

Проект

Этап 2

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

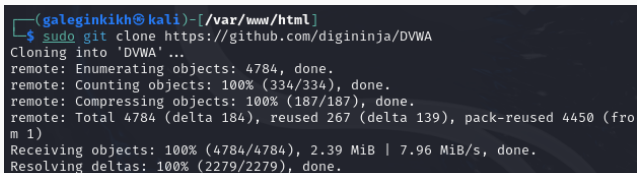
Информация

- Легиньких Галина Андреевна
- НФИбд-02-21
- Российский университет дружбы народов
- 1032216447@pfur.ru
- <https://github.com/galeginkikh>

Выполнение

Преобретение практических навыков по установке DVWA.

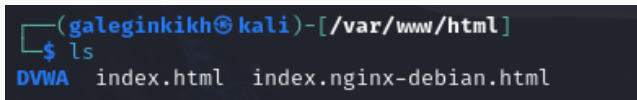
1. Перешла в директорию /var/www/html. Затем клонировала репозиторий.

A terminal window with a dark background and light-colored text. The prompt is (galeginkikh@kali)-[/var/www/html]. The command sudo git clone https://github.com/digininja/DVWA is entered. The output shows the cloning progress: 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 | 7.96 MiB/s, done., and Resolving deltas: 100% (2279/2279), done.

```
(galeginkikh@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
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 | 7.96 MiB/s, done.
Resolving deltas: 100% (2279/2279), done.
```

Рис. 1: Репозиторий

2. Проверяю, что файл скопировался. Повышаю права доступа к папке до 777.

A terminal window with a dark background. The prompt is `(galeginkikh@kali)-[/var/www/html]`. The user has entered `$ ls`. The output is `DVWA index.html index.nginx-debian.html`.

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

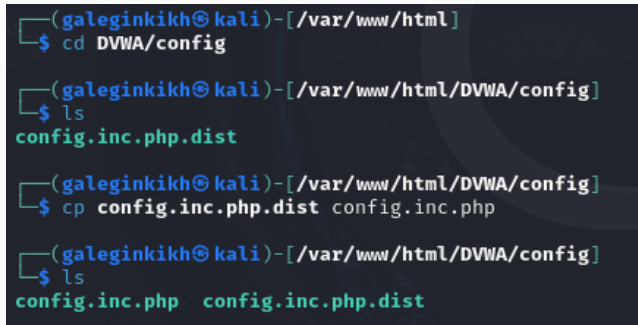
Рис. 2: Наличие папки

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

(galeginkikh@kali)-[/var/www/html]
$ ls -l
total 20
drwxrwxrwx 12 root  4096 Sep 20 18:00 DVWA
-rw-r--r--  1 root 10701 Sep 10 12:37 index.html
-rw-r--r--  1 root   615 Sep 10 12:38 index.nginx-debian.html
```

Рис. 3: Повышение прав

3. Перешла в каталог `/dvwa/config`. Создала копию файла.



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

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

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

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

Рис. 4: Каталог `/dvwa/config`

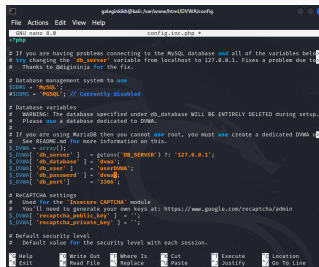
4. Открыла файл в текстовом редакторе.

A terminal window with a dark background. The prompt is `(galeginkikh@kali)-[/var/www/html/DVWA/config]`. The user has entered the command `$ sudo nano config.inc.php`.

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

Рис. 5: Редактор

5. Изменила данные об имени пользователя и пароле.



```
galapagos@kali: /usr/www/html/DWA/config
File Actions Edit View Help
GNU nano 3.0 config.inc.php
<?php
# If you are having problem connecting to the MySQL database and all of the variables below
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to
# Thanks to omgimagine for the fix.

# Database management system to use
$dbms = 'mysql';
$host = 'localhost'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DWA
# See README for more information on this.
$dbms = array();
$dbms[ 'db_server' ] = getenv( 'DB_SERVER' ) ? '127.0.0.1' :
$dbms[ 'db_database' ] = 'dwa';
$dbms[ 'db_user' ] = 'userDWA';
$dbms[ 'db_password' ] = '1300';
$dbms[ 'db_port' ] = '3306';

# ReCAPTCHA settings
# Used for the 'Basecore CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$dbms[ 'recaptcha_public_key' ] = '';
$dbms[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
```

Рис. 6: Имя и пароль

6. Запустила mysql.

```
(galeginkikh@kali)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(galeginkikh@kali)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 10.11.7 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 18:08:53 MSK; 22s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 18064 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld>
   Process: 18066 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITIO>
   Process: 18069 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || V>
   Process: 18143 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITI>
   Process: 18145 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 18130 (mariabdd)
    Status: "Taking your SQL requests now..."
    Tasks: 14 (limit: 38224)
   Memory: 210.2M (peak: 213.4M)
      CPU: 393ms
   CGroup: /system.slice/mariadb.service
           └─18130 /usr/sbin/mariabdd

Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Note] InnoDB: Loading buffer p>
Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Note] Plugin 'FEEDBACK' is dis>
Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Warning] You need to use --log>
Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Note] InnoDB: Buffer pool(s) l>
Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Note] Server socket created on>
Sep 20 18:08:53 kali mariabdd[18130]: 2024-09-20 18:08:53 0 [Note] /usr/sbin/mariabdd: read>
Sep 20 18:08:53 kali mariabdd[18130]: Version: '10.11.7-MariaDB-4' socket: '/run/mysqld/my>
Sep 20 18:08:53 kali systemd[1]: Started mariadb.service - MariaDB 10.11.7 database server.
Sep 20 18:08:53 kali /etc/mysql/debian-start[18148]: Upgrading MariaDB tables if necessary.
Sep 20 18:08:53 kali /etc/mysql/debian-start[18160]: Checking for insecure root accounts.
lines 1-28/28 (END)
```

Рис. 7: mysql

7. Авторизовалась в базе от имени пользователя root. Создала нового пользователя.

```
(galeginkikh@kali)-[/var/www/html/DVWA/config]
$ 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: 10.11.7-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.

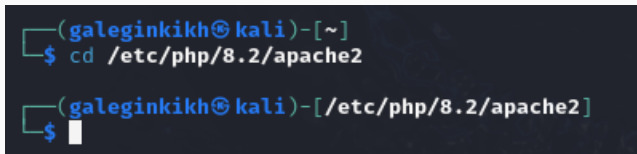
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified "dvwa"
→ ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds
to your MariaDB server version for the right syntax to use near '"dvwa"' at line 1
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified "dvwa";
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds
to your MariaDB server version for the right syntax to use near '"dvwa"' at line 1
MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by "dv
wa";
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> exit
Bye
```

Рис. 8: Новый пользователь

8. Перешла в директорию.



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

A terminal window with a dark background. The prompt is a green square icon. The text is in a monospaced font. The first line shows the user 'galeginkikh' at host 'kali' in the home directory '~'. The second line shows the command 'cd /etc/php/8.2/apache2' being executed. The third line shows the prompt after the command, now in the directory '/etc/php/8.2/apache2'. The fourth line shows a new prompt with a white cursor.

Рис. 9: apache2

9. В файле `php.ini` изменила один параметр.

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

Рис. 10: Параметр

10. Запустила службу веб-сервера apache.

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

(galeginkikh@kali)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-09-20 18:24:17 MSK; 26s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 25843 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 25867 (apache2)
     Tasks: 6 (limit: 5791)
    Memory: 19.8M (peak: 20.1M)
       CPU: 67ms
   CGroup: /system.slice/apache2.service
           └─25867 /usr/sbin/apache2 -k start
             └─25870 /usr/sbin/apache2 -k start
               └─25871 /usr/sbin/apache2 -k start
                 └─25872 /usr/sbin/apache2 -k start
                   └─25873 /usr/sbin/apache2 -k start
                     └─25874 /usr/sbin/apache2 -k start

Sep 20 18:24:17 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Sep 20 18:24:17 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Рис. 11: Запуск веб-сервера

11. Зашла в веб-сервер.

Setup :: Damn Vulnerable x +

127.0.0.1/DVWA/setup.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Setup DVWA

Instructions

About

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

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix


PHP version: 8.2.18
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

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

12. Авторизовалась.



The DVWA logo is centered at the top of the login page. It features the text "DVWA" in a bold, dark blue font. To the right of the text is a stylized circular graphic composed of two curved lines, one green and one dark blue, forming a partial circle.

Username

Password

Login

Рис. 13: Авторизация

Вывод

Преобрела практические навыки по установке DVWA.