Индивидуальный проект 3

Генералов Даниил, 1032212280

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

В этом этапе индивидуального проекта требуется использовать Hydra – приложение для взлома паролей – для получения доступа к серверу DVWA.

2 Выполнение лабораторной работы

Hydra требует указания цели, а также метода, которым мы будем пробовать логин-пароль. Чтобы определить метод, мы должны сначала сделать свой запрос к веб-сервису, чтобы определить, каким образом эти данные передаются на сервер. Как видно из рис. 2.1, этот метод – это GET-запрос с аргументами в адресе.

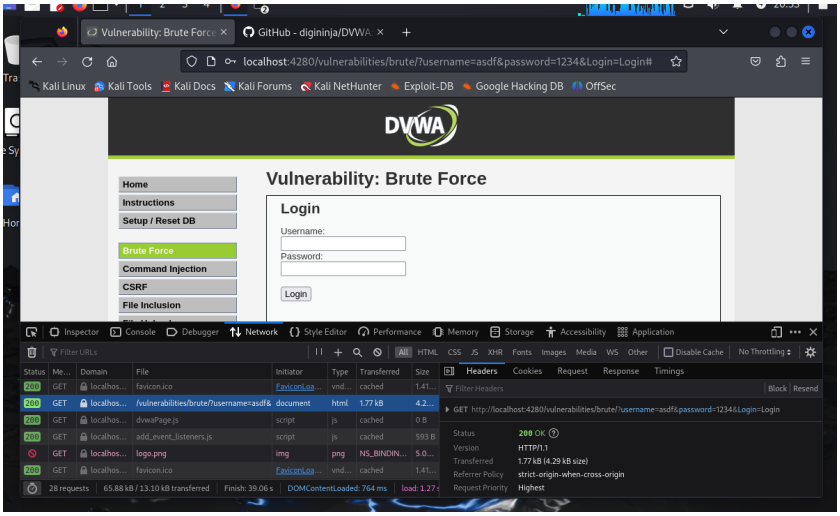

Рис. 2.1: dvwa

После этого мы формируем команду Hydra, чтобы получить доступ, на основании информации, которую мы получили в предыдущем этапе. Эта команда имеет вид:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz -o /tmp/hydra.log -f -V -s 4280
```

Как видно на рис. 2.2, мы быстро находим, что пароль для этого пользователя – `password`.

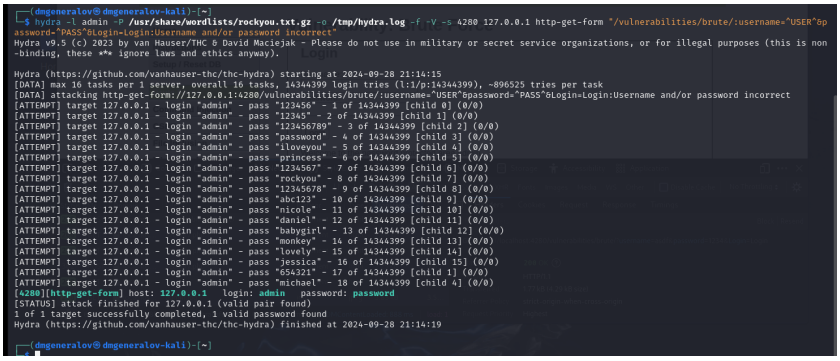

Рис. 2.2: hydra

Наконец, мы пробуем использовать этот пароль в веб-интерфейсе и получаем доступ к защищенной картинке на рис. 2.3.

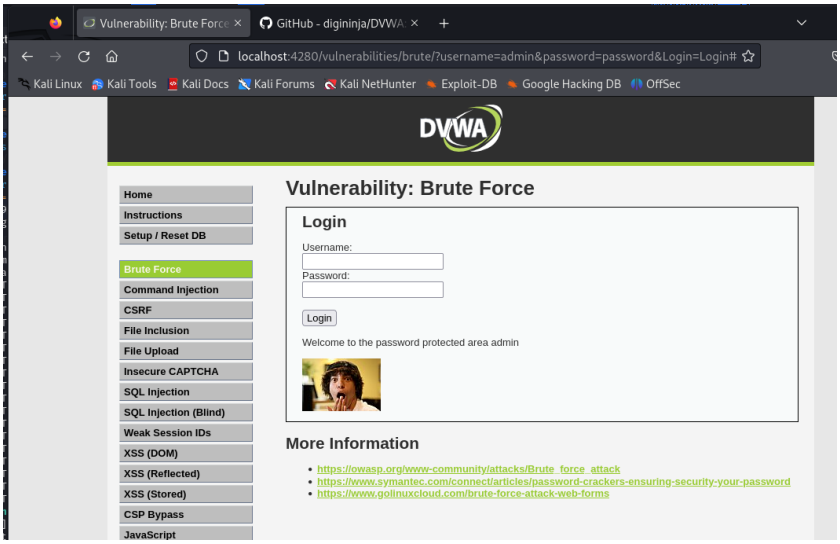

Рис. 2.3: dvwa

3 Выводы

Мы успешно использовали Hydra, чтобы эксплуатировать уязвимость, связанную с низким уровнем защиты от bruteforce и простым паролем.