Отчет по проекту

Этап 3

Легиньких Галина Андреевна

Содержание

# 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=^PASS^:Invalid username"

* 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:Invalid 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. 1) (рис. 2)

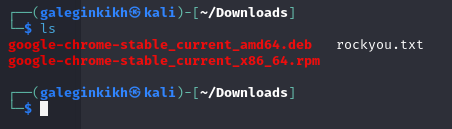


Рис. 1: Загрузки

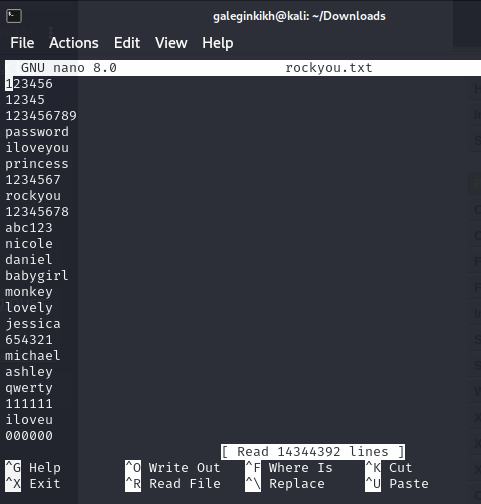


Рис. 2: Пароли

**2.** Захожу на сайт DVWA, созданный на прошлом этапе. (рис. 3)

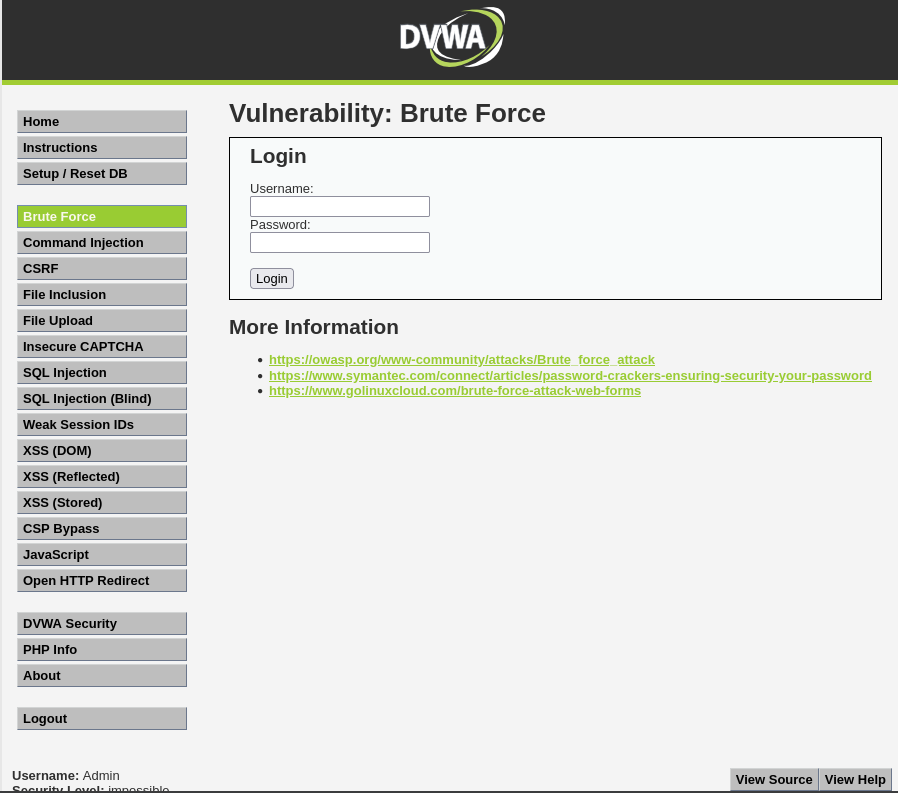


Рис. 3: DVWA

