

Отчёт по выполнению 2-ого этапа индивидуального проекта

Дисциплина: Основы информационной безопасности

Зинченко Анастасия Романовна

Содержание

Цель работы	1
Задание	1
Выполнение 2-ого этапа индивидуального проекта.....	1
Загрузка DVWA	1
Настройка DVWA	2
Настройка базы данных.....	4
Настройка сервера Apache.....	5
Открытие DVWA в веб-браузере.....	6
Выводы.....	8
Список литературы.....	8

Цель работы

Приобретение практических навыков по установке DVWA.

Задание

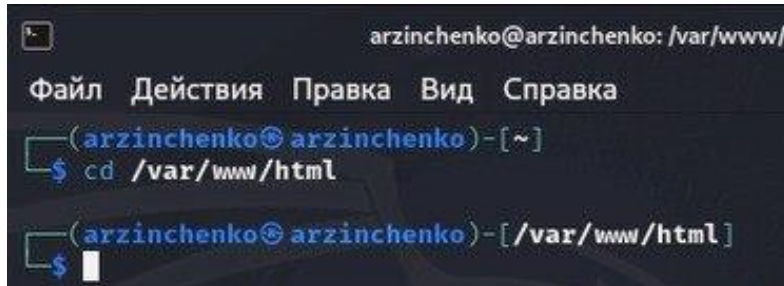
1. Установить DVWA в гостевую систему Kali Linux.

Выполнение 2-ого этапа индивидуального проекта

Загрузка DVWA

DVWA (Damn Vulnerable Web Application) - это веб приложение на PHP/MySQL, которое “чёртовски уязвимо”. Его главная цель - помочь профессионалам или новичкам протестировать их навыки в сфере информационной безопасности. На сайте <https://nooblinux.com/how-to-install-dvwa/> очень хорошо и подробно описано как устанавливать и настраивать DVWA в гостевой системе Kali Linux. Поскольку мы

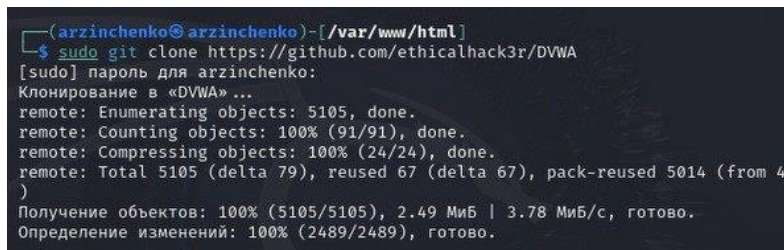
будем настраивать DVWA на нашем локальном хосте, запустим терминал и перейдём в `/var/www/html`: `cd /var/www/html`. Это место, где хранятся файлы локального хоста (рис. [-@fig:001])



```
arzinchenko@arzinchenko: /var/www/html
Файл Действия Правка Вид Справка
(arzinchenko@arzinchenko)-[~]
$ cd /var/www/html
(arzinchenko@arzinchenko)-[/var/www/html]
$
```

Переход в каталог `/var/www/html`

Далее склонируем репозиторий <https://github.com/digininja/DVWA> в каталог `/html` с помощью команды: `sudo git clone https://github.com/digininja/DVWA` (рис. [-@fig:002])

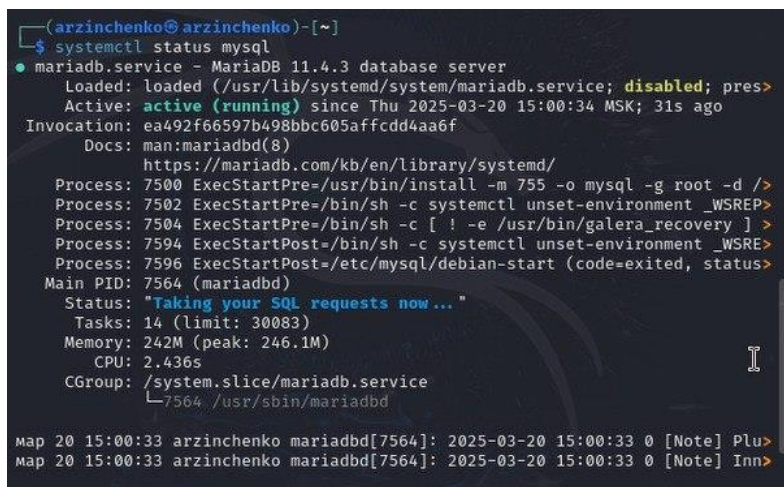


```
(arzinchenko@arzinchenko)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] пароль для arzinchenko:
Клонирование в «DVWA» ...
remote: Enumerating objects: 5105, done.
remote: Counting objects: 100% (91/91), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)
Получение объектов: 100% (5105/5105), 2.49 МиБ | 3.78 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.
```

