



Filters: or and true false union like = > < -- /* */ admin

filter.php 내용에서 다음과 같은 값을 필터링하고 있다.

SELECT username, password FROM users WHERE username='guest' AND password='guest'

Filtered SQLite Injection Challenge #3

not admin

Username

Password

SIGN IN

SELECT username, password FROM users WHERE username='guest' AND password='guest'

사용자가 입력한 값들은 각각 username과 password에 들어간다.

admin으로 로그인을 해야하는데, admin 문자열을 필터링하고 있다.

그래서 admin 값을 쪼개서 넘겨주기로 한다.

adm'||'in 이렇게 ']' 문자를 써서 넘겨주면 필터링에 걸리지 않으면서 admin 문자열을 완

성시킬 수 있다.

그리고 password는 GLOB을 통해 와일드카드를 이용할 수 있다.

a' GLOB '*' 을 입력하면 'a' 문자가 모든 문자열 패턴(*)과 매칭된다. 라는 의미로 항상 참을 반환한다.

```
<?php
session_start();

if (!isset($_SESSION["winner3"])) {
    $_SESSION["winner3"] = 0;
}
$win = $_SESSION["winner3"];
$view = ($_SERVER["PHP_SELF"] == "/filter.php");

if ($win === 0) {
    $filter = array("or", "and", "true", "false", "union", "like", "=", ">", "<", ";", "--", "/*", "*/", "admin"
    if ($view) {
        echo "Filters: ".implode(" ", $filter)."<br/>";
    }
} else if ($win === 1) {
    if ($view) {
        highlight_file("filter.php");
    }
    $_SESSION["winner3"] = 0;           // <- Don't refresh!
} else {
    $_SESSION["winner3"] = 0;
}

// picoCTF{k3ep_1t_sh0rt_ef4a5b40aa736f5016b4554fecb568d0}
?>
```