Структура научной презентации

Простейший шаблон

Машков И. Е.

08 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

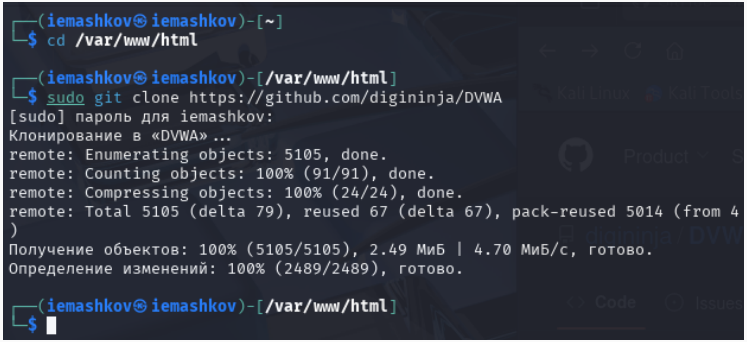
Докладчик

- Машков Илья Евгеньевич
- Студент 2-го курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- https://github.com/7S7eVe7N7

Цель работы

Приобретение практических навыков по установке DVWA.

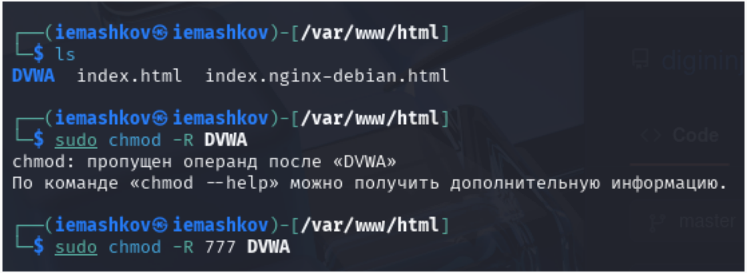
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[~]
└─$ cd /var/www/html

┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA
[sudo] пароль для iemashkov:
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 | 4.70 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.

┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ █
```

Рис. 1: Клонирование репозитория

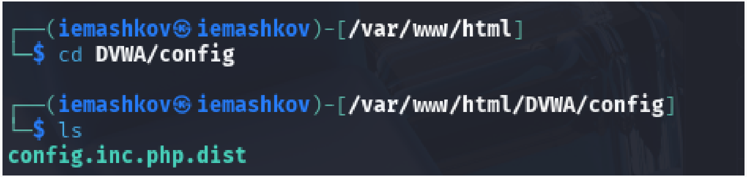
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ ls
DVWA  index.html  index.nginx-debian.html

┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ sudo chmod -R DVWA
chmod: пропущен операнд после «DVWA»
По команде «chmod --help» можно получить дополнительную информацию.

┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA
```

Рис. 2: Изменение прав доступа

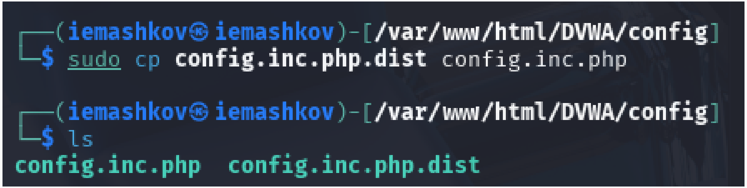
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/var/www/html]
└─$ cd DVWA/config

┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist
```

Рис. 3: Перемещение по директориям

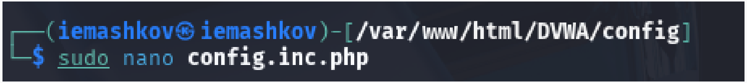
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config.inc.php

┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php  config.inc.php.dist
```

Рис. 4: Создание копии файла

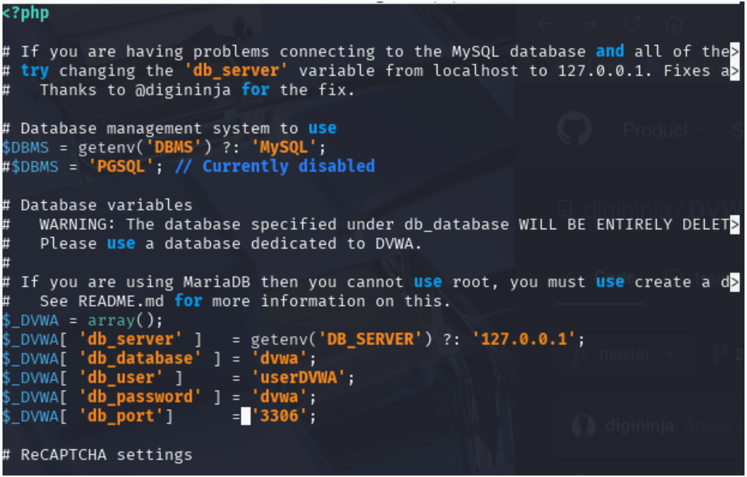
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ sudo nano config.inc.php
```

Рис. 5: Открытие файла в редакторе

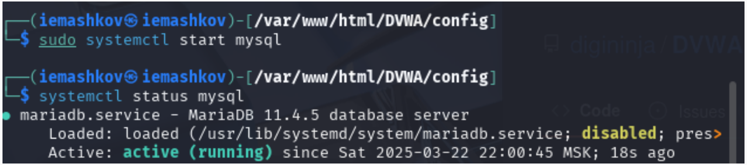
Выполнение лабораторной работы



