

Отчёт второму этапу индивидуального проекта

Информационная безопасность

Арбатова Варвара Петровна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	16
	Список литературы	17

Список таблиц

Список иллюстраций

4.1	Клонирование репозитория	9
4.2	Добавляю права	9
4.3	Перехожу в папку	10
4.4	Копирование файла	10
4.5	Открываю файл в редакторе	10
4.6	Меняю имя пользователя и пароль	11
4.7	Запуск mysql	11
4.8	Авторизация	12
4.9	Выдаю привилегии	12
4.10	Переход в директорию	12
4.11	Открытие файла	12
4.12	Редактирование файла	13
4.13	Запуск	13
4.14	Переход на сайт	14
4.15	Кнопка	14
4.16	Вход	15

1 Цель работы

Установить DVWA в гостевую систему к Kali Linux.

2 Задание

Установите DVWA в гостевую систему к Kali Linux.

3 Теоретическое введение

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 три 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, указанный в задании к этому этапу индивидуального проекта

```
(vparbatova@vparbatova)~  
$ cd /var/www/html  
  
(vparbatova@vparbatova)-[/var/www/html]  
$ sudo git clone https://github.com/ethicalhack3r/DVWA  
[sudo] пароль для vparbatova:  
Клонирование в «DVWA» ...  
remote: Enumerating objects: 5105, done.  
remote: Counting objects: 100% (91/91), done.  
remote: Compressing objects: 100% (24/24), done.  
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)  
Получение объектов: 100% (5105/5105), 2.49 Миб | 350.00 КиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
  
(vparbatova@vparbatova)-[/var/www/html]  
$
```

Рис. 4.1: Клонирование репозитория

Проверяю, что всё правильно скопировалось и добавляю права на этот файл, чтобы у меня был полный доступ к нему

```
(vparbatova@vparbatova)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(vparbatova@vparbatova)-[/var/www/html]  
$ sudo chmod -R 777 DVWA
```

Рис. 4.2: Добавляю права

Перехожу в папку и смотрю, какие в ней файлы

```
(vparbatova@vparbatova)-[/var/www/html]
$ cd DVWA/config

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

Рис. 4.3: Перехожу в папку

Копирую файл и проверяю, как он скопировался. Делаю это для того, чтобы в случае, если что-то пойдет не так, у меня был запасной вариант

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

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

Рис. 4.4: Копирование файла

Открываю файл в текстовом редакторе

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

Рис. 4.5: Открываю файл в редакторе

Меняю информацию об имени пользователя и пароле

```

GNU nano 8.2                                config.inc.php *
# 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'] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA['recaptcha_private_key'] = getenv('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
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.

Имя файла для записи [Формат DOS]: config.inc.php
^G Справка      M-D Формат DOS      M-A Доп. в начало    M-B Резерв. копия
^C Отмена       M-M Формат Mac      M-P Доп. в конец    ^T Обзор

```

Рис. 4.6: Меняю имя пользователя и пароль

Запускаю mysql, он изначально установлен в Kali Linux, поэтому скачивать не надо и проверяю, запустился ли

```

└─$ sudo systemctl start mysql

(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
└─$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-03-20 20:12:28 MSK; 25s ago
   Invocation: a860e12aa3ef4080b8e2f9de62f2f7e
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 7578 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 7588 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 7591 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/>
   Process: 7674 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 7676 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 7652 (mariadb)
    Status: "Taking your SQL requests now..."
     Tasks: 14 (limit: 30079)
    Memory: 242.5M (peak: 247M)
       CPU: 2.148s
    CGroup: /system.slice/mariadb.service
            └─7652 /usr/sbin/mariadb

мар 20 20:12:27 vparbatova mariadb[7652]: 2025-03-20 20:12:27 0 [Note] Plugin 'FEEDBACK' is disabled
мар 20 20:12:27 vparbatova mariadb[7652]: 2025-03-20 20:12:27 0 [Note] Plugin 'wsrep-provider' is disabled
мар 20 20:12:27 vparbatova mariadb[7652]: 2025-03-20 20:12:27 0 [Note] InnoDB: Buffer pool(s) built
мар 20 20:12:27 vparbatova mariadb[7652]: 2025-03-20 20:12:27 0 [Note] Server socket created on
мар 20 20:12:28 vparbatova mariadb[7652]: 2025-03-20 20:12:28 0 [Note] mariadb: Event Scheduler
мар 20 20:12:28 vparbatova mariadb[7652]: 2025-03-20 20:12:28 0 [Note] /usr/sbin/mariadb: ready for
мар 20 20:12:28 vparbatova mariadb[7652]: Version: '11.4.3-MariaDB-1' socket: '/run/mysqld/mysq
мар 20 20:12:28 vparbatova systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.

```

Рис. 4.7: Запуск mysql

Авторизуюсь 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

