

Индивидуальный проект - Этап 2

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	10
4	Список литературы	11

Список иллюстраций

2.1	Клонирование из репозитория	5
2.2	Перенос файлов	5
2.3	Инициализация apache2	6
2.4	Копирование конфига	6
2.5	создаю database user	7
2.6	database user успешно создан	7
2.7	Create/Reset Database	8
2.8	Успешно!	8
2.9	admin & password	9
2.10	DVWA успешно установлен	9

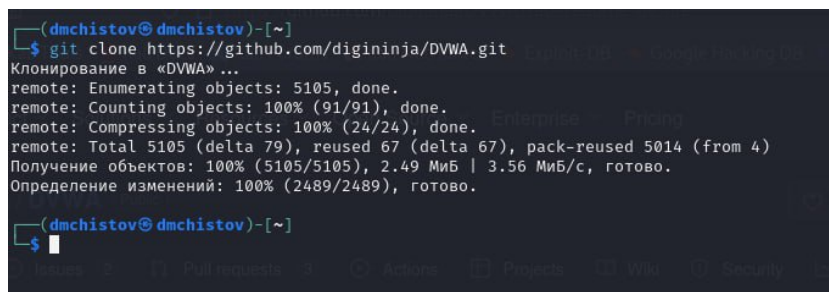
1 Цель работы

Установка дистрибутива DVWA на Kali Linux

2 Выполнение лабораторной работы

Данную работу я выполнял, следуя видео руководству, прикреплённому к официальному репозиторию.

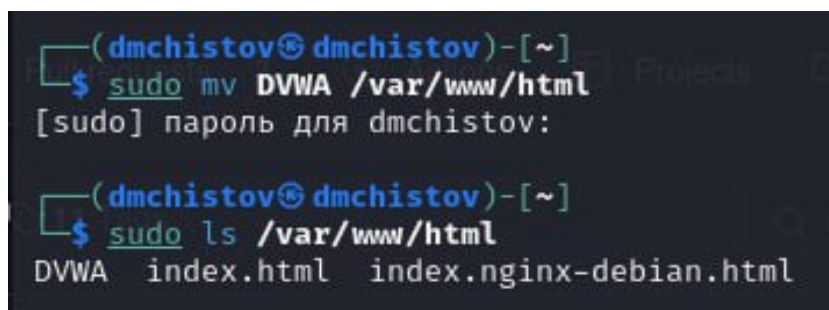
Клонирую DVWA из официального репозитория (рис. 2.1).



```
(dmchistov@dmchistov)-[~]  
$ git clone https://github.com/digininja/DVWA.git  
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 | 3.56 МиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
  
(dmchistov@dmchistov)-[~]  
$
```

Рис. 2.1: Клонирование из репозитория

Далее специально перевожу установленную папку в раздел /var/www/html, чтобы можно было пользоваться DVWA через localhost (рис. 2.2).



```
(dmchistov@dmchistov)-[~]  
$ sudo mv DVWA /var/www/html  
[sudo] пароль для dmchistov:  
  
(dmchistov@dmchistov)-[~]  
$ sudo ls /var/www/html  
DVWA index.html index.nginx-debian.html
```

Рис. 2.2: Перенос файлов

Чтобы пользоваться DVWA нам также требуется запустить apache2 (рис. 2.3).

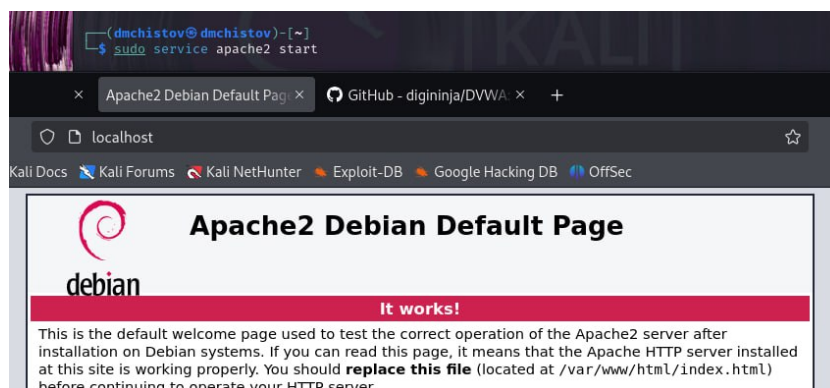


Рис. 2.3: Инициализация apache2

Однако пока DVWA не работает - нам пишут, что требуется скопировать файл конфигурации таким образом, чтобы у него исчезло расширение .dist. Таким образом у нас всегда будет резервная копия конфига, а также так нас призывают к самостоятельной настройке этого самого конфига (рис. 2.4).

