

Отчет по второму этапу проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

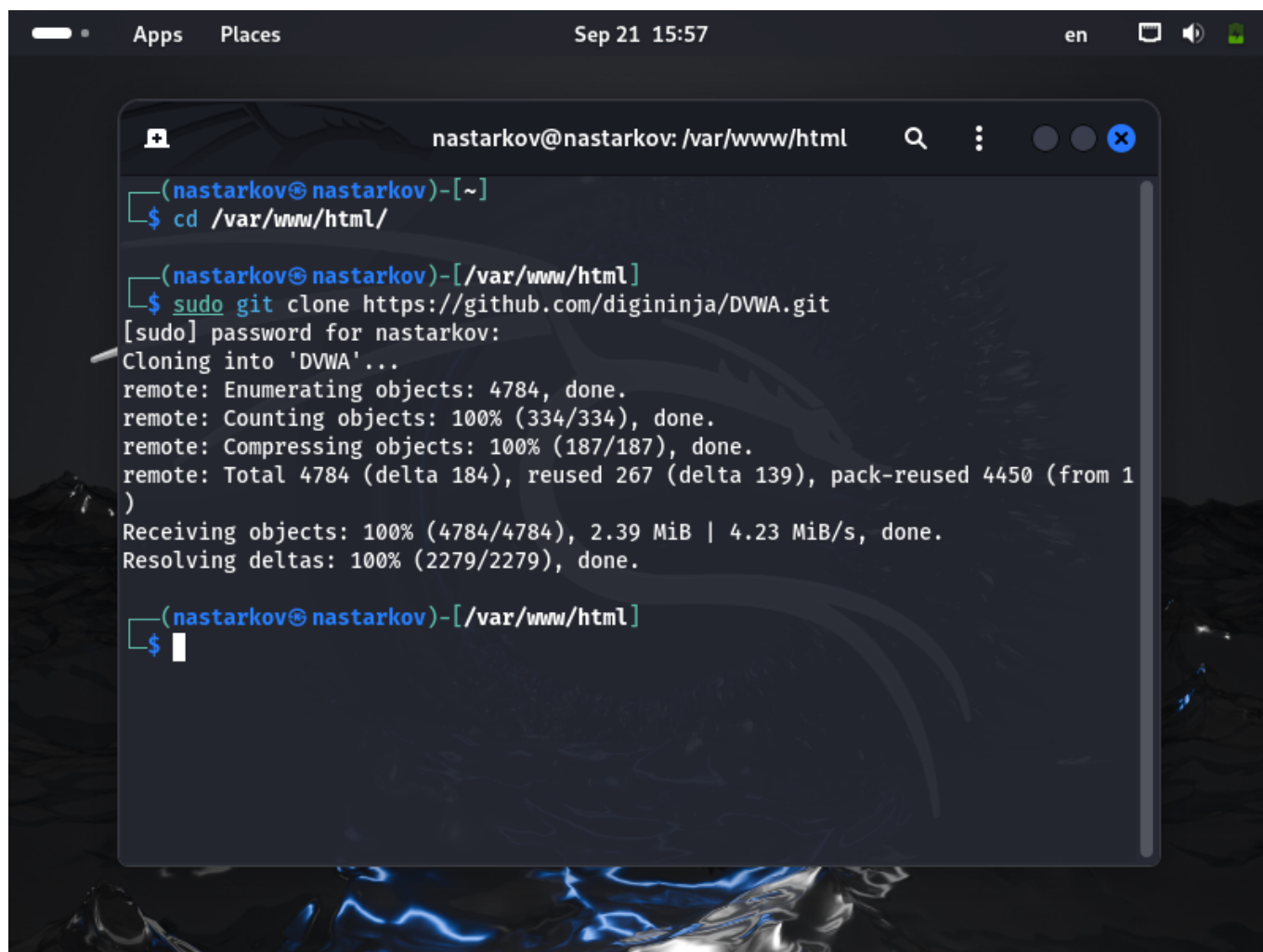
author: Старков Н.А.

Цель работы

Приобретение практического навыка установки и развертывания веб-приложения DVWA в гостевую систему к Kali Linux.

Выполнение работы

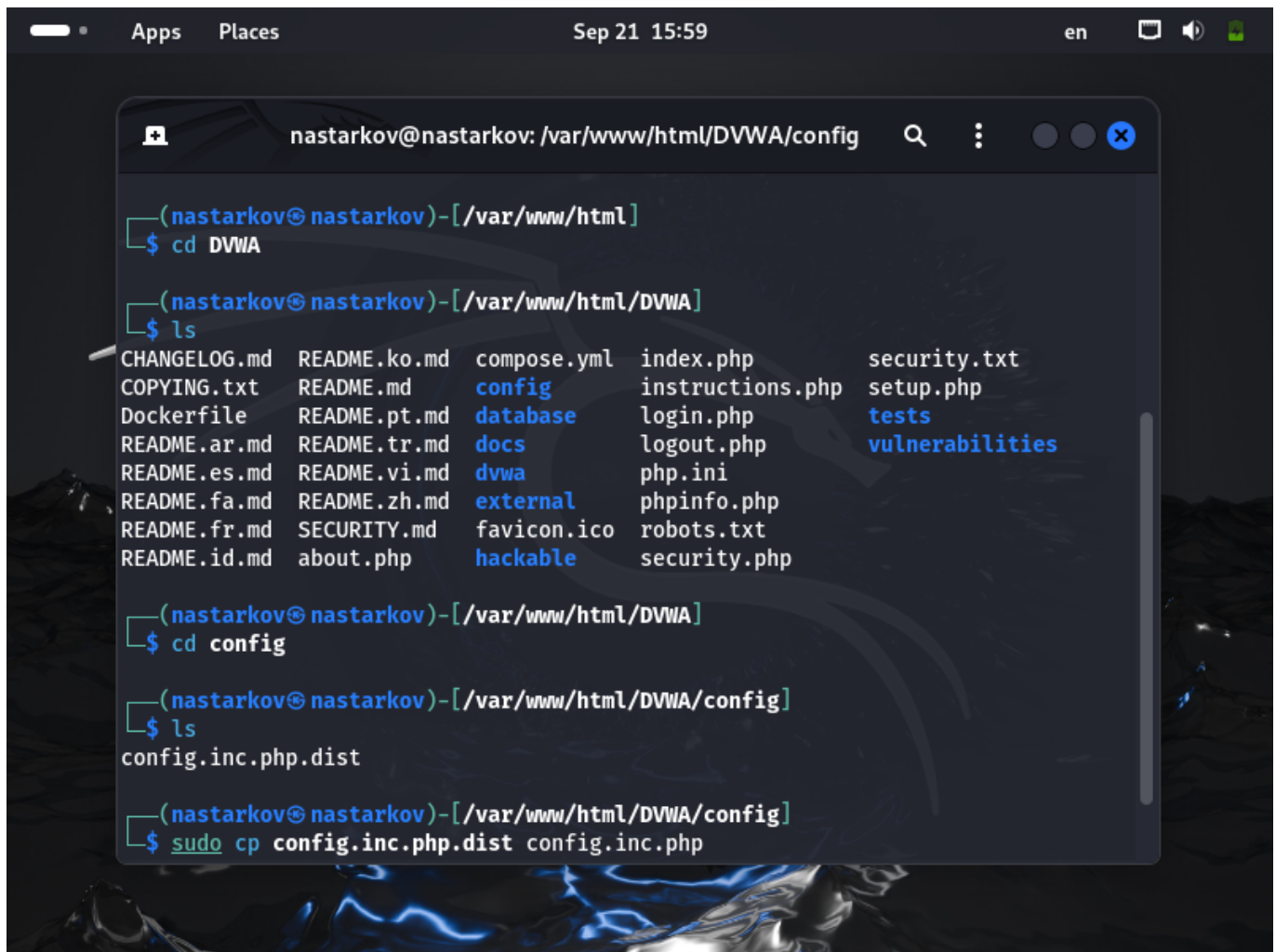
1. Перейдем в директорию /var/www/html/ и склонируем репозиторий <https://github.com/digininja/DVWA.git>

