

# Индивидуальный проект. Этап DVWA

---

Кадров В.М.

16 марта 2024

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Установить уязвимый веб-сервер DVWA.

## Задание

---

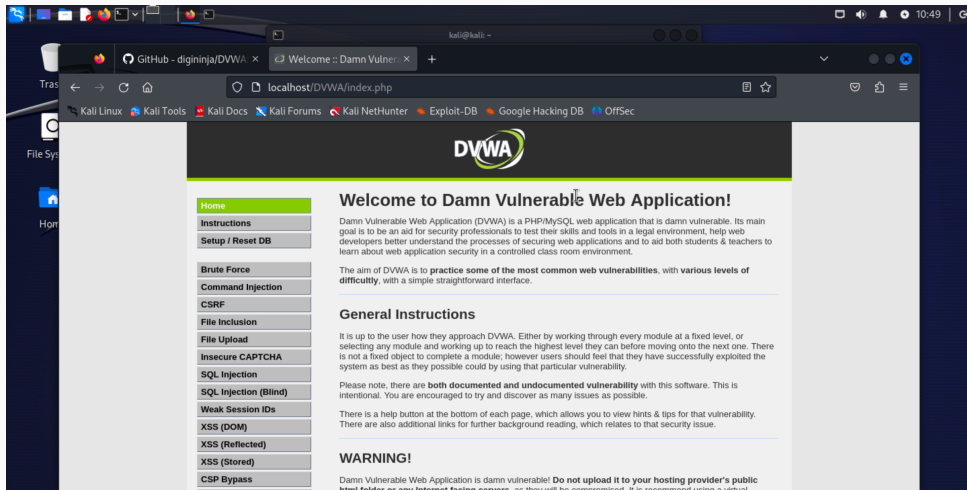
1. Установка приложения
2. Тестирование уязвимостей

## **Выполнение лабораторной работы**

---

# Установка приложения

Заходим на github, скачиваем себе установочный скрипт и выполняем его. В итоге на виртуальную машину устанавливается уязвимый веб-сервер.



Ищем веб-уязвимости.

Browser tabs: GitHub - digi..., Vulnerabili..., Command Inj..., Command Inj..., Online - Reve..., 0.0.0.0 and [...], PayloadsAllIT..., From Hex - C..., What does th...

Address bar: localhost/DVWA/vulnerabilities/exec/#

Browser extensions: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, PayloadsAllTheThings..., CyberChef

**DVWA**

Home  
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

## Vulnerability: Command Injection

### Ping a device

Enter an IP address:

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 3075ms  
www-data

### More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- [https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)



## Выводы

---

В ходе лабораторной работы был установлен уязвимый веб-сервер DVWA.