

Индивидуальный проект. Второй этап

Установка DVWA

Чемоданова Ангелина Александровна

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	10

Список иллюстраций

3.1	Клонирование репозитория	7
3.2	Запуск скрипта	7
3.3	Смена прав	8
3.4	Установка	8
3.5	Логин и пароль для DVWA	8
3.6	Запущенный сайт	9
3.7	База данных	9

1 Цель работы

Установка DVWA в гостевую систему к Kali Linux.

2 Теоретическое введение

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.

3 Выполнение лабораторной работы

Для начала мы клонируем репозиторий DVWA.(рис. 3.1).

```
(kali@kali)-[~]
$ 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 | 4.06 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.

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

Рис. 3.1: Клонирование репозитория

Запускаем скрипт. (рис. 3.2).

```
(kali@kali)-[~]
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
--2024-03-15 15:07:56-- https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443 ... connect
ed.
HTTP request sent, awaiting response... 200 OK
Length: 16688 (16K) [text/plain]
Saving to: 'Install-DVWA.sh'

Install-DVWA.sh      100%[=====>] 16.30K  --.-KB/s  in 0.001s

2024-03-15 15:07:57 (11.6 MB/s) - 'Install-DVWA.sh' saved [16688/16688]

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

Рис. 3.2: Запуск скрипта

Изменяем права на скрипт. (рис. 3.3).

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

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

Рис. 3.3: Смена прав

Производим установку. (рис. 3.4).

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

DVWA
INSTALLER

Welcome to the DVWA setup!
Script Name: Install-DVWA.sh
Author: IamCarron
Github Repo: https://github.com/IamCarron/DVWA-Script
Installer Version: 1.0.4

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 [19.8 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.1 MB]
37% [2 Packages store 0 B] [3 Contents-amd64 46.3 kB/47.1 MB 0%]
```

Рис. 3.4: Установка

Получаем логин и пароль для DVWA. (рис. 3.5).

```
Default credentials:
Username: root

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

With ♥ by IamCarron

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

Рис. 3.5: Логин и пароль для DVWA

Запускаем сайт. (рис. 3.6).

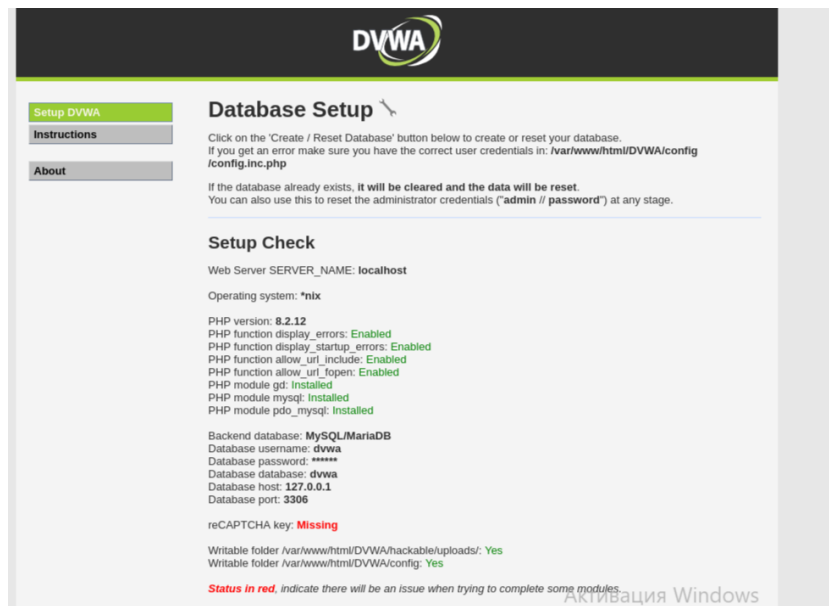


Рис. 3.6: Запущенный сайт

Создаем базу данных. (рис. 3.7).

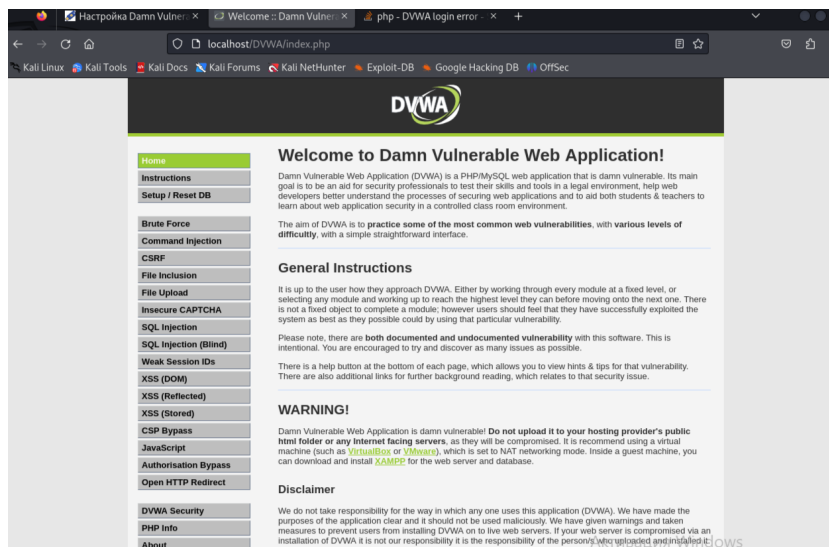


Рис. 3.7: База данных

4 Выводы

Мы установили DVWA в гостевую систему к Kali Linux.