Diana Margarian

TP Chocolatein

Question 1 : Expliquer pourquoi l'hébergeur a pu ne pas donner son accord ?

→ L'hébergeur pourrait refuser pour diverses raisons :

- Risque d'attaque pendant les tests
- Pour protéger ses machines contre tout impact potentiel

Question 2 : A quoi l'équipe technique a-t' elle du veiller pour construire la plateforme de test simulant les serveurs de l'hébergeur ?

→L'équipe technique a du vérifier que le service web fonctionnait correctement et que chaque machine était connecter à tous les réseaux.

Tests de connectivité.

Depuis sweb-chocolatein :

```
sio@sweb-mutualise-chocolatein:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=48.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=48.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 48.210/48.457/48.704/0.247 ms
```

```
sio@sweb-mutualise-chocolatein:~$ ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=0.426 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.399 ms
^C
--- 10.0.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 32ms
rtt min/avg/max/mdev = 0.399/0.412/0.426/0.024 ms
```

```
sio@sweb-mutualise-chocolatein:~$ ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.531 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.957 ms
^C
--- 172.16.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 0.531/0.744/0.957/0.213 ms
sio@sweb-mutualise-chocolatein:~$
```

Depuis sbdd-chocolatein :

```
sio@sbdd-chocolatein:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=77.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=153 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=101 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 77.749/110.719/153.232/31.548 ms
```

```
sio@sbdd-chocolatein:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.897 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.435 ms
^C
--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 0.435/0.666/0.897/0.231 ms
```

```
sio@sbdd-chocolatein:~$ ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.528 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.707 ms
^C
--- 172.16.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 25ms
rtt min/avg/max/mdev = 0.528/0.617/0.707/0.092 ms
sio@sbdd-chocolatein:~$
```

B. Procédure d’installation de Kali dans le réseau LAN.

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:1b:be:da brd ff:ff:ff:ff:ff:ff
    inet 172.16.95.192/16 brd 172.16.255.255 scope global dynamic noprefixrou
te eth0
       valid_lft 6070sec preferred_lft 6070sec
    inet6 fe80::bfe0:122a:b754:5949/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

→ ***Tests de connectivité.***

Depuis la machine kali :

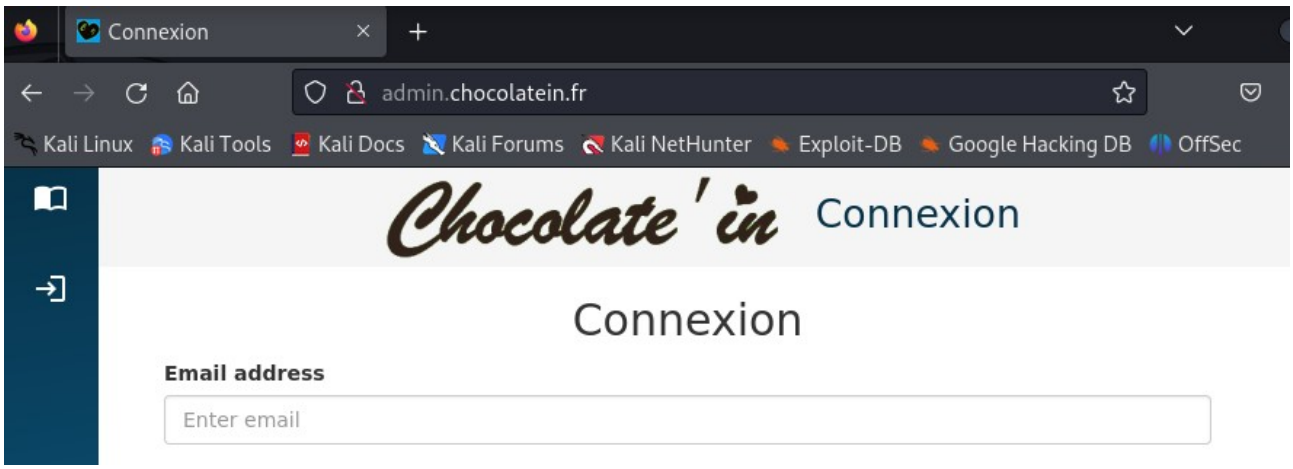
```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=59.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=60.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=41.6 ms
^C
── 8.8.8.8 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 41.591/53.776/60.179/8.620 ms
```

