Prevent Code Injection In PHP

The htmlentities() 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
$safeInput = htmlentities($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 htmlentities() function in the above example, the injected code would execute as intended by the malicious user.

php