

Отчет по первому этапу индивидуального проекта

Информационная безопасность

Кармацкий Никита Сергеевич

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	8
5	Выводы	15

Список иллюстраций

4.1	Клонирования репозитория	8
4.2	Изменение прав доступа	9
4.3	Создание копии файла	9
4.4	Редактирование файла	10
4.5	Редактирование файла	10
4.6	Настройка в базе данных	11
4.7	Переход в директорию с apache2	11
4.8	Настройка apache2	12
4.9	Запуск apache2	12
4.10	Запуск веб-приложения	13
4.11	“Создание базы данных”	13
4.12	Авторизация	14
4.13	Домашняя страница DVWA	14

1 Цель работы

Приобретение практических навыков по установке DVWA.

2 Задание

1. Установить DVWA на дистрибутив Kali Linux.

3 Теоретическое введение

DVWA - это уязвимое веб-приложение, разработанное на PHP и MYSQL.

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 четыре 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.

4 Выполнение лабораторной работы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).

```
(nskarmatskiy@kali)-[~]
└─$ cd /var/www/html

(nskarmatskiy@kali)-[/var/www/html]
└─$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for nskarmatskiy:
Cloning into 'DVWA'...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 4758 (delta 168), reused 240 (delta 122), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.36 MiB | 605.00 KiB/s, done.
Resolving deltas: 100% (2279/2279), done.
```

Рис. 4.1: Клонирования репозитория

Проверяем, что файлы скопировались правильно, далее повышаем права доступа к этому каталогу до 777 (рис. 2).


```

(nskarmatskiy@kali)-[/var/www/html]
$ ls -l
total 20
drwxr-xr-x 12 root root 4096 Sep 20 17:10 DVWA
-rw-r--r-- 1 root root 10701 Sep 11 17:42 index.html
-rw-r--r-- 1 root root 615 Sep 11 17:44 index.nginx-debian.html

(nskarmatskiy@kali)-[/var/www/html]
$ chmod 777 DVWA
chmod: changing permissions of 'DVWA': Operation not permitted

(nskarmatskiy@kali)-[/var/www/html]
$ chmod /777 DVWA
chmod: invalid mode: '/777'
Try 'chmod --help' for more information.

(nskarmatskiy@kali)-[/var/www/html]
$ sudo chmod 777 DVWA

```

Рис. 4.2: Изменение прав доступа

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`, затем нужно отредактировать файл `config/config.inc.php`, который мы получаем копируя шаблон (рис. 3).

```

(nskarmatskiy@kali)-[/var/www/html]
$ cd DVWA/config

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
$ cp config.inc.php.dist config.inc.php

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php config.inc.php.dist

```

Рис. 4.3: Создание копии файла

Открываем файл на редактирование и меняем имя пользователя и пароль (рис. 4).

```
File Actions Edit View Help
GNU nano 7.2 config.inc.php *
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a 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
$_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',
$_DVWA['default_security_level'] = 'impossible';

Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify
```

Рис. 4.4: Редактирование файла

Запускаем сервис sql и проверяем, что он запущен. (рис. 5).

```
(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl enable mysql
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/systemd/system/mariadb.service.

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl start mysql

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
└─$ sudo systemctl status mysql
● mariadb.service - MariaDB 10.11.7 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 17:13:49 MSK; 7s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 6040 ExecStartPre=/usr/bin/install -m 755 -o mysql -f root -d /var/run/mysql (code=exited, status=0/SUCCESS)
   Process: 6040 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 6050 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR= cd /usr/bin/ && ./galera_recovery (code=exited, status=0/SUCCESS)
   Process: 6124 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 6126 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 6110 (mariadbd)
    Status: "Taking your SQL requests now..."
     Tasks: 14 (limit: 14084)
    Memory: 110.9M (peak: 114.3M)
```

Рис. 4.5: Редактирование файла

Авторизируемся в базе данных MariaDB под именем пользователя, которого мы задали в файле config.inc.php, а так же представляем привелегии для работы с этой базой данных (рис. 6).

```

(nskarmatskiy@kali)-[/var/www/html/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: 10.11.7-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' identifies 'dvwa'
-> ^C
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identifies 'dvwa';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB
server version for the right syntax to use near 'identifies 'dvwa'' at line 1
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified 'dvwa';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB
server version for the right syntax to use near 'identified 'dvwa'' at line 1
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified 'dvwa';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB
server version for the right syntax to use near 'dvwa' at line 1
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.030 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.010 sec)

MariaDB [(none)]> exit
Bye

```

Рис. 4.6: Настройка в базе данных

Далее настраиваем сервер apache2, для этого переходим в каталог с настройками(рис. 7).

```

(nskarmatskiy@kali)-[/var/www/html/DVWA/config]
└─$ cd /etc/php/8.2/apache2

(nskarmatskiy@kali)-[/etc/php/8.2/apache2]
└─$ ls
conf.d  php.ini