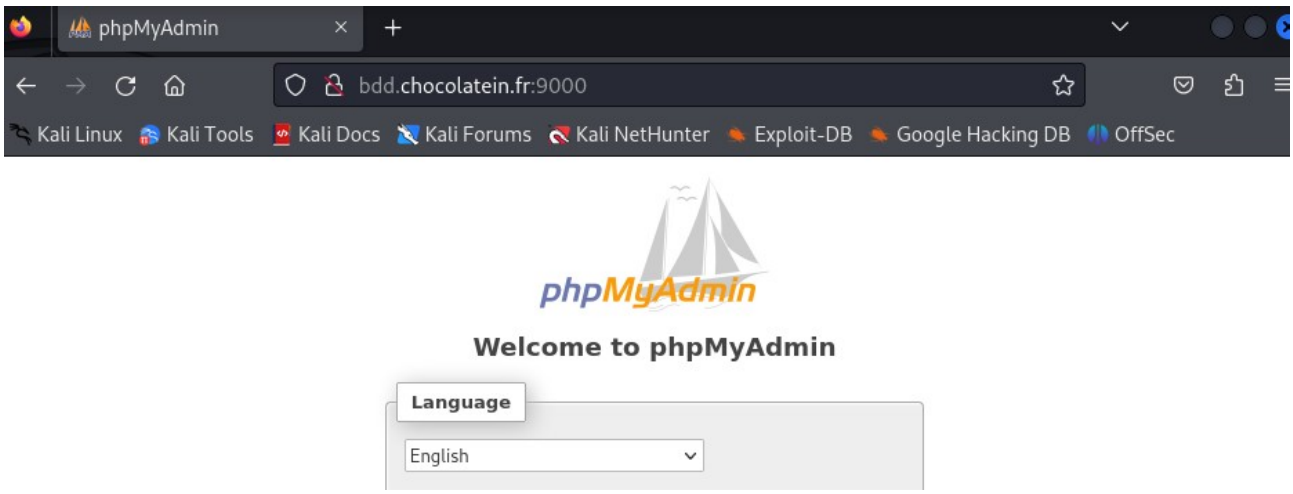
```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=1.23 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=63 time=1.56 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=63 time=2.10 ms
^C
── 10.0.0.2 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.232/1.627/2.095/0.355 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=63 time=0.931 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=63 time=1.51 ms
^C
── 10.0.0.4 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.931/1.220/1.509/0.289 ms
```

```
┌──(kali㉿kali)-[~]
└─$ ping chocolatein.fr
PING chocolatein.fr (10.0.0.2) 56(84) bytes of data.
64 bytes from admin.chocolatein.fr (10.0.0.2): icmp_seq=1 ttl=63 time=1.09 ms
64 bytes from admin.chocolatein.fr (10.0.0.2): icmp_seq=2 ttl=63 time=1.17 ms
64 bytes from admin.chocolatein.fr (10.0.0.2): icmp_seq=3 ttl=63 time=1.61 ms
^C
── chocolatein.fr ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 1.086/1.286/1.607/0.228 ms
```

Affichage des pages :

