Индивидуальный проект. Этап №3

Отчёт к этапу индивидуального проекта

Зайцева Анна Дмитриевна, НПМбд-02-21

Table of Contents

# Цель работы

Цель работы — Приобретение практических навыков по использованию инструмента Hydra для брутфорса (подбора) паролей.

# Выполнение этапа индивидуального проекта

1. Для перебора поаролей мне понадобится файл, содержащий их. Например, находящийся в директории usr/share/wordlists/ в архиве rockyou.txt.gz. Скопирую архив в директорию Downloads и разархивирую его (Рис. [-@fig:001]):

Копирую архив в директорию Downloads и разархивирую его – файл с паролями

1. Открою в браузере приложение DVWA, но предварительно запущу сервисы MySQL и Apache2 (Рис. [-@fig:002]):

Запуск сервисов

1. Форма для взлома находится в разделе Brute Force (Рис. [-@fig:003]):

Форма для брут-форса

В форме есть два тега: input с атрибутами name, равными ‘username’ и ‘password’ соответственно.

1. Также мне понадобятся фрагменты-cookie приложения. Это PHPSESSID и security (Рис. [-@fig:004]):

Фрагменты-cookie

1. Воспользовалась утилитой hydra, введя следующую команду:

hydra -l <login> -P <path\_to\_file> -s <port> <host> http-<method>-form "<url>:username=^USER^&password=^PASS^&Login=Login:H=Cookie:<key=value>;<key=value>:F=<error\_message>"

где \* login - логин для авторизации (в нашем случае admin) \* path\_to\_file - путь до файла с паролями (в нашем случае ~/Downloads/rockyou.txt) \* port - порт, по которому доступно приложение (в нашем случае 80) \* host - домен или ip приложения (в нашем случае localhost) \* method - метод запроса (в нашем случае get) \* url - адрес относительно корня сайта (в нашем случае /DVWA/vulnerabilities/brute/) \* key=value - имена и значения cookie-переменных (в нашем случае PHPSESSID и security) \* error\_message - сообщение, выводимое при неверных логине и пароле (в нашем случае Username and/or password incorrect.)

Итоговая команда имеет следующие опции:

hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium;PHPSESSID=of74bg222ffc6vigcsjfqbvhq7:F=Username and/or password incorrect."

1. Утилита подобрала данные для ввода (Рис. [-@fig:005]):

Данные найдены

1. Ввела данные в соответствующее поле. Операция прошла успешно (Рис. [-@fig:006]):

Успешная авторизация

# Вывод

Приобрела практический навык по использованию инструмента Hydra для брутфорса (подбора) паролей.

# Библиография

* https://github.com/digininja/DVWA?tab=readme-ov-file
* https://www.kali.org/
* https://spy-soft.net/rockyou-txt/
* https://losst.pro/kak-polzovatsya-hydra#perebor-parolya-autentifikcii-http