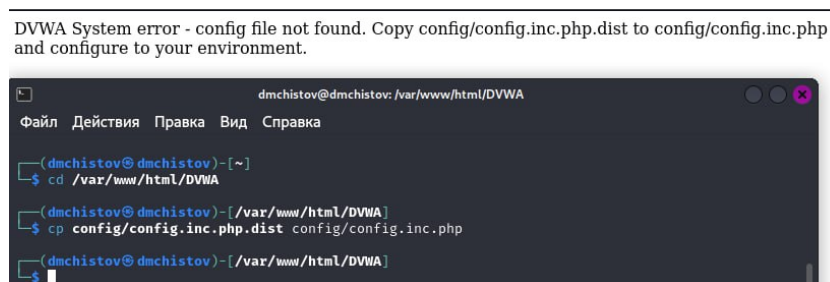


Рис. 2.4: Копирование конфига

Т.к. я пользуюсь Kali Linux, у меня установлен MariaDB и в связи с этим от меня требуется самостоятельно создать “database user”. Поэтому становлюсь рут пользователем, запускаю mysql и прописываю пару команд, которые есть в официальном репозитории, таким образом я создал пользователя баз данных и теперь успешно могу создавать свои базы данных для работы с DVWA (рис. 2.5).

```
(dmchistov@dmchistov)-[/var/www/html/DVWA]
$ sudo su -
[sudo] пароль для dmchistov:
(dmchistov@dmchistov)-[~]
# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
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 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 (0,004 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]>
```

Рис. 2.5: создаю database user

Удостоверяюсь, что пользователь успешно создан. Всё работает (рис. 2.6).

```
(dmchistov@dmchistov)-[~]
$ mysql -u dvwa -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)]> use dvwa;
Database changed
MariaDB [dvwa]>
```

Рис. 2.6: database user успешно создан

Теперь возвращаюсь в DVWA и нажимаю “Create/Reset Database” (рис. 2.7).

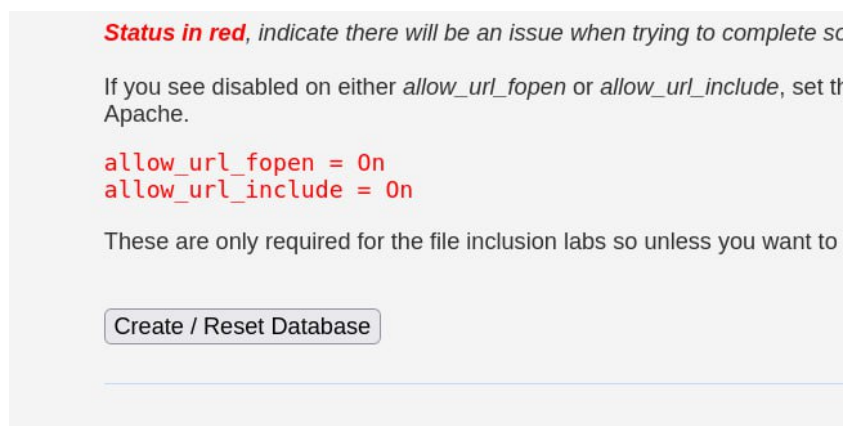


Рис. 2.7: Create/Reset Database

База данных успешно создана (рис. 2.8).

