

Шаблон отчёта по проект 2

Установка DVWA

Туем Гислен

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	16

Список иллюстраций

4.1	рис 1	10
4.2	рис 2	10
4.3	рис 3	11
4.4	рис 4	11
4.5	рис 5	12
4.6	рис 6	12
4.7	рис 7	12
4.8	рис 8	13
4.9	рис 9	13
4.10	рис 10	14
4.11	рис 11	14
4.12	рис 12	15

Список таблиц

1 Цель работы

Установить DVWA в гостевую систему к Kali Linux.

2 Задание

1. Скачать DVWA
2. Настройка DVWA
3. Настройка База данных
4. Настройка сервера Apache
5. Откройте DVWA в своем веб-браузере

3 Теоретическое введение

1. Установите DVWA в гостевую систему к Kali Linux.
2. Репозиторий: <https://github.com/digininja/DVWA>.
3. Некоторые из уязвимостей веб приложений, который содержит DVWA:

Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования

Исполнение (внедрение) команд: Выполнение команд уровня операционной системы

Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль

Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные

SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля

Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы

Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб

Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

Невозможный – этот уровень должен быть безопасным от всех уязвимостей. Он и

Высокий – это расширение среднего уровня сложности, со смесью более сложных

Средний – этот уровень безопасности предназначен главным образом для того,

Низкий – этот уровень безопасности совершенно уязвим и совсем не имеет защи

4 Выполнение лабораторной работы

1. клонировать репозиторий DVWA GitHub(рис. [4.1]).
2. назначьте разрешения на чтение, запись и выполнение (777) для папки DVWA[4.2]).
3. посмотреть содержимое каталога конфигурации и создать копию файла с именем `config.inc.php`(рис. [4.3]).
4. Теперь откройте файл `config.inc.php` в редакторе `nano`, чтобы выполнить необходимые настройки(рис. [4.4]).
5. запустить службу MySQL и проверьте, запущена ли служба(рис. [4.5]).
6. войти в базу данных(рис. [4.6]).
7. создайте нового пользователя и предоставьте этому пользователю полные права доступа к базе данных `dvwa`(рис. [4.7]).
8. запустите терминал и выполните мониторинг в каталоге `/etc/php/8.2/apache2`, а затем выполните команду `sudo nano php.ini`, найдите строки `allow_url_fopen` и `allow_url_include` и убедитесь, что для обоих установлено значение «ON»(рис. [4.8]).
9. запустите и посмотрите статус `apache2`(рис. [4.9]).
10. Запустите веб-браузер и введите URL-адрес: `127.0.0.1/DVWA`(рис. [4.10]).

11. Нажмите кнопку «Создать/сбросить базу данных» в конце страницы(рис. [4.11]).
12. После успешного входа в систему вас встретит домашняя страница DVWA.(рис. [4.12]).

```
(gtuem1@gtuemkali)-[/etc/php]
$ cd /var/www/html

(gtuem1@gtuemkali)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for gtuem1:
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), 2.27 MiB | 3.01 MiB/s, done.
Resolving deltas: 100% (2128/2128), done.

(gtuem1@gtuemkali)-[/var/www/html]
$ ls
DVWA  index.html  index.nginx-debian.html
```

Рис. 4.1: рис 1

```
(gtuem1@gtuemkali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
[sudo] password for gtuem1:

(gtuem1@gtuemkali)-[/var/www/html]
$
```

Рис. 4.2: рис 2

```

(gtuem1@gtuemkali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist

(gtuem1@gtuemkali)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(gtuem1@gtuemkali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist

```

Рис. 4.3: рис 3

```

GNU nano 7.2                                config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
# 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
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must create a database
# 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';

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

