переходим в браузер и переходим по ссылке на страницу DVWA.



Вход в систему DVWA

Далее мы входим в систему DVWA, вводим пароль и имя



Username

admin

Password

.....|

После успешного входа мы попали на домашнюю страницу DVWA

← → ↻ 🏠 🔍 127.0.0.1/DVWA/index.php

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

DVWA

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

Cryptography

API

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA Security

PHP Info

About

В результате мы установили DVWA в гостевую систему Kali Linux

Надеюсь, что работа с этим веб-приложением будет полезной для меня и моей карьеры

...