**Индивидуальный проект. Отчёт о выполнении №3**

**Информационная безопасность**

**Использование Hydra**

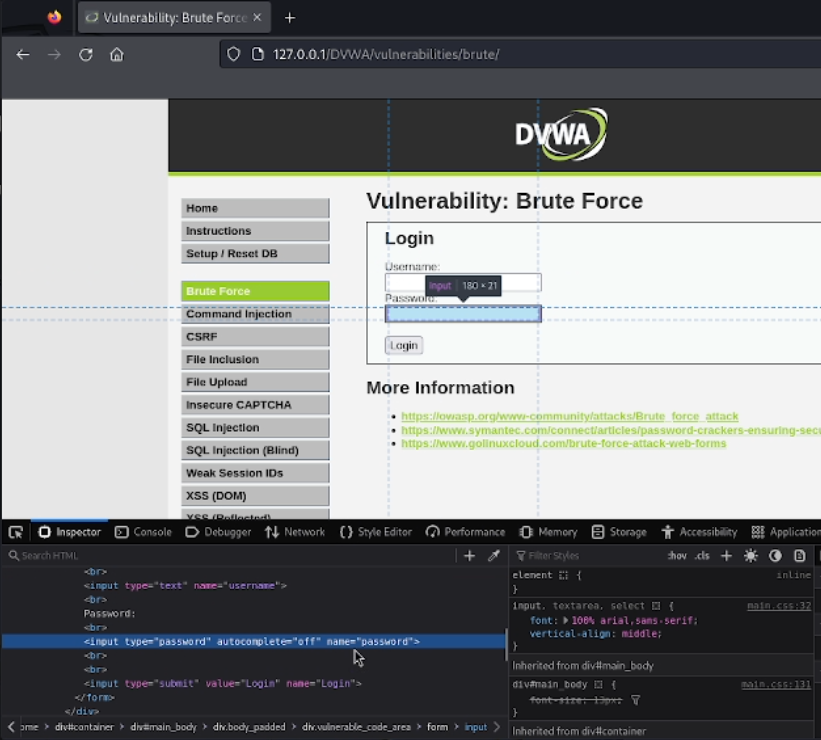
**Выполнил: Фаик Карим Яссерович**

# Цель работы

Научиться пользоваться утилитой hydra.

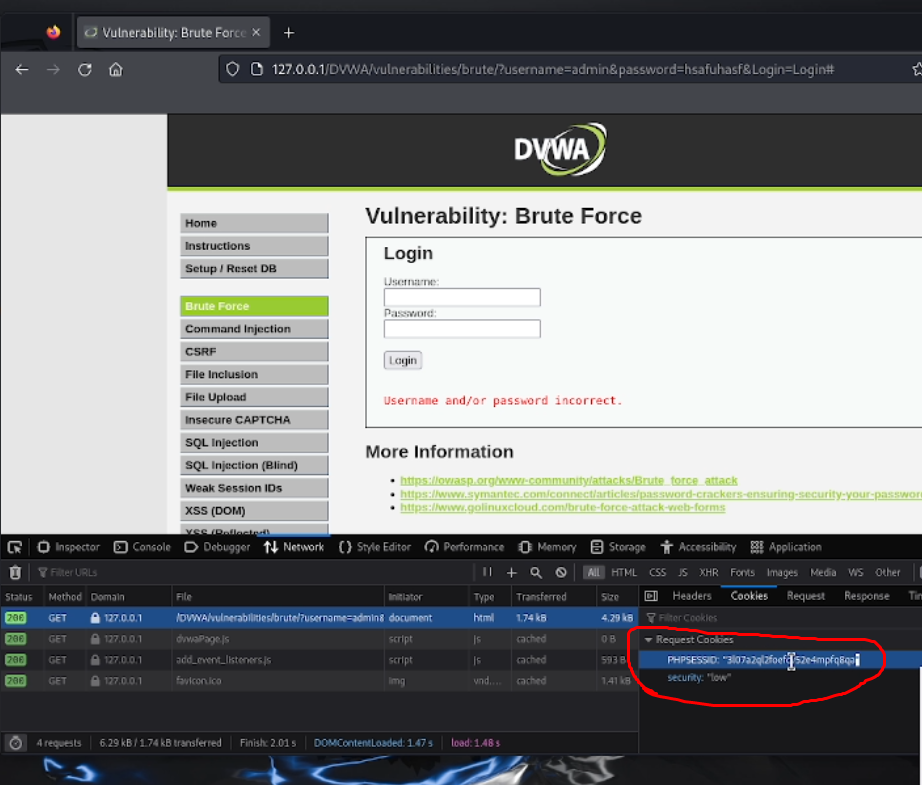
# Использование Hydra

Открываем DVWA, устанавливаем уровень сложности на low, и переходим в раздел Brute force, просматриваем код страницы. Это нужно для того чтобы определить ввод логина и пароля, для заполнения запроса при использовании hydra.



