

Презентация по Этапу №2 ИП

Основы информационной безопасности

Коннова Татьяна Алексеевна

16 марта 2024

- Коннова Татьяна Алексеевна
- НПИбд-01-22

- Установить DVWA в гостевую систему к Kali Linux.

Выполнение работы

Клонирование репо

```
File Actions Edit View Help
(konnovata@root)-[~]
$ sudo nano /etc/hostname
sudo: unable to resolve host root: Name or service not known
[sudo] password for konnovata:

(konnovata@root)-[~]
$ cd /var/www/html

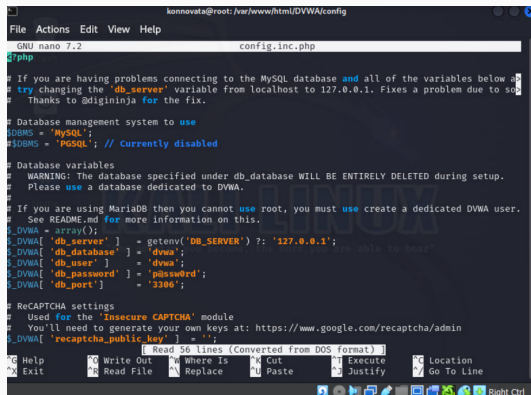
(konnovata@root)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
sudo: unable to resolve host root: Name or service not known
[sudo] password for konnovata:
Sorry, try again.
[sudo] password for konnovata:

zsh: suspended sudo git clone https://github.com/digininja/DVWA.git

(konnovata@root)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA.git
sudo: unable to resolve host root: Name or service not known
[sudo] password for konnovata:
Sorry, try again.
[sudo] password for konnovata:
Sorry, try again.
[sudo] password for konnovata:
Cloning into 'DVWA'...
remote: Enumerating objects: 4500, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 4500 (delta 17), reused 33 (delta 10), pack-reused 4450
Receiving objects: 100% (4500/4500), 2.30 MiB | 2.74 MiB/s, done.
```

Рис. 1: Переход, клонирование

Изменение config.inc.php



```
konnovata@root: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 7.2 config.inc.php
<?php
# If you are having problems connecting to the MySQL database and all of the variables below a
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to so
# Thanks to @diginiinja for the fix.

# Database management system to use
$DBMS = 'MySQL';
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.

# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# 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
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';
```

Рис. 2: config.inc.php

```
(konnovata@ root)-[/var/www/html/DVWA/config]
$ sudo apt-get update
sudo: unable to resolve host root: Name or service not known
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.8 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.1 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [893 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.0 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.8 kB]
Fetched 68.5 MB in 3min 43s (308 kB/s)
Reading package lists... Done

(konnovata@ root)-[/var/www/html/DVWA/config]
$ sudo apt-get -y install apache2 mariadb-server php php-mysql php-gd libapache2-mod-php
sudo: unable to resolve host root: Name or service not known
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'php8.2-mysql' instead of 'php-mysql'
php is already the newest version (2:8.2+93).
php set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93).
libapache2-mod-php set to manually installed.
The following additional packages will be installed:
  apache2-bin apache2-utils libapache2-mod-php8.2 libmariadb3 mariadb-client
  mariadb-client-core mariadb-common mariadb-plugin-provider-bzip2
  mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
```

Рис. 3: mariadb

```
(konnovata@ root)-[/var/www/html/DVWA/config]
Reading state information... Done
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
php is already the newest version (2:8.2+93).
php set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93).
libapache2-mod-php set to manually installed.
The following additional packages will be installed:
  apache2-bin apache2-utils libapache2-mod-php8.2 libmariadb3 mariadb-client
  mariadb-client-core mariadb-common mariadb-plugin-provider-bzip2
  mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server-core php8.2 php8.2-cli php8.2-common
  php8.2-gd php8.2-opcache php8.2-readline
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear mailx mariadb-test
  netcat-openbsd
The following NEW packages will be installed:
  php-gd php8.2-gd
```

