

# Моя научная работа

---

имя:ван яо

группа:НПМбд-02-21

билет:1032215430

## цель

---

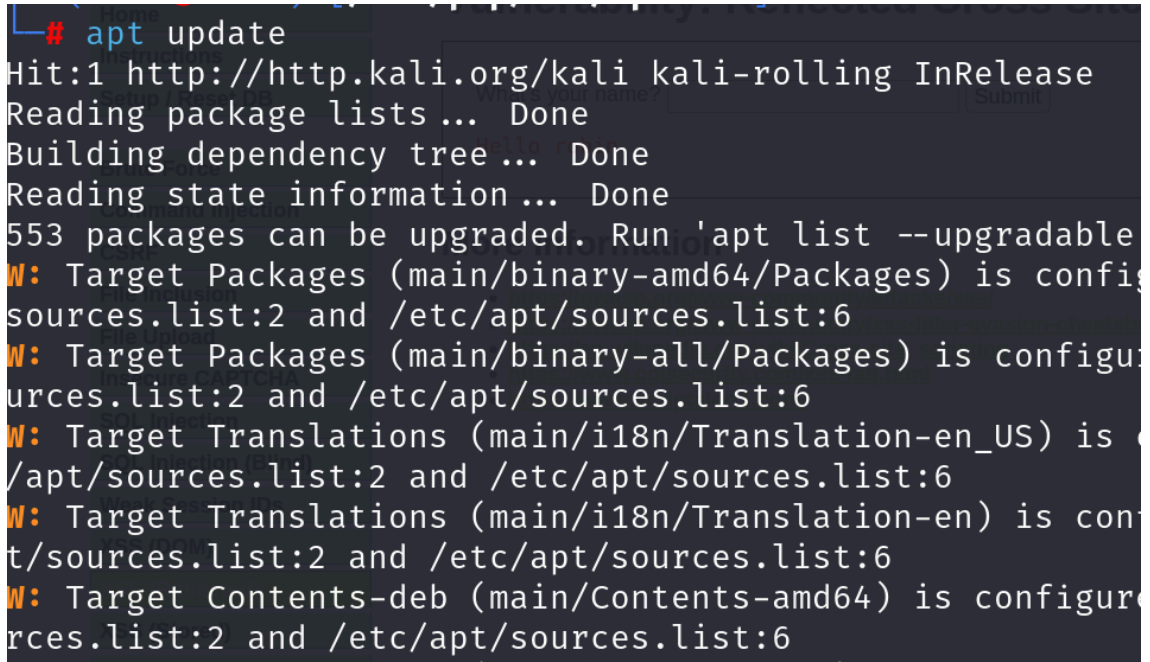
установка DVWA

## Подготовка перед установкой

### 1.Обновление системы

- Убедитесь, что ваша система Kali Linux обновлена до последней версии:

`sudo apt update && sudo apt upgrade -y`

A screenshot of a terminal window showing the output of the 'apt update' command. The output includes the following lines: 'Hit:1 http://http.kali.org/kali kali-rolling InRelease', 'Reading package lists ... Done', 'Building dependency tree ... Done', 'Reading state information ... Done', '553 packages can be upgraded. Run 'apt list --upgradable' to see them.', and several warning messages (W:) about target packages and translations. The terminal has a dark background with light-colored text.

```
# apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
553 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: Target Packages (main/binary-amd64/Packages) is configured on file /etc/apt/sources.list:2 and /etc/apt/sources.list:6
W: Target Packages (main/binary-all/Packages) is configured on file /etc/apt/sources.list:2 and /etc/apt/sources.list:6
W: Target Translations (main/i18n/Translation-en_US) is configured on file /etc/apt/sources.list:2 and /etc/apt/sources.list:6
W: Target Translations (main/i18n/Translation-en) is configured on file /etc/apt/sources.list:2 and /etc/apt/sources.list:6
W: Target Contents-deb (main/Contents-amd64) is configured on file /etc/apt/sources.list:2 and /etc/apt/sources.list:6
```

### 2.Проверка веб-сервера

- Убедитесь, что Apache2, PHP и база данных MySQL уже установлены. В Kali Linux эти компоненты обычно уже установлены по умолчанию:

