

Отчет по второму этапу индивидуального проекта

Основы информационной безопасности

Ничипорова Елена Дмитриевна

Содержание

Цель работы	1
Задание	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Выводы.....	7
Список литературы.....	8

Цель работы

Приобретение практических навыков по установке DVWA.

Задание

1. Установить DVWA на дистрибутив Kali Linux.

Теоретическое введение

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

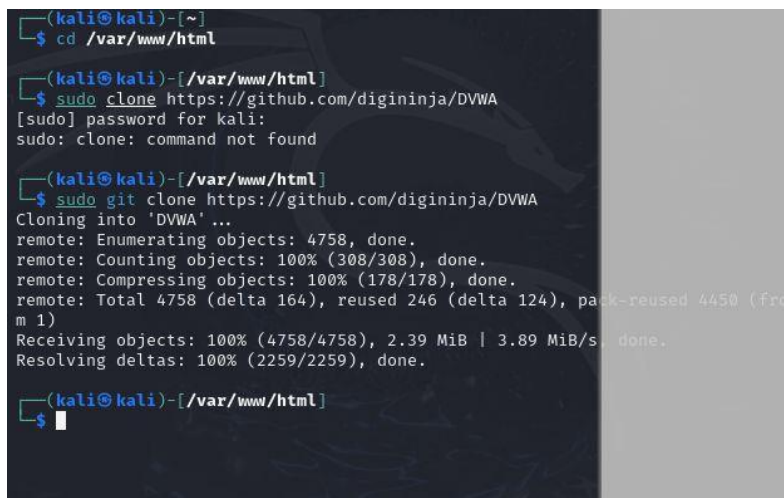
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной 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. [@guide, @parasram]

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).



```
(kali㉿kali)-[~]
$ cd /var/www/html

(kali㉿kali)-[/var/www/html]
$ sudo clone https://github.com/digininja/DVWA
[sudo] password for kali:
sudo: clone: command not found

(kali㉿kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (178/178), done.
remote: Total 4758 (delta 164), reused 246 (delta 124), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 3.89 MiB/s, done.
Resolving deltas: 100% (2259/2259), done.

(kali㉿kali)-[/var/www/html]
$
```

Клонирование репозитория

Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777 (рис. 2.)

```
(kali㉿kali)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(kali㉿kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Изменение прав доступа

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

```
(kali㉿kali)-[/var/www/html]
$ cd DVWA/config

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

Перемещение по директориям

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 (рис. 4)

```
(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

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

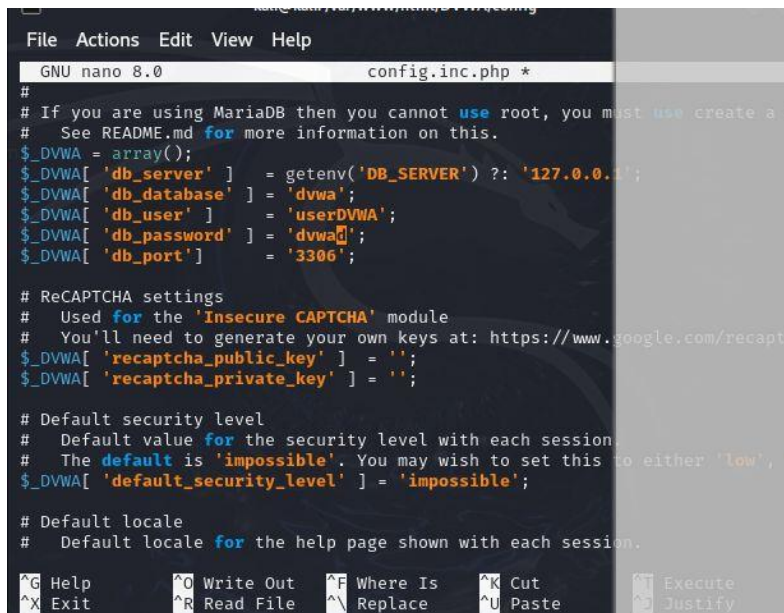
Создание копии файла

Далее открываю файл в текстовом редакторе (рис. 5)

```
(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php
```

Открытие файла в редакторе

Изменяю данные об имени пользователя и пароле (рис. 6)

A screenshot of a terminal window showing the nano text editor editing the file config.inc.php. The editor's menu bar at the top includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom shows 'GNU nano 8.0' and 'config.inc.php *'. The code content includes database configuration for DVWA, such as db_server, db_database, db_user, db_password, db_port, and security settings like default_security_level and default_locale.

