How does XSS(cross site scripting attack) happens?

Here a hacker basically enter any url into filed of mysql table.

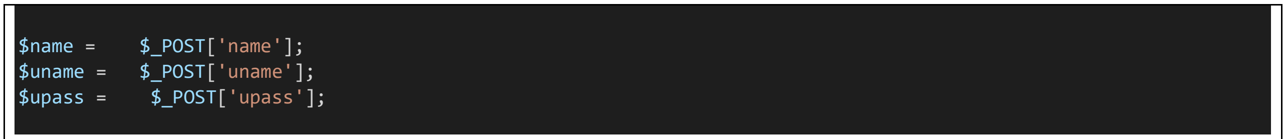
url like : https://brightsec.com/blog/cross-site-scripting-php/#:~:text=Cross%2DSite%20Scripting%20(XSS),as%20JavaScript%2C%20PHP%2C%20HTML.

- For preventing this type of attack PHP has a function which treat a url as a simple text. Which is htmlspecialchars()

Victim code –

Without input filter when code send to database.

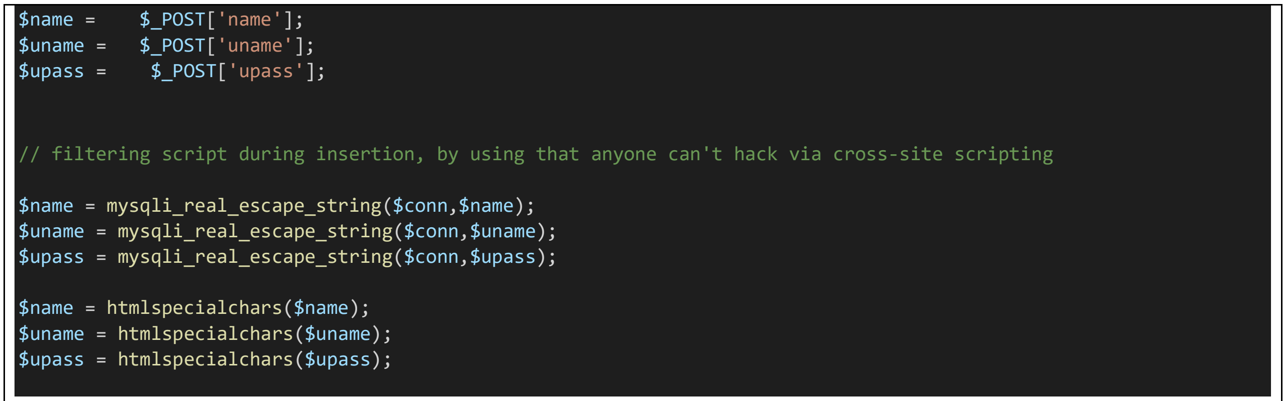
name = <script>alert("Hello! I am an alert box!!");</script>



```
$name =    $_POST['name'];
$uname =   $_POST['uname'];
$upass =    $_POST['upass'];
```

Safe code – now we filter all inputs into database.

mysqli_real_escape_string() -> function is **used to escape characters in a string,**



```
$name =    $_POST['name'];
$uname =   $_POST['uname'];
$upass =    $_POST['upass'];


// filtering script during insertion, by using that anyone can't hack via cross-site scripting

$name = mysqli_real_escape_string($conn,$name);
$uname = mysqli_real_escape_string($conn,$uname);
$upass = mysqli_real_escape_string($conn,$upass);

$name = htmlspecialchars($name);
$uname = htmlspecialchars($uname);
$upass = htmlspecialchars($upass);
```