A screenshot of a terminal window on a Kali Linux system. The window title is 'nastarkov@nastarkov: /var/www/html'. The terminal shows the user navigating to the /var/www/html directory and cloning the DVWA repository from GitHub. The output of the git clone command shows the progress of cloning, including enumerating, counting, and compressing objects, and finally resolving deltas. The terminal ends with a prompt in the /var/www/html directory.

```
(nastarkov@nastarkov)-[~]  
$ cd /var/www/html/  
  
(nastarkov@nastarkov)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git  
[sudo] password for nastarkov:  
Cloning into 'DVWA'...  
remote: Enumerating objects: 4784, done.  
remote: Counting objects: 100% (334/334), done.  
remote: Compressing objects: 100% (187/187), done.  
remote: Total 4784 (delta 184), reused 267 (delta 139), pack-reused 4450 (from 1)  
Receiving objects: 100% (4784/4784), 2.39 MiB | 4.23 MiB/s, done.  
Resolving deltas: 100% (2279/2279), done.  
  
(nastarkov@nastarkov)-[/var/www/html]  
$
```

2. Перейдем в директорию config и скопируем содержимое файла config.inc.php.dist в файл config.inc.php командой

```
cp config.inc.php.dist config.inc.php
```



The screenshot shows a terminal window titled "nastarkov@nastarkov: /var/www/html/DVWA/config". The terminal output is as follows:

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

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

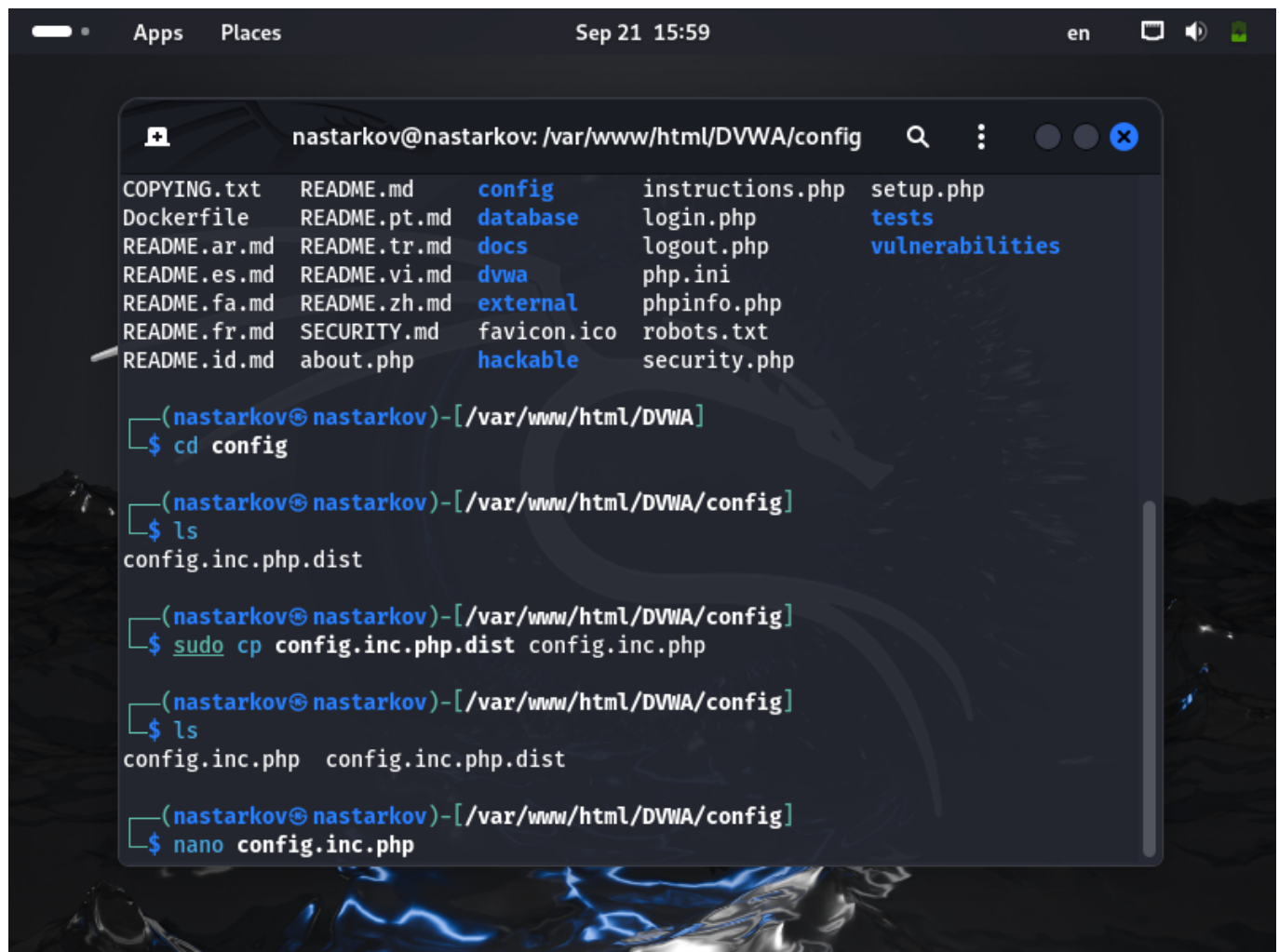
(nastarkov@nastarkov)-[/var/www/html/DVWA]
$ cd config

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

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

3. Откроем файл командой

```
nano config.inc.php
```



The image shows a terminal window titled "nastarkov@nastarkov: /var/www/html/DVWA/config". The window displays a directory listing of files and folders. Below the listing, a series of commands are entered and executed in the terminal.

```
nastarkov@nastarkov: /var/www/html/DVWA/config
```

COPYING.txt	README.md	config	instructions.php	setup.php
Dockerfile	README.pt.md	database	login.php	tests
README.ar.md	README.tr.md	docs	logout.php	vulnerabilities
README.es.md	README.vi.md	dvwa	php.ini	
README.fa.md	README.zh.md	external	phpinfo.php	
README.fr.md	SECURITY.md	favicon.ico	robots.txt	
README.id.md	about.php	hackable	security.php	