**3.** Для запроса hydra мне понадобятся параметры cookie с этого сайта. я скачала расширение для браузера. (рис. 4)

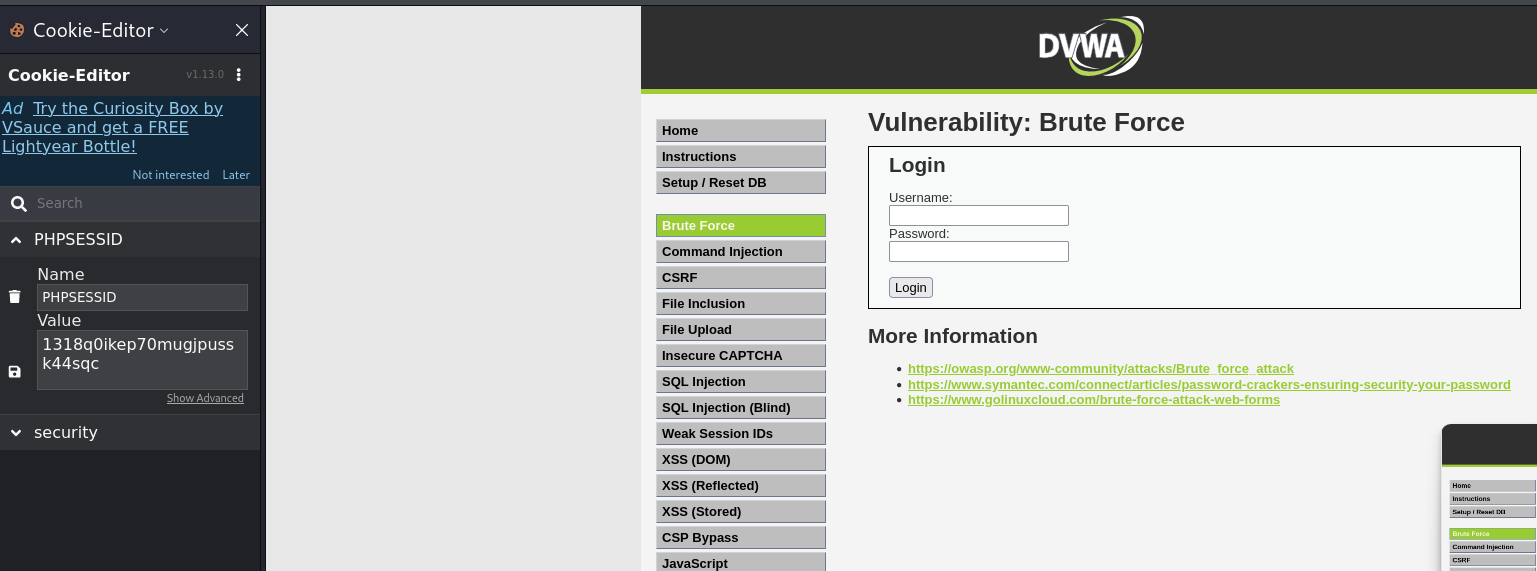


Рис. 4: cookie

**4.** Ввела в hydra запрос с нужную информацию. (рис. 5)

Рис. 5: Hydra

Рис. 5: Hydra

**5.** В итоге выводится результат с подходящими паролями. (рис. 6)

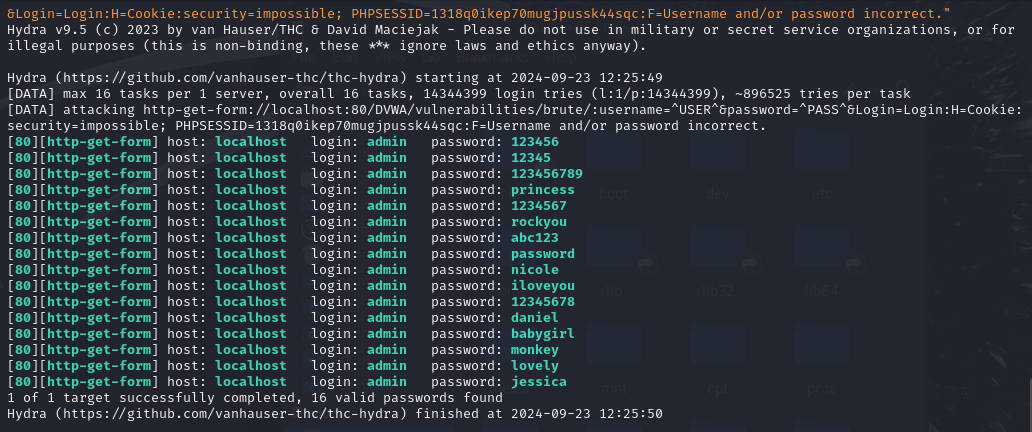


Рис. 6: Подходящие пароли

**6.** Ввела полученные данные на сайт для проверки. Получила положительный результат. (рис. 7)

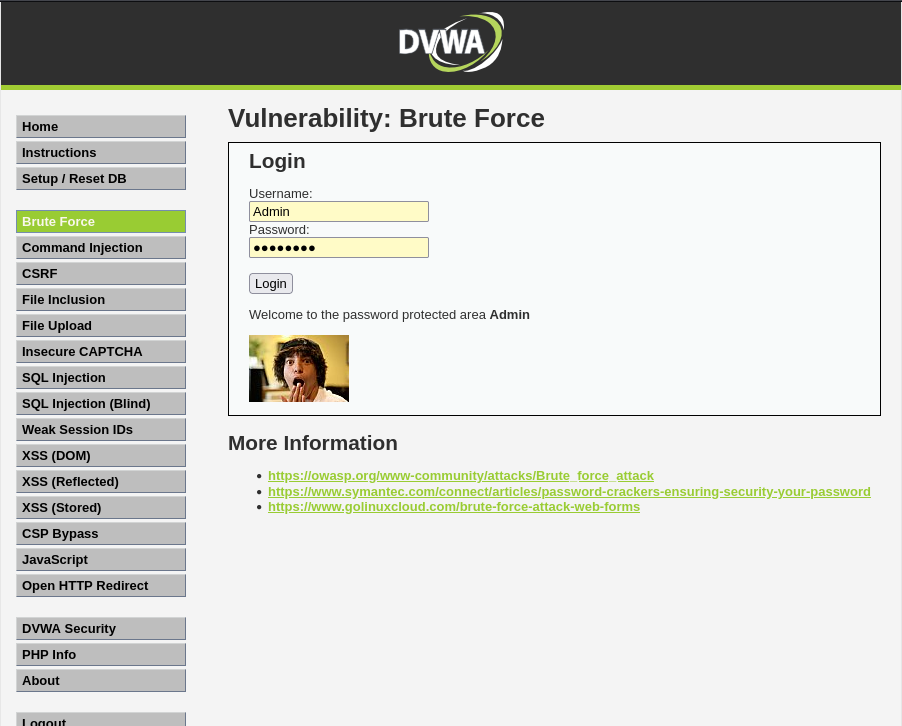


Рис. 7: Результат

# 4 Вывод

Научилась работать с hydra.