Клонирование репозитория DVWA

Настройка DVWA

После успешного клонирования репозитория выполним команду `ls`, чтобы проверить успешное клонирование DVWA (рис. [-@fig:003])



```
(arzinchenko@arzinchenko)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Thu 2025-03-20 15:00:34 MSK; 31s ago
  Invocation: ea492f66597b498bbc605affcdd4aa6f
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 7500 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d />
   Process: 7502 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP>
   Process: 7504 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] >
   Process: 7594 ExecStartPost=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 7596 ExecStartPost=/etc/mysql/debian-start (code=exited, status>
  Main PID: 7564 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 14 (limit: 30083)
  Memory: 242M (peak: 246.1M)
       CPU: 2.436s
   CGroup: /system.slice/mariadb.service
           └─7564 /usr/sbin/mariabdd

мар 20 15:00:33 arzinchenko mariabdd[7564]: 2025-03-20 15:00:33 0 [Note] Plu>
мар 20 15:00:33 arzinchenko mariabdd[7564]: 2025-03-20 15:00:33 0 [Note] Inn>
```

Проверка успешного клонирования

Теперь назначим разрешения Read, Write и Execute (777) для папки DVWA. Для этого выполним команду `sudo chmod -R 777 DVWA` (рис. [-@fig:004])

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

Разрешения для папки DVWA

Для настройки и конфигурации DVWA перейдём в каталог DVWA/config: `cd DVWA/config`. И посмотрим содержимое этого каталога (рис. [-@fig:005])

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

Переход в каталог DVWA/config и его содержимое

Мы видим файл с именем `config.inc.php.dist`. Этот файл содержит конфигурации DVWA по умолчанию. Не будем его трогать, и он будет нашей резервной копией, если дела пойдут не так. Вместо этого создадим копию этого файла с именем `config.inc.php`, которое будем использовать для настройки DVWA: `sudo cp config.inc.php.dist config.inc.php` (рис. [-@fig:006])

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

Создание копии файла `config.inc.php.dist`

Теперь откроем `config.inc.php` файл в nano редакторе, чтобы выполнить необходимые настройки. Прокрутим вниз до точки, где мы увидим параметры, такие как `db_database`, `db_user`, `db_password` и т. д. Поменяем эти значения как нам удобно (рис. [-@fig:007]), (рис. [-@fig:008])

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

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

Открытие файла `config.inc.php`

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

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

Редактирование файла *config.inc.php*

Настройка базы данных

По умолчанию Kali Linux поставляется с установленной системой управления реляционной базой данных MariaDB. Поэтому нам не нужно устанавливать никаких пакетов. Сначала запустим службу *mysql*: *sudo systemctl start mysql* (рис. [-@fig:009])

```
GNU nano 8.2      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 @diginiinja for the fix.

# Database management system to use
$dbms = getenv('DBMS') ?: 'MySQL';
#$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 use create a db
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server']   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA['db_user']     = getenv('DB_USER') ?: 'userDVWA';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'dvwa';
$_DVWA['db_port']     = getenv('DB_PORT') ?: '3306';
```

Запуск службы *mysql*

Проверим запущена ли служба: *systemctl status mysql* (рис. [-@fig:010])

```
(arzinchenko@arzinchenko)-[~]
$ sudo systemctl start mysql
```

Проверка статуса службы *mysql*

Для входа в базу данных используем команду *sudo mysql -u root -p*. В нашем случае мы используем *root*, так как это имя суперпользователя, установленное в нашей системе. Появляется командная строка с приглашением “MariaDB”, далее создадим в ней нового пользователя, используя учетные данные из файла *config.inc.php* с помощью команды *create user 'userDVWA'@'127.0.0.1' identified by 'dvwa'* (рис. [-@fig:011])


```
(arzinchenko@arzinchenko)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Thu 2025-03-20 15:00:34 MSK; 31s ago
   Invocation: ea492f66597b498bbc605affcdd4aa6f
   Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
   Process: 7500 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d />
   Process: 7502 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP>
   Process: 7504 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] >
   Process: 7594 ExecStartPost=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 7596 ExecStartPost=/etc/mysql/debian-start (code=exited, status>
```

Создание нового пользователя

Теперь нам нужно предоставить этому пользователю полную привилегию над dvwaбазой данных. Выполним команду *grant all privileges on dvwa. to 'userDVWA'@'127.0.0.1' identified by "dvwa"* (рис. [-@fig:012])

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

Предоставление пользователю полных привилегий над dvwa

Настройка сервера Apache

Веб-сервер Apache установлен по умолчанию в Kali Linux. Поэтому нам не нужно устанавливать никаких дополнительных пакетов. Чтобы приступить к настройке Apache2, запустив терминал и перейдём в /etc/php/8.2/apache2 (рис. [-@fig:013])

```
(arzinchenko@arzinchenko)-[~]
$ cd /etc/php/8.2/apache2
```

Переход в каталог /etc/php/8.2/apache2

Далее откроем файл php.ini и найдём строки allow_url_fopen и allow_url_include. Они должны обе иметь значение On (рис. [-@fig:014]), (рис. [-@fig:015])

```
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0,004 sec)
```

Открытие файла php.ini

```
(arzinchenko@arzinchenko)-[~]
$ 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/ser
ver
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.
```

Редактирование файла php.ini

Далее запустим службу веб-сервера apache с помощью `sudo systemctl start apache2` (рис. [-@fig:016])

```
;;;;;;;;;;  
; 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
```

Запуск службы apache

В проверим запущена ли служба: `systemctl status apache` (рис. [-@fig:017])

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

Проверка статуса службы apache

Открытие DVWA в веб-браузере

К этому моменту мы настроили DVWA, базу данных и веб-сервер Apache. Теперь мы можем приступить к запуску приложения DVWA. Запустите веб-браузер и перейдём на страницу `http://127.0.0.1/DVWA/setup.php` (рис. [-@fig:018])



Запуск веб-приложения

Прокрутив страницу вниз, нажмём кнопку «Создать/сбросить базу данных» в конце страницы (рис. [-@fig:019])

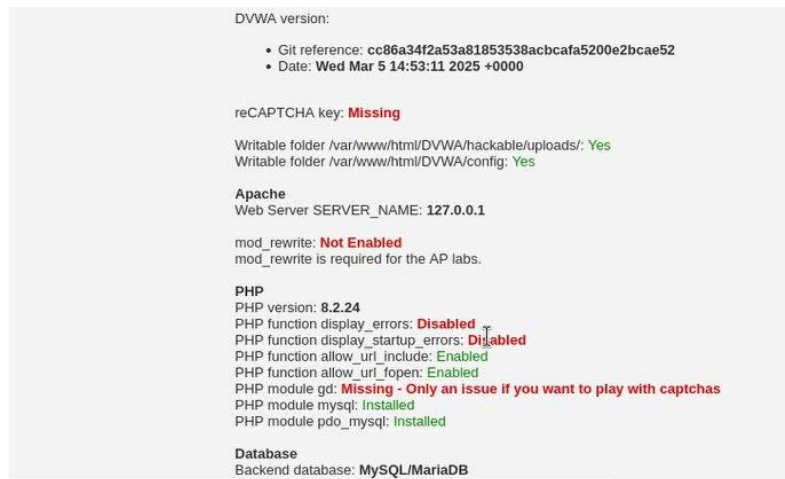


Создание базы данных

Это создаст и настроит базу данных DVWA. Через несколько секунд мы будем перенаправлены на страницу входа в DVWA. Для входа используем учетные данные по умолчанию:

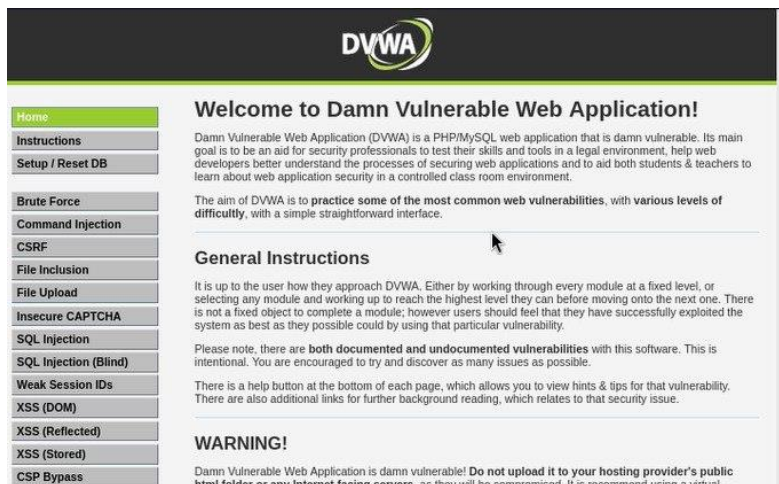
- Имя пользователя: admin
- Пароль: password

(рис. [-@fig:020])



Авторизация

После успешного входа в систему мы окажемся на домашней странице DVWA (рис. [-@fig:021])



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing servers, as they will be compromised. It is recommend using a virtual

Домашняя страница DVWA

Выводы

В ходе выполнения 2-ого этапа индивидуального проекта мы установили DVWA в гостевую систему Kali Linux

Список литературы

1. Этапы реализации проекта [Электронный ресурс] URL: <https://esystem.rudn.ru/mod/page/view.php?id=1220336>
2. Репозиторий DVWA [Электронный ресурс] URL: <https://github.com/digininja/DVWA>