```
(vparbatova@vparbatova)-[/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: 11.4.3-MariaDB-1 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 (0,028 sec)
```

Рис. 4.8: Авторизация

Выдаю пользователю все привилегии и выхожу

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0,005 sec)

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

Рис. 4.9: Выдаю привилегии

Теперь надо настроить сервер apache2, для этого перехожу в соответствующую директорию

```
(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2
```

Рис. 4.10: Переход в директорию

Открываю файл в текстовом редакторе

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

Рис. 4.11: Открытие файла

Нахожу параметры `allow_url_fopen` и `allow_url_include`. Эти параметры должны быть on

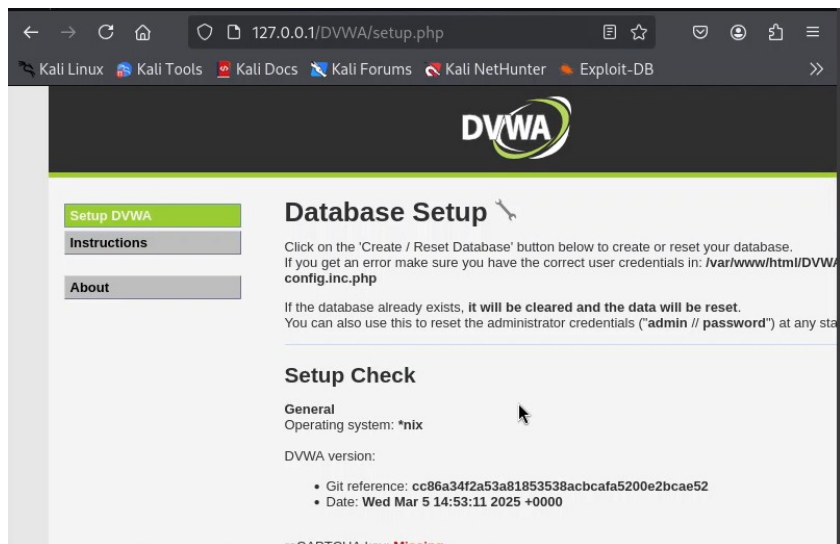


Рис. 4.14: Переход на сайт

Прокручиваем страницу вниз и нажимаем на кнопку

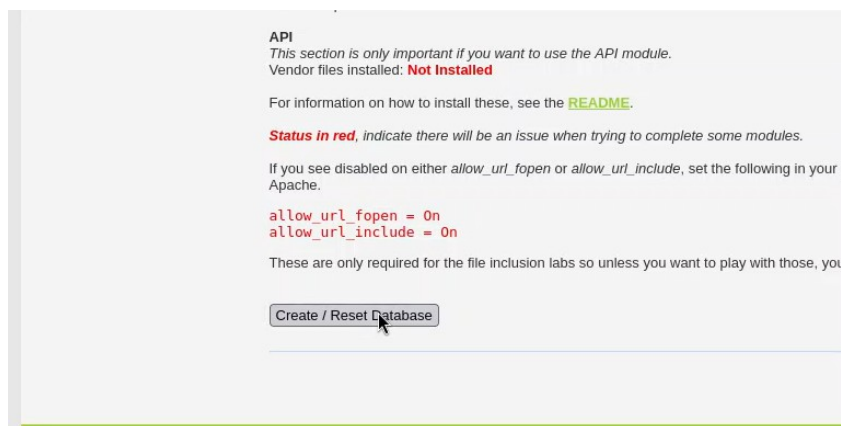
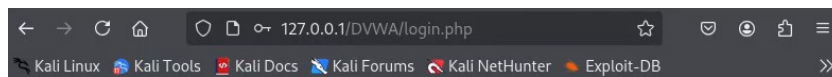


Рис. 4.15: Кнопка

Вхожу с данными, предложенными по умолчанию



Username

Password

Login

[Damn Vulnerable Web Application \(DVWA\)](#)

Рис. 4.16: Вход

5 Выводы

Установила DVWA в гостевую систему к Kali Linux.

Список литературы