

Prevent Code Injection In PHP

The `htmlspecialchars()` function converts HTML into HTML entities. `<` would become `<`, and `>` would become `>`. By doing so, the browser can't run HTML tags that a malicious user might try to inject.

For Example:

```
//data submitted by a malicious user
$maliciousInput = "<script type='text/javascript'>
    alert('I am going to inject code! LULZ!')
</script>";

//convert HTML into HTML entities to prevent code injection
$safeInput = htmlspecialchars($maliciousInput);

//now it's ok to display it
echo "$safeInput";
```

Output:

```
&lt;script type="text/javascript&gt;
alert('I am going to inject code! LULZ!')
&lt;/script&gt;
```

If we did not use the `htmlspecialchars()` function in the above example, the injected code would execute as intended by the malicious user.

[php](#)

From:

<https://kbase.devtoprd.com/> - **Knowledge Base**

Permanent link:

https://kbase.devtoprd.com/doku.php?id=prevent_code_injection_in_php

Last update: **2025/06/08 07:19**

