Индивидуальный проект. Этап №3

Использование Hydra

Камкина Арина Леонидовна

Содержание

# Цель работы

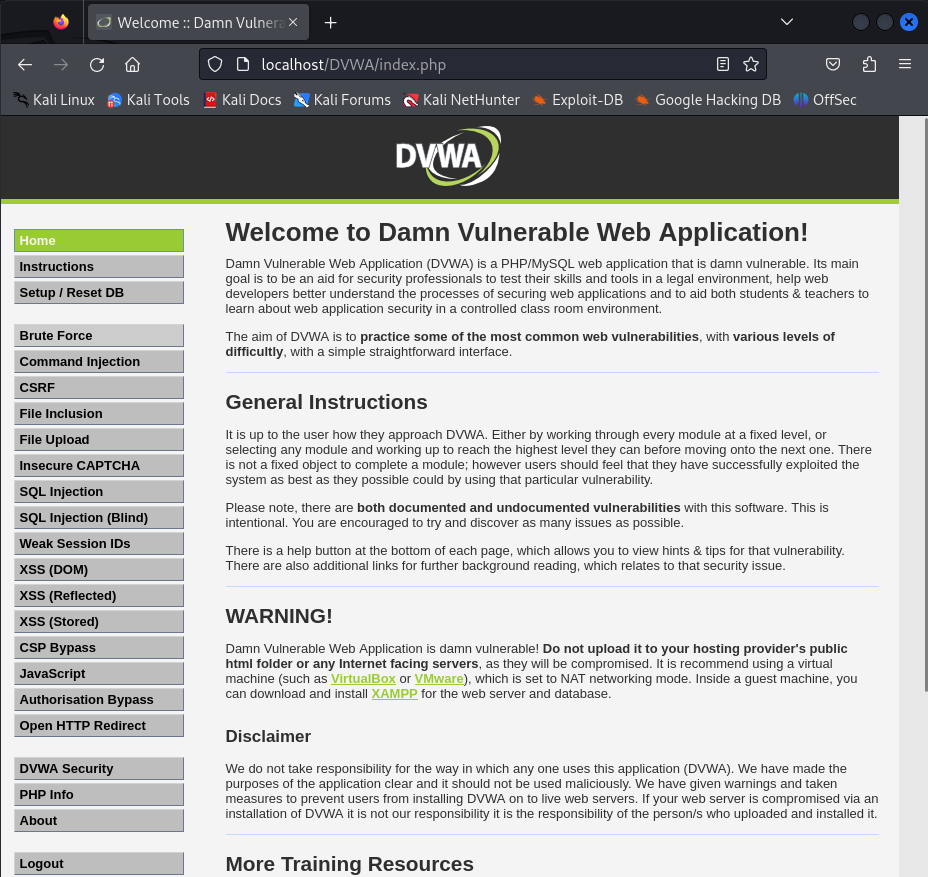
Подобрать пароль для пользователя, используя Hydra.

# Теоретические сведения

**Hydra** – это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак. Пользователь быстро и с легкостью может добавить новые модули. Hydra предоставляет специалистам в сфере ИБ возможность узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства.

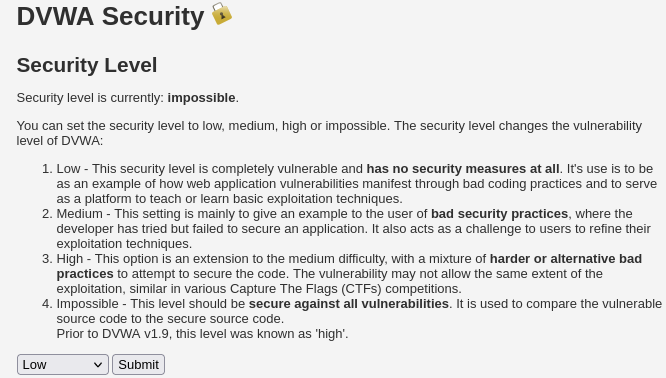
# Выполнение лабораторной работы

Перейдём на наш веб сервер DVWA(рис. [-@fig:001])



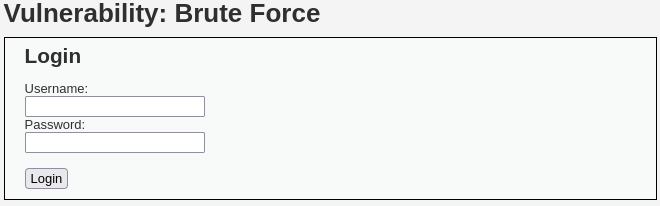
Стартовая страница

И для начала установим самый низкий уровень защиты DVWA(рис. [-@fig:002])