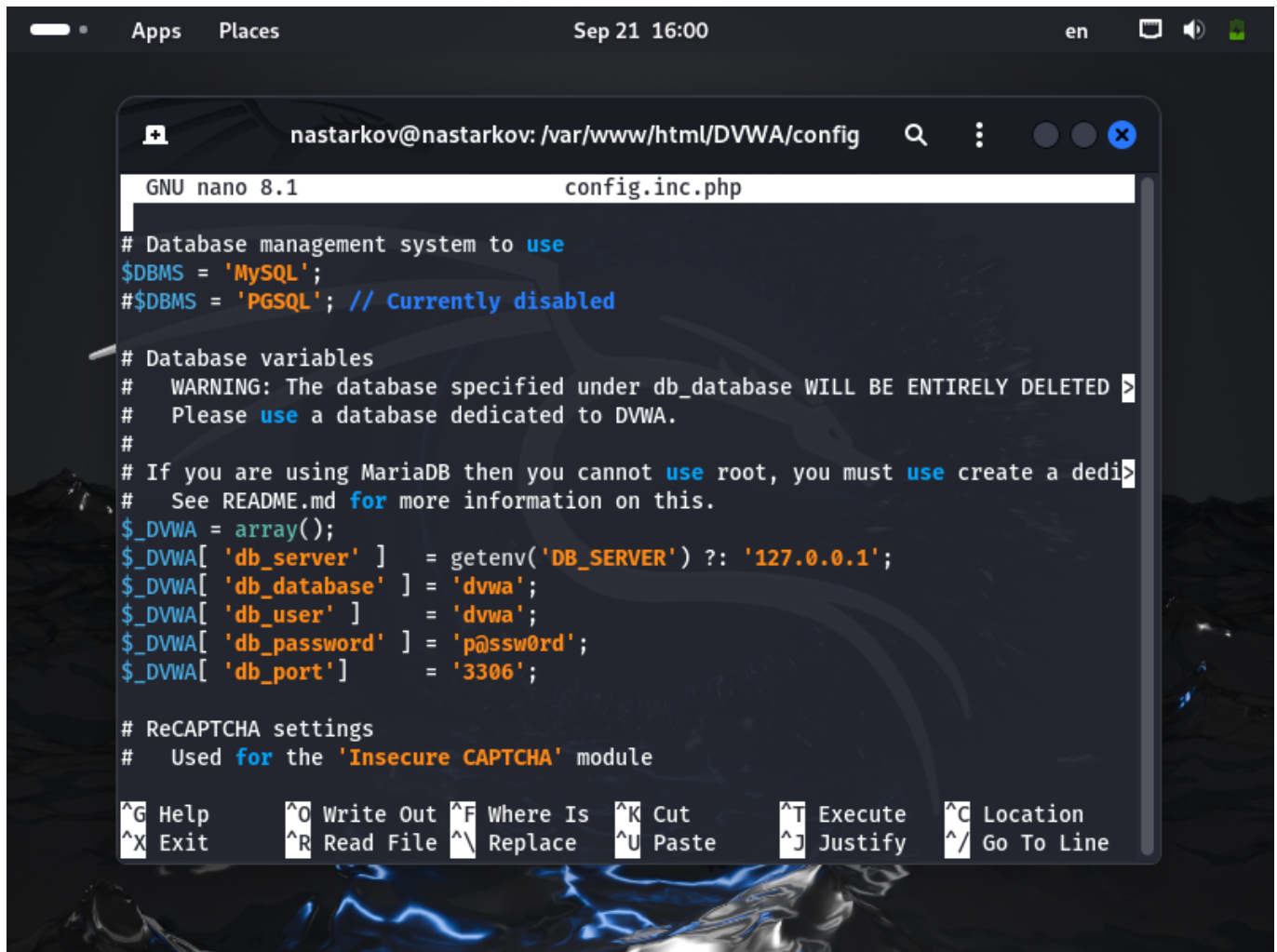
```
(nastarkov@nastarkov)-[/var/www/html/DVWA]
$ cd config

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

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

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

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



```
GNU nano 8.1 config.inc.php

# Database management system to use
$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 dedi
# 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'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_DVWA['db_port'] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module

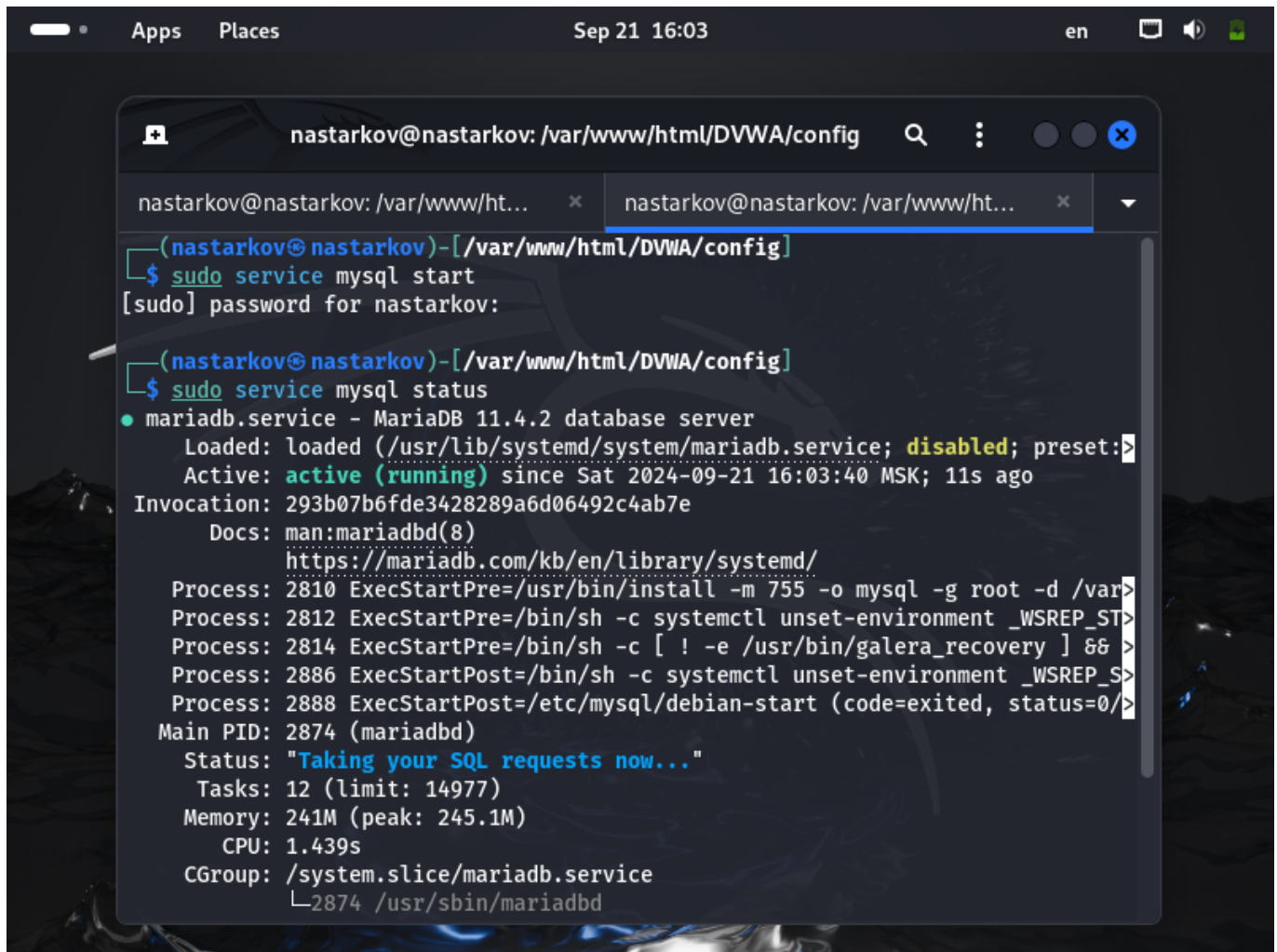
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

