

# Индивидуальный проект. Второй этап

---

Королёв Иван Андреевич

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Королёв Иван Андреевич
- студент
- Российский университет дружбы народов

## Цель работы

---

Установить DVWA в гостевую систему к Kali Linux.

## Задание

---

Установить DVWA в гостевую систему к Kali Linux. Удалить основные ошибки

## Теоретическое введение

---



Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP / MySQL, которое чертовски уязвимо.

Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений и помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемой среде.

## Выполнение лабораторной работы

---

## Установка DVWA

---

## Установка DVWA

```
(iakorolev@kali)-[~]
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 4494 (delta 15), reused 30 (delta 8), pack-reused 4450
Receiving objects: 100% (4494/4494), 2.26 MiB | 619.00 KiB/s, done.
Resolving deltas: 100% (2126/2126), done.

(iakorolev@kali)-[~]
$ sudo mv DVWA /var/www/html

(iakorolev@kali)-[~]
$ cd /var/www/html

(iakorolev@kali)-[/var/www/html]
$ ll
total 20
drwxr-xr-x 12 iakorolev iakorolev 4096 Mar 12 09:55 DVWA
-rw-r--r--  1 root      root      10701 Mar  1 12:13 index.html
-rw-r--r--  1 root      root        615 Mar  1 12:14 index.nginx-debian.html

(iakorolev@kali)-[/var/www/html]
$ sudo server apache2 start
sudo: server: command not found

(iakorolev@kali)-[/var/www/html]
$ sudo service apache2 start

(iakorolev@kali)-[/var/www/html]
$
```

## Установка DVWA

---

```
(iakorolev@kali)-[~]
└─$ sudo su -
[sudo] password for iakorolev:
└─(root@kali)-[~]
   └─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.11.6-MariaDB-2 Debian n/a

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement

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

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

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

MariaDB [(none)]>
```

## Установка 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: **localhost**

Operating system: **\*nix**

PHP version: **8.2.12**

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/`: **No**

Writable folder `/var/www/html/DVWA/config`: **No**

**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
```



Убираем основные ошибки в  
запуске

---

# Убираем основные ошибки в запуске

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

DVWA Security

PHP Info

About

Logout

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: localhost

Operating system: \*nix

PHP version: 8.2.12  
PHP function display\_errors: Enabled  
PHP function display\_startup\_errors: Enabled  
PHP function allow\_url\_include: Enabled  
PHP function allow\_url\_fopen: Enabled  
PHP module gd: Installed  
PHP module mysql: Installed  
PHP module pdo\_mysql: Installed

Backend database: MySQL/MariaDB  
Database username: dvwa  
Database password: dvwa  
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

**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

Рис. 6: DVWA

## Выводы

---

Установил DVWA в гостевую систему к Kali Linux.

## Список литературы

---

