

# **Индивидуальный проект этап2**

**Основы информационной безопасности**

Сабралиева Марворид Нуралиевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>14</b>
	<b>Список литературы</b>	<b>15</b>

## Список иллюстраций

4.1	Процесс установки . . . . .	9
4.2	Процесс установки . . . . .	10
4.3	Процесс установки . . . . .	10
4.4	Процесс установки . . . . .	10
4.5	Процесс установки . . . . .	11
4.6	Процесс установки . . . . .	11
4.7	Процесс установки . . . . .	12
4.8	Процесс установки . . . . .	12
4.9	Процесс установки . . . . .	13
4.10	Процесс установки . . . . .	13

## Список таблиц

# 1 Цель работы

Научиться основным способам тестирования веб приложений

## 2 Задание

Установите DVWA в гостевую систему к Kali Linux.

### 3 Теоретическое введение

Некоторые из уязвимостей веб приложений, который содержит DVWA:

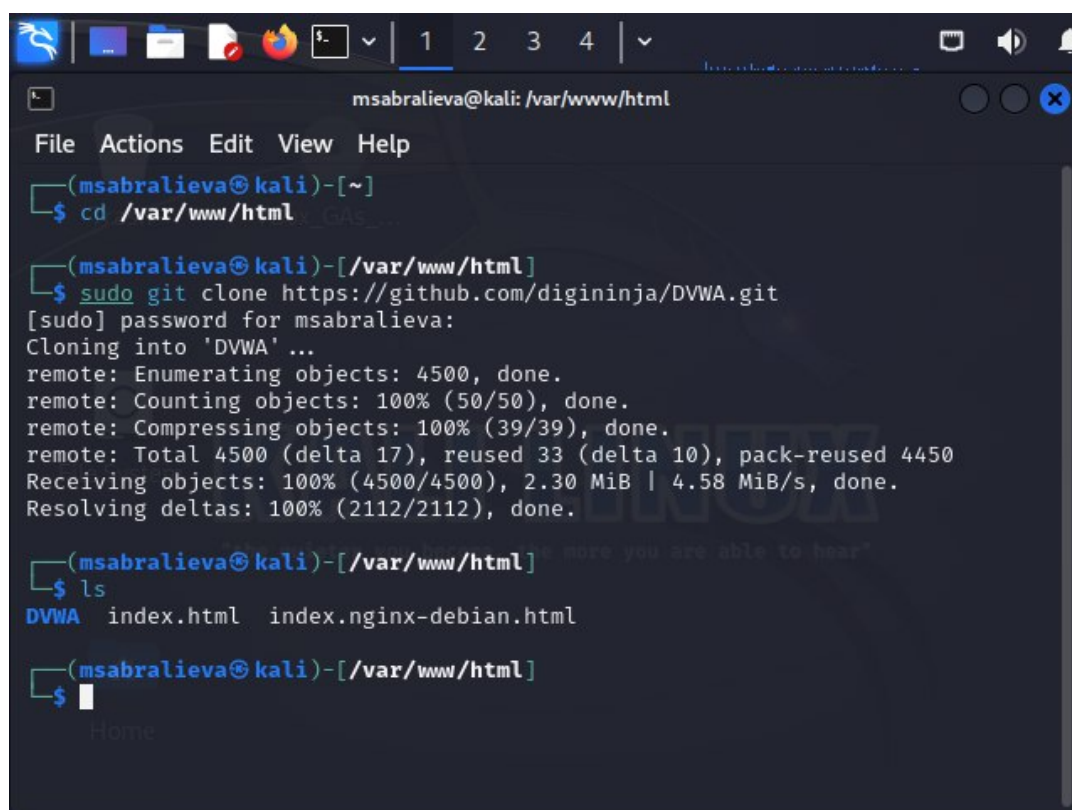
Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» 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 безопасно-

сти, 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

Установим DVWA в гостевую систему к Kali Linux с помощью клонирования из гитхаба и проведем дальнейшую установку



```
msabralieva@kali: /var/www/html
File Actions Edit View Help
(msabralieva@kali)~
$ cd /var/www/html
(msabralieva@kali)~/var/www/html
$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for msabralieva:
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), 2.30 MiB | 4.58 MiB/s, done.
Resolving deltas: 100% (2112/2112), done.
(msabralieva@kali)~/var/www/html
$ ls
DVWA  index.html  index.nginx-debian.html
(msabralieva@kali)~/var/www/html
$
```