```

Рис. 4.4: рис 4

```

(gtuem1@gtuemkali)-[/var/www/html/DVWA/config]
$ systemctl start mysql

(gtuem1@gtuemkali)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 10.11.5 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: >
   Active: active (running) since Sat 2024-03-16 10:43:37 MSK; 5min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 47764 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d >
   Process: 47766 ExecStartPre=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 47768 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ]>
   Process: 47880 ExecStartPost=/bin/sh -c systemctl unset-environment _WSR>
   Process: 47882 ExecStartPost=/etc/mysql/debian-start (code=exited, statu>
  Main PID: 47837 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 8 (limit: 4597)
    Memory: 226.1M
       CPU: 5.247s
    CGroup: /system.slice/mariadb.service
            └─47837 /usr/sbin/mariabdd

Mar 16 10:43:36 gtuemkali mariabdd[47837]: 2024-03-16 10:43:36 0 [Note] Inno>
Mar 16 10:43:36 gtuemkali mariabdd[47837]: 2024-03-16 10:43:36 0 [Warning] Y>
Mar 16 10:43:36 gtuemkali mariabdd[47837]: 2024-03-16 10:43:36 0 [Note] Serv>
Mar 16 10:43:36 gtuemkali mariabdd[47837]: 2024-03-16 10:43:36 0 [Note] Inno>

```

Рис. 4.5: рис 5

```

(gtuem1@gtuemkali)-[~]
$ 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: 10.11.5-MariaDB-3 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

```

Рис. 4.6: рис 6

```

(gtuem1@gtuemkali)-[~]
$ sudo mysql -u root -p
[sudo] password for gtuem1:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.5-MariaDB-3 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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 (0.033 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' ident
ified by 'dvwa';
Query OK, 0 rows affected (0.032 sec)

MariaDB [(none)]>

```

Рис. 4.7: рис 7

```

; 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: рис 8