4. Как видим, файл содержит конфигурацию для подключения к СУБД MySQL как к СУБД по умолчанию.

Запускаем СУБД командой и смотрим работу следующими командами:

```
sudo service mysql start
```

```
sudo service mysql status
```

A terminal window titled 'nastarkov@nastarkov: /var/www/html/DVWA/config' with two tabs. The first tab shows the command 'sudo service mysql start' and a password prompt. The second tab shows the command 'sudo service mysql status' and its output. The output indicates that the mariadb.service is loaded, active (running), and has been running since 2024-09-21 16:03:40 MSK. It also lists various process details like PID, status, tasks, memory, CPU, and CGroup.

```
nastarkov@nastarkov: /var/www/html/DVWA/config
nastarkov@nastarkov: /var/www/ht... x nastarkov@nastarkov: /var/www/ht... x
(nastarkov@nastarkov)-[/var/www/html/DVWA/config]
$ sudo service mysql start
[sudo] password for nastarkov:

(nastarkov@nastarkov)-[/var/www/html/DVWA/config]
$ sudo service mysql status
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset:en>
   Active: active (running) since Sat 2024-09-21 16:03:40 MSK; 11s ago
   Invocation: 293b07b6fde3428289a6d06492c4ab7e
      Docs: man:mariadb(8)
            https://mariadb.com/kb/en/library/systemd/
   Process: 2810 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var>
   Process: 2812 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_ST>
   Process: 2814 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] &&>
   Process: 2886 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_S>
   Process: 2888 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/>
  Main PID: 2874 (mariadb)
    Status: "Taking your SQL requests now..."
     Tasks: 12 (limit: 14977)
    Memory: 241M (peak: 245.1M)
       CPU: 1.439s
    CGroup: /system.slice/mariadb.service
            └─2874 /usr/sbin/mariadb
```

5. Теперь перейдем к созданию базы данных и пользователя в соответствии с файлом config.inc.php:

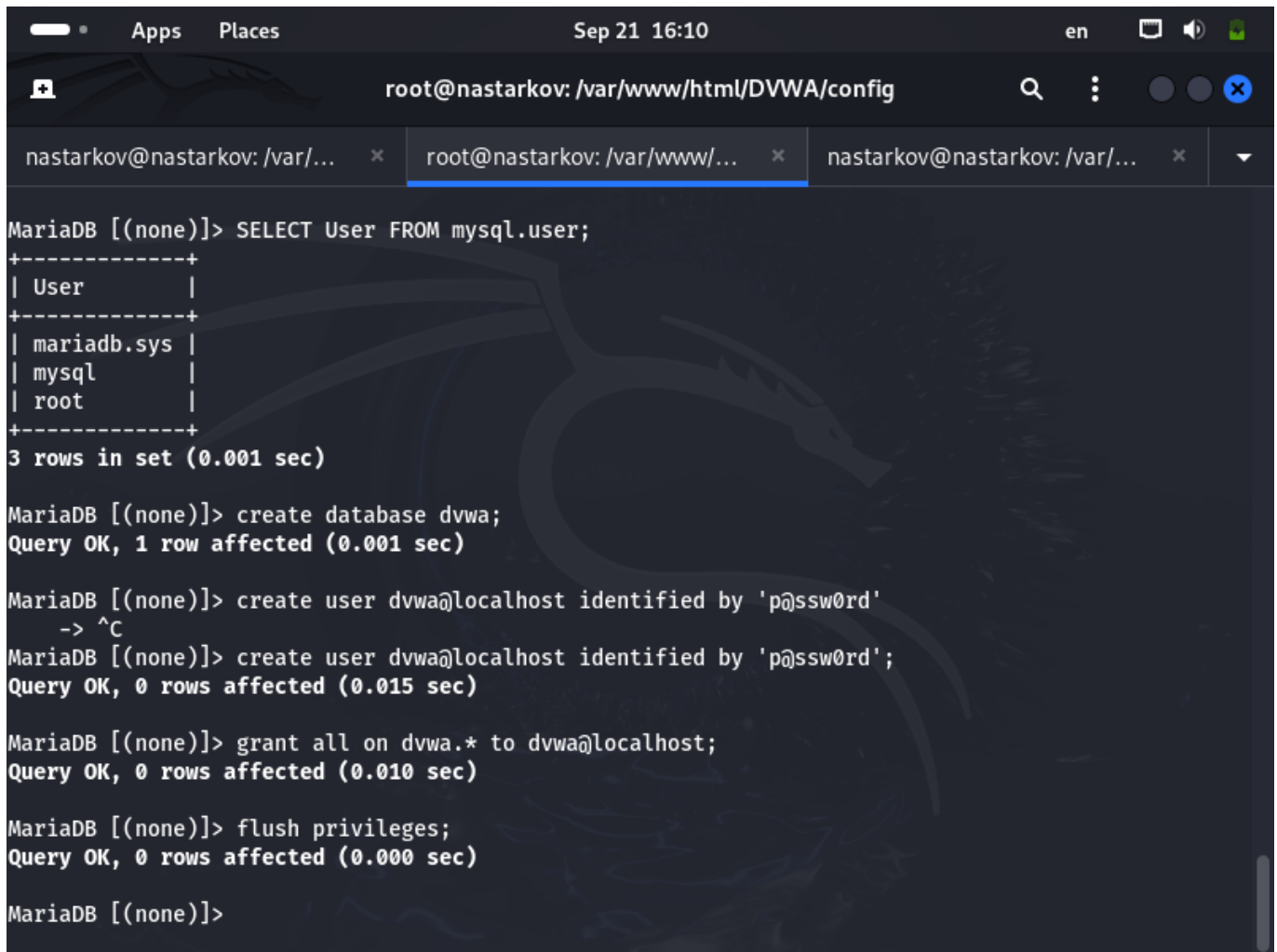
```
Apps Places Sep 21 16:07 en
root@nastarkov: /var/www/html/DVWA/config
nastarkov@nastarkov: /var/... x root@nastarkov: /var/www/... x nastarkov@nastarkov: /var/... x
$ sudo su
(root@nastarkov)-[/var/www/html/DVWA/config]
# mysql
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.2-MariaDB-4 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)]> SELECT User FROM mysql.user;
- - - - -
| User          |
- - - - -
| mariadb.sys   |
| mysql         |
| root          |
- - - - -
3 rows in set (0.001 sec)

MariaDB [(none)]> 
```

