# Индивидуальный проект шаг 2

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

# Задание

# Задание

В этом этапе индивидуального проекта требуется установить Damn Vulnerable Web Application (DVWA) на виртуальную машину, которую мы установили в предыдущем этапе.

# Выполнение

# DVWA-Install.sh

# Docker

# Docker

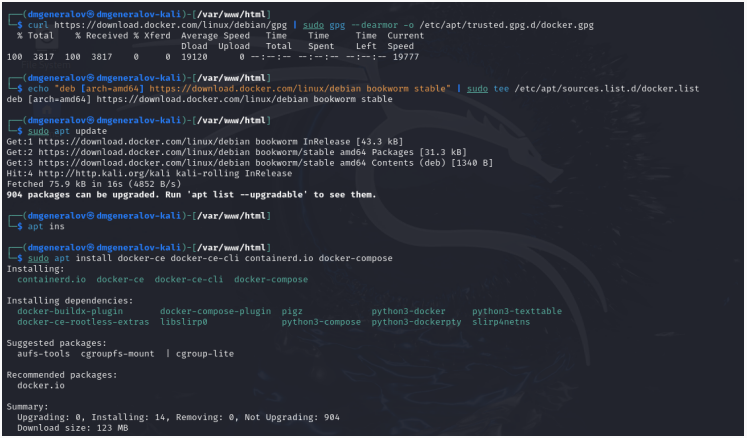


**Рис. 2:** docker

# Docker Compose

# Docker Compose

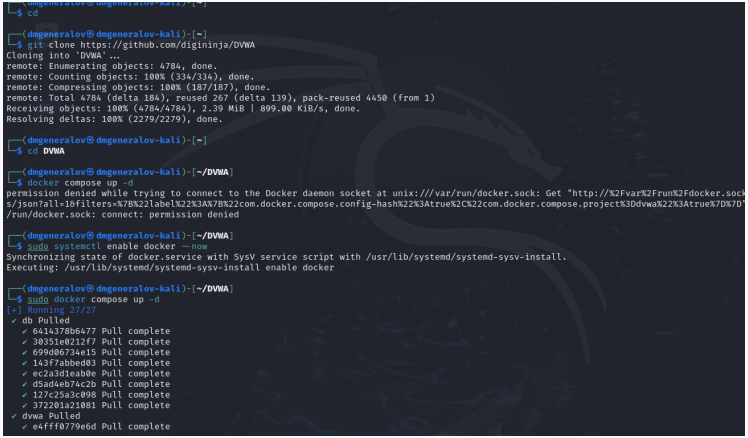


**Рис. 3:** docker-compose

# DVWA

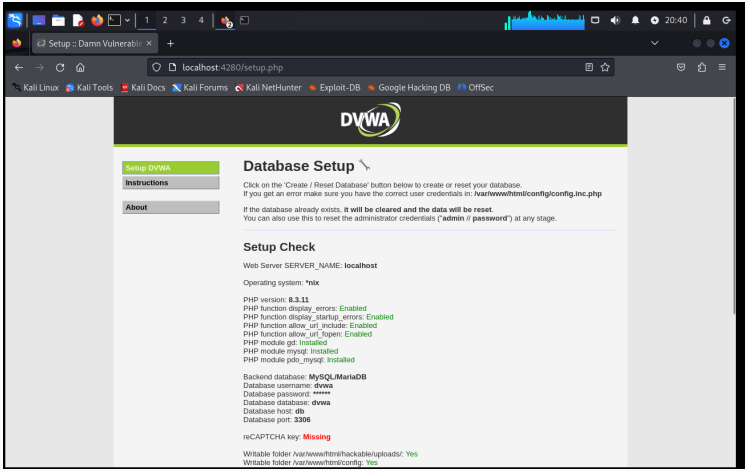
Setup :: Damn Vulnerable
localhost:4280/setup.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/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: 8.3.11
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: ******
Database database: dvwa
Database host: db
Database port: 3306
reCAPTCHA key: Missing
Writable folder /var/www/html/hackable/uploads/: Yes
Writable folder /var/www/html/config: Yes

**Рис. 4:** dvwa

# DVWA

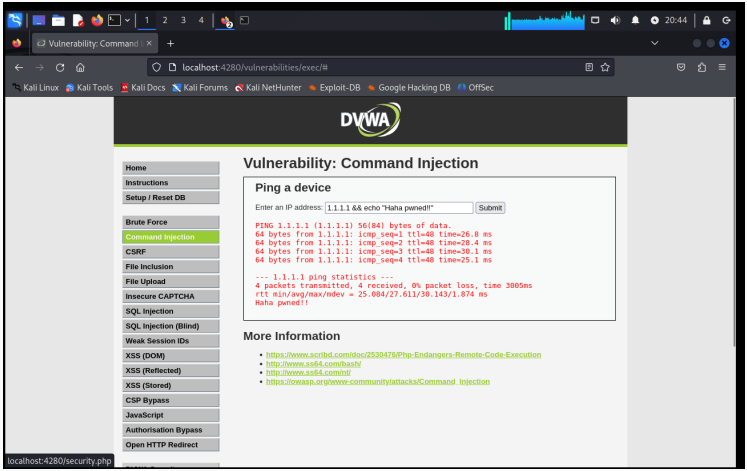
Vulnerability: Command
localhost:4280/vulnerabilities/exec/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (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: 1.1.1.1 && echo "Haha pwned!!"
Submit
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=48 time=26.8 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=48 time=28.4 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=48 time=30.1 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=48 time=25.1 ms
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 25.084/27.611/30.143/1.874 ms
Haha pwned!!
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
localhost:4280/security.php

**Рис. 5:** dvwa

# Выводы

# Выводы

Мы успешно установили DVWA и попробовали эксплуатировать одну из уязвимостей. Это доказывает, что установка была осуществлена успешно.