```

(gtuem1@gtuemkali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(gtuem1@gtuemkali)-[/etc/php/8.2/apache2]
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-03-16 11:18:43 MSK; 1min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 65507 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 65531 (apache2)
    Tasks: 6 (limit: 4597)
   Memory: 19.8M
      CPU: 630ms
   CGroup: /system.slice/apache2.service
           └─65531 /usr/sbin/apache2 -k start
             └─65534 /usr/sbin/apache2 -k start
               └─65535 /usr/sbin/apache2 -k start
                 └─65536 /usr/sbin/apache2 -k start
                   └─65537 /usr/sbin/apache2 -k start
                     └─65538 /usr/sbin/apache2 -k start

```

Рис. 4.9: рис 9

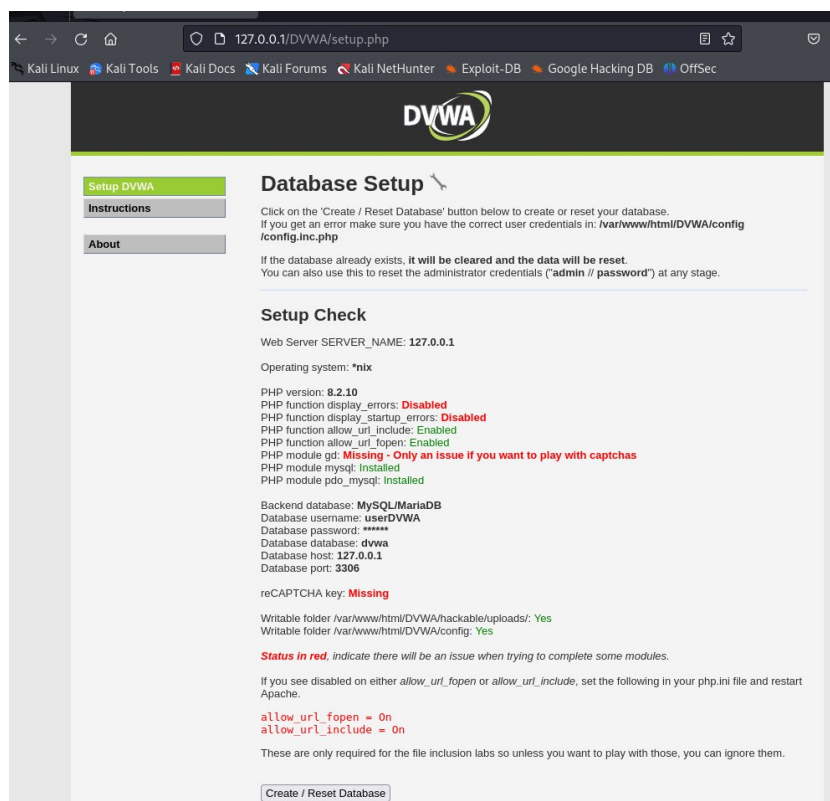


Рис. 4.10: рис 10

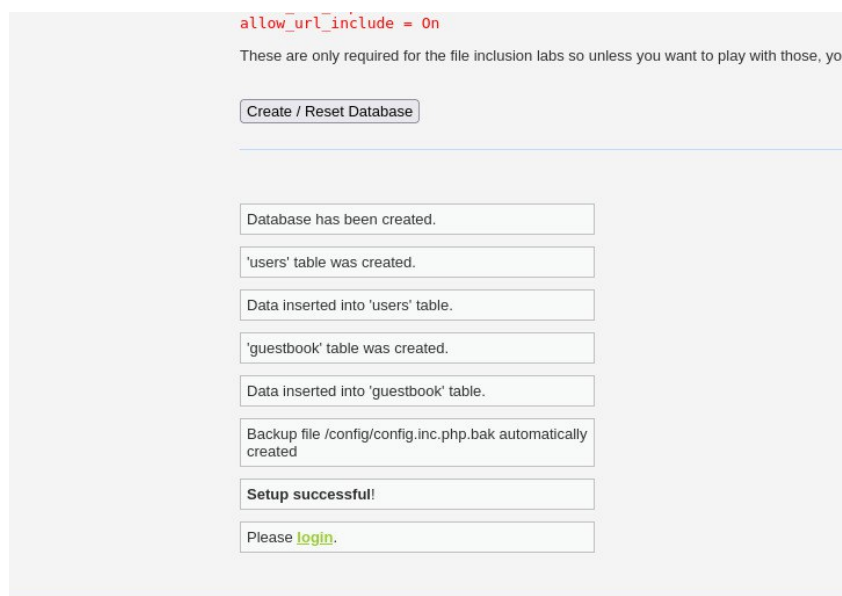


Рис. 4.11: рис 11

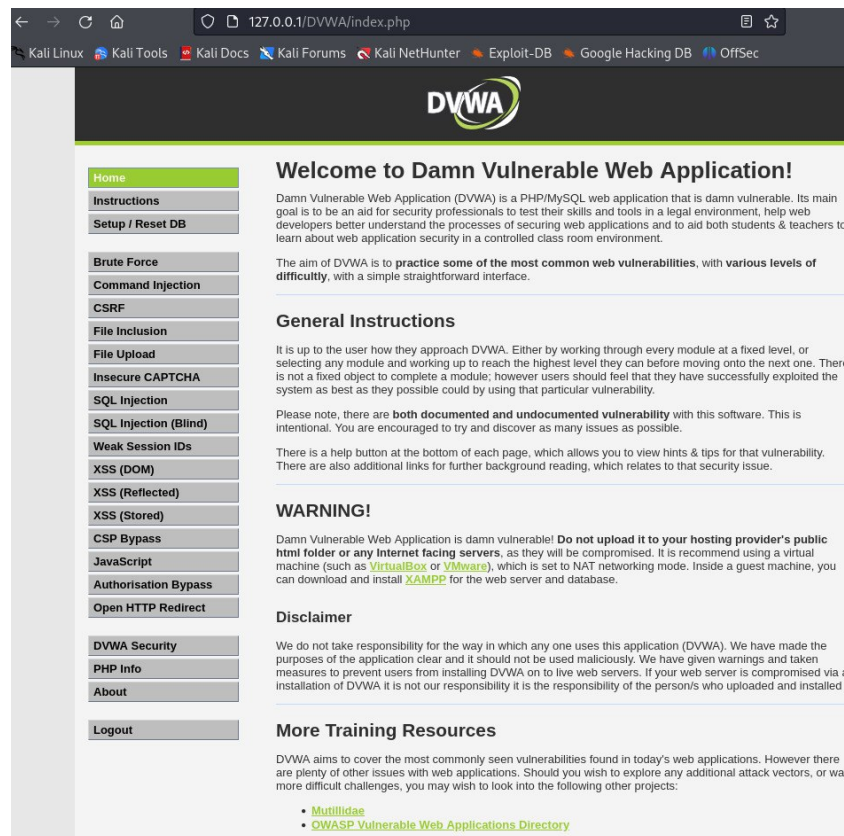


Рис. 4.12: рис 12

5 Выводы

DVWA — отличная платформа как для начинающих, так и для опытных пользователей благодаря многоуровневой поддержке безопасности. Я считаю, что этот пост дал вам подробное руководство по настройке DVWA в вашей системе Kali Linux.