A terminal window titled 'root@nastarkov: /var/www/html/DVWA/config' is shown. The terminal displays the following commands and output:

```
MariaDB [(none)]> SELECT User FROM mysql.user;
+-----+
| User           |
+-----+
| mariadb.sys    |
| mysql          |
| root           |
+-----+
3 rows in set (0.001 sec)

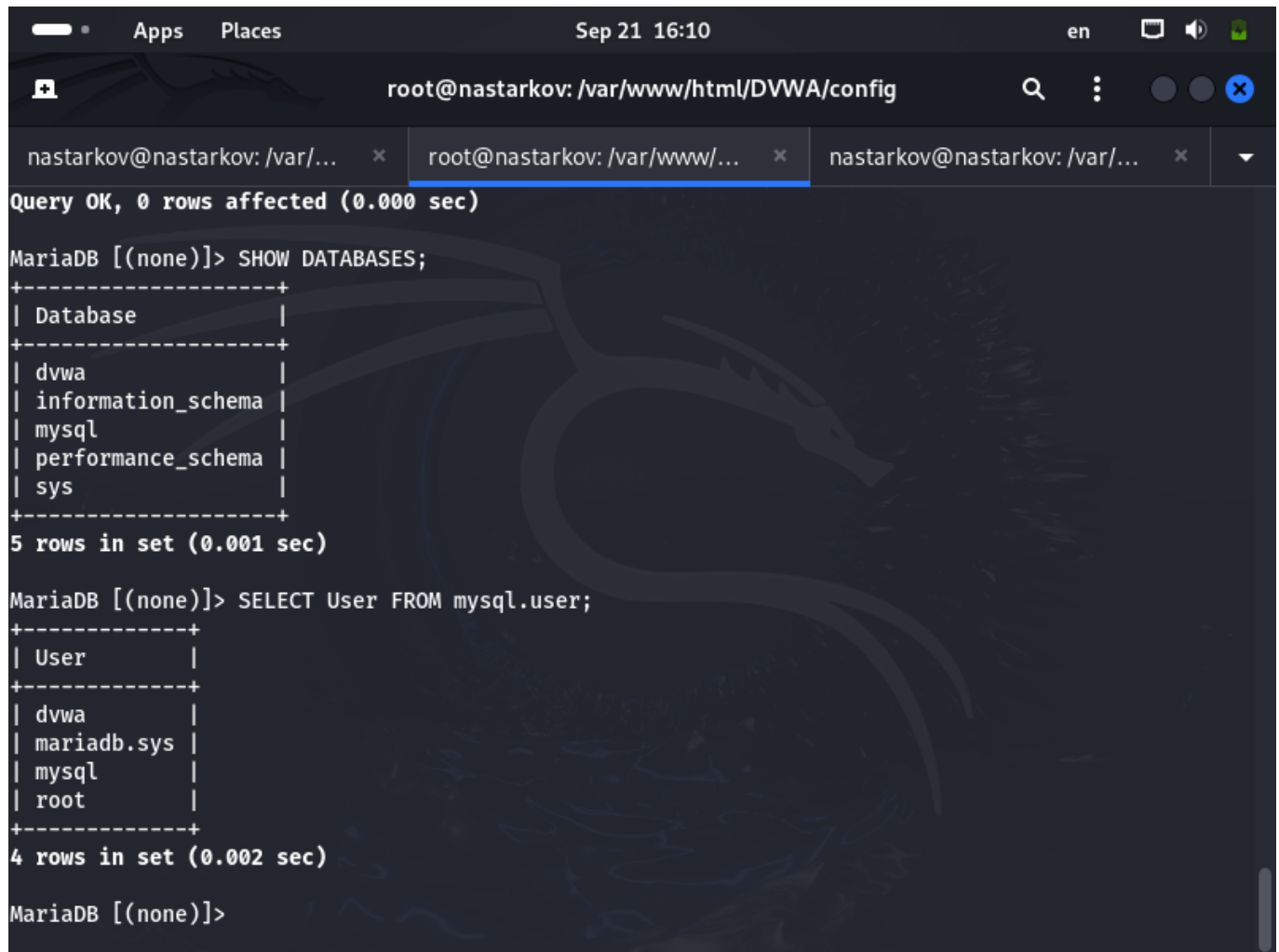
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd'
-> ^C
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.015 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.010 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]>
```

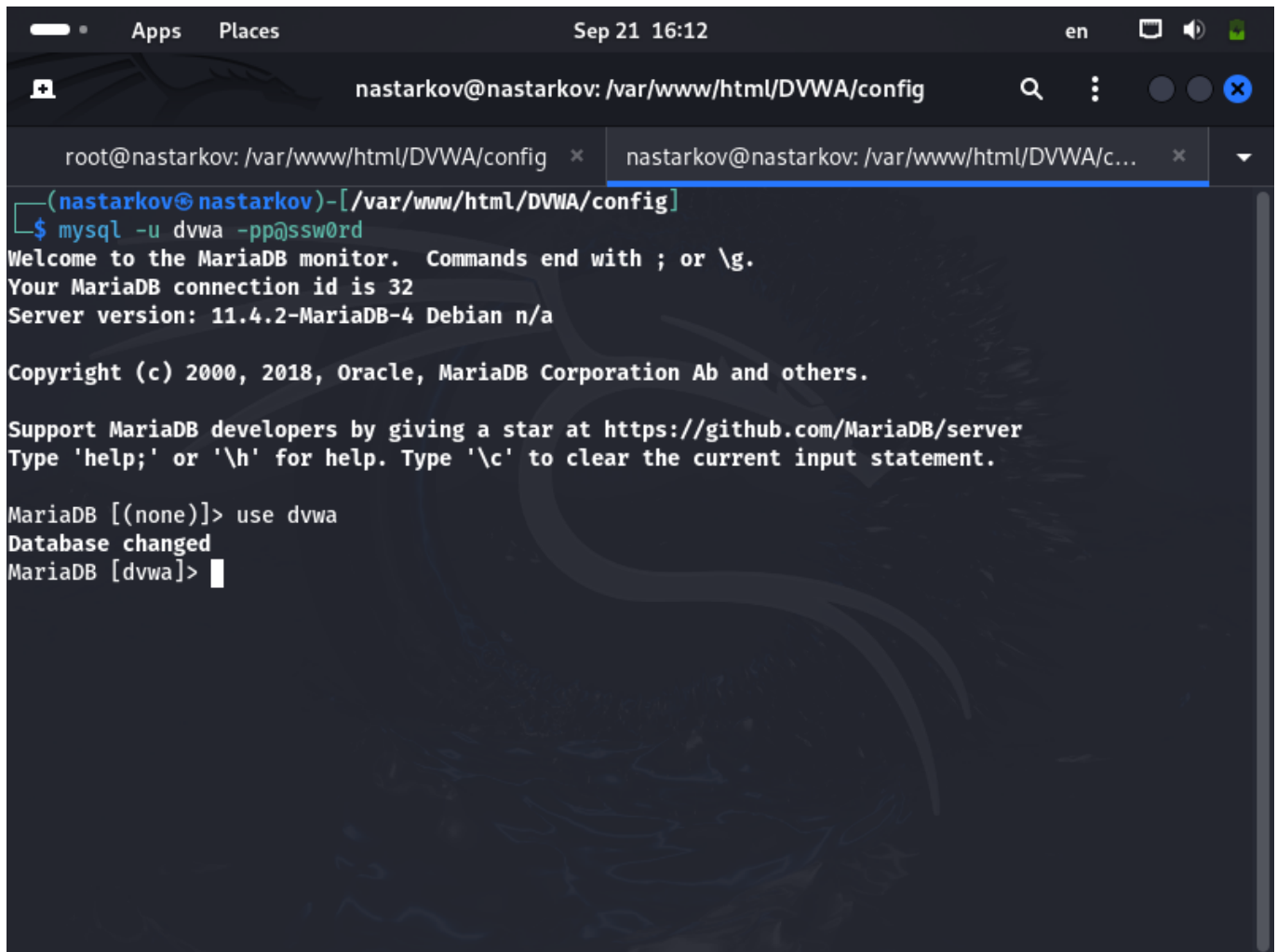


```
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| dvwa      |
| information_schema |
| mysql     |
| performance_schema |
| sys       |
+-----+
5 rows in set (0.001 sec)

MariaDB [(none)]> SELECT User FROM mysql.user;
+-----+
| User |
+-----+
| dvwa  |
| mariadb.sys |
| mysql |
| root  |
+-----+
4 rows in set (0.002 sec)

MariaDB [(none)]>
```