```
File Actions Edit View Help
GNU nano 8.0 config.inc.php *
#
# If you are using MariaDB then you cannot use root, you must use create a
# 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';

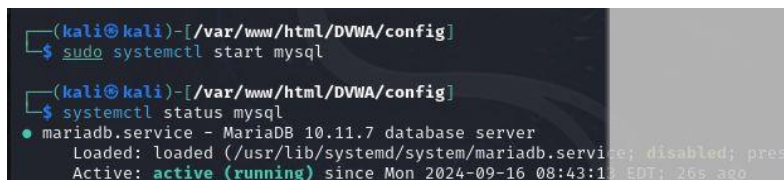
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recapt
$_DVWA['recaptcha_public_key'] = '';
$_DVWA['recaptcha_private_key'] = '';

# 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';

# Default locale
# Default locale for the help page shown with each session.
```

Редактирование файл

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

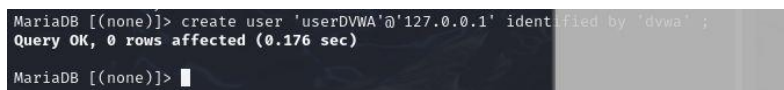
A screenshot of a terminal window showing the execution of systemctl commands to start and check the status of the MySQL service. The prompt is (kali@kali)-[/var/www/html/DVWA/config].

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

(kali@kali)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 10.11.7 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres
   Active: active (running) since Mon 2024-09-16 08:43:11 EDT; 26s ago
```

Запуск mysql

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 (рис. 8)

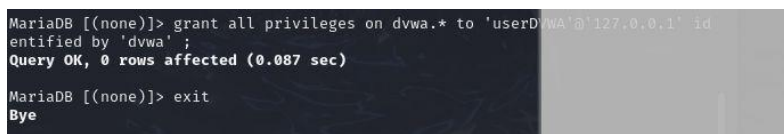
A screenshot of the MariaDB command prompt showing the creation of a new user. The prompt is MariaDB [(none)]>.

```
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by 'dvwa' ;
Query OK, 0 rows affected (0.176 sec)

MariaDB [(none)]> 
```

Авторизация в базе данных

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

A screenshot of the MariaDB command prompt showing the granting of all privileges to the userDVWA user. The prompt is MariaDB [(none)]>.

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' id
entified by 'dvwa' ;
Query OK, 0 rows affected (0.087 sec)

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

Изменение прав

Необходимо настроить сервер apache2, перехожу в соответствующую директорию (рис. 10)

```
(kali@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2
cd: no such file or directory: /etc/php/8.2/apache2
```

Перемещение между директориями

В файле php.ini нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис. 11)

```
(kali@kali)-[/var/www/html/DVWA/config]
$ sudo nano php.ini
```

Открытие файла в текстовом редакторе

В файле параметры allow_url_fopen и allow_url_include должны быть поставлены как On (рис. 12)

```
;;;;;;;;;;;;;
; 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
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default sett
; 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.

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Редактирование файла

Запускаем службу веб-сервера apache и проверяем, запущена ли служба (рис. 13)

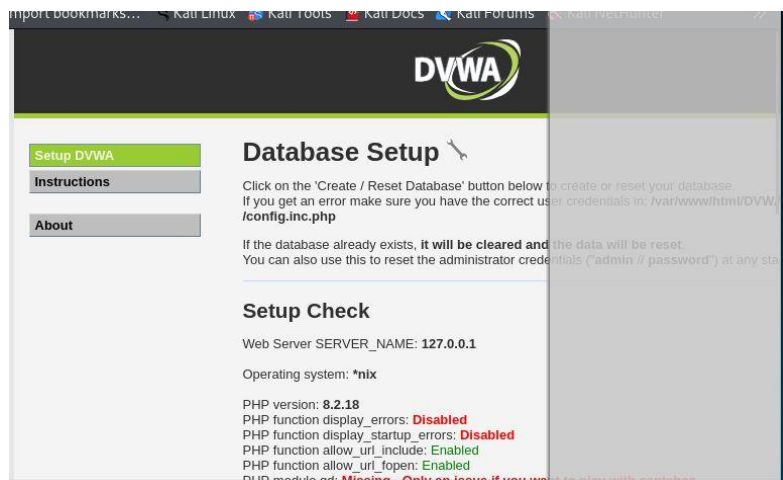
```
(kali@kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(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; pres>
   Active: active (running) since Mon 2024-09-16 08:59:57 EDT; 26s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 17055 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 17071 (apache2)
    Tasks: 6 (limit: 2272)
  Memory: 19.5M (peak: 20.0M)
     CPU: 100ms
    CGroup: /system.slice/apache2.service
            └─17071 /usr/sbin/apache2 -k start
              17074 /usr/sbin/apache2 -k start
              17075 /usr/sbin/apache2 -k start
              17076 /usr/sbin/apache2 -k start
              17077 /usr/sbin/apache2 -k start
              17078 /usr/sbin/apache2 -k start

