

**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.

---

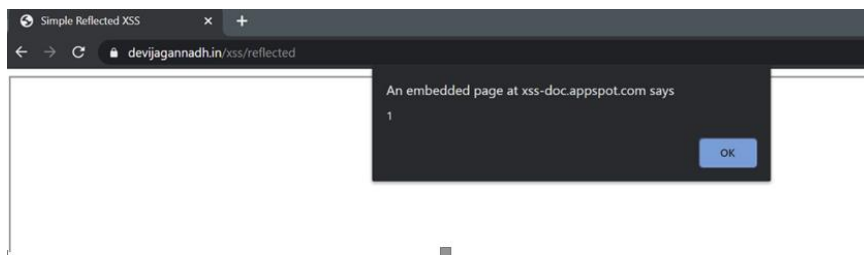
Reflected XSS on <http://devijagannadh.in/xss/reflected>

Alert message



`<script>alert("an alert");`

Search



Italic search

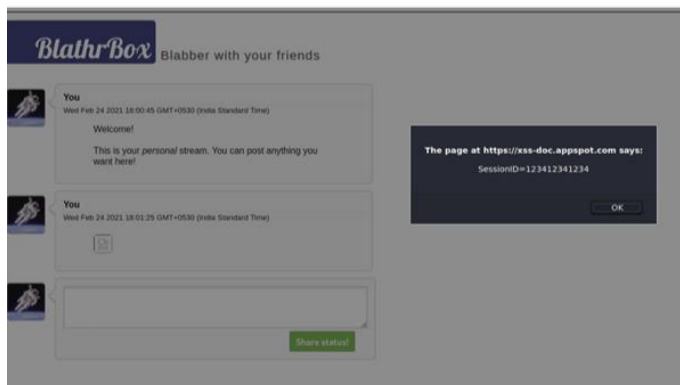
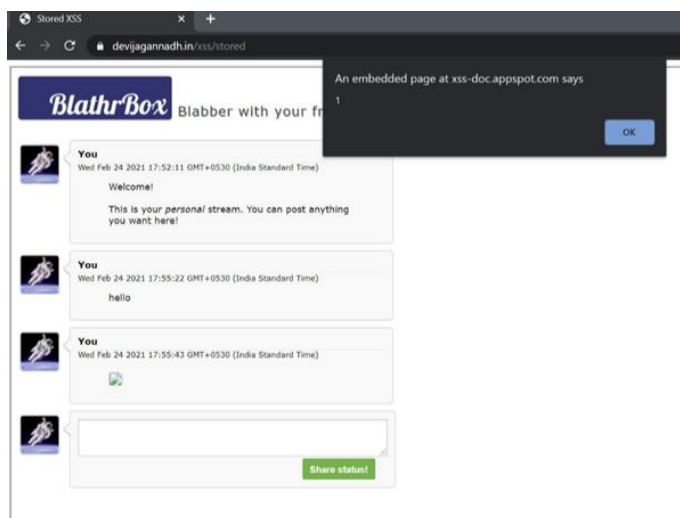


Search

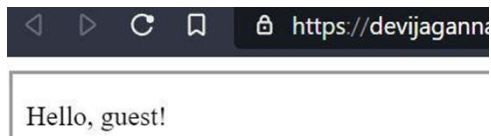


Sorry, no results were found for *italics*. [Try again.](#)

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



DOM XSS on [devijagannadh.in/xss/dom](http://devijagannadh.in/xss/dom)



Page source of [devijagannadh.in/xss/dom](https://devijagannadh.in/xss/dom)

```
1 <html>
2 <title>DOM XSS</title>
3
4 <iframe src="https://brutelogic.com.br/tests/sinks.html" height="100%" width="100%" title="Iframe Example"></iframe>
5
6 <h4>This site is for educational purposes only!!</h4>
7 <h4>Author : Devi Jagannadh Kotha</h4>
8 </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>

← → ↻ 🔒 brutelogic.com.br/tests/sinks.html?name=Pavana

Hello, Pavana!

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

The banner features the VIT-AP University logo on the left. The navigation menu includes: ADMISSIONS, ACADEMICS, PLACEMENT, FACILITIES, CAMPUS LIFE, RESEARCH, ABOUT, and VIT