

NAME: SHAIK VAZEEM

REG : 19BCN7227

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: ``



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:


 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



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

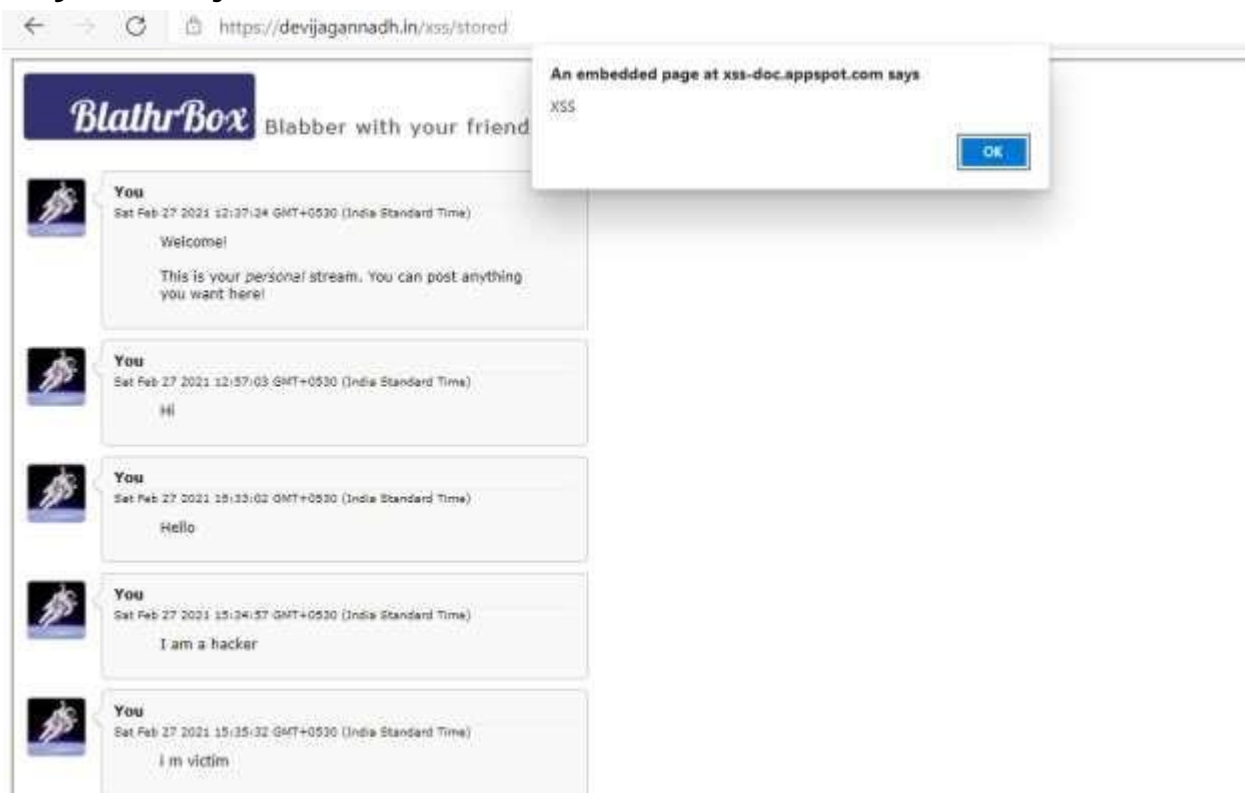


You
Sat Feb 27 2021 15:35:32 GMT+0530 (India Standard Time)
i m victim



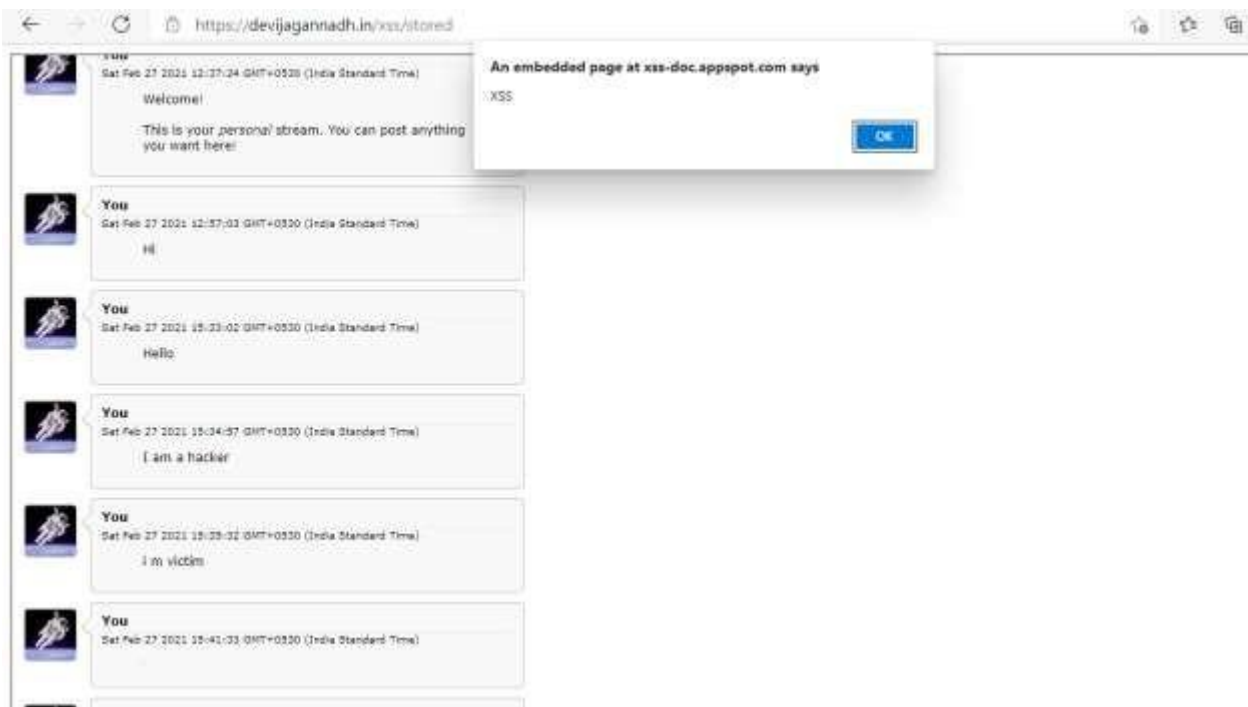
Injecting payload from attacker console:

Payload injected: `<IMG SRC=x`



`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!

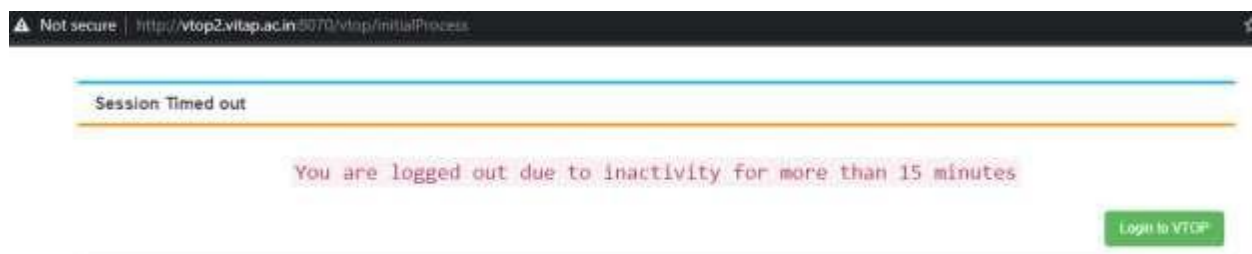
Let us add a payload into this and check what happens

Payload used: `<style>`

Here redir in also a sink so let us redirect it by linking to some other website

Here I have given vtop link

Output:



(Q) Solution of 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 8

alert(1)

Output

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

Console output

```
alert(1)
```

Test iframe

3-Links :

devijagannadh.in/xss/reflected

devijagannadh.in/xss/stored

devijagannadh.in/xss/dom

Challenge : alf.nu/alert1