

Secure Coding

Nomesh P

18BCN7105

Lab-5

1. How secure coding related to XSS?

Ans:

XSS is a vulnerability which allows attackers to inject malicious scripts in a website.

There are various types of XSS.

EX: DOM XSS, stored XSS, reflected XSS

By taking important measure while creating a website we can avoid being a victim to XSS attack. One such example is input sanitization to avoid attackers from injecting malicious scripts.

2.Rxss on demo website.



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

1

OK

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

Search

3. Stored xss on demo website

Lab report 5.pdf

Stored XSS

devijagannadh.in/xss/stored

BlathrBox

Blabber with your friends



You

Thu Mar 04 2021 19:56:39 GMT+0530 (India Standard Time)

Welcome!

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



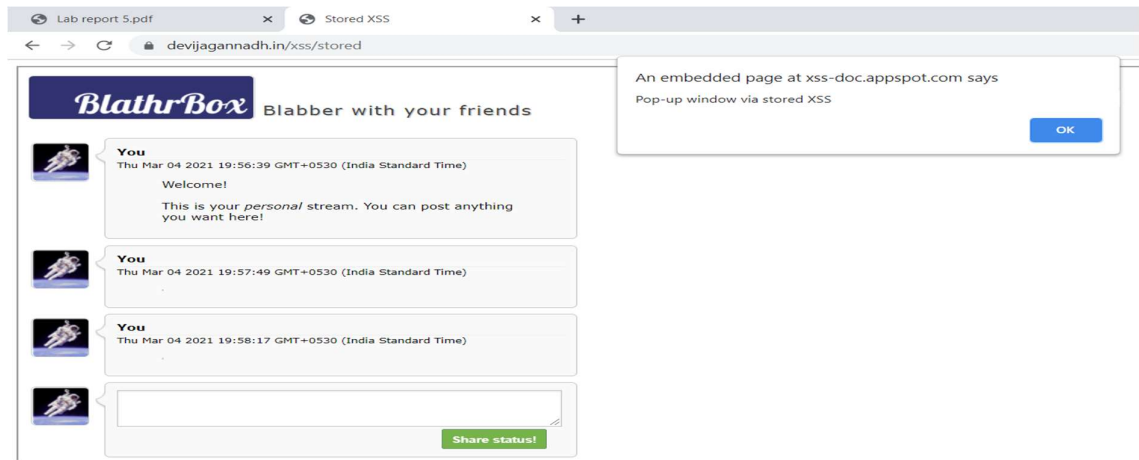
You

Thu Mar 04 2021 19:57:49 GMT+0530 (India Standard Time)

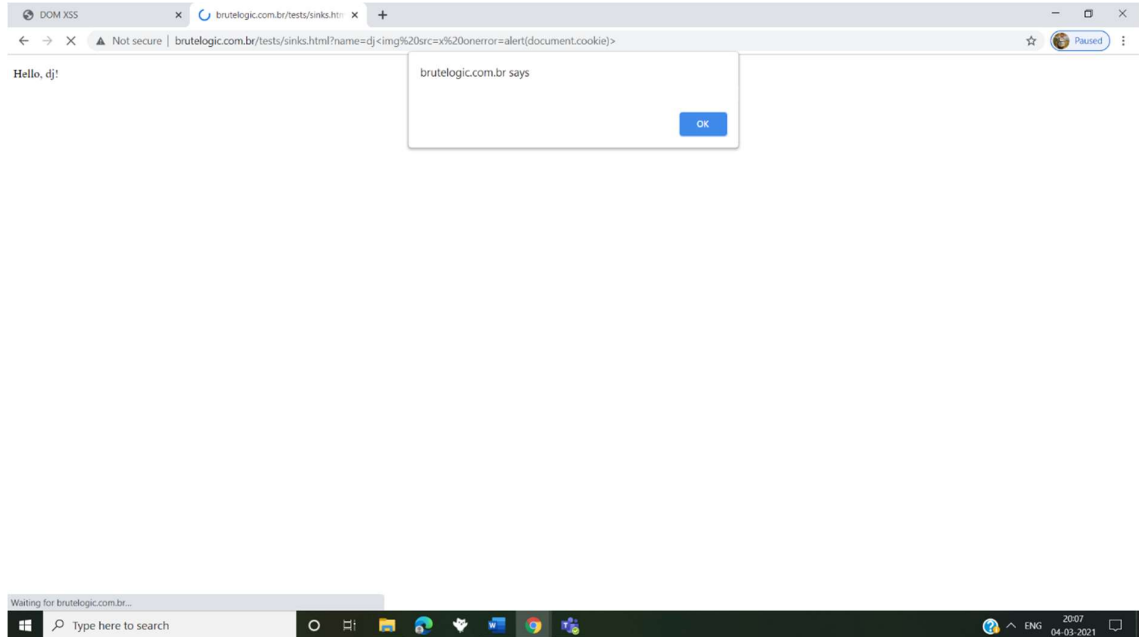


`<img src=x onerror="alert(document.cookie);"`

Share status!



4.DOM xss on demo website



5.Solution of alf.nu/alert1

Lab report 5.pdf

alert(1) to win

← → ↻ ⚠ Not secure | alf.ru/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: *****

User	Score	Browser
... ShabbyMe	7 0	Firefox/77
geniusmaster33 don't worry about less than 12 its a hack	7 4	Chrome/86
Jay 123	7 11	Chrome/86
<input type="text" value="Your name"/>	12	Chrome/89
Sai Vamsi	7 12	Chrome/89
ma	7 12	Chrome/88
Kyzer 12	7 12	Firefox/84
OvO How less ummm	7 12	Chrome/87
._. rick roll	7 12	Chrome/88
czapek ->	7 12	Chrome/87

Warmup (12)

Adobe

JSON

Type here to search

2011
04-03-2021