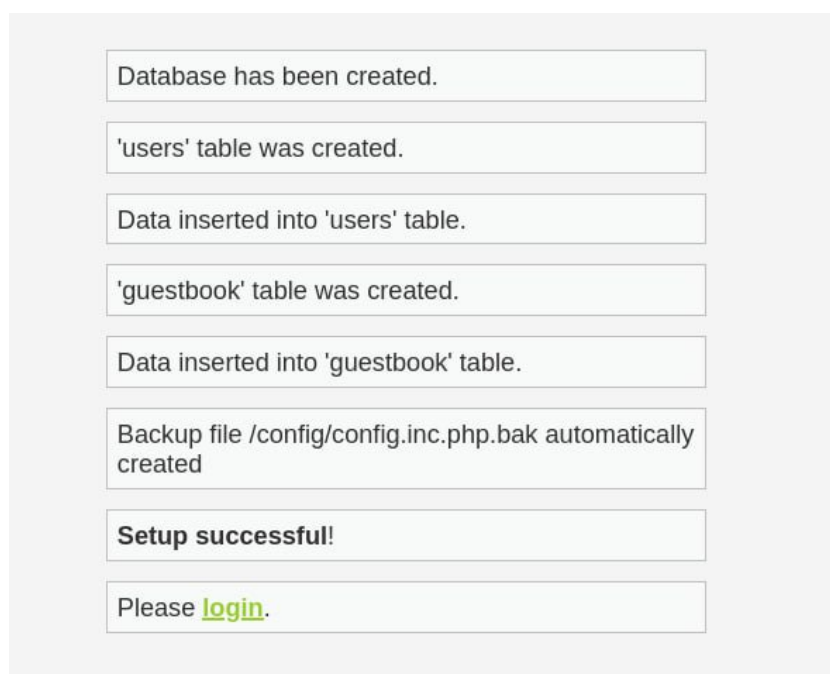



Рис. 2.8: Успешно!

Теперь меня автоматически переводит на страницу входа, ввожу данные по умолчанию - admin и его пароль (рис. 2.9).



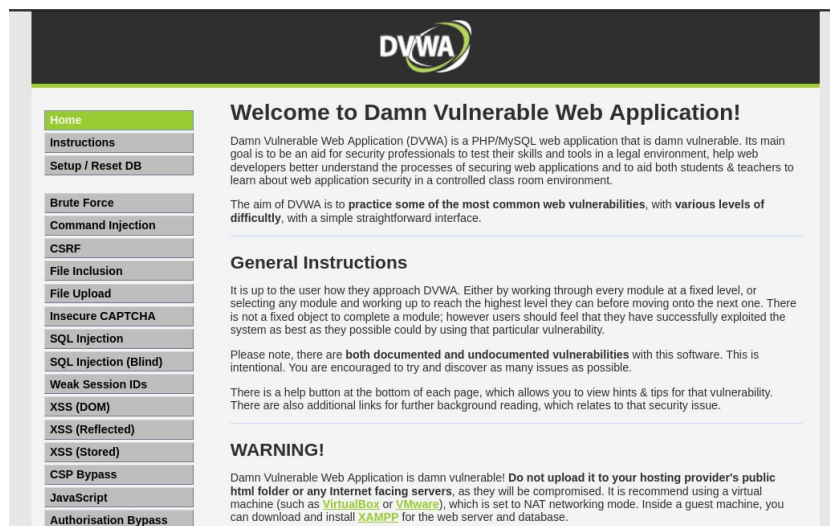
Username

Password

Login

Рис. 2.9: admin & password

DVWA успешно установлена и конфигурация завершена (рис. 2.10).



The image shows the DVWA welcome screen. At the top is the DVWA logo. Below it is a sidebar with a list of modules: Home (highlighted), 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, and Authorisation Bypass. The main content area has the heading 'Welcome to Damn Vulnerable Web Application!' followed by a paragraph about the application's purpose. Below that is a section titled 'General Instructions' with more details and a 'WARNING!' section at the bottom.

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 possibly 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.

Рис. 2.10: DVWA успешно установлен

3 Выводы

При выполнении данной работы я успешно установил Damn Vulnerable Web Application.

4 Список литературы

Индивидуальный проект

DVWA

Видео руководство по установке DVWA на Kali Linux