

report

Отчет по 2 этапу проекта "Установка DVWA"

Подъярова Ксения Витальевна

Цель работы

Приобретение практических навыков по установке DVWA.

Выполнение лабораторной работы

- Установить DVWA на дистрибутив Kali Linux.
1. Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию /var/www/html. Затем клонирую нужный репозиторий GitHub.

```
(kali㉿kali)-[~]  
$ sudo git clone https://github.com/digininja/DVWA  
[sudo] password for kali:  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4784, done.  
remote: Counting objects: 100% (334/334), done.  
remote: Compressing objects: 100% (187/187), done.  
remote: Total 4784 (delta 184), reused 267 (delta 139), pack-reused 4450 (from 1)  
Receiving objects: 100% (4784/4784), 2.39 MiB | 2.97 MiB/s, done.  
Resolving deltas: 100% (2279/2279), done.
```

2. Проверяю, что файлы скопировались правильно, далее повышаю права доступа к этой папке до 777.

```
(kali㉿kali)-[~]  
$ ls  
Desktop Downloads Music Public Videos  
Documents DVWA Pictures Templates  
  
(kali㉿kali)-[~]  
$ sudo chmod -R 777 DVWA
```

3. Чтобы настроить DVWA, нужно перейти в каталог /dvwa/config, затем проверяю содержимое каталога.

```

(kali㉿kali)-[~]
$ cd DVWA/config

(kali㉿kali)-[~/DVWA/config]
$ ls
config.inc.php.dist

```

4. Создаем копию файла, используемого для настройки DVWA config.inc.php.dist с именем config.inc.php. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так.

```

(kali㉿kali)-[~/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(kali㉿kali)-[~/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist

```

5. Далее открываю файл в текстовом редакторе.

```

(kali㉿kali)-[~/DVWA/config]
$ sudo nano config.inc.php

```

6. Изменяю данные об имени пользователя и пароле.

```

File Actions Edit View Help
GNU nano 8.1 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'userDVWA';
$_DVWA[ 'db_password' ] = 'dvwa';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default locale

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line  M-E Redo

```

7. По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс.

```
(kali@kali)-[~/DVWA/config]
$ sudo systemctl start mysql

(kali@kali)-[~/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 07:19:17 EDT; 27s ago
     Invocation: a0def86f5bb8436db800ad0c08f06ed6
       Docs: man:mariadb(8)
```

8. Авторизируюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением "MariaDB", далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php

```
(kali@kali)-[~/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.2-MariaDB-4 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 (0.017 sec)
```

9. Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> exit
Bye
```

10. Необходимо настроить сервер apache2, перехожу в соответствующую директорию. В файле php.ini нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе.

```
(kali@kali)-[~/DVWA/config]
$ cd /etc/php/8.2/apache2

(kali@kali)-[/etc/php/8.2/apache2]
$ sudo nano php.ini

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

11. В файле параметры allow_url_fopen и allow_url_include должны быть поставлены как On.

```

;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;

; 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

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to
; automatically detect the EOL character in those files so that
; fgets() and file() will work regardless of the source of the file.

```

[^]G Help [^]O Write Out [^]F Where Is [^]K Cut [^]T Execute [^]C Location
[^]X Exit [^]R Read File [^]\ Replace [^]U Paste [^]J Justify [^]/ Go To L

