

NAME: C NAVNEEN

REG : 19BCE7028

LAB EXPERIMENT 5

(Q) How Secure Coding is related to XSS?

With the help of XSS we are able to find out the vulnerabilities of a website or web application. Here we apply payloads to test the website if it is vulnerable. With the help of XSS the user can write a better code to cover these vulnerabilities. It is just like a reality check for the creator of the website.

(Q) Rxss on demo website?

Payload used: <IMG SRC=x
onerror="alert(String.fromCharCode(88,83,83))">



<IMG SRC=javascript:ale

Search

OUTPUT Generated:

ted

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

XSS

OK

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

Q) Storedxss on demo website

Attacker console:

The screenshot shows a web application interface for 'BlathrBox'. At the top, there's a dark blue header with the text 'BlathrBox' in white and 'Blabber with your friends' below it. The main content area displays a list of messages in a scrollable box. Each message is enclosed in a light gray box with rounded corners. On the left side of each message box is a small icon of an astronaut floating in space. To the right of the icon, the word 'You' is displayed in bold, followed by the timestamp and the message content.

Message Content	Timestamp
Welcome!	Sat Feb 27 2021 12:37:24 GMT+0530 (India Standard Time)
This is your <i>personal</i> stream. You can post anything you want here!	Sat Feb 27 2021 12:57:03 GMT+0530 (India Standard Time)
Hi	Sat Feb 27 2021 15:33:02 GMT+0530 (India Standard Time)
Hello	Sat Feb 27 2021 15:34:57 GMT+0530 (India Standard Time)
I am a hacker	Sat Feb 27 2021 15:34:57 GMT+0530 (India Standard Time)

At the bottom right of the message area, there is a green button labeled 'Share status!'

Victim console:

BlathrBox Blabber with your friends

 **You**
Sat Feb 27 2021 12:37:24 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!

 **You**
Sat Feb 27 2021 12:57:03 GMT+0530 (India Standard Time)
Hi

 **You**
Sat Feb 27 2021 15:33:02 GMT+0530 (India Standard Time)
Hello

 **You**
Sat Feb 27 2021 15:34:57 GMT+0530 (India Standard Time)
I am a hacker

 **You**
Sat Feb 27 2021 15:35:32 GMT+0530 (India Standard Time)
i m victim

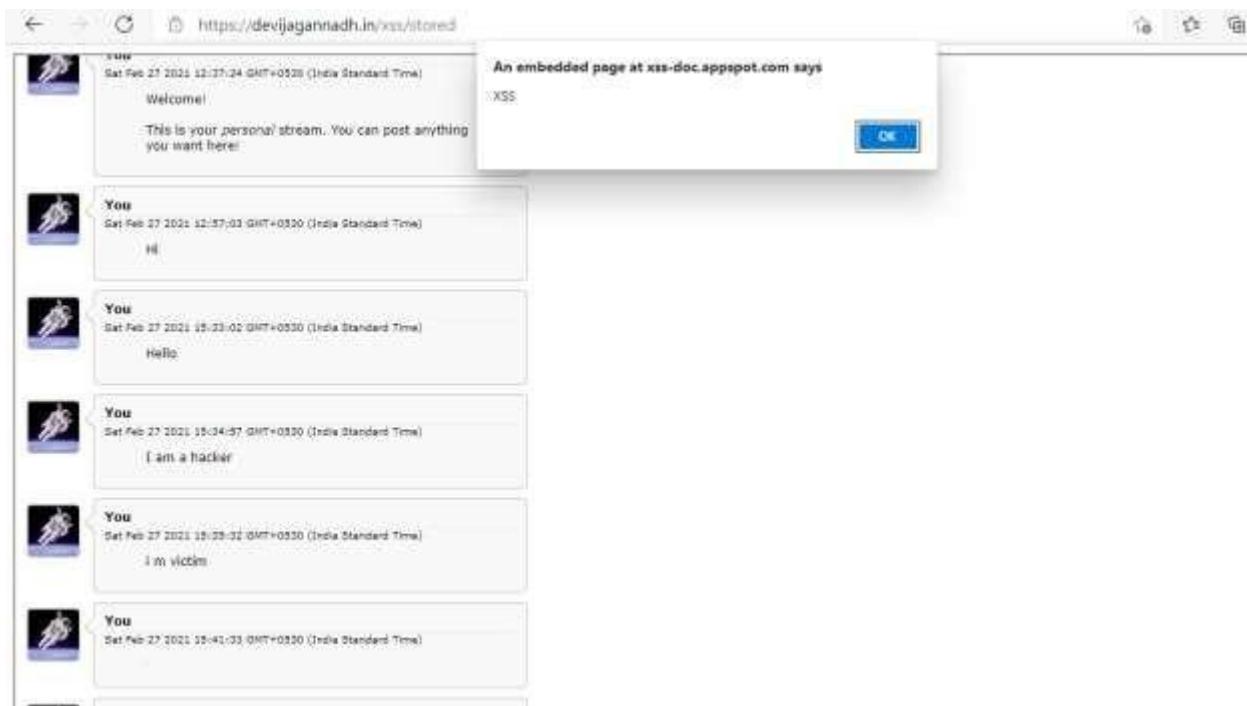
Injecting payload from attacker console:

Payload injected: <IMG SRC=x

The screenshot shows a web browser window with the URL <https://devijagannadh.in/xss/stored>. The page displays a stream from 'BlathrBox' titled 'Blabber with your friend'. The stream shows five messages from the user 'You' at different times on Feb 27, 2021. The messages are: 'Welcome!', 'This is your personal stream. You can post anything you want here!', 'Hi', 'Hello', and 'I am a hacker'. An embedded dialog box from 'xss-doc.appspot.com' says 'An embedded page at https://devijagannadh.in/xss/stored says XSS' with an 'OK' button. At the bottom of the page, the following JavaScript code is visible:

```
onerror="alert(String.fromCharCode(88,83,83))">
```

Payload alert message reflected on victim's window:



(Q) DOM XSS on demo website



Checking ways to enter the website:

Page source:

```
<!DOCTYPE html>
<body>
<p id="p1">Hello, guest!</p>
<script>

var currentSearch = document.location.search;
var searchParams = new URLSearchParams(currentSearch);

/** Document Sink **/

var username = searchParams.get('name');

if (username !== null) {
    document.getElementById('p1').innerHTML = 'Hello, ' + username + '!';
}

/** Location Sink **/

var redir = searchParams.get('redir');

if (redir !== null) {
    document.location = redir;
}

/** Execution Sink **/

var nasdaq = 'AAAA';
var dowjones = 'BBBB';
var sp500 = 'CCCC';

var market = [];
var index = searchParams.get('index').toString();

eval('market.index=' + index);

document.getElementById('p1').innerHTML = 'Current market index is ' + market.index + '.';

</script>
</body>
</html>
```

From this we can alter the name and redir values

Previously it was hello guest!

Let us add a payload into this and check what happens

Payload used: <style>';
}
```

**Input** 8

```
alert(1)
```

**Output**

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

**Console output**

```
alert(1)
```

**Test iframe**

**3-Links :**

**[devijagannadh.in/xss/reflected](http://devijagannadh.in/xss/reflected)**

**[devijagannadh.in/xss/stored](http://devijagannadh.in/xss/stored)**

**[devijagannadh.in/xss/dom](http://devijagannadh.in/xss/dom)**

**Challenge : [alf.nu/alert1](http://alf.nu/alert1)**