A terminal window with a dark background. The title bar shows 'Apps', 'Places', and the date/time 'Sep 21 16:12'. The address bar shows 'nastarkov@nastarkov: /var/www/html/DVWA/config'. The terminal content shows a user logging into MySQL as 'dvwa' with password 'pp@ssw0rd'. It displays the MariaDB monitor welcome message, connection ID 32, and server version 11.4.2-MariaDB-4 Debian n/a. The user then enters 'use dvwa' and the prompt changes to 'MariaDB [dvwa]>'.

```
(nastarkov@nastarkov)-[/var/www/html/DVWA/config]
$ mysql -u dvwa -pp@ssw0rd
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.4.2-MariaDB-4 Debian n/a

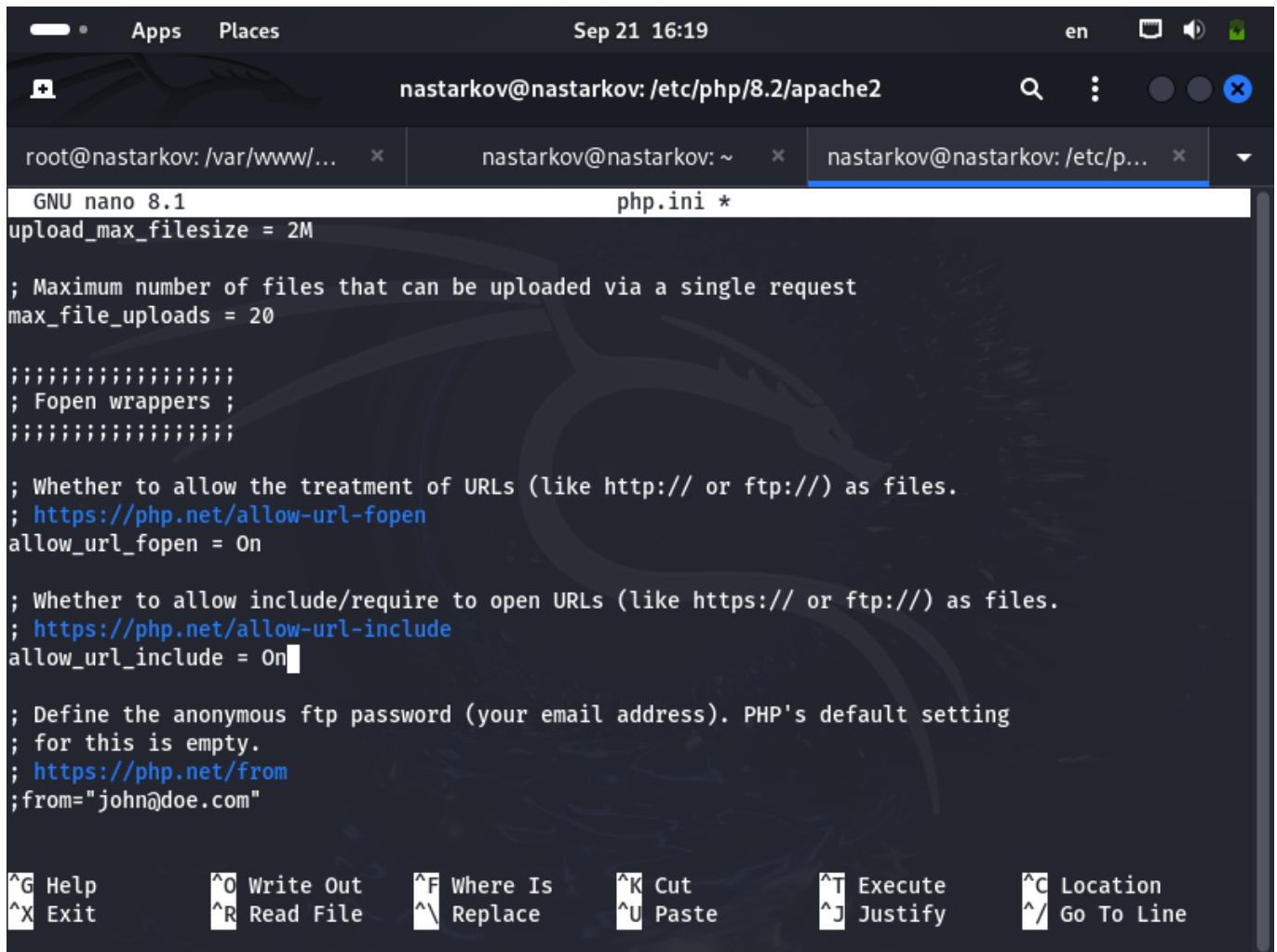
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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)]> use dvwa
Database changed
MariaDB [dvwa]> 
```

6. После мы должны внести изменение в конфигурационный файл `php.ini` веб-сервера `apache2`.

