Name: Pavana Lakshmi Durga Chikkala
Reg No.: 19BCN7090
Slot: L23+24

Secure Coding and XSS

Cross-site scripting is a security vulnerability that allows compromise of the interactions that users have with a vulnerable application. It allows an attacker to inject malicious code into input fields in the web application.
Using secure coding while creating the application can prevent this.

Mitigation:

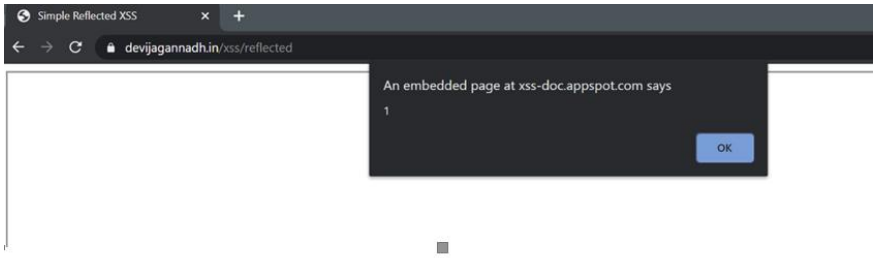
- Input sanitization
- Escaping - encoding all input
- String input validation
- Filter input on arrival
- Encode data on output.

Types of XSS:

1. Reflected XSS: malicious script comes from current http request.
2. Stored XSS: malicious script gets stored in database.
3. DOM XSS: input is stored in DOM.

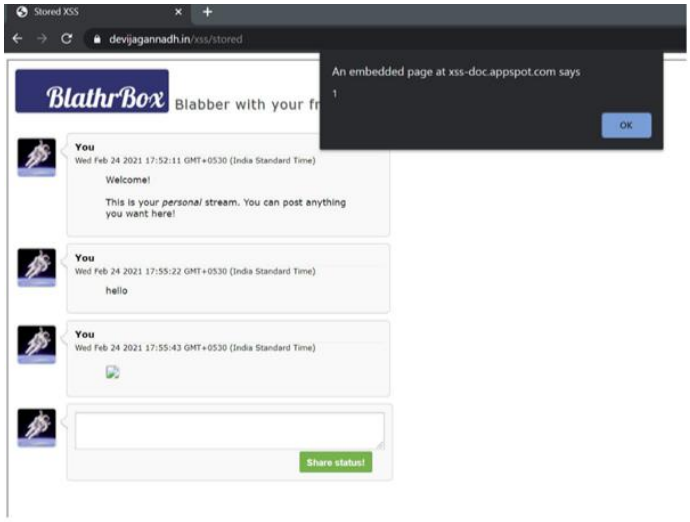
Reflected XSS on http://devijagannadh.in/xss/reflected

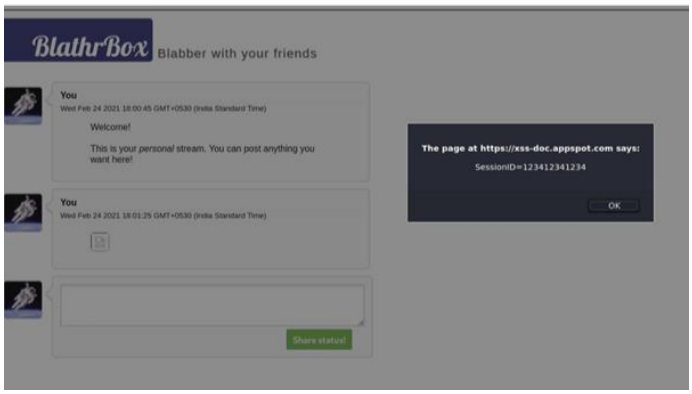
Alert message



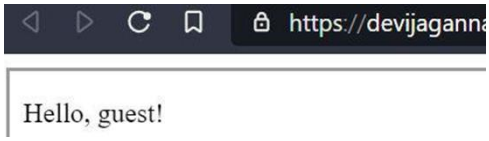
Italic search

Stored XSS on http://devijagannadh.in/xss/stored





DOM XSS on devijagannadh.in/xss/dom



Page source of devijagannadh.in/xss/dom

```
<html>
<title>DOM XSS</title>

<iframe src="https://brutelogic.com.br/tests/sinks.html" height="100%" width="100%" title="Iframe Example"></iframe>

<h4>This site is for educational purposes only!!</h4>
<h4>Author : Devi Jagannadh Kotha</h4>
</html>
```

Page source of view-source:https://brutelogic.com.br/tests/sinks.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>
```

https://brutelogic.com.br/tests/sinks.html?name=Pavana

Hello, Pavana!

https://brutelogic.com.br/tests/sinks.html?redir=https://vitap.ac.in/

https://brutelogic.com.br/tests/sinks.html?index=3

Current market index is 3.