Отчет по проекту

Этап 3

Легиньких Галина Андреевна

Содержание

Список иллюстраций

Список таблиц

1 Теоретическое введение

Пример работы: * Исходные данные: * IP сервера 178.72.90.181; * Сервис http на стандартном 80 порту; * Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test_password; * В случае не удачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again. * Запрос к Hydra будет выглядеть примерно так:

```
  hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -
f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^
```

- Используется http-post-form потому, что авторизация происходит по http методом post.
- После указания этого модуля идёт строка /cgi-bin/luci:username=^{USER}&password=^{PASS}:Invali username, у которой через двоеточие (:) указывается:
- путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);
- строка, которая передаётся методом POST, в которой логин и пароль заменены на ^{USER} и ^{PASS} соответственно (username=^{USER}&password=^{PASS});
- строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

2 Цель работы

Использование Hydra.

3 Выполнение этапа 3

1. Нашла и скачала список частоиспользуемых паролей из интернета. rockyou.txt (рис. 3.1) (рис. 3.2)

Рис. 3.1: Загрузки

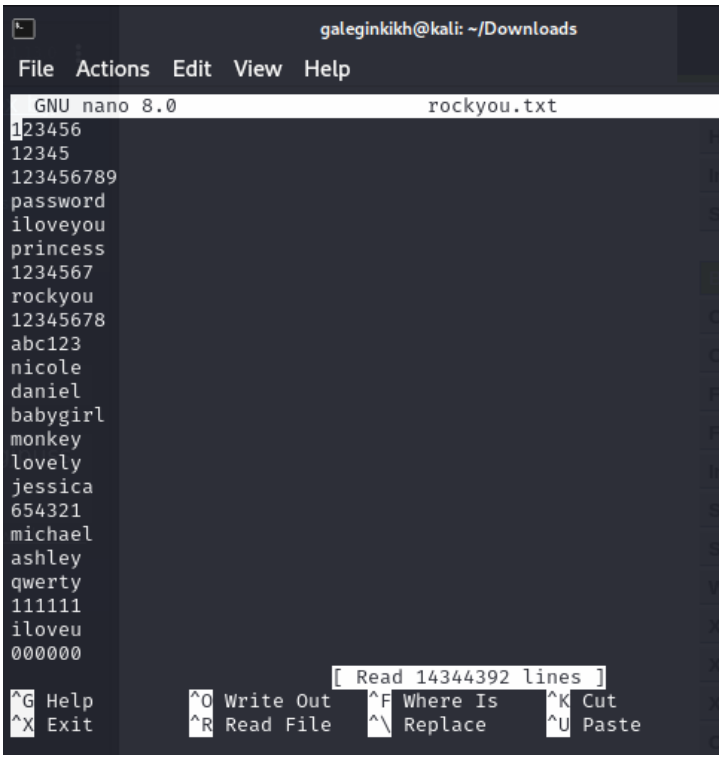

Рис. 3.2: Пароли

2. Захожу на сайт DVWA, созданный на прошлом этапе. (рис. 3.3)

