

## Correction du challenge 053 BillCipher

Pour rappel :

Voici les commandes à effectuer lors de la configuration :

```
ubuntu@ubuntuVM:~/Documents/Projet/challenge_billcipher$ docker-compose build
challenge_053-syd-academy-billcipher uses an image, skipping
ubuntu@ubuntuVM:~/Documents/Projet/challenge_billcipher$ docker-compose up -d
Creating challenge_053-syd-academy-billcipher ... done
ubuntu@ubuntuVM:~/Documents/Projet/challenge_billcipher$ docker exec -ti challenge_053-syd-academy-billcipher /bin/bash
root@dfbdd492cf3d:/BillCipher#
```

Pour lancer l'outil, on utilise la commande suivante : `python3 billcipher.py`

On doit obtenir ceci :

```
#####          #####  
#   #   #       #   #   #   #####   #   #   #####   #####  
#   #   #       #   #   #   #   #   #   #   #   #   #  
#####   #   #   #   #   #   #   #   #####   #####   #  
#   #   #       #   #   #   #####   #   #   #####  
#   #   #       #   #   #   #   #   #   #   #   #   #  
#####   #   #   #       #   #   #   #   #   #   #   #  
#####   #   #####   #####   #####   #   #   #   #####   #   #   2.1  
Information Gathering tool for a Website or IP address
```

Are you want to collect information of website or IP address? [web]

On tape : Website puis on renseigne le nom du site → [sydacademy.secyourdev.com](https://sydacademy.secyourdev.com)

On obtient le menu suivant :

```
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: syd-academy.secyourdev.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)
```

But du Challenge BillCipher : Collecter un maximum d'informations et répondre aux questions suivantes.

1. Quelle site avez-vous renseigné ?

→ syd-academy/secyourdev.com

2. Combien d'options de scans sont disponibles dans l'outil BillCipher ?

```
1) DNS Lookup          13) Host DNS Finder
2) Whois Lookup        14) Reserve IP Lookup
3) GeoIP Lookup         15) Email Gathering (use Infoga)
4) Subnet Lookup        16) Subdomain listing (use Sublist3r)
5) Port Scanner         17) Find Admin login site (use Breacher)
6) Page Links           18) Check and Bypass CloudFlare (use HatCloud)
7) Zone Transfer        19) Website Copier (use httrack)
8) HTTP Header          20) Host Info Scanner (use WhatWeb)
9) Host Finder          21) About BillCipher
10) IP-Locator          22) Fuck Out Of Here (Exit)
11) Find Shared DNS Servers
12) Get Robots.txt
```

→ 20

Pour les 2 questions suivantes :

```
What information would you like to collect? (1-20): 1
A : 185.190.142.131
MX : 10 mx01.ionos.fr.
MX : 10 mx00.ionos.fr.
```

3. Trouvez-vous des enregistrements DNS (oui/non) du site ?

→ oui.

4. Quel est le premier enregistrement DNS de type MX ?

→ 10 mx01.ionos.fr.

Pour les 3 questions suivantes :

```
What information would you like to collect? (1-20): 3
IP Address: 185.190.142.131
Country: Germany
State: Bavaria
City: Nuremberg
Latitude: 49.4527
Longitude: 11.0783
```

5. Quelle est son adresse IP ?

→ 185.190.142.131

6. Dans quel pays se situe cette adresse IP ?

→ germany

7. Position en latitude ?

→ 49.4527

8. Masque de sous-réseau ?

```
What information would you like to collect? (1-20): 4
Address      = 185.190.142.131
Network      = 185.190.142.131 / 32
Netmask      = 255.255.255.255
Broadcast    = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
Hosts Bits   = 0
Max. Hosts   = 1    (2^0 - 0)
Host Range   = { 185.190.142.131 - 185.190.142.131 }
```

→ 255.255.255.255

9. Existe-t-il sur le site des liens vers des ressources externes ? (indiquer oui/non)

```
What information would you like to collect? (1-20): 6
error getting links
```

→ error getting links

Pour les 3 questions suivantes :

```
What information would you like to collect? (1-20): 8
HTTP/1.1 301 Moved Permanently
Server: nginx/1.23.0
Date: Mon, 10 Apr 2023 13:23:03 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: https://syd-academy.secyourdev.com/

HTTP/1.1 200 OK
Server: nginx/1.23.0
Date: Mon, 10 Apr 2023 13:23:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: PHPSESSID=96e02606cabb9540968495f9df833245; expires=Mon, 10-Apr-2023 14:23:04 GMT; Max-Age=3600; path=/; HttpOnly; SameSite=Strict; Secure
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'self'; font-src 'self'; connect-src 'self'; img-src 'self'; style-src 'self'; frame-ancestors 'self'; form-action 'self';
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Permissions-Policy: accelerometer=(), geolocation=('self'), fullscreen=(), ambient-light-sensor=(), autoplay=(), battery=(), camera=(), display-capture=('self')
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

10. Quel type de serveur est utilisé ?

→ nginx

11. Sa version ?

→ 1.23.0

12. Quel est le type de contenu sur le site (content-type) ?

→ text/html

Cette réponse donne le flag : billchallenge

Il sera utilisé pour répondre à la dernière question.

Du côté utilisateur, il devrait se retrouver avec la fenêtre suivante :

*Attention ! Vous ne pouvez utiliser les outils de scan à l'infini. Vous avez maximum 15 essais par jour.*

**Veuillez répondre aux questions suivantes :**

[Indice](#)

1. Quelle site avez-vous renseignée ?  [Valider la réponse](#)

Bonne réponse !

2. Combien d'options de scan sont disponibles dans l'outil BillCipher ?  [Valider la réponse](#)

Bonne réponse !

3. Trouvez-vous des engistements DNS (oui/non) du site ?  [Valider la réponse](#)

Bonne réponse !

4. Quel est le premier enregistrement DNS de type MX ?  [Valider la réponse](#)

Bonne réponse !

5. Quelle est son adresse IP ?  [Valider la réponse](#)

Bonne réponse !

6. Dans quel pays se situe cette adresse IP ?  [Valider la réponse](#)

Bonne réponse !

7. Position en latitude ?  [Valider la réponse](#)

Bonne réponse !

8. Masque de sous-réseau ?  [Valider la réponse](#)

Bonne réponse !

9. Existe-t-il sur le site des liens vers des ressources externes ? (indiquer le message obtenu)  [Valider la réponse](#)

Bonne réponse !

10. Quelle type de serveur est utilisé ?  [Valider la réponse](#)

Bonne réponse !

11. Sa version ?  [Valider la réponse](#)

Bonne réponse !

12. Quel est le type de contenu sur le site (content-type) ?  [Valider la réponse](#)

Bonne réponse ! flag : billchallenge

Pour valider ce tutoriel, veuillez entrer le flag trouvé dans la réponse de la dernière question.

Validation Challenge BillCipher ?  [Valider la réponse](#)

Félicitations !!! Vous venez de finir le Challenge 053 BillCipher.