Для корректной работы переменные `allow_url_include` и `allow_url_fopen` должны иметь значение `On`.



```
GNU nano 8.1 php.ini *
upload_max_filesize = 2M

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

;;;;;;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;;;;;;

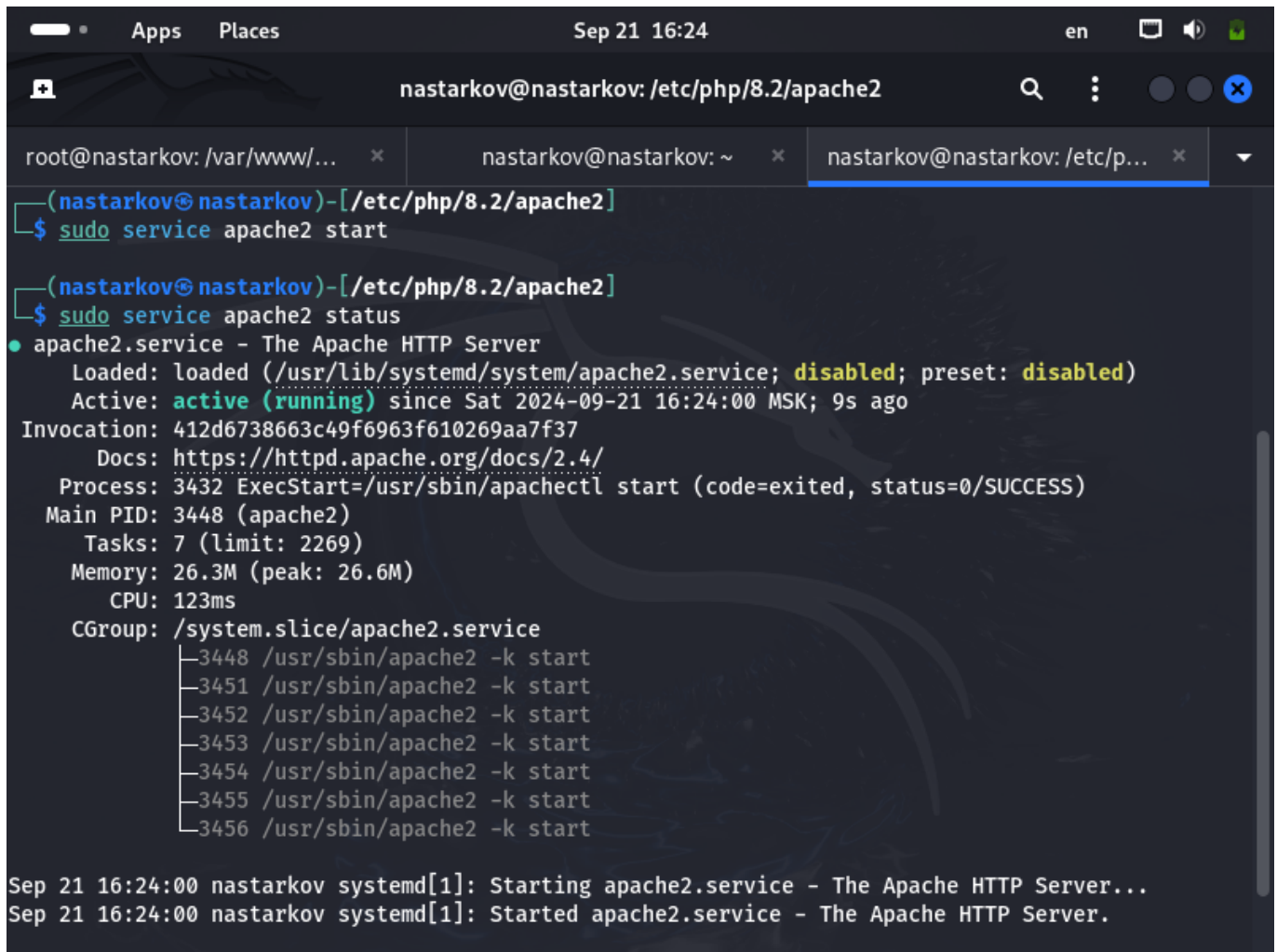
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

7. Запустим процесс веб-сервера аналогично MySQL:



```

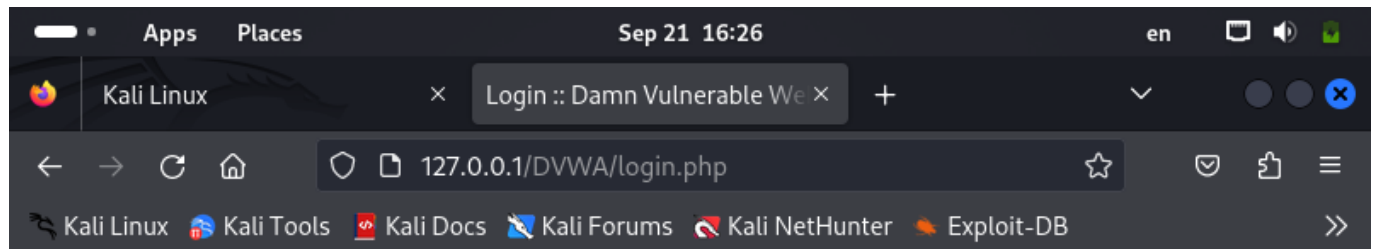
nastarkov@nastarkov: /etc/php/8.2/apache2

(nastarkov@nastarkov)-[/etc/php/8.2/apache2]
$ sudo service apache2 start

(nastarkov@nastarkov)-[/etc/php/8.2/apache2]
$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 16:24:00 MSK; 9s ago
 Invocation: 412d6738663c49f6963f610269aa7f37
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 3432 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 3448 (apache2)
   Tasks: 7 (limit: 2269)
  Memory: 26.3M (peak: 26.6M)
     CPU: 123ms
    CGroup: /system.slice/apache2.service
            └─3448 /usr/sbin/apache2 -k start
              └─3451 /usr/sbin/apache2 -k start
                └─3452 /usr/sbin/apache2 -k start
                  └─3453 /usr/sbin/apache2 -k start
                    └─3454 /usr/sbin/apache2 -k start
                      └─3455 /usr/sbin/apache2 -k start
                        └─3456 /usr/sbin/apache2 -k start