Sep 16 08:59:57 kali systemd[1]: Starting apache2.service - The Apache HTTP >
Sep 16 08:59:57 kali apachectl[17070]: AH00558: apache2: Could not reliably >
Sep 16 08:59:57 kali systemd[1]: Started apache2.service - The Apache HTTP S>
```

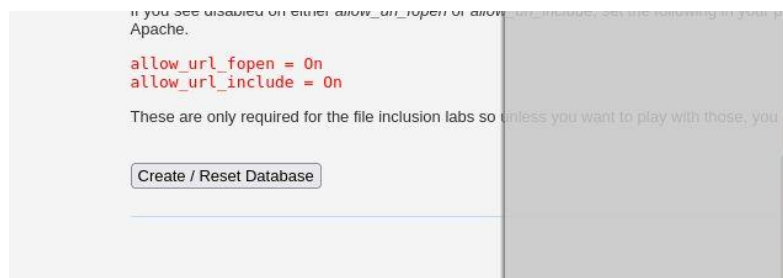
Запуск арче

Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA (рис. 14)



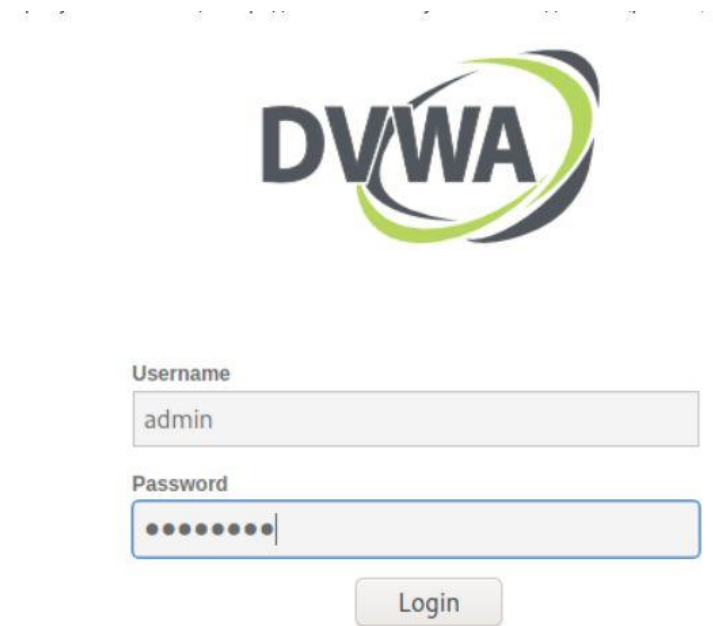
Запуск веб-приложения

Прокручиваем страницу вниз и нажимаем на кнопку create\reset database (рис. 15)



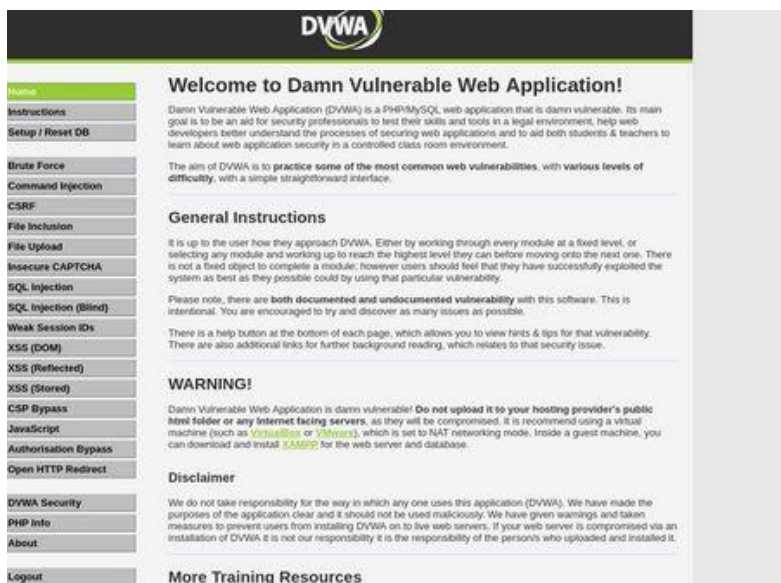
“Создание базы данных”

Авторизуюсь с помощью предложенных по умолчанию данных (рис. 16)



Авторизация

Оказываюсь на домашней странице веб-приложения, на этом установка окончена (рис. 17)



Домашняя страница DVWA

Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

Список литературы