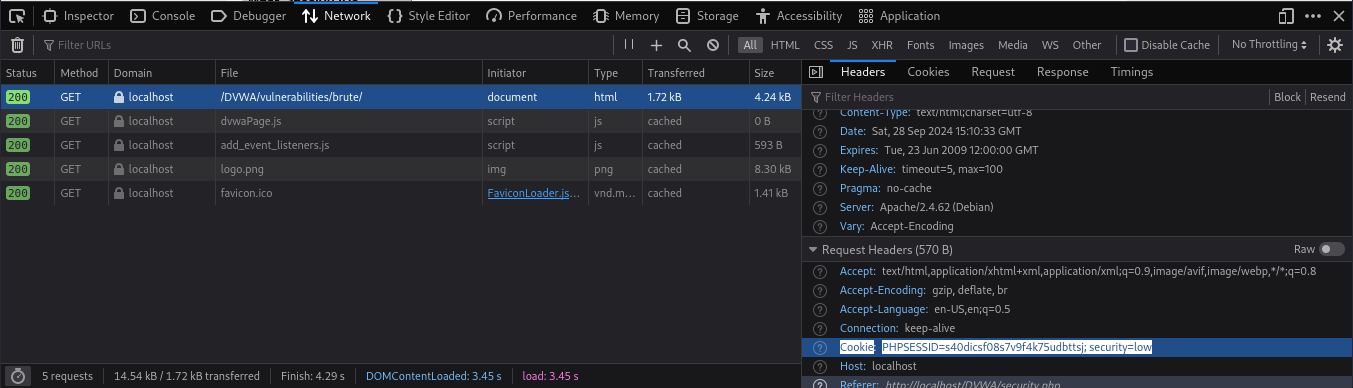
Уровень защиты

Перейдём на старницу brute force атаки - так выглядит окно для логина(рис. [-@fig:003])



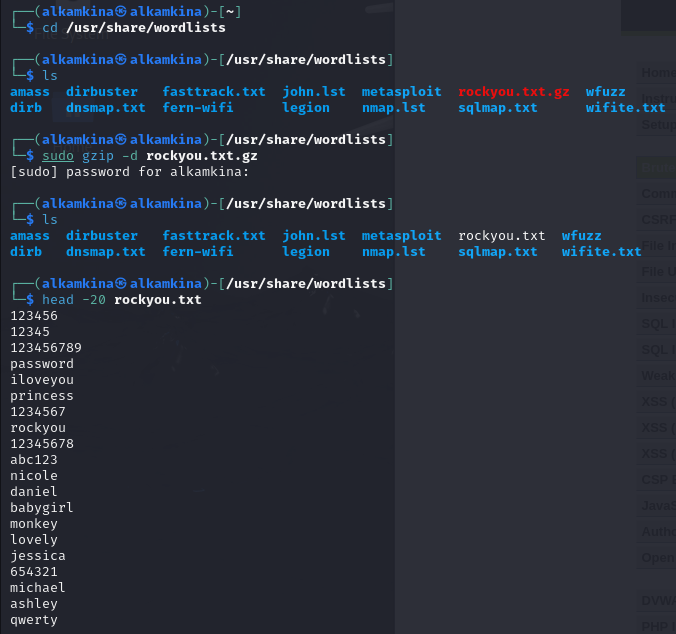
Форма для логина

Левой кнопкой мыши кликаем на экран и выбираем последний пукт - выходит следующее окно - из него берём инофрмацию по Cookies на вкладке Network(рис. [-@fig:004])



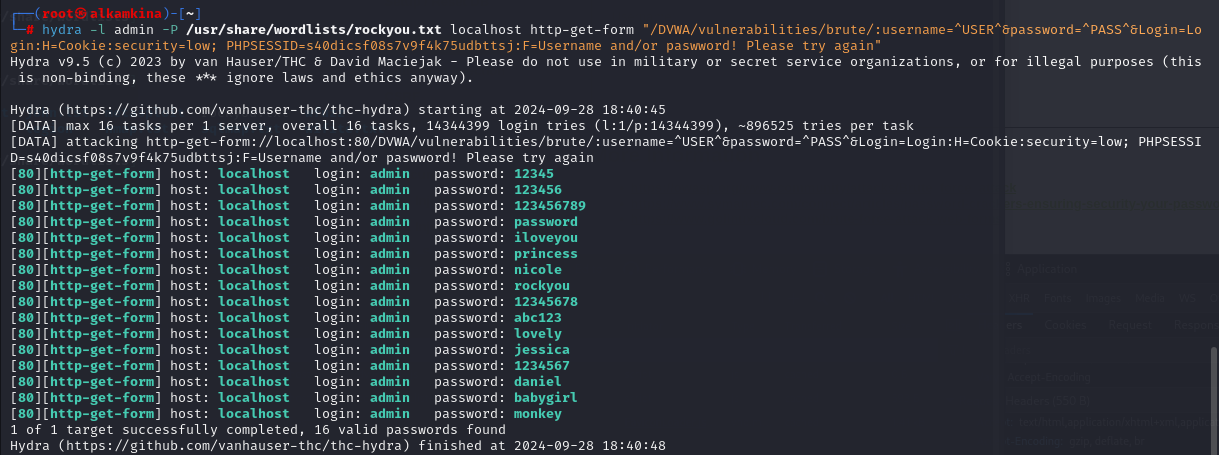
Окно Network

Распаковываем зип файл, в котором находятся все популярные пароли(рис. [-@fig:005])



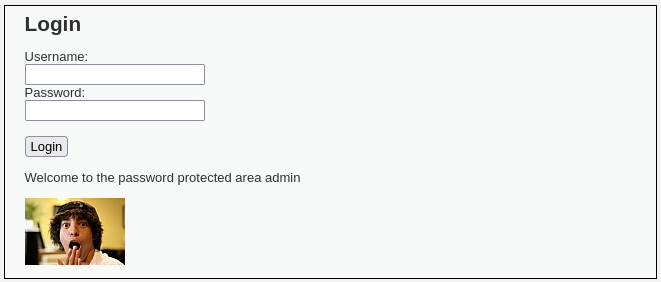
Распаковка файла

Вводим следующий запрос к Hydra и получаем пароли(рис. [-@fig:006])



Пароли

Вводим нужный логин и пароль - выходит следующее окно(рис. [-@fig:007])



Верный логин и пароль

# Вывод

В ходе выполнения работы была проведена brute force атака c помощью Hydra.