

# **Отчет по третьему этапу индивидуального проекта**

**Основы информационной безопасности**

Дворкина Ева, НКАбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>12</b>
	<b>Список литературы</b>	<b>13</b>

## Список иллюстраций

4.1	Распаковка архива 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 [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 "/cgi-bin/luci:username=^USER^&password=^P  
username"
```

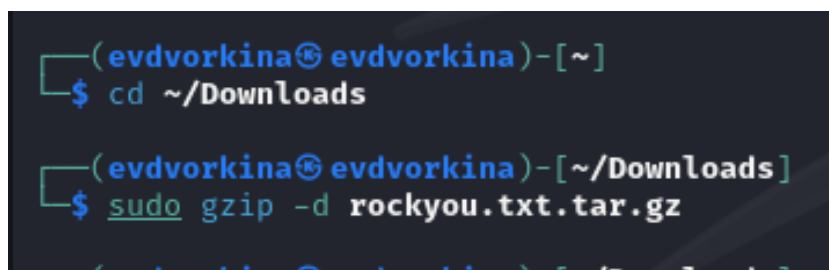
- Используется `http-post-form` потому, что авторизация происходит по http методом `post`.
- После указания этого модуля идёт строка `/cgi-bin/luci:username=USER&password=PASS:Invalid username`, у которой через двоеточие (:) указывается:

- путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);
- строка, которая передаётся методом POST, в которой логин и пароль заменены на <sup>USER</sup> и <sup>PASS</sup> соответственно (username=<sup>USER</sup>&password=<sup>PASS</sup>);
- 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 часто-используемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей `rockyou.txt` для kali linux (рис. 1).



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

Рис. 4.1: 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).

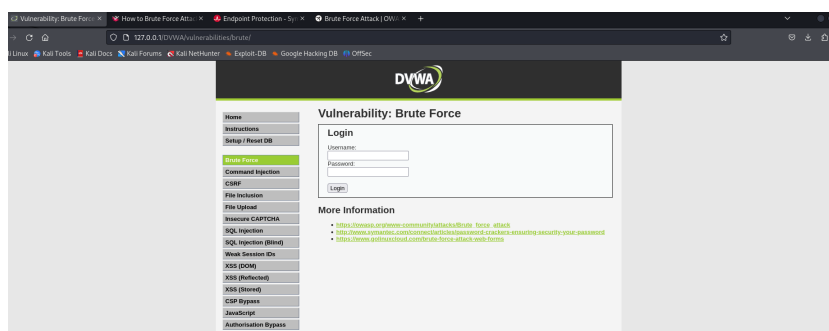


Рис. 4.2: Сайт, с которого получаем информацию о параметрах Cookie

Чтобы получить информацию о параметрах cookie я установила соответству-

ющее расширение для браузера [4], теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).

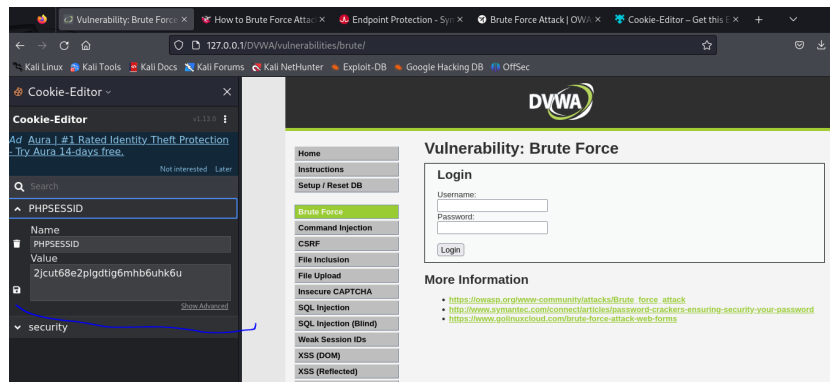


Рис. 4.3: Информация о параметрах Cookie

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).

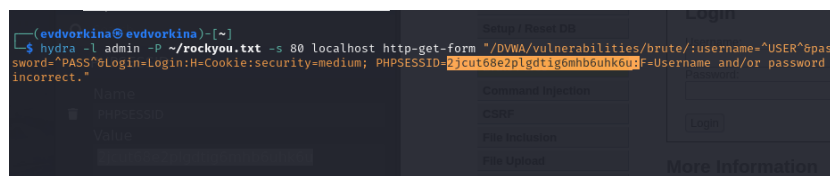


Рис. 4.4: Запрос Hydra

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

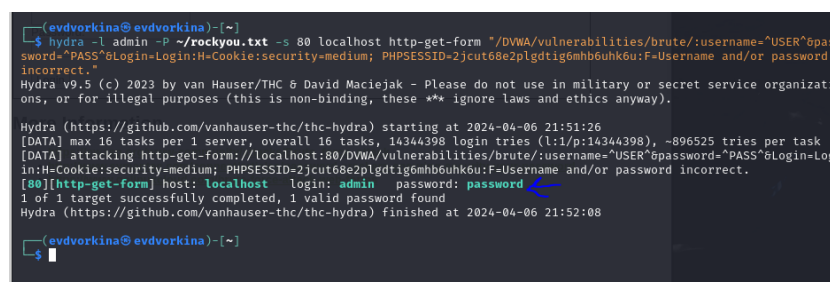
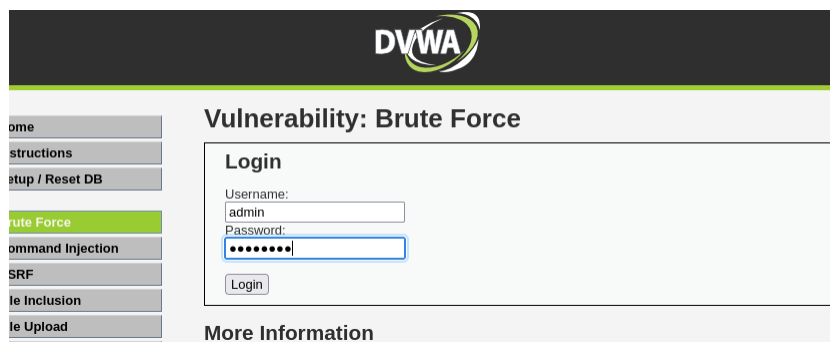


Рис. 4.5: Результат запроса

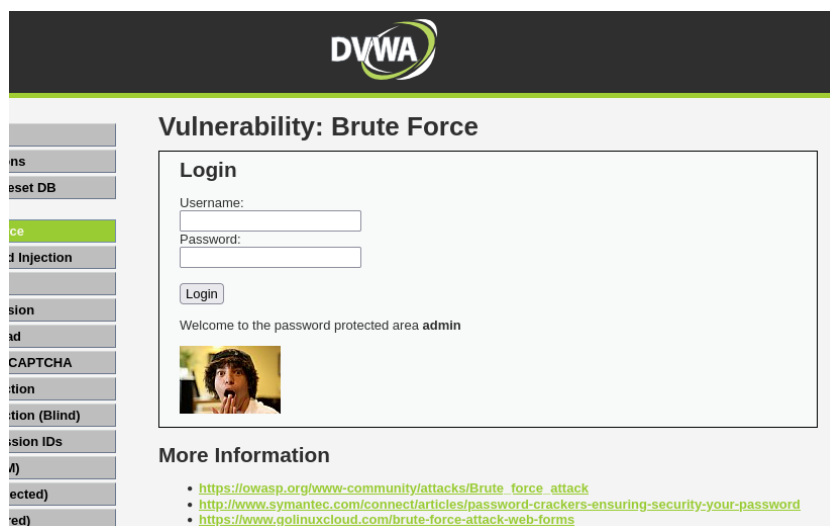
Вводим полученные данные на сайт для проверки (рис. 6).



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top header features the DVWA logo. On the left, a sidebar contains a list of vulnerability categories: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, SRF, File Inclusion, and File Upload. The main content area is titled 'Vulnerability: Brute Force'. It contains a 'Login' form with two input fields: 'Username:' with the value 'admin' and 'Password:' with masked characters '\*\*\*\*\*'. A 'Login' button is positioned below the password field. Below the login form, there is a section titled 'More Information'.

Рис. 4.6: Ввод полученного результата в уязвимую форму

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



The screenshot shows the DVWA interface after a successful login. The sidebar on the left is the same as in the previous image. The main content area is still titled 'Vulnerability: Brute Force'. The 'Login' form now has empty input fields for 'Username:' and 'Password:'. Below the form, a 'Login' button is present. A message reads: 'Welcome to the password protected area admin'. Below this message is a small image of a person with a surprised expression. At the bottom, the 'More Information' section lists three links: [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack), <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

Рис. 4.7: Результат

## 5 Выводы

Приобрела 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/>.
2. Brute Force Attack [Электронный ресурс]. URL: [https://owasp.org/www-community/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/en-US/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).