```
<?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
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELET>
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a d>
#   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
```

Рис. 6: Редактирование файл

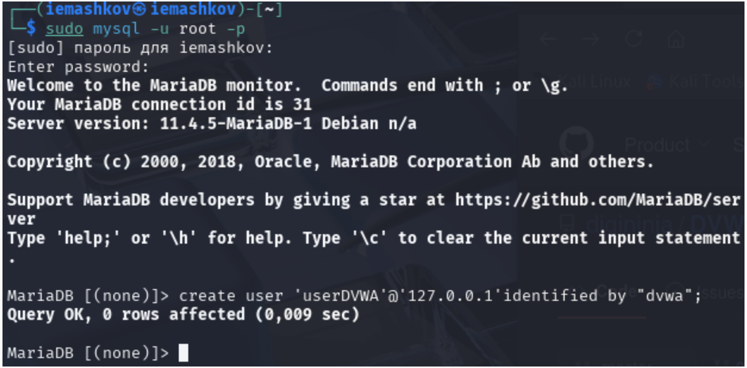
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ sudo systemctl start mysql

┌──(iemashkov㉿iemashkov)-[/var/www/html/DVWA/config]
└─$ systemctl status mysql
● mariadb.service - MariaDB 11.4.5 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
     Active: active (running) since Sat 2025-03-22 22:00:45 MSK; 18s ago
```

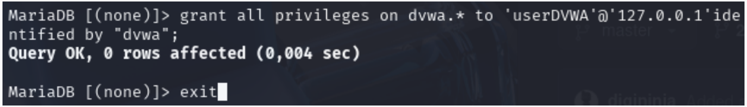
Рис. 7: Запуск mysql

Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[~]
└─$ sudo mysql -u root -p
[sudo] пароль для iemashkov:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.5-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
.

MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1'identified by "dvwa";
Query OK, 0 rows affected (0,009 sec)

MariaDB [(none)]> 
```

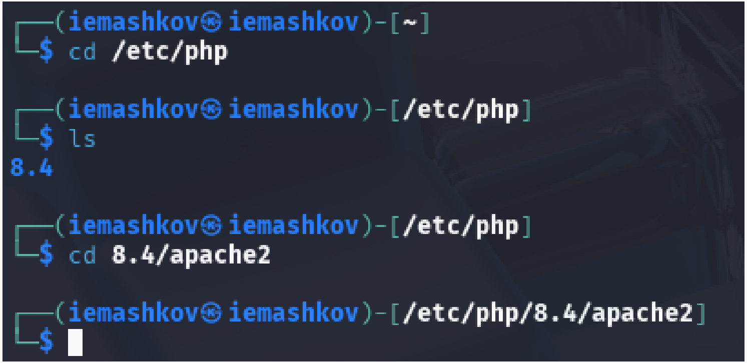
Рис. 8: Авторизация в базе данных



```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1'ide
ntified by "dvwa";
Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> exit
```

Рис. 9: Изменение прав

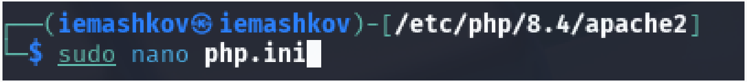
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[~]
└─$ cd /etc/php

┌──(iemashkov㉿iemashkov)-[/etc/php]
└─$ ls
8.4

┌──(iemashkov㉿iemashkov)-[/etc/php]
└─$ cd 8.4/apache2

┌──(iemashkov㉿iemashkov)-[/etc/php/8.4/apache2]
└─$ 
```

Рис. 10: Перемещение между директориями

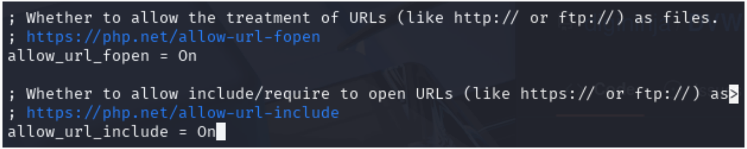
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/etc/php/8.4/apache2]
└─$ sudo nano php.ini
```

Рис. 11: Открытие файла в текстовом редакторе

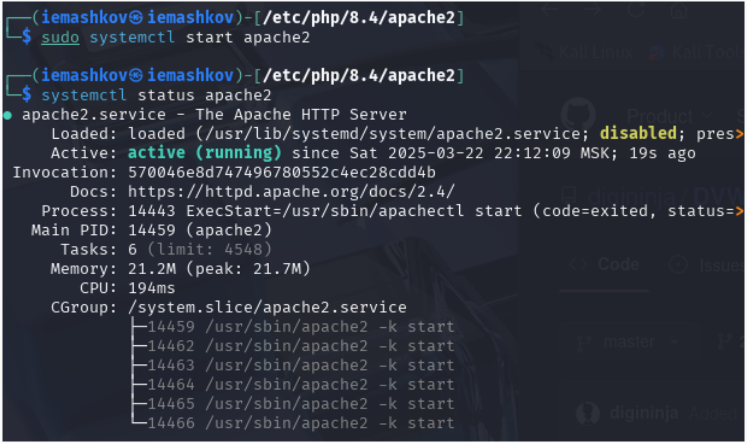
Выполнение лабораторной работы