```

Рис. 4.7: Переход в директорию с apache2

Открываем файл `apache2.conf`. В файле параметры `allow_url_fopen` и `allow_url_include` должны быть поставлены как `on` (рис. 8)

```
GNU nano 2.2 php.ini *
max_file_uploads = 20

;::::::::::::::::::
; 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"
```

Рис. 4.8: Настройка apache2

Запускаем сервис apache2 и проверяем, что он запущен (рис. 9).

```
(nskarmatskiy@kali)~[/etc/php/8.2/apache2]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install
.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apac
he2.service.

(nskarmatskiy@kali)~[/etc/php/8.2/apache2]
└─$ sudo systemctl start apache2

(nskarmatskiy@kali)~[/etc/php/8.2/apache2]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 17:24:04 MSK; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 6768 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 6801 (apache2)
      Tasks: 7 (limit: 2134)
     Memory: 25.0M (peak: 26.2M)
        CPU: 7ms
     CGroup: /system.slice/apache2.service
            └─6801 /usr/sbin/apache2 -k start
```

Рис. 4.9: Запуск apache2

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0.1/DVWA (рис. 10)

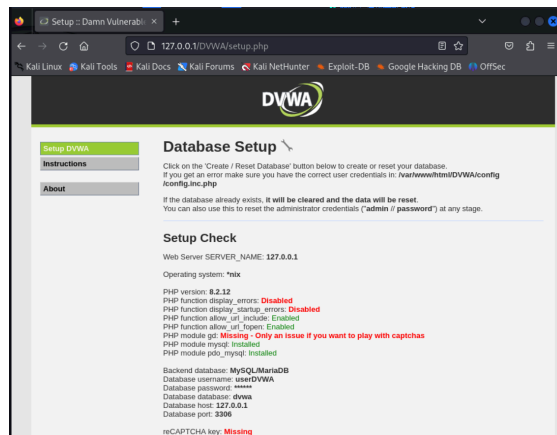


Рис. 4.10: Запуск веб-приложения

Прокручиваем страницу вниз и нажимаем на кнопку `create\reset database` (рис. 11)

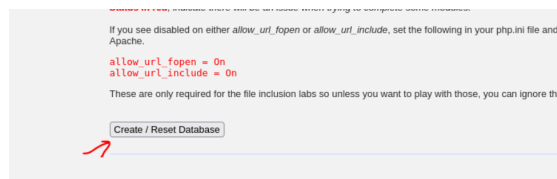
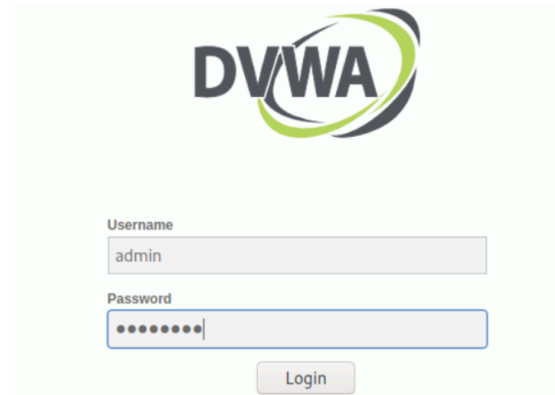


Рис. 4.11: “Создание базы данных”

Авторизуемся с помощью предложенных по умолчанию данных (admin:password) (рис. 12)



The image shows the login page of the DVWA application. At the top is the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a green and blue circular graphic element to the right. Below the logo are two input fields: 'Username' with the text 'admin' and 'Password' with a masked password represented by dots. A 'Login' button is positioned below the password field.

Рис. 4.12: Авторизация

Оказываемся на домашней странице веб-приложения, на этом установка окончена (рис. 13)

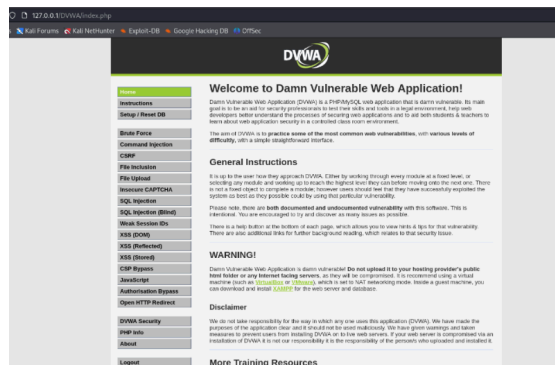


Рис. 4.13: Домашняя страница DVWA

5 Выводы

Приобрели практические навыки по установке уязвимого веб-приложения DVWA.