`sudo service apache2 status`

`sudo service mysql status`

## Установка DVWA

### 1.Загрузка DVWA

- Скачайте последнюю версию DVWA с GitHub

```
cd /var/www/html
```

```
sudo git clone https://github.com/digininja/DVWA.git
```

```
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (178/178), done.
remote: Total 4758 (delta 164), reused 246 (delta 124), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 3.80 MiB/s, done.
Resolving deltas: 100% (2259/2259), done.
```

## 2. Настройка базы данных

- Перейдите в каталог DVWA:

```
(root@kali)~# cd /etc/php
(root@kali)/etc/php# ls
8.2
(root@kali)/etc/php# cd 8.2
(root@kali)/etc/php/8.2# ls
apache2 cli mods-available
(root@kali)/etc/php/8.2# cd apache2
(root@kali)/etc/php/8.2/apache2# ls
conf.d php.ini
```

```
cd DVWA
```

- Создайте базу данных для DVWA:

```
sudo mysql -u root -p
```

После ввода пароля пользователя root выполните следующие команды:

```
CREATE DATABASE dvwa;
```

```
GRANT ALL ON dvwa.* TO 'dvwa'@'localhost' IDENTIFIED BY 'password';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

## 3. Импорт базы данных DVWA

- Импортируйте SQL файл DVWA:

```
sudo mysql -u dvwa -p dvwa < dvwa.sql
```

```
(kali㉿kali)-[~]
└─$ sudo mv DVWA /var/www/html
[sudo] password for kali:
mv: cannot move 'DVWA' to '/var/www/html/DVWA': D

(kali㉿kali)-[~]
└─$ cd /var/www/html

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

#### 4. Конфигурация DVWA

- Отредактируйте конфигурационный файл DVWA:

```
sudo nano dvwa/vulnerabilities/config.inc.php
```

- Измените параметры подключения к базе данных:

```
$db['host'] = 'localhost';
$db['username'] = 'dvwa';
$db['password'] = 'password'; // Замените на ваш пароль
$db['database'] = 'dvwa';
```