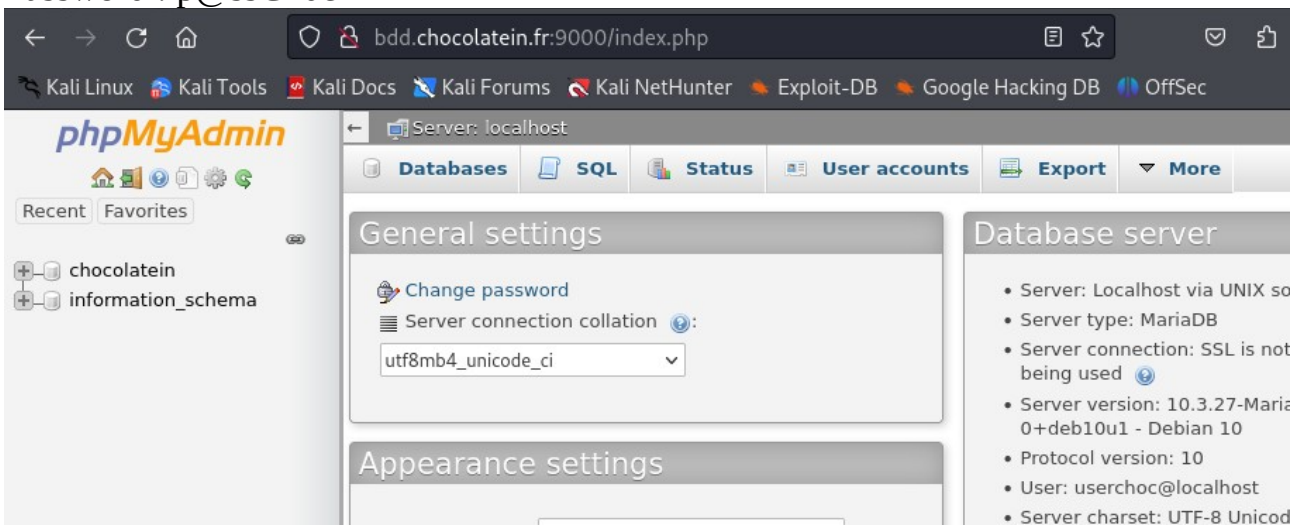




→ ***Accès à la base de données :***

Question 3 : Recopiez les informations permettant l'accès aux bases de données et vérifiez l'accès depuis bdd.chocolatein.fr aux données.

Login : userchoc
Password : p@ssCh0c



→ ***Accès au code des 2 applications.***

Commandes à effectuer pour installer Filezilla client :

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] Mot de passe de kali :
Désolé, essayez de nouveau.
[sudo] Mot de passe de kali :
Réception de :1 http://archive-4.kali.org/kali kali-rolling InRelease [41,5 k
B]
Réception de :2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packag
es [19,5 MB]
Réception de :3 http://archive-4.kali.org/kali kali-rolling/main amd64 Conten
ts (deb) [45,9 MB]
Réception de :4 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Pac
kages [116 kB]
Réception de :5 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Con
tents (deb) [247 kB]
Réception de :6 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Pa
ckages [193 kB]
Réception de :7 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Co
ntents (deb) [884 kB]
Réception de :8 http://archive-4.kali.org/kali kali-rolling/non-free-firmware
 amd64 Packages [33,1 kB]
Réception de :9 http://archive-4.kali.org/kali kali-rolling/non-free-firmware
 amd64 Contents (deb) [16,9 kB]
67,0 Mo réceptionnés en 52s (1 287 ko/s)
Lecture des listes de paquets ... Fait
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update --fix-missing
Atteint :1 http://http.kali.org/kali kali-rolling InRelease
Lecture des listes de paquets ... Fait
```

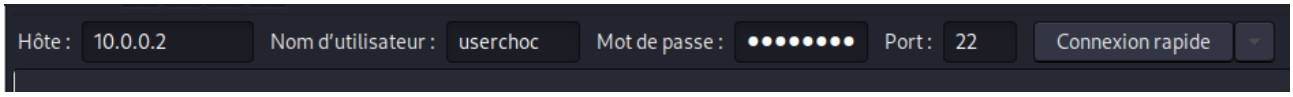
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install filezilla
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus néces
aires :
  libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev
  libopenblas0 libpython3-all-dev libpython3.12 libpython3.12-dev
  libxsimd-dev python3-all-dev python3-beniget python3-gast python3-pythran
  python3.12-dev xtl-dev
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  filezilla-common libfilezilla-common libfilezilla42 libpcre2-32-0
  libpugixml1v5 libwxbase3.2-1 libwxgtk3.2-1
Les NOUVEAUX paquets suivants seront installés :
  filezilla filezilla-common libfilezilla-common libfilezilla42
  libpcre2-32-0 libpugixml1v5 libwxbase3.2-1 libwxgtk3.2-1
0 mis à jour, 8 nouvellement installés, 0 à enlever et 228 non mis à jour.
Il est nécessaire de prendre 10,7 Mo dans les archives.
Après cette opération, 43,4 Mo d'espace disque supplémentaires seront utilis
s.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive-4.kali.org/kali kali-rolling/main amd64 filez
lla-common all 3.66.5-2 [2 312 kB]
Réception de :6 http://http.kali.org/kali kali-rolling/main amd64 libwxbase3
2-1 amd64 3.2.4+dfsg-3 [1 011 kB]
```