12. Запускаем службу веб-сервера apache и проверяем, запущена ли служба

```

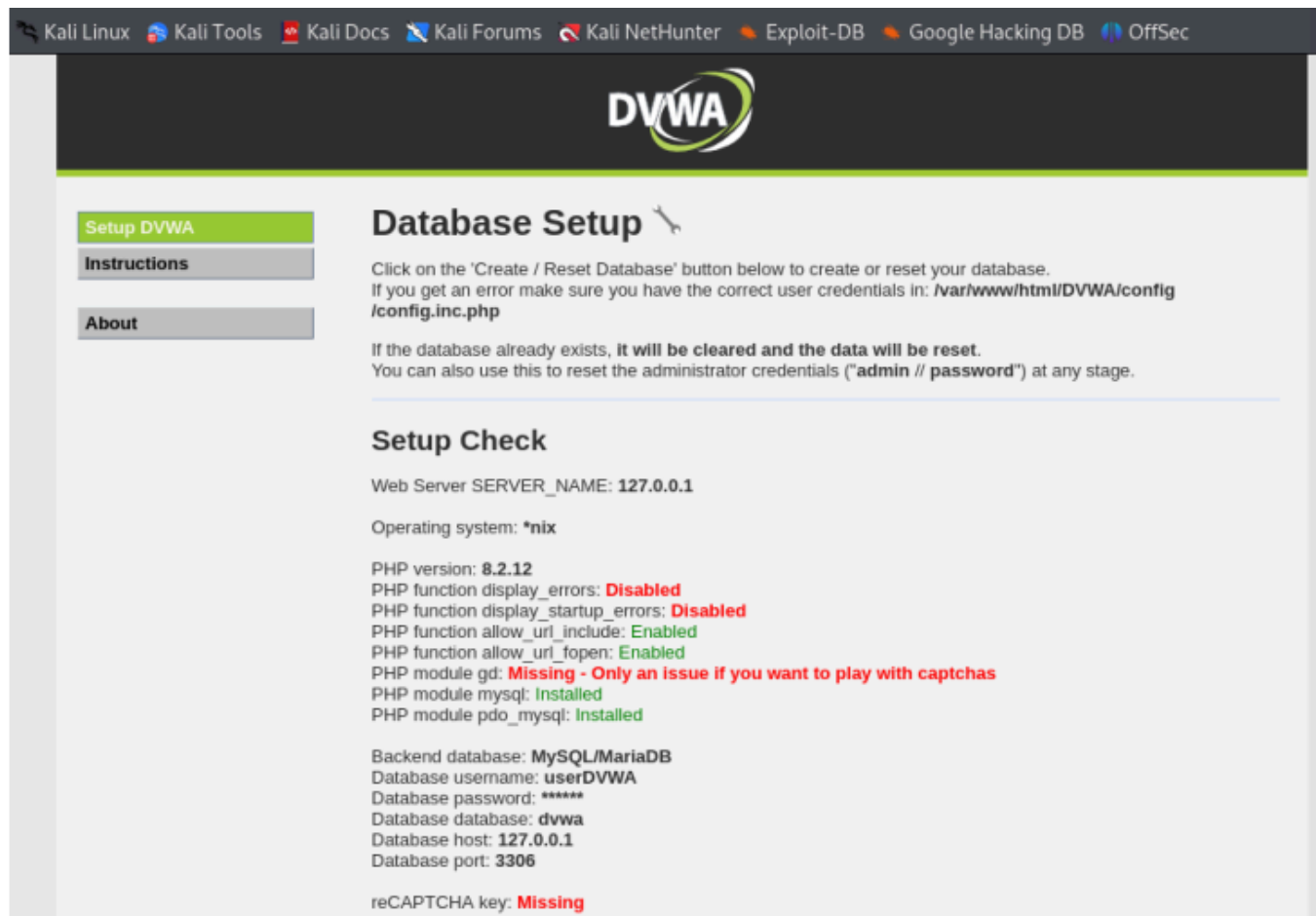
(kali@kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(kali@kali)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 07:33:13 EDT; 21s ago
 Invocation: 1d8e78ea34294cb2aa69fe8db1c106c7
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 21621 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 21637 (apache2)
   Tasks: 6 (limit: 2269)
  Memory: 25.3M (peak: 25.5M)
     CPU: 168ms
    CGroup: /system.slice/apache2.service
            └─21637 /usr/sbin/apache2 -k start
              └─21640 /usr/sbin/apache2 -k start
                └─21641 /usr/sbin/apache2 -k start
                  └─21642 /usr/sbin/apache2 -k start
                    └─21643 /usr/sbin/apache2 -k start
                      └─21644 /usr/sbin/apache2 -k start

Sep 21 07:33:13 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 21 07:33:13 kali apachectl[21636]: AH00558: apache2: Could not reliably determine the server's fully>
Sep 21 07:33:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-22/22 (END)

```

13. Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA



Setup DVWA

Instructions

About

Database Setup

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.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

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: **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: **userDVWA**

Database password: *********

Database database: **dvwa**

Database host: **127.0.0.1**

Database port: **3306**

reCAPTCHA key: **Missing**

14. Прокручиваем страницу вниз и нажимаем на кнопку create/reset database.
Авторизуюсь с помощью предложенных по умолчанию данных.



DVWA

Username

admin

Password

.....

Login

15. Оказываюсь на домашней странице веб-приложения, на этом установка окончена



Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.