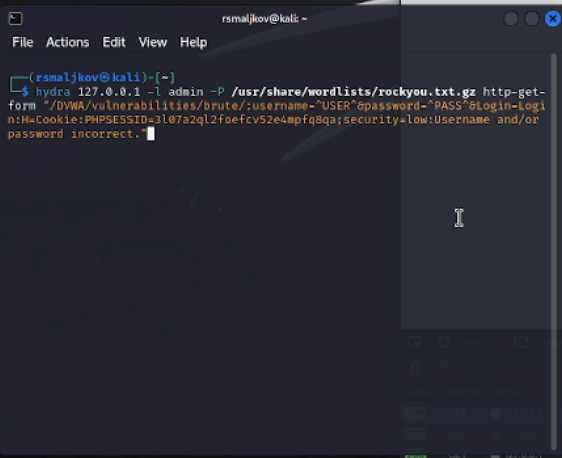
DVWA html

Введем какой либо неверный логин и пароль, а затем перейдем в раздел Network для просомтра Cookies, чтобы определить код сессии. Это нужно для того чтобы hydra могла остаться в рамках одной сессии, иначе страница будет обновляться, что приведет к исчезнвоению строки он неверно введенном пароле, по которому hydra и определяет верность ввода.



DVWA Cookies

Запрос выглядит следующим образом:



Запрос

Где первым параметром дается ip адрес, второй параметр -l admin задает логин пользователя, чей пароль мы пытаемся подобрать, -P /usr/share/wordlists/rockyou.txt.gz набор распространенных паролей, http-get-form запрос к серверу который определяется следующим оразом:

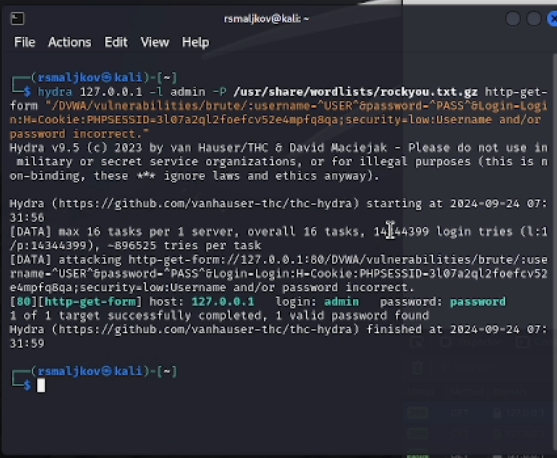
Путь к странице входа: /DVWA/valnirabilities/brute/

Тело ввода логина и пароля: username=USER&password=PASS&Login=Login

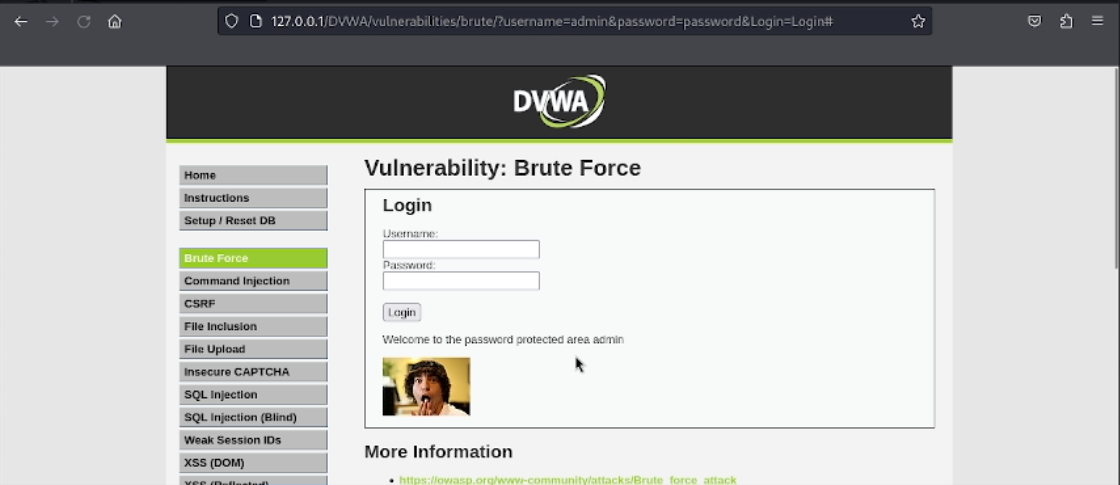
Сессия Cookie:H=Cookie:PHPSESSID=3l07a2ql2foefcv52e4mpfq8qa;security=“low”

Текст информирующий о неверном вводе пароля: Username and/or password incorrect.

Выполняем команду, получаем пароль и проверяем



Получение пароля



Успешный ввод

# Заключение

Были полученны базовые навыки работы с утилитой hydra.

# Ссылки

using Hydra on Login pages with a right method: dvwa training: https://medium.com/@hamidullahbayram/using-hydra-on-login-pages-with-a-right-method-dvwa-training-1e85e8d4f5fd

DVWA Brute Force (Hydra): https://dmcxblue.net/2018/07/11/dvwa-brute-force-hydra/

Dictionary attack na formularz HTTP POST z THC-Hydra: https://haker.edu.pl/2016/01/25/http-post-dictionary-attack-hydra/