

Lab: Stored XSS into HTML context with nothing encoded

This lab contains a [stored cross-site scripting](#) vulnerability in the comment functionality.

To solve this lab, submit a comment that calls the `alert` function when the blog post is viewed.

The outcome of this lab is to submit and alert script in the comments. When the comment is posted it is baked into the html. When a user then visits the page the "alert" pops up as a webpage pop up box displaying the message articulated in the script.

Find Injection Point

Leave a comment

Comment:

Name:

Use Injectable

Leave a comment

Comment:

<script>alert(HELLO)</script>

Profit

 a33004403de1340c075b42700090037.web-security-academy.net

1

OK