

# **Отчёт по этапу №2 индивидуального проекта**

**Установка DVWA**

Хусаинова Динара Айратовна, НПИбд-02-21, 1032212283

# Содержание

<b>Цель работы</b>	<b>4</b>
<b>Теоретическое введение</b>	<b>5</b>
<b>Выполнение этапа</b>	<b>7</b>
Установка DVWA . . . . .	7
<b>Вывод</b>	<b>11</b>
<b>Список литературы. Библиография</b>	<b>12</b>

## Список иллюстраций

1	Вход на репозиторий для скачивания DVWA . . . . .	7
2	Выполнение команды <code>wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh</code> . . . . .	8
3	Делаем скрипт исполняемым и запускаем скрипт от имени root . . . . .	8
4	Загрузка . . . . .	9
5	Ввод учетных данных для sql пользователя . . . . .	9
6	Конец загрузки . . . . .	10

## **Цель работы**

Установить DVWA.

# Теоретическое введение

Damn Vulnerable Web Application (DVWA) — это веб-приложение на PHP/MySQL, которое содержит различные уязвимости [1].

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.

# Выполнение этапа

## Установка DVWA

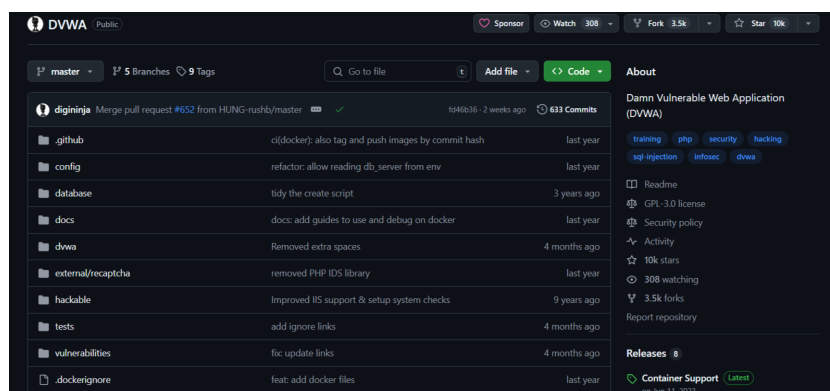


Рис. 1: Вход на репозиторий для скачивания DVWA

```
File Actions Edit View Help
(dakhusainova@kali)-[~]
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
--2024-09-18 10:06:05-- https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16904 (17K) [text/plain]
Saving to: 'Install-DVWA.sh'

Install-DVWA.sh  100%[=====>] 16.51K  --.-KB/s  in 0.007s

2024-09-18 10:06:05 (2.46 MB/s) - 'Install-DVWA.sh' saved [16904/16904]

(dakhusainova@kali)-[~]
$
```

Рис. 2: Выполнение команды `wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh`

```
(dakhusainova@kali)-[~]
$ chmod +x Install-DVWA.sh

(dakhusainova@kali)-[~]
$ sudo ./Install-DVWA.sh
[sudo] password for dakhusainova:

  DVWA
INSTALLER

Welcome to the DVWA setup!
Script Name: Install-DVWA.sh
Author: IamCarron
Github Repo: https://github.com/IamCarron/DVWA-Script
Installer Version: 1.0.5

Updating repositories...
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]
71% [3 Contents-amd64 30.4 MB/49.2 MB 62%] 6894 kB/s 2s
```

Рис. 3: Делаем скрипт исполняемым и запускаем скрипт от имени root



```

Get:2 http://kali.download/kali kali-rolling/main amd64 php8.2-opcache amd64
8.2.23-1 [352 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 php8.2-mysql amd64 8.
2.23-1 [118 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libapache2-mod-php8.2
amd64 8.2.23-1 [1689 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 php8.2-cli amd64 8.2.
23-1 [1748 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 php8.2-common amd64 8
.2.23-1 [685 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 php8.2-gd amd64 8.2.2
3-1 [29.2 kB]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 php-gd all 2:8.2+93+n
mu1 [3776 B]
Get:9 http://mirror.cs.spacehostings.com/kali kali-rolling/main amd64 php8.2 al
l 8.2.23-1 [41.9 kB]
Fetched 4679 kB in 7s (699 kB/s)
(Reading database ... 395169 files and directories currently installed.)
Preparing to unpack .../0-php8.2-readline_8.2.23-1_amd64.deb ...
Unpacking php8.2-readline (8.2.23-1) over (8.2.21-1+b1) ...
Preparing to unpack .../1-php8.2-opcache_8.2.23-1_amd64.deb ...
Unpacking php8.2-opcache (8.2.23-1) over (8.2.21-1+b1) ...
Preparing to unpack .../2-php8.2-mysql_8.2.23-1_amd64.deb ...
Unpacking php8.2-mysql (8.2.23-1) over (8.2.21-1+b1) ...
Preparing to unpack .../3-libapache2-mod-php8.2_8.2.23-1_amd64.deb ...
Unpacking libapache2-mod-php8.2 (8.2.23-1) over (8.2.21-1+b1) ...
Preparing to unpack .../4-php8.2-cli_8.2.23-1_amd64.deb ...
Unpacking php8.2-cli (8.2.23-1) over (8.2.21-1+b1) ...
Preparing to unpack .../5-php8.2-common_8.2.23-1_amd64.deb ...
Unpacking php8.2-common (8.2.23-1) over (8.2.21-1+b1) ...
Selecting previously unselected package php8.2-gd.
Preparing to unpack .../6-php8.2-gd_8.2.23-1_amd64.deb ...
Unpacking php8.2-gd (8.2.23-1) ...
Selecting previously unselected package php-gd.
Preparing to unpack .../7-php-gd_2%3a8.2+93+nm1_all.deb ...
Unpacking php-gd (2:8.2+93+nm1) ...
Preparing to unpack .../8-php8.2_8.2.23-1_all.deb ...
Unpacking php8.2 (8.2.23-1) over (8.2.21-1) ...
Setting up php8.2-common (8.2.23-1) ...
Progress: [ 51%] [ ]

```

Рис. 4: Загрузка

```

Password: [no password just hit enter]
Enter SQL user: root
Enter SQL password (press Enter for no password):
SQL commands executed successfully.
Configuring DVWA...
Configuring permissions...
Configuring PHP...
Enabling Apache...

```

Рис. 5: Ввод учетных данных для sql пользователя

```
Restarting Apache ...  
DVWA has been installed successfully. Access http://localhost/DVWA to get started.  
Credentials:  
Username: admin  
Password: password  
  
With ♥ by IamCarron  
  
(dakhusainova@kali)~]  
$
```

Рис. 6: Конец загрузки

## **Вывод**

Успешно установлен DVWA.

# **Список литературы. Библиография**

[1] Документация по DVWA: <https://kali.tools/?p=1820>