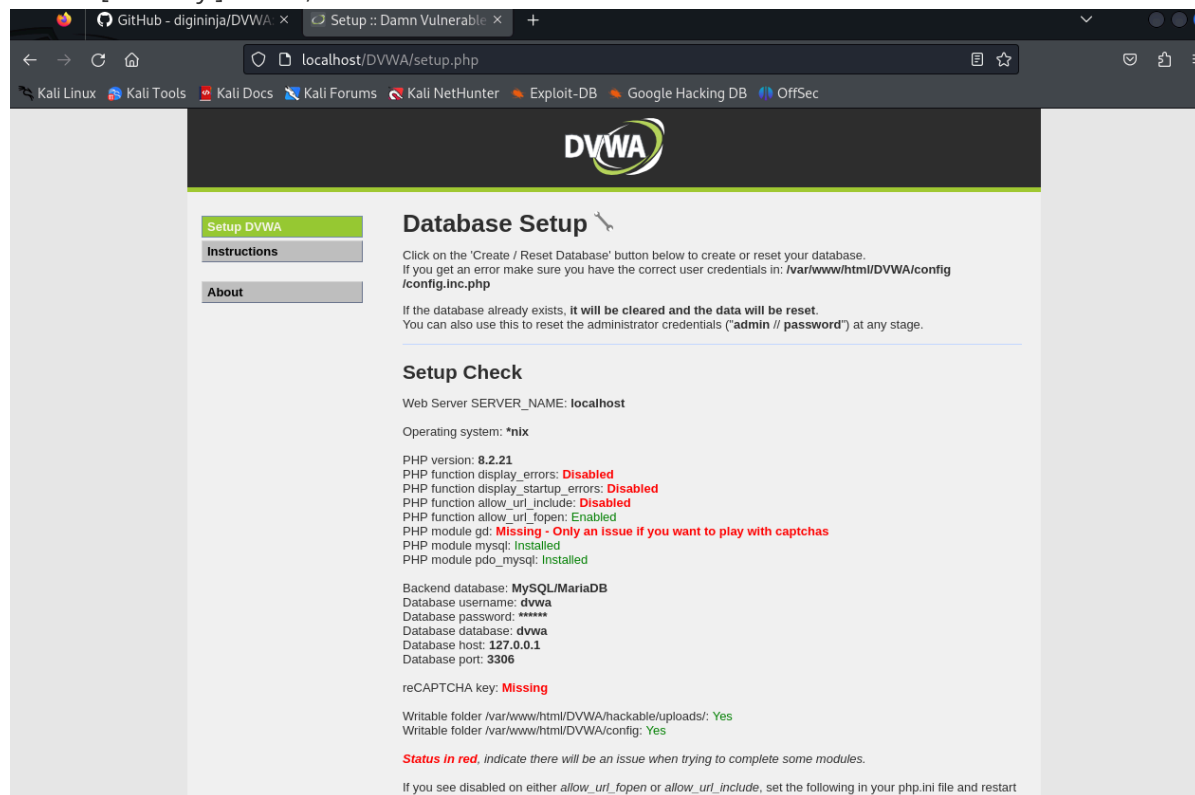
#### 5. Настройка уровня безопасности

- По умолчанию DVWA устанавливает определенный уровень безопасности. Вы можете изменить его, отредактировав файл security.php:

```
sudo nano dvwa/hackable/users/admin/config.php
```

- Измените уровень безопасности:

```
$DVWA['security'] = 'low';
```



## 6. Перезапуск Apache

- Перезапустите Apache, чтобы применить изменения:

```
sudo systemctl restart apache2
```

## Доступ к DVWA

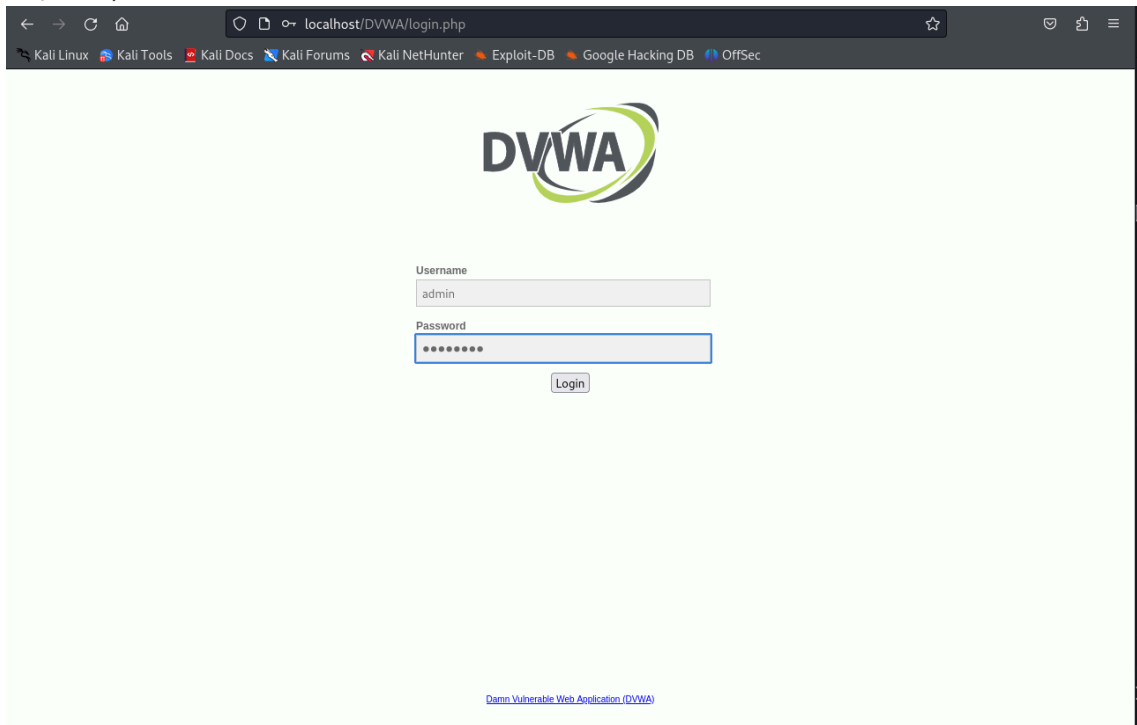
- Откройте браузер и перейдите по адресу:

<http://localhost/DVWA/>

- Логин и пароль по умолчанию:

- Имя пользователя: admin

Пароль: password



The screenshot shows a web browser window with the address bar displaying `localhost/DVWA/login.php`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area features the DVWA logo at the top center. Below the logo, there is a login form with two input fields: 'Username' containing the text 'admin' and 'Password' containing eight dots. A 'Login' button is positioned below the password field. At the bottom center of the page, there is a small blue link that reads 'Damn Vulnerable Web Application (DVWA)'.