

Лабораторная работа №2

Дисциплина - основы информационной безопасности

Пронякова О.М.

15 марта 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Пронякова Ольга Максимовна
- студент НКАбд-02-22
- факультет физико-математических и естественных наук
- Российский университет дружбы народов

Создание презентации

Установить DVWA в гостевую систему к Kali Linux.

Этапы выполнения работы

Устанавливаем DVWA через репозиторий на гитхабе(рис.1).

File Actions Edit View Help

(ompronyakova@kali)-[~]

\$ git clone https://github.com/digininja/DVWA.git~

Cloning into 'DVWA.git~' ...

remote: Repository not found.

fatal: repository 'https://github.com/digininja/DVWA.git~/' not found

(ompronyakova@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 | 2.17 MiB/s, done.

Resolving deltas: 100% (2112/2112), done.

(ompronyakova@kali)-[~]

\$ sudo mv DVWA /var/www/html

[sudo] password for ompronyakova:

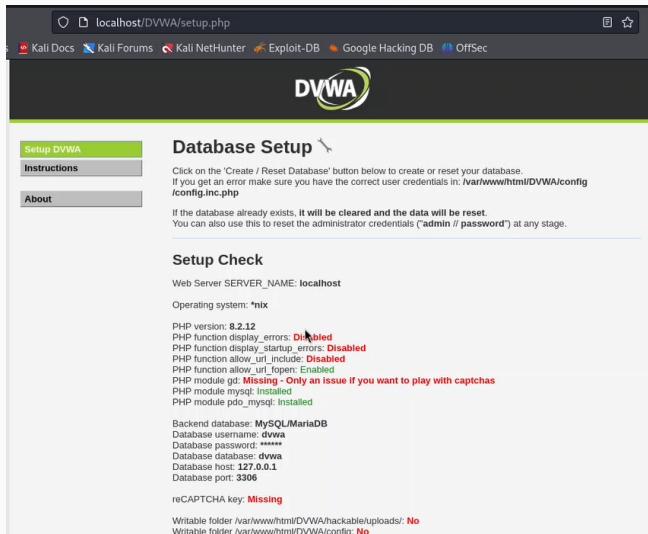
(ompronyakova@kali)-[~]

\$ cd /var/www/html


(ompronyakova@kali)-[/var/www/html]

\$

Переходим на setup DVWA и проверяем настройки(рис.2).



Создаем database в DVWA(рис.3), (рис.4).



```
mysql> create database dvwa;  
Query OK, 1 row affected (0.00 sec)  
  
mysql> create user dvwa@localhost identified by 'p@ssw0rd';  
Query OK, 0 rows affected (0.01 sec)  
  
mysql> grant all on dvwa.* to dvwa@localhost;  
Query OK, 0 rows affected (0.01 sec)  
  
mysql> flush privileges;  
Query OK, 0 rows affected (0.00 sec)
```

Рис. 3: Инструкция по созданию database в DVWA

Этапы выполнения работы

```
File Actions Edit View Help
ompronyakova@ka...r/www/html/DVWA x root...i: ~ x omprony...kali: ~ x

Enter password:
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password
: YES)

(ompronyakova@kali)-[~]
$ mysql -u dvwa -p
Enter password:
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password
: YES)

(ompronyakova@kali)-[~]
$ mysql -u dvwa -p
Enter password:
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password
: YES)

(ompronyakova@kali)-[~]
$ mysql -u dvwa -p
Enter password:
ERROR 1045 (28000): Access denied for user 'dvwa'@'localhost' (using password
: YES)

(ompronyakova@kali)-[~]
$ mysql -u dvwa -p
Enter password: █
```

Задаем логин и пароль на сайте(рис.5).



The logo for DVWA (Damn Vulnerable Web Application) is displayed at the top. It features the letters "DVWA" in a bold, dark blue font. To the right of the text is a stylized circular graphic composed of two curved, overlapping bands, one in a light green color and the other in a dark blue color.

Username

Password

Below the password field, there is a small, light gray button with a dark gray icon, likely representing a "login" or "submit" action.

Этапы выполнения работы

Устраняем неполадки в настройках сайта(рис.6), (рис.7), (рис.8).

The image shows a web browser displaying the DVWA (Damn Vulnerable Web Application) homepage. The browser's address bar shows the URL `http://kali:8080/`. The page has a dark theme with a navigation menu on the left and a main content area. The navigation menu includes links like 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, and DVWA Security. The main content area is titled "Database Setup" and contains instructions for creating or resetting the database. It also includes a "Setup Check" section with various system and application details.

The terminal window on the right shows the following commands and output:

```
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
ompronyakov...w/html/DVWA x ... x omp...: ~ x root@ka...apache2 x
(ompronyakova@kali)-[~]
$ cd /var/www/html/DVWA
(ompronyakova@kali)-[/var/www/html/DVWA]
$ sudo su -
[sudo] password for ompronyakova:
(ompronyakova@kali)-[~]
$ cd /etc/php
(root@kali)-[/etc/php]
$ ls
8.2
(root@kali)-[/etc/php]
$ cd 8.2
(root@kali)-[/etc/php/8.2]
$ ls
apache2 cli mods-available
(root@kali)-[/etc/php/8.2]
$ cd apache2
(root@kali)-[/etc/php/8.2/apache2]
$ ls
```

The "Database Setup" section contains the following text:

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.

The "Setup Check" section displays the following information:

- Web Server SERVER_NAME: localhost
- Operating system: *nix
- PHP version: 8.2.12
- PHP function display_errors: Disabled
- PHP function display_startup_errors: Disabled
- PHP function allow_url_include: Disabled
- PHP function allow_url_fopen: Enabled
- PHP module gd: Missing - Only an issue if you want to play with captchas
- 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/: No
- Writable folder /var/www/html/DVWA/config: No

Этапы выполнения работы

```
root@kali: /etc/php/8.2/apache2

File Actions Edit View Help

ompronyakov...w/html/DVWA x ... x omp...: ~ x root@ka...apache2 x

(root@kali)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 ompronyakova ompronyakova 4096 Mar 15 06:05 .
drwxr-xr-x 5 ompronyakova ompronyakova 4096 Mar 15 06:05 ..
-rw-r--r-- 1 ompronyakova ompronyakova 667 Mar 15 06:05 dvwa_email.png

(root@kali)-[/etc/php/8.2/apache2]
# chown www-data /var/www/html/DVWA/hackable/uploads/

(root@kali)-[/etc/php/8.2/apache2]
# ls -al /var/www/html/DVWA/hackable/uploads/
total 12
drwxr-xr-x 2 www-data      ompronyakova 4096 Mar 15 06:05 .
drwxr-xr-x 5 ompronyakova ompronyakova 4096 Mar 15 06:05 ..
-rw-r--r-- 1 ompronyakova ompronyakova 667 Mar 15 06:05 dvwa_email.png

(root@kali)-[/etc/php/8.2/apache2]
# chmod 777 /var/www/html/DVWA/hackable/uploads/
chmod: missing operand after '/var/www/html/DVWA/hackable/uploads/'
Try 'chmod --help' for more information.

(root@kali)-[/etc/php/8.2/apache2]
#
```

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: ***nix**

PHP version: **8.2.12**

PHP function display_errors: **Disabled**

PHP function display_startup_errors: **Disabled**

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**

Установила DVWA в гостевую систему к Kali Linux.