Sep 21 16:24:00 nastarkov systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 21 16:24:00 nastarkov systemd[1]: Started apache2.service - The Apache HTTP Server.
```

8. Теперь перейдем по адресу 127.0.0.1/DVWA/login.php. В форму авторизации введем имя пользователя admin и пароль password:



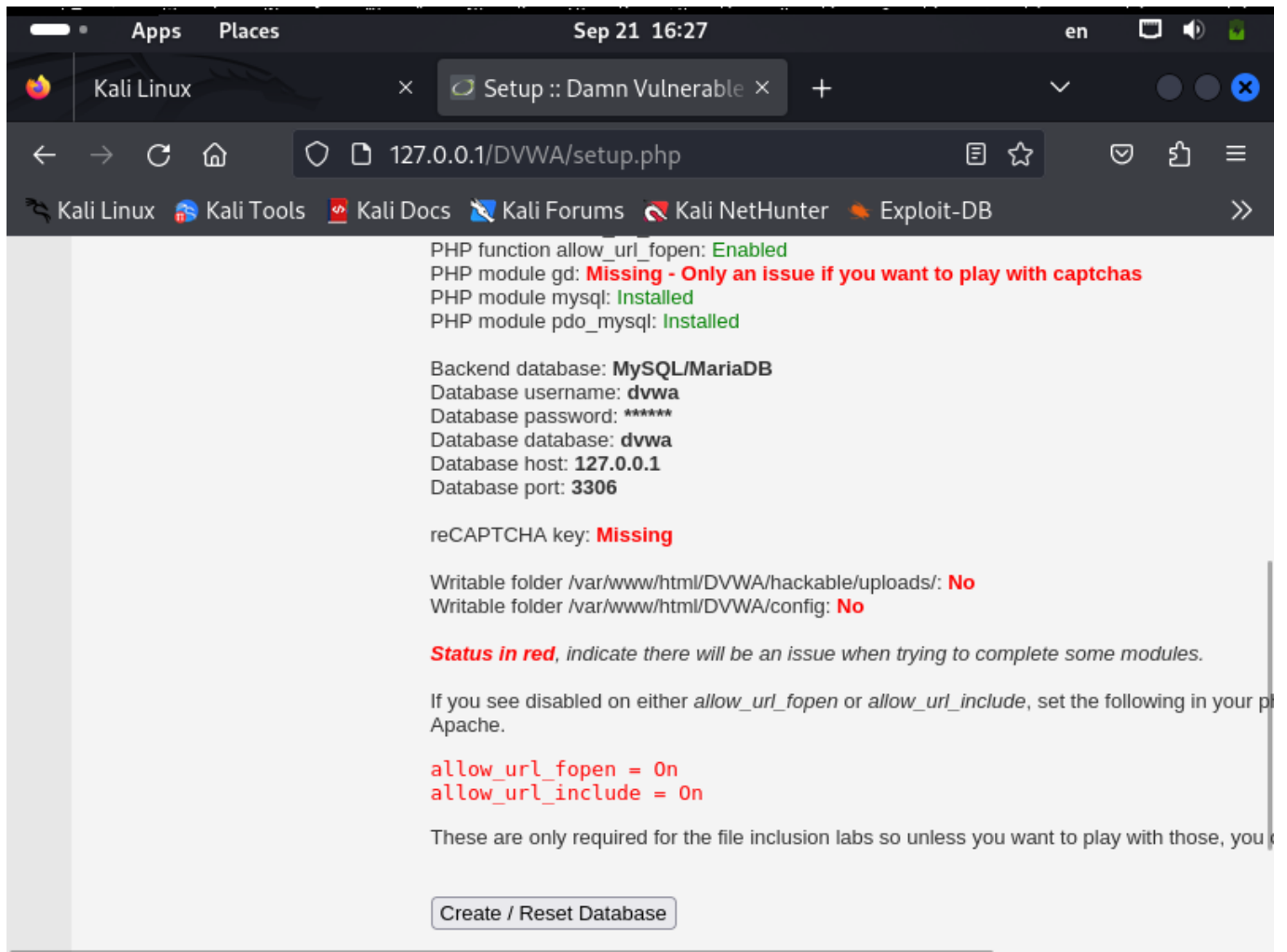
Username

Password

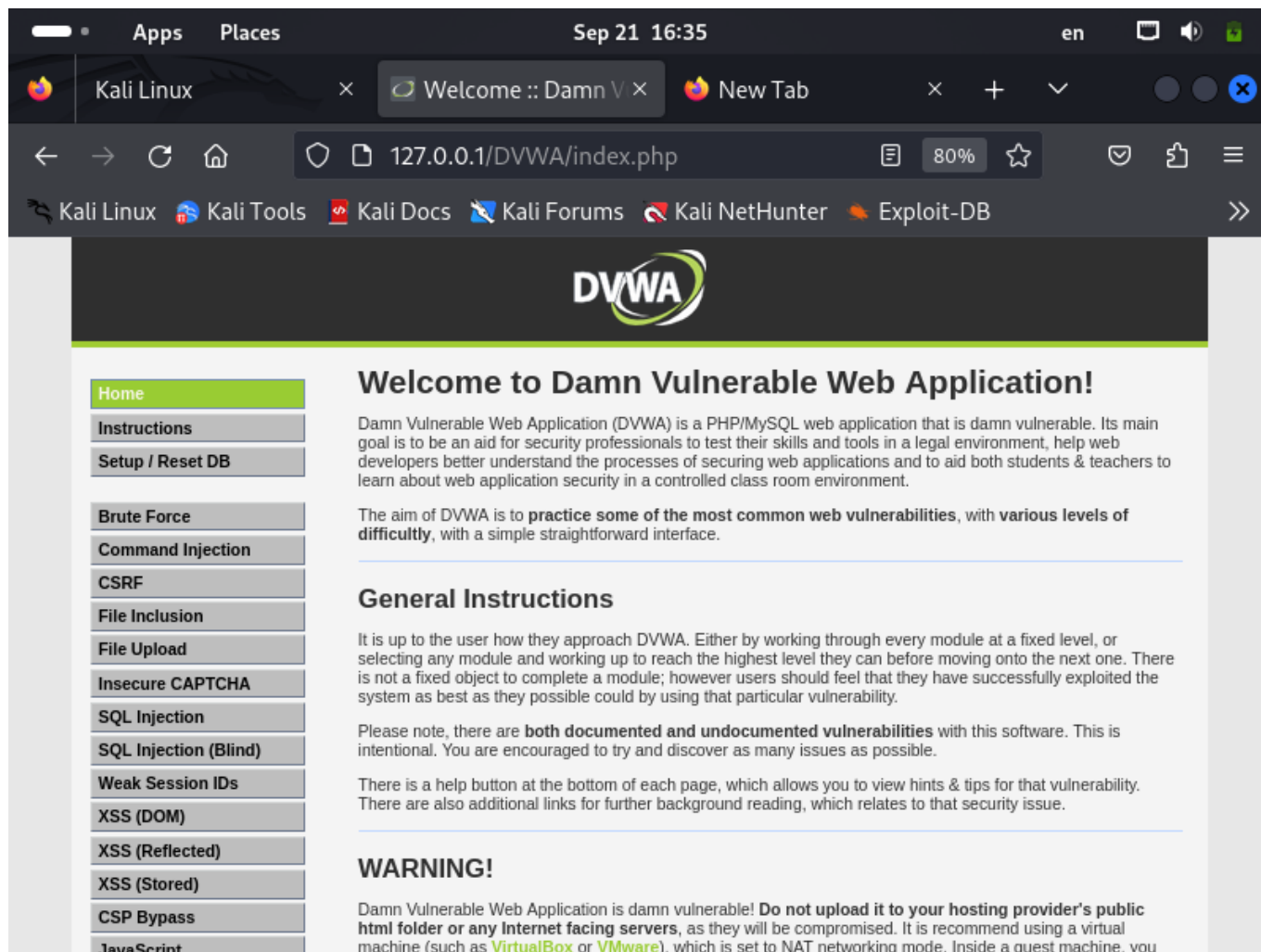
Login

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

9. Перейдя на страницу приложения, прокрутим ее вниз до кнопки "Create / Reset Database" и нажмем на нее, после чего авторизуемся повторно:



10. Веб-приложение DVWA развернуто.



Вывод

В ходе выполнения второго этапа проекта я получил практический навык установки и развертывания веб-приложения DVWA в гостевую систему к Kali Linux.