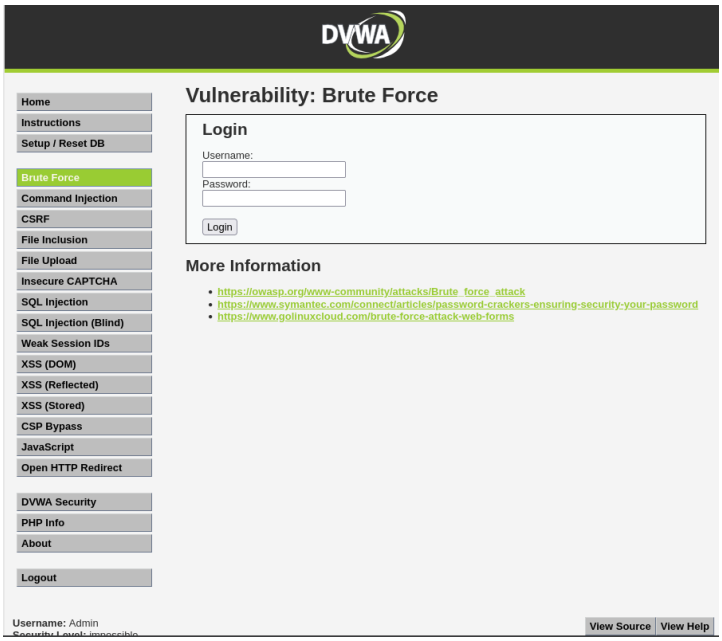

Рис. 3.3: DVWA

3. Для запроса hydra мне понадобятся параметры cookie с этого сайта. я скачала расширение для браузера. (рис. 3.4)

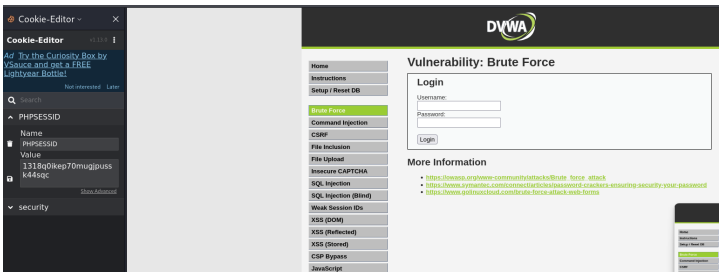

Рис. 3.4: cookie

4. Ввела в hydra запрос с нужную информацию. (рис. 3.5)

Рис. 3.5: Hydra

5. В итоге выводится результат с подходящими паролями. (рис. 3.6)

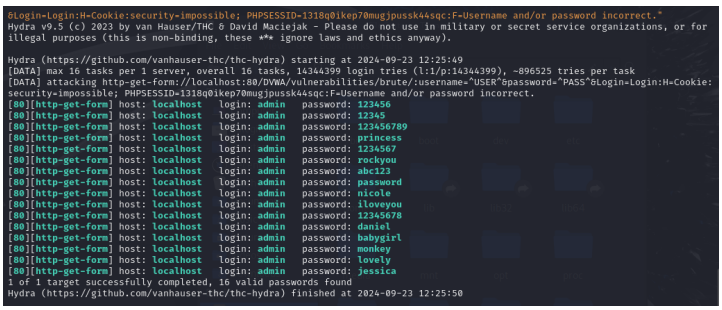

Рис. 3.6: Подходящие пароли

6. Ввела полученные данные на сайт для проверки. Получила положительный результат. (рис. 3.7)

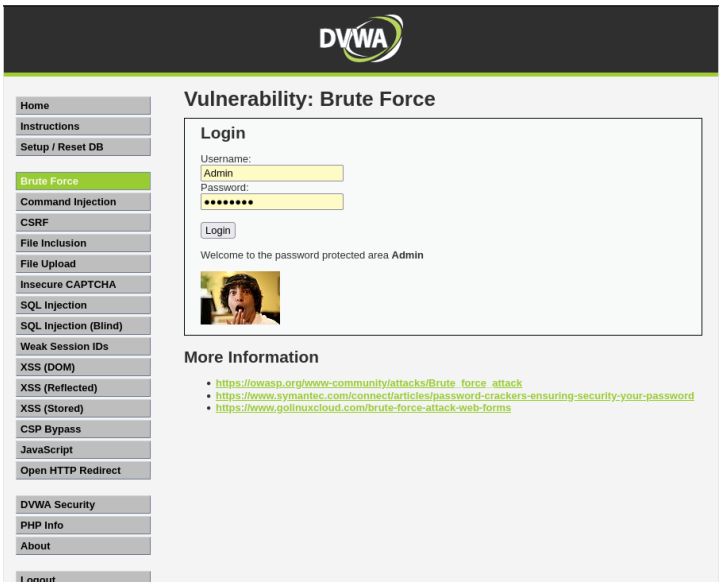

Рис. 3.7: Результат

4 Вывод

Научилась работать с hydra.