

htmlspecialchars();



```
htmlspecialchars(string, flags, character-set, double_encode );
```

- String
 - ➔ Input om te converteren
- Flags
 - ➔ Optioneel, veranderd behaviour ivm: quotes, invalid encoding & doctype
- Character set
 - ➔ Bv. `EUC-JP` voor Japans, default `UTF_8`
- Double encode
 - ➔ Non-special characters ook encoden?

Ok, but why?

Safety

User input verwerken:

- String doorgeven naar url  XSS
- User input naar database sturen  SQL injection

Meer info



Output

```
<b>bold</b> blabla
```

```
&lt;b>bold&lt1;/b> blabla
```

- Speciale characters worden "*geneutraliseerd*"
- Kan je eventueel nog gaan filteren, `/`'s en alles dat tussen `%` en `;` staat weghalen.



Example

```
<form Method="post">
  <label for="input">Input:</label>
  <input type="field" name="input">
</form>
```

```
$output = htmlspecialchars(
    $_POST['input'],    //Input
    ENT_QUOTES,        //Flags
    'UTF-8',           //Character-set
    FALSE              //Double encode
);
```

```
<a><?=htmlentities($output)?></a>
```

Sources

- Php manual (duh)
- W3schools
- deze Quora thread

Links

- Github repo (.md file van presentatie 😊 & code van in't voorbeeld)