Log Me In (25)

Description

http://tenjin.compfest.web.id:10338/

Write up

- Opening the website gives us a plain login form
- Viewing the source `Ctrl + U` and analyzing the javascript file in `/assets/js/script.js` gives us this file:

```
function login(){
    if($('#user').val() === ""){
        alert("Please fill the username");
    } else if($('#pass').val() === ""){
        alert("Please fill the password");
    } else {
        $.ajax({
            url: "login.php",
            method: "POST",
            data: {
                'username': $('#user').val(),
                'password': $('#pass').val(),
            },
            success: function(data){
                alert(data);
            },
        })
    }
}

function surpass(){

    $.ajax({
        url: "flag.php",
        method: "POST",
        data: {
            'token': 'bwDWYRByDsMfczD4BqlHawPoy8TAcTspgxgV6o2a',
        },
        success: function(data){
            alert(data);
        },
    });
}
```

- The `surpass()` function seems suspicious. We can then just run `surpass()` in the browser console `Ctrl + Shift + I` to make a POST request to flag.php with the token.
- This gives us the flag: `COMPFEST9{javascript_to_java_is_like_carpet_to_car}`