```
; 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
```

Рис. 12: Редактирование файла

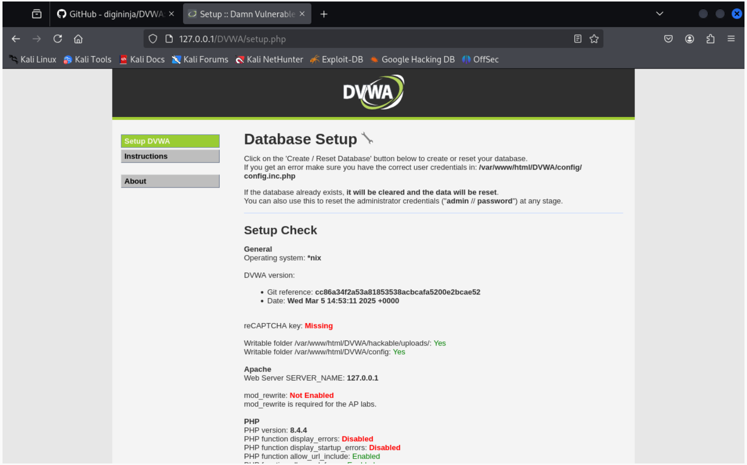
Выполнение лабораторной работы



```
┌──(iemashkov㉿iemashkov)-[/etc/php/8.4/apache2]
└─$ sudo systemctl start apache2

┌──(iemashkov㉿iemashkov)-[/etc/php/8.4/apache2]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pres>
     Active: active (running) since Sat 2025-03-22 22:12:09 MSK; 19s ago
 Invocation: 570046e8d747496780552c4ec28cdd4b
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 14443 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 14459 (apache2)
      Tasks: 6 (limit: 4548)
     Memory: 21.2M (peak: 21.7M)
        CPU: 194ms
     CGroup: /system.slice/apache2.service
             ├─14459 /usr/sbin/apache2 -k start
             ├─14462 /usr/sbin/apache2 -k start
             ├─14463 /usr/sbin/apache2 -k start
             ├─14464 /usr/sbin/apache2 -k start
             ├─14465 /usr/sbin/apache2 -k start
             └─14466 /usr/sbin/apache2 -k start
```

Рис. 13: Запуск apche

Выполнение лабораторной работы



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

General
Operating system: ***nix**

DVWA version:

- Git reference: **cc86a34f2a53a81853538acbcafa5200e2bcae52**
- Date: **Wed Mar 5 14:53:11 2025 +0000**

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

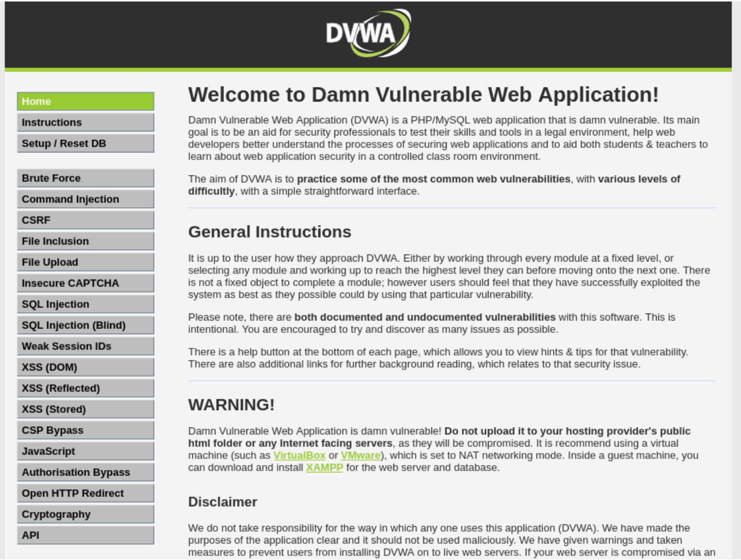
Apache
Web Server SERVER_NAME: **127.0.0.1**

mod_rewrite: **Not Enabled**
mod_rewrite is required for the AP labs.

PHP
PHP version: **8.4.4**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled

Рис. 14: Запуск веб-приложения

Выполнение лабораторной работы



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 difficultly**, 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.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an

Выводы

Приобрёл практические навыки по установке уязвимого веб-приложения DVWA.