Рис. 4.1: Процесс установки

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

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

(msabralieva@kali)-[/var/www/html]
$
```

Рис. 4.2: Процесс установки

```
(msabralieva@kali)-[/var/www/html]
$ cd DVWA

(msabralieva@kali)-[/var/www/html/DVWA]
$ ls
CHANGELOG.md  README.es.md  README.md  SECURITY.md  database  favicon.ico  login.php  robots.txt  tests
COPYING.txt  README.fa.md  README.pt.md  about.php  docs      hackable     logout.php  security.php  vulnerabilities
Dockerfile    README.fr.md  README.tr.md  compose.yml  dvwa      index.php    php.ini    security.txt  setup.php
README.ar.md  README.id.md  README.zh.md  config      external  instructions.php  phpinfo.php
```

Рис. 4.3: Процесс установки

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

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

(msabralieva@kali)-[/var/www/html/DVWA/config]
$ cp
Devices

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

(msabralieva@kali)-[/var/www/html/DVWA/config]
$ sudo mousepad config.inc.php
```

Рис. 4.4: Процесс установки

```
msabralieva@kali: /var/www/html/DVWA/config
File Actions Edit View Help
• mariadb.service - MariaDB 10.11.5 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-03-16 21:06:49 MSK; 21s ago
  Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
  Process: 12193 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
  Process: 12195 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
  Process: 12198 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR='cd /usr/bin/..; /usr/bin/galera_recovery'
  Process: 12279 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
  Process: 12282 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 12257 (mariadbd)
  Status: "Taking your SQL requests now..."
  Tasks: 14 (limit: 2259)
  Memory: 232.3M
  CPU: 1.118s
  CGroup: /system.slice/mariadb.service
          └─12257 /usr/sbin/mariadbd

Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] InnoDB: Buffer pool(s) load completed at 240316 21:06:49
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] Server socket created on IP: '127.0.0.1'.
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] /usr/sbin/mariadbd: ready for connections.
Mar 16 21:06:49 kali mariadbd[12257]: Version: '10.11.5-MariaDB-3' socket: '/run/mysql/mysql.sock' port: 3306 Debian n/a
Mar 16 21:06:49 kali systemd[1]: Started mariadb.service - MariaDB 10.11.5 database server.
Mar 16 21:06:49 kali /etc/mysql/debian-start[12284]: Upgrading MariaDB tables if necessary.
Mar 16 21:06:49 kali /etc/mysql/debian-start[12296]: Checking for insecure root accounts.
Lines 1-27
```

Рис. 4.5: Процесс установки

```
msabralieva@kali: /var/www/html/DVWA/config
File Actions Edit View Help
└─$ sudo systemctl start mysql
msabralieva@kali:~/var/www/html/DVWA/config$
└─$ sudo systemctl status mysql
• mariadb.service - MariaDB 10.11.5 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: disabled)
  Active: active (running) since Sat 2024-03-16 21:06:49 MSK; 21s ago
  Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
  Process: 12193 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
  Process: 12195 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
  Process: 12198 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR='cd /usr/bin/..; /usr/bin/galera_recovery'
  Process: 12279 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
  Process: 12282 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 12257 (mariadbd)
  Status: "Taking your SQL requests now..."
  Tasks: 14 (limit: 2259)
  Memory: 232.3M
  CPU: 1.118s
  CGroup: /system.slice/mariadb.service
          └─12257 /usr/sbin/mariadbd

Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] InnoDB: Buffer pool(s) load completed at 240316 21:06:49
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] Server socket created on IP: '127.0.0.1'.
Mar 16 21:06:49 kali mariadbd[12257]: 2024-03-16 21:06:49 0 [Note] /usr/sbin/mariadbd: ready for connections.
Mar 16 21:06:49 kali mariadbd[12257]: Version: '10.11.5-MariaDB-3' socket: '/run/mysql/mysql.sock' port: 3306 Debian n/a
```

Рис. 4.6: Процесс установки

```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
(msabralieva@kali)-[/var/www/html/DVWA/config]
└─$ sudo su
(root@kali)-[/var/www/html/DVWA/config]
└─$ 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)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'admin'@'127.0.0.1';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye
(root@kali)-[/var/www/html/DVWA/config]
```