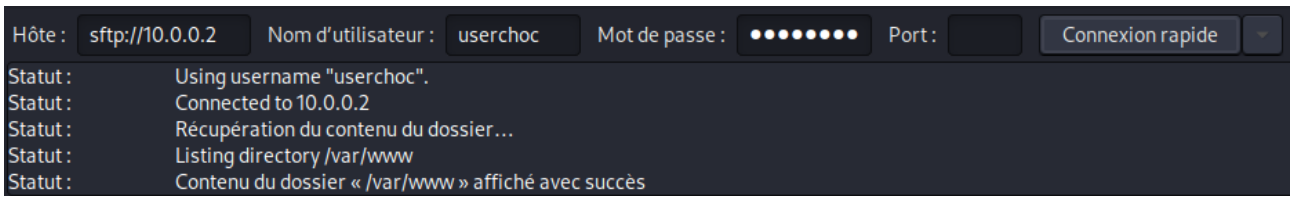
Question 4 : Recopiez les informations permettant l'accès en ssh au code des 2 sites.

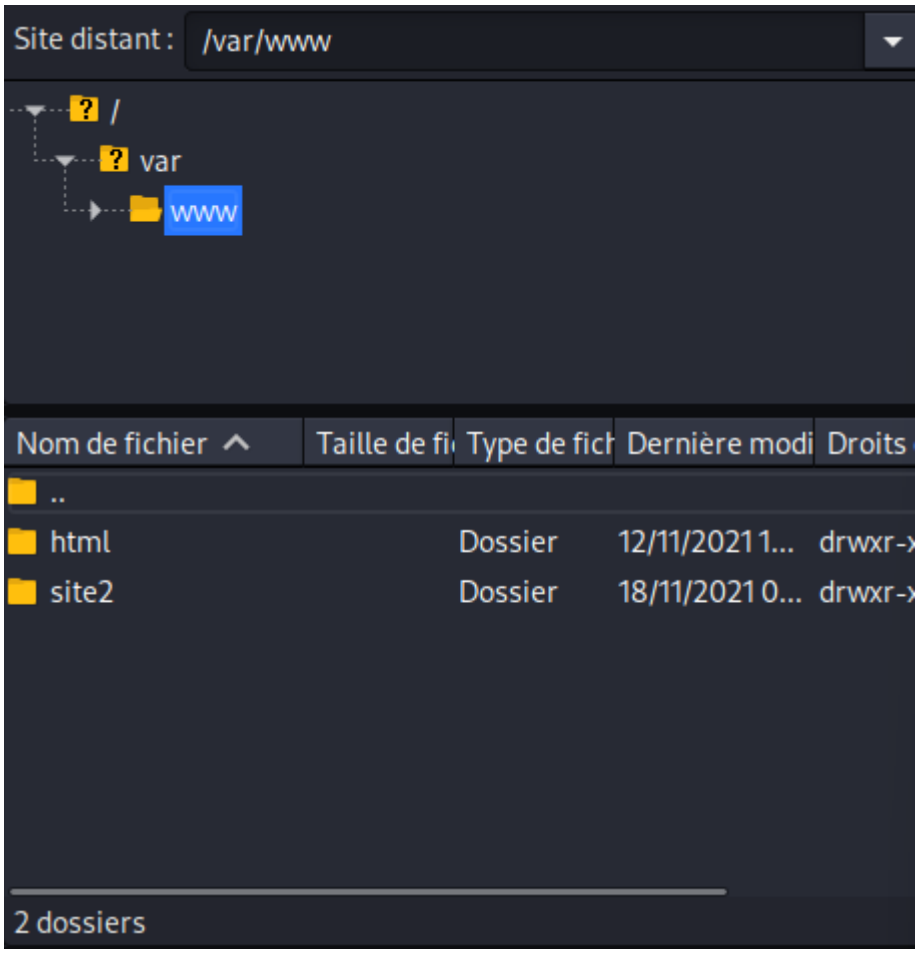
Accès en ssh :

