**Отчет по третьему этапу индивидуального проекта**

**Основы информационной безопасности**

Авдадаев Джамал, НКАбд-01-23

Содержание

[1 Цель работы 1](#_Toc2973)

[2 Задание 1](#_Toc2974)

[3 Теоретическое введение 1](#_Toc2975)

[4 Выполнение лабораторной работы 2](#_Toc2976)

[5 Выводы 4](#_Toc2977)

[Список литературы 4](#_Toc2978)

# Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

# Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

# Теоретическое введение

* Hydra используется для подбора или взлома имени пользователя и пароля.
* Поддерживает подбор для большого набора приложений [3].

**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 неудачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.
* Запрос к Hydra будет выглядеть примерно так:

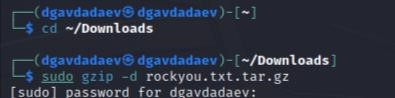
hydra -l root -P ~/pass\_lists/dedik\_passes.txt -o ./hydra\_result.log -f -V -s 80

178.72.90.181 http-post-form "/cgibin/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 /cgibin/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).

# Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей rockyou.txt для kali linux (рис. 1).



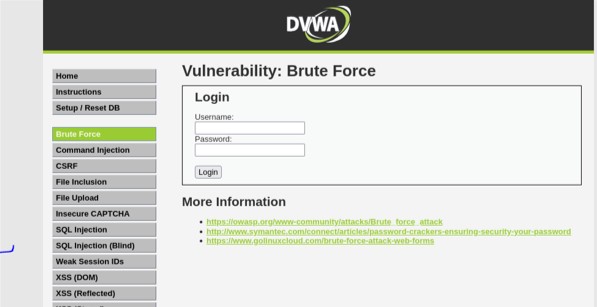
*Распаковка архива со списком паролей*

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта (рис. 2).



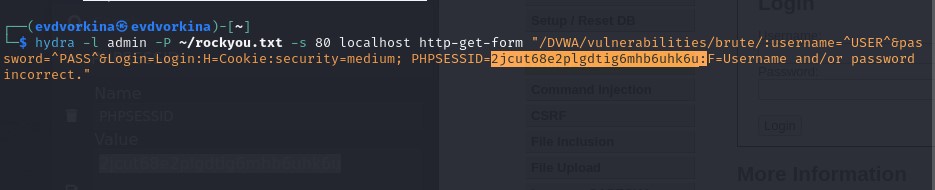
*Сайт, с которого получаем информацию о параметрах Cookie*

Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера [4], теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).



*Информация о параметрах Cookie*

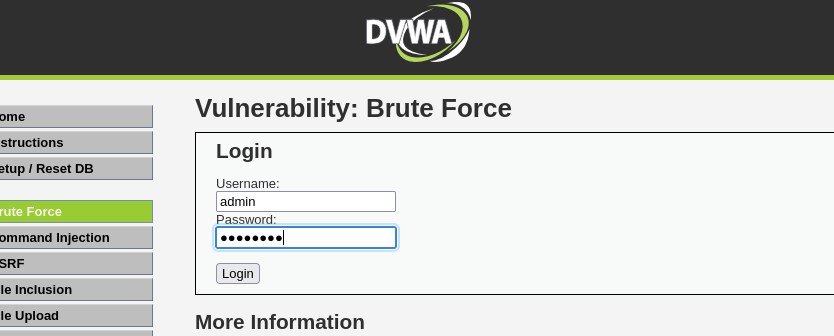
Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).



*Запрос Hydra*

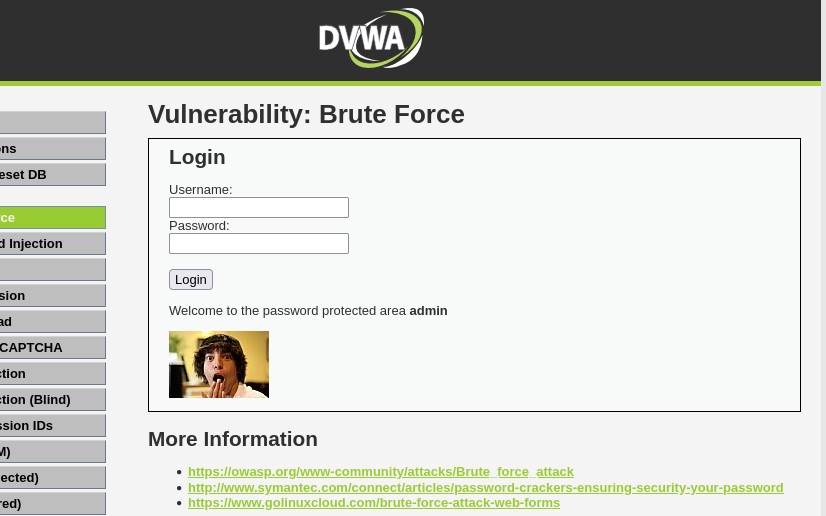
*Результат запроса*

Вводим полученные данные на сайт для проверки (рис. 5).



*Ввод полученного результата в уязвимую форму*

Получаем положительный результат проверки пароля. Все сделано верно (рис. 6).



*Результат*

# Выводы

Приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей

# Список литературы

1. How to Brute Force Attack on Web Forms? [Step-by-Step] [Электронный ресурс]. URL: [https://www.golinuxcloud.com/brute-force-attack-web-forms/.](https://www.golinuxcloud.com/brute-force-attack-web-forms/)
2. Brute Force Attack [Электронный ресурс]. URL: [https://owasp.org/wwwcommunity/attacks/Brute\_force\_attack.](https://owasp.org/www-community/attacks/Brute_force_attack)
3. Ш. Парасрам Т.Х.и.др. А. Замм. Kali Linux: Тестирование на проникновение и безопасность: для профессионалов. Питер, 2022. 448 с.
4. Cookie-Editor [Электронный ресурс]. URL: [https://addons.mozilla.org/enUS/firefox/addon/cookie-editor/?utm\_campaign=external-cookie-editor.com.](https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/?utm_campaign=external-cookie-editor.com)