Рис. 4.7: Процесс установки

```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
(root@kali)-[/var/www/html/DVWA/config]
└─$ systemctl start apache2
(root@kali)-[/var/www/html/DVWA/config]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-03-16 21:17:45 MSK; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 17827 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 17845 (apache2)
       Tasks: 6 (limit: 2259)
      Memory: 19.8M
         CPU: 95ms
    CGroup: /system.slice/apache2.service
           └─17845 /usr/sbin/apache2 -k start
             17848 /usr/sbin/apache2 -k start
             17849 /usr/sbin/apache2 -k start
             17850 /usr/sbin/apache2 -k start
             17851 /usr/sbin/apache2 -k start
             17852 /usr/sbin/apache2 -k start

Mar 16 21:17:45 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 16 21:17:45 kali apachectl[17842]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 1>
Mar 16 21:17:45 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

Рис. 4.8: Процесс установки

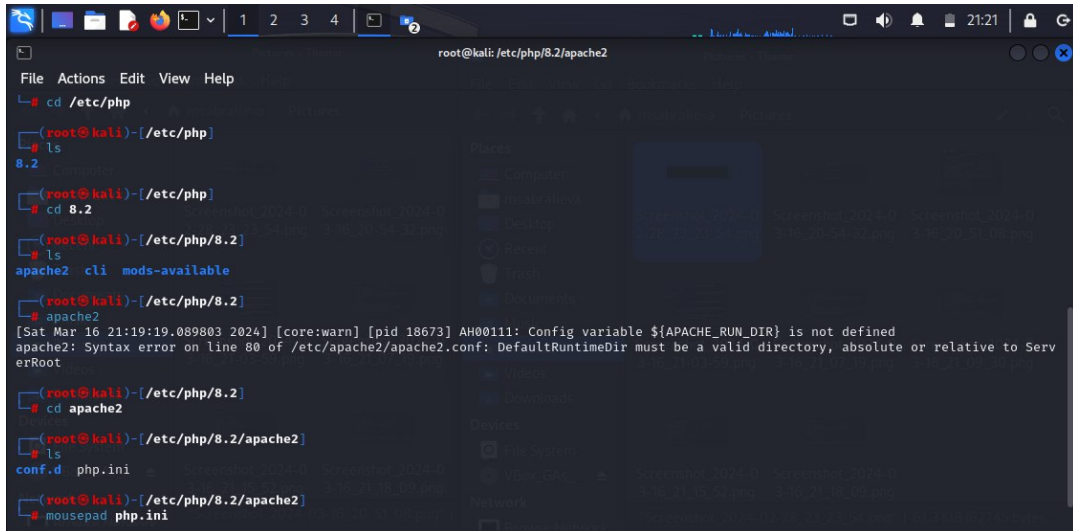


Рис. 4.9: Процесс установки

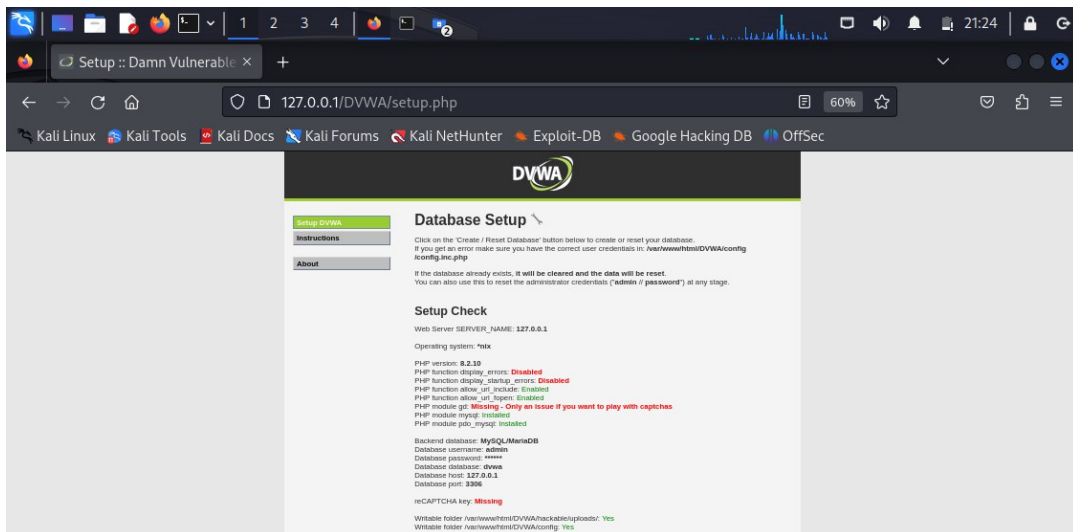


Рис. 4.10: Процесс установки

## 5 Выводы

В ходе выполнения данного этапа мы установили DVWA в гостевую систему к Kali Linux

## **Список литературы**