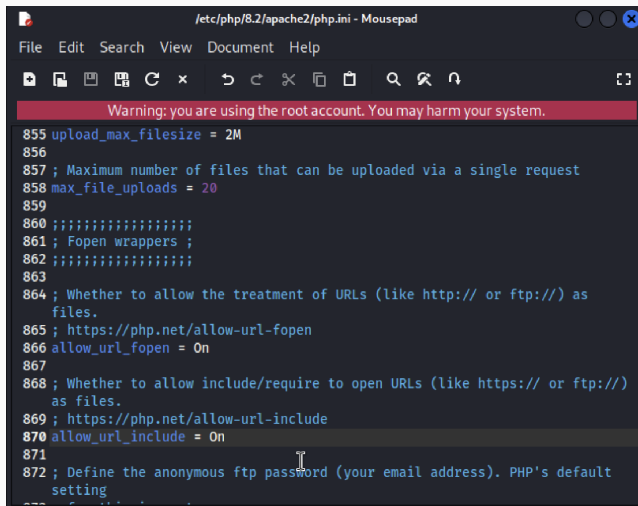
Рис. 4: БД

Настройка сервера

```
(konnovata@root)-[/var/www/html/DVWA/config]
Reading state information ... Done
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
php is already the newest version (2:8.2+93).
php set to manually installed.
libapache2-mod-php is already the newest version (2:8.2+93).
libapache2-mod-php set to manually installed.
The following additional packages will be installed:
  apache2-bin apache2-utils libapache2-mod-php8.2 libmariadb3 mariadb-client
  mariadb-client-core mariadb-common mariadb-plugin-provider-bzip2
  mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server-core php8.2 php8.2-cli php8.2-common
  php8.2-gd php8.2-opcache php8.2-readline
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear mailx mariadb-test
  netcat-openbsd
The following NEW packages will be installed:
  php-gd php8.2-gd
```

Рис. 5: Apache

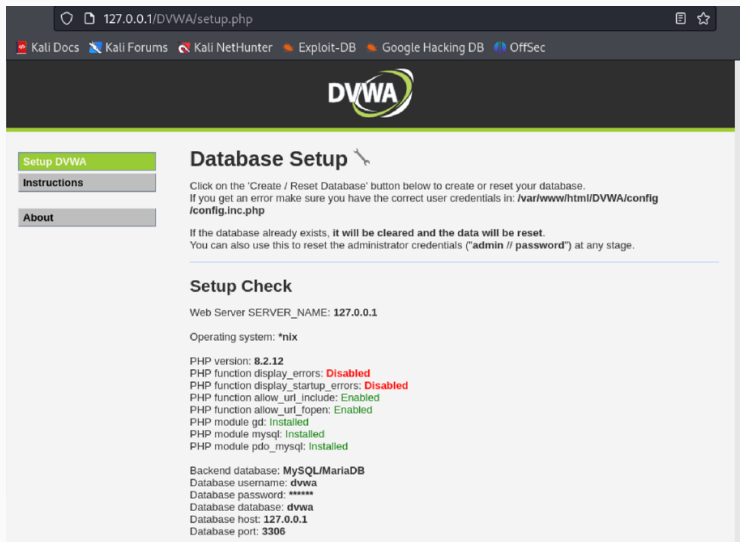
Изменение параметров



```
855 upload_max_filesize = 2M
856
857 ; Maximum number of files that can be uploaded via a single request
858 max_file_uploads = 20
859
860 ;;;;;;;;;;;;;;;;;;
861 ; Fopen wrappers ;
862 ;;;;;;;;;;;;;;;;;;
863
864 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
   files.
865 ; https://php.net/allow-url-fopen
866 allow_url_fopen = On
867
868 ; Whether to allow include/require to open URLs (like https:// or ftp://)
   as files.
869 ; https://php.net/allow-url-include
870 allow_url_include = On
871
872 ; Define the anonymous ftp password (your email address). PHP's default
   setting
```

Рис. 6: php.ini


Заполнение параметров входа в браузере



Заполнение параметров входа в браузере

127.0.0.1/DVWA/login.php

Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Username

Password

Рис. 8: Вход

Заполнение параметров входа в браузере

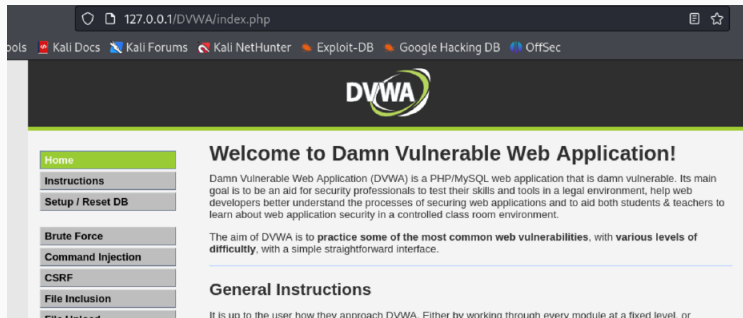


Рис. 9: Hello page

- В ходе выполнения данной лабораторной работы проведена установка DVWA в Kali Linux.