

Отчёт по этапу №2 индивидуального проекта

Основы информационной безопасности

Мурашов И. В., НКАбд-03-23

22 марта 2025

Российский университет дружбы народов, Москва, Россия

- Мурашов Иван Вячеславович
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132236018@rudn.ru
- <https://neve7mind.github.io>

Приобретение практических навыков по установке DVWA.

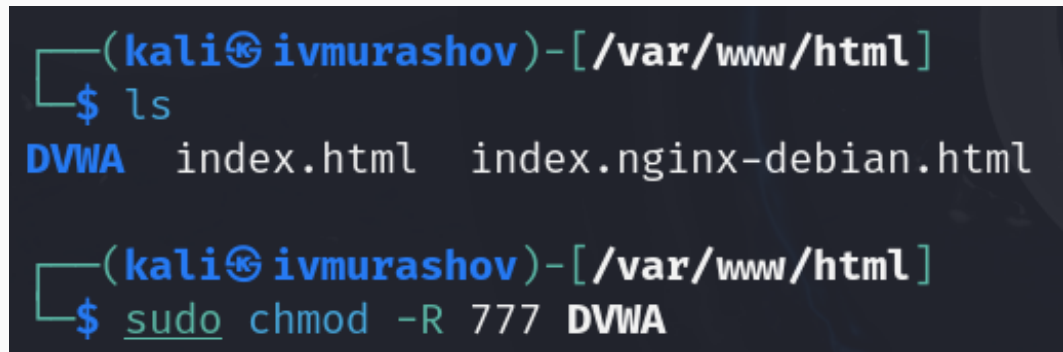
Выполнение лабораторной работы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).

```
(kali@ivmurashov)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for kali:
Cloning into '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)
Receiving objects: 100% (5105/5105), 2.49 MiB | 3.70 MiB/s, done.
Resolving deltas: 100% (2489/2489), done.
```

Выполнение лабораторной работы

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

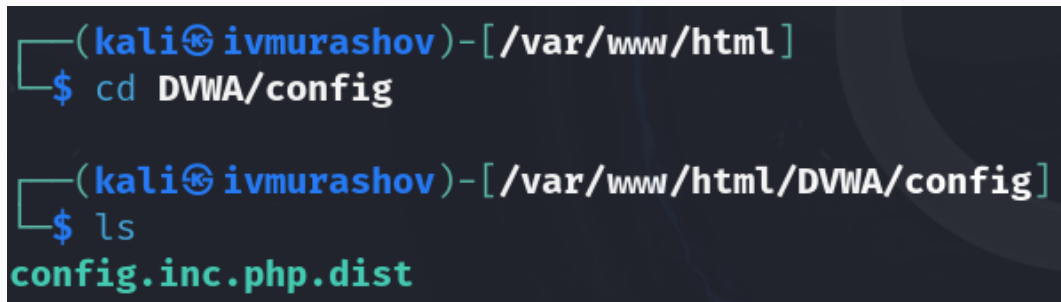
A terminal window with a dark background. The prompt is '(kali@ivmurashov)-[/var/www/html]'. The user enters '\$ ls' and the output is 'DVWA index.html index.nginx-debian.html'. Then the user enters '\$ sudo chmod -R 777 DVWA'.

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

Рис. 2: Изменение прав доступа

Выполнение лабораторной работы

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

A terminal window with a dark background and light blue/green text. The prompt is `(kali@ivmurashov) - [/var/www/html]`. The first command is `$ cd DVWA/config`. The second prompt is `(kali@ivmurashov) - [/var/www/html/DVWA/config]`. The second command is `$ ls`. The output is `config.inc.php.dist` in green text.

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

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

Рис. 3: Перемещение по директориям

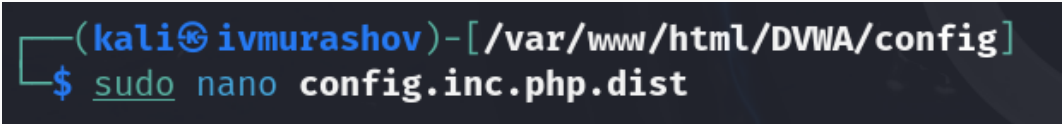
Выполнение лабораторной работы

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@ivmurashov)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php
[sudo] password for kali:

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

Далее открываю файл в текстовом редакторе (рис. 5)

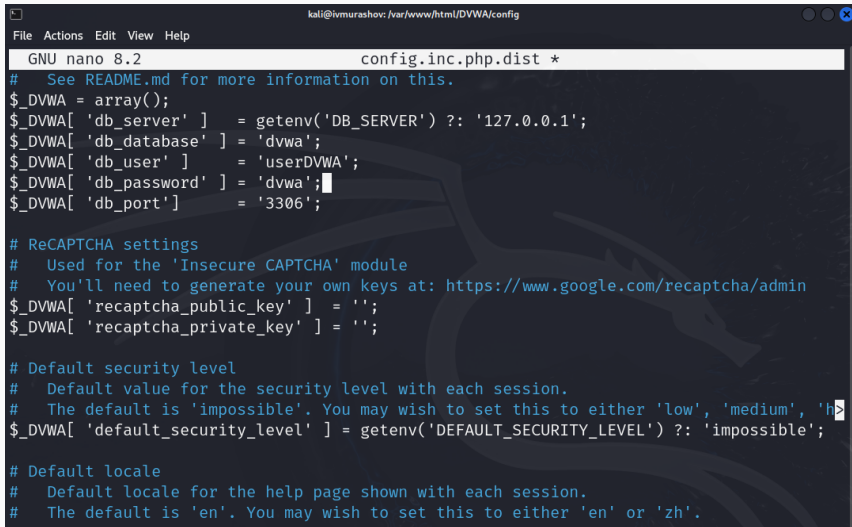
A terminal window with a dark background. The prompt is '(kali@ivmurashov)-[/var/www/html/DVWA/config]'. Below the prompt, the command '\$ sudo nano config.inc.php.dist' is entered. The word 'sudo' is underlined in green, and 'nano' is in blue. The file path 'config.inc.php.dist' is in white.

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

Рис. 5: Открытие файла в редакторе

Выполнение лабораторной работы

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



```
kali@ivmurashov: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.2 config.inc.php.dist *
# 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' ] = '';
$_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', 'medium', 'h
$_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'.
```

Выполнение лабораторной работы

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

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

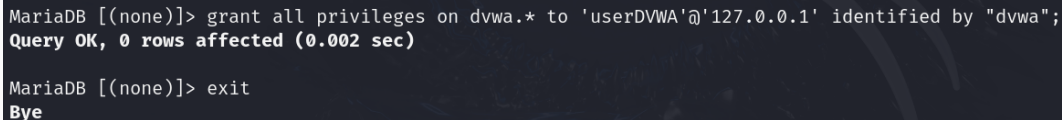
(kali@ivmurashov)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disable>
   Active: active (running) since Sat 2025-03-22 19:03:56 MSK; 12s ago
   Invocation: acdccb820f414437a01aa225382aa950
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 6246 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mys>
   Process: 6248 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSI>
   Process: 6251 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || >
   Process: 6332 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POS>
   Process: 6335 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 6310 (mariabdd)
   Status: "Taking your SQL requests now..."
   Tasks: 14 (limit: 38008)
   Memory: 242.1M (peak: 247.1M)
   CPU: 1.312s
   CGroup: /system.slice/mariadb.service
```

Выполнение лабораторной работы

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)

```
(kali@ivmurashov)-[~]  
$ sudo mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 32  
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 (0.004 sec)
```

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

A screenshot of a terminal window with a dark background. The text is white and shows a MariaDB command prompt. The first line shows the command 'grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by "dvwa";' followed by the response 'Query OK, 0 rows affected (0.002 sec)'. The second line shows the command 'exit' followed by the response 'Bye'.

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by "dvwa";  
Query OK, 0 rows affected (0.002 sec)  
  
MariaDB [(none)]> exit  
Bye
```

Рис. 9: Изменение прав

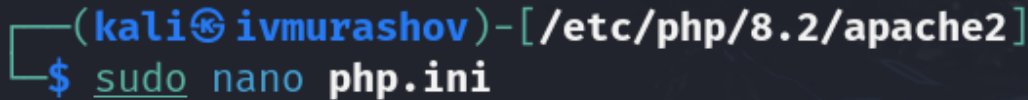
Выполнение лабораторной работы

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

```
(kali@ivmurashov)~  
$ cd /etc/php/  
  
(kali@ivmurashov)/etc/php  
$ ls  
8.2  
  
(kali@ivmurashov)/etc/php  
$ cd 8.2
```

Выполнение лабораторной работы

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

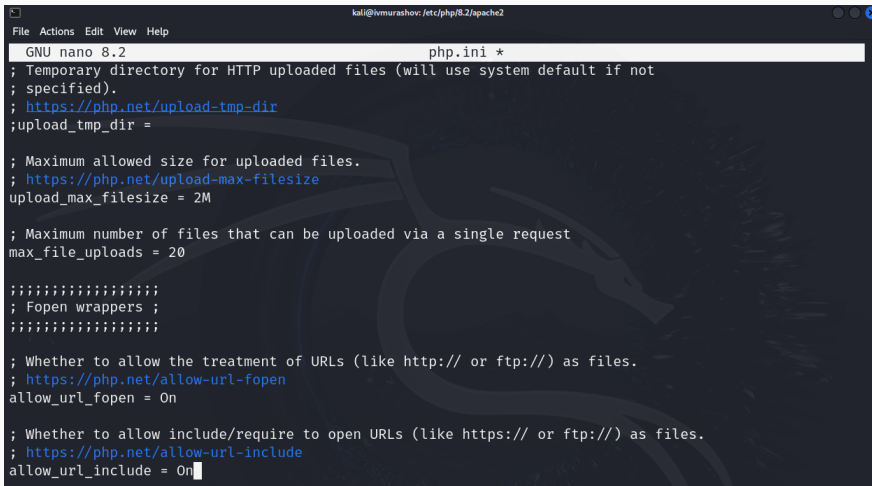
A terminal window with a dark background. The prompt is `(kali@ivmurashov) - [/etc/php/8.2/apache2]`. Below the prompt, the command `$ sudo nano php.ini` is entered. The word `sudo` is underlined, and `php.ini` is in bold.

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

Рис. 11: Открытие файла в текстовом редакторе

Выполнение лабораторной работы

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



```
kali@ivmurashov: /etc/php/8.2/apache2
File Actions Edit View Help
GNU nano 8.2                                php.ini *
; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

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

Выполнение лабораторной работы

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

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

(kali@ivmurashov)-[/etc/php/8.2/apache2]
$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2025-03-22 19:14:54 MSK; 10s ago
 Invocation: 9b9735dc0bd44a08a8564a5dd9541666
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 12041 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 12057 (apache2)
    Tasks: 6 (limit: 5758)
  Memory: 20.2M (peak: 20.9M)
     CPU: 81ms
   CGroup: /system.slice/apache2.service
           └─12057 /usr/sbin/apache2 -k start
             └─12060 /usr/sbin/apache2 -k start
               └─12061 /usr/sbin/apache2 -k start
                 └─12062 /usr/sbin/apache2 -k start
                   └─12063 /usr/sbin/apache2 -k start
                     └─12064 /usr/sbin/apache2 -k start
```


Выполнение лабораторной работы

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

API

This section is only important if you want to use the API module.

Vendor files installed: **Not Installed**

For information on how to install these, see the [README](#).

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.


```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Выполнение лабораторной работы

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



The logo for DVWA (Damn Vulnerable Web Application) is centered at the top. It features the letters "DVWA" in a bold, dark grey sans-serif font. To the right of the text is a stylized circular graphic composed of two curved, overlapping bands, one in a light green color and the other in a dark grey color.

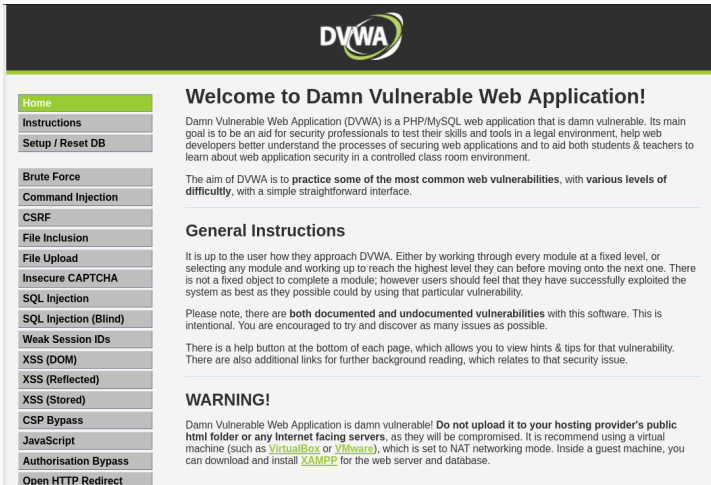
Username

Password

Login

Выполнение лабораторной работы

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



DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

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 machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Приобретены практические навыки по установке уязвимого веб-приложения DVWA.