Login : userchoc
Password : p@ssCh0c

Question 5 : Vérifiez la présence du code des 2 sites web.

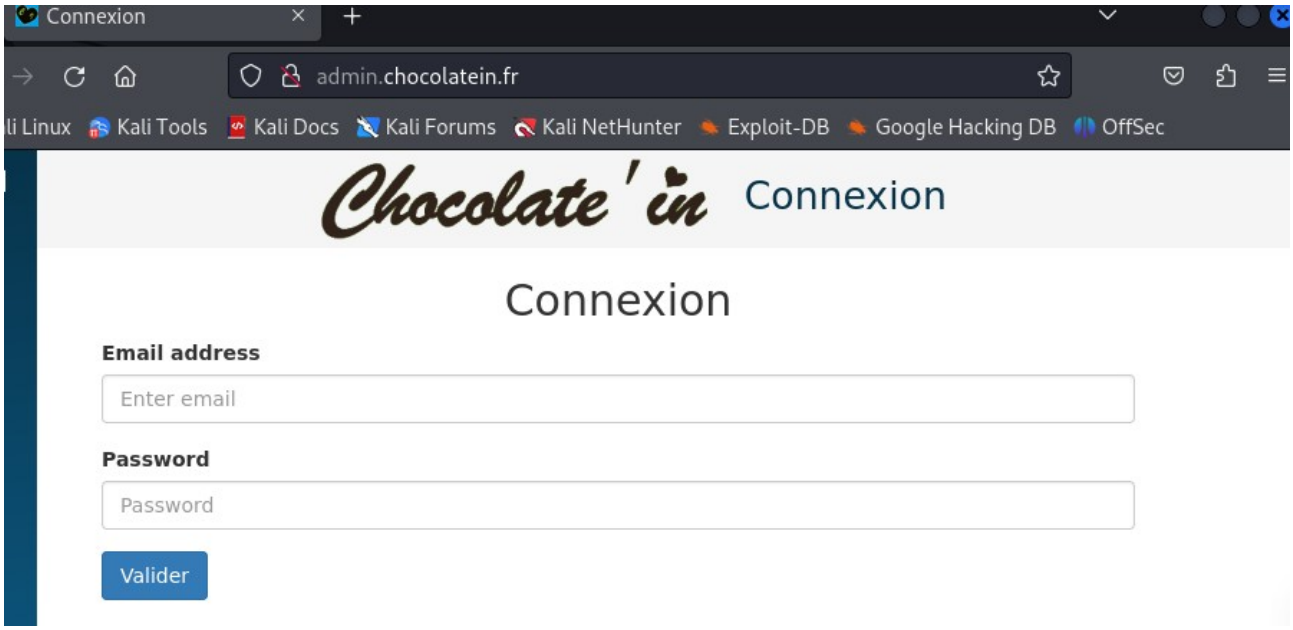






2. Accès aux 2 applications.

Question 6 : Faites une copie d'écran des pages d'accueil des 2 sites :



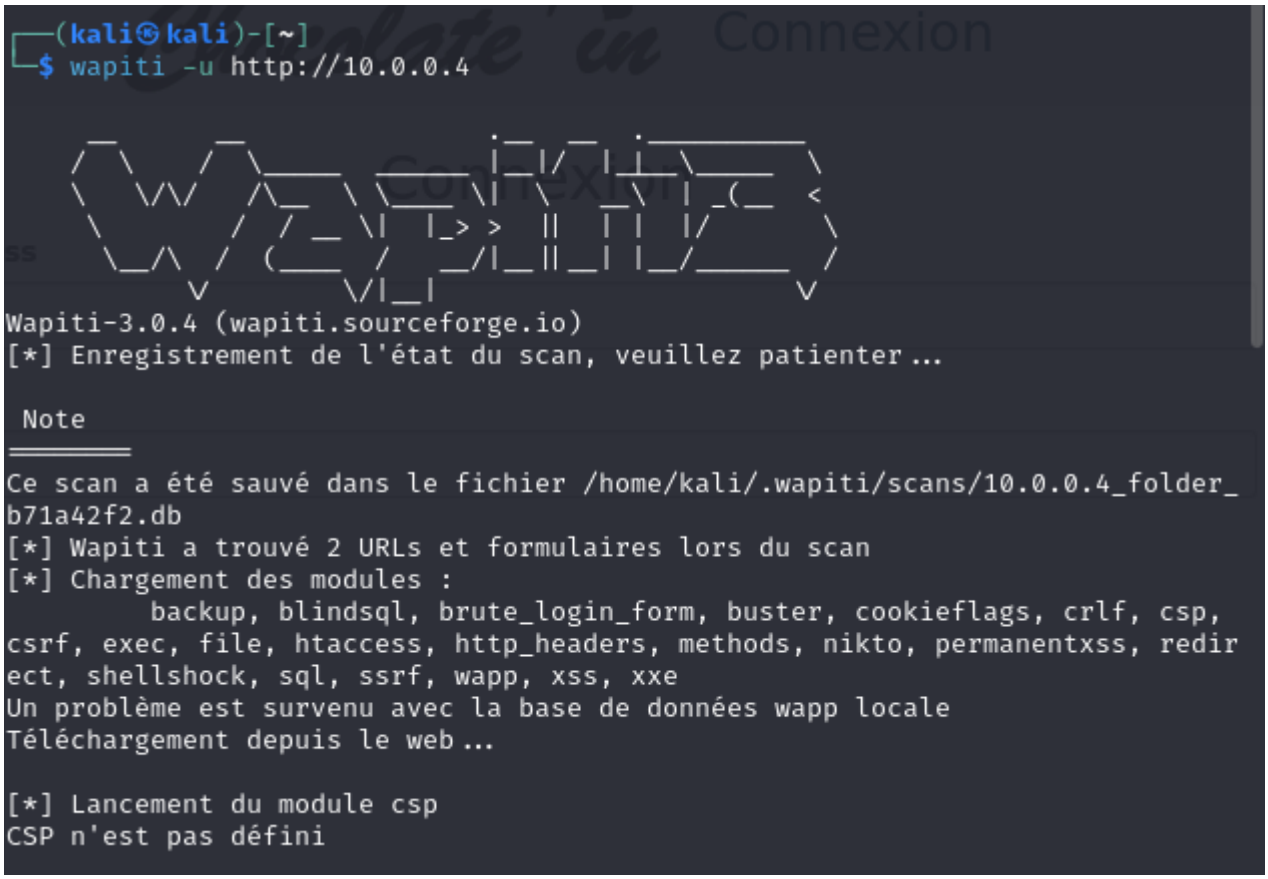
3. Vérification de vulnérabilité sur un service réseau.

```
┌──(root㉿kali)-[~]
└─# nmap -A 10.0.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 04:26 EDT
Nmap scan report for 10.0.0.2
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 be:82:5d:76:e4:cd:ea:88:b4:76:2e:98:7a:21:a5:f0 (RSA)
|   256 a6:51:9d:77:92:a7:49:a6:2c:fc:15:7a:ac:a2:80:65 (ECDSA)
|_  256 58:91:cc:6e:60:04:77:57:4a:5a:c4:6d:3c:7c:d6:1a (ED25519)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Chocolat'in - Chocolats et confiseries \xC3\xA0 Bordeaux
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.38 (Debian)
9000/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: phpMyAdmin
| http-robots.txt: 1 disallowed entry
|_/
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/2%OT=22%CT=1%CU=40281%PV=Y%DS=2%DC=T%G=Y%TM=660BC

|_/
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/2%OT=22%CT=1%CU=40281%PV=Y%DS=2%DC=T%G=Y%TM=660BC
OS:153%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%II=I%TS=A)OPS(O1
OS:=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW
OS:7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=
OS:Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT     ADDRESS
1   1.54 ms 172.16.1.1
2   2.67 ms admin.chocolatein.fr (10.0.0.2)

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.82 seconds

┌──(root㉿kali)-[~]
└─#
```

Question 7 : Que constatez-vous ?

On constate la présence de trois ports (22,80,9000) qui sont ouverts sur le serveur web.

4. Codage sécurisé, scanner de vulnérabilités.



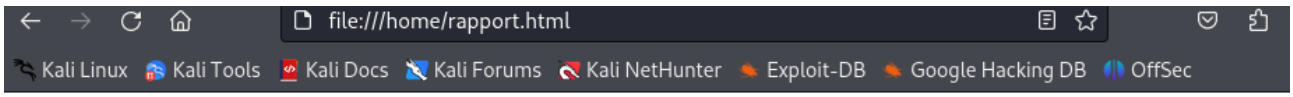
```
┌──(root㉿kali)-[~]
└─# wapiti -u http://10.0.0.2/
```

```
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Enregistrement de l'état du scan, veuillez patienter...

 Note
════════
Ce scan a été sauvé dans le fichier /root/.wapiti/scans/10.0.0.2_folder_2748b
185.db
[*] Wapiti a trouvé 91 URLs et formulaires lors du scan
[*] Chargement des modules :
         backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp,
csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redir
ect, shellshock, sql, ssrf, wapp, xss, xxe
Un problème est survenu avec la base de données wapp locale
Téléchargement depuis le web...

[*] Lancement du module csp
CSP n'est pas défini
```

Rapport du scanner wapiti :

```
Rapport
──────
Un rapport a été généré dans le fichier /root/.wapiti/generated_report
Ouvrez /root/.wapiti/generated_report/10.0.0.2_04022024_0835.html dans un nav
igateur pour voir ce rapport.
```

Question 8 : Faites une copie d’écran de vos résultats



Wapiti vulnerability report

Target: http://10.0.0.2/

Date of the scan: Tue, 02 Apr 2024 08:35:38 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Copie de sauvegarde	0
Injection SQL en aveugle	0
Identifiants faibles	0
Injection CRLF	0
Configuration de la stratégie de securité du contenu (CSP)	1
Cross Site Request Forgery	0
Fichier potentiellement dangereux	0
Exécution de commande	0
Traversée de dossiers	0
Contournement de htaccess	0
HTTP Secure Headers	4
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
Injection SQL	0
Server Side Request Forgery	0
Cross Site Scripting	2
XML External Entity	0
Erreur interne au serveur	0
Consommation anormale de ressource	0
Technologie web identifiée	0

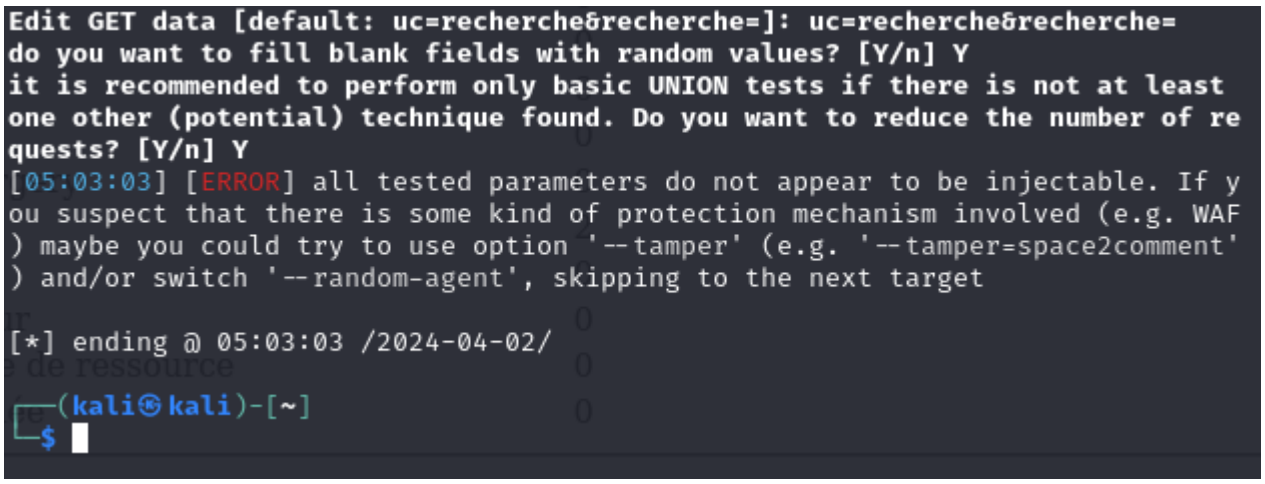
Question 9 : Que constatez-vous ?

On constate qu'il y a plusieurs failles.

5. Vérification de vulnérabilité SQL.

Question 10 : Faites une copie d’écran de vos résultats

```
Please enter full target URL (-u): http://chocolatein.fr
POST data (--data) [Enter for None]:

[04:59:14] [WARNING] no GET and/or POST parameter(s) found for testing (e.g.
GET parameter 'id' in 'http://www.site.com/vuln.php?id=1'). Will search for f
orms
Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
> 3
Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
> 3

sqlmap is running, please wait..

[1/2] Form:
POST http://chocolatein.fr?uc=inscriptionInfolettre
POST data: email=
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: email=] (Warning: blank fields detected): email=
do you want to fill blank fields with random values? [Y/n] Y
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
it is recommended to perform only basic UNION tests if there is not at least
one other (potential) technique found. Do you want to reduce the number of re
quests? [Y/n] Y
injection not exploitable with NULL values. Do you want to try with a random
integer value for option '--union-char'? [Y/n] Y
[05:00:58] [ERROR] all tested parameters do not appear to be injectable. Also
, you can try to rerun by providing a valid value for option '--string' as pe
rhaps the string you have chosen does not match exclusively True responses. I
f you suspect that there is some kind of protection mechanism involved (e.g.
WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comme
nt') and/or switch '--random-agent', skipping to the next target
[2/2] Form:
GET http://chocolatein.fr?uc=recherche&recherche=
do you want to test this form? [Y/n/q]
> Y
Edit GET data [default: uc=recherche&recherche=]: uc=recherche&recherche=
do you want to fill blank fields with random values? [Y/n] Y
it is recommended to perform only basic UNION tests if there is not at least
one other (potential) technique found. Do you want to reduce the number of re
quests? [Y/n] Y
[05:03:03] [ERROR] all tested parameters do not appear to be injectable. If y
ou suspect that there is some kind of protection mechanism involved (e.g. WAF
```



Question 11 : Que constatez-vous ?

La commande évalue les formulaires pour repérer les injections sql et renseigne sur leur méthode. Les deux formulaires ont réussi, cependant le premier utilise GET, donc il faut éviter les altérations d'URL pour accéder aux données.

Question 12 : Effectuer une recherche internet sur les outils de pentest les plus utilisés.

- theHarvester
- OWASP ZAP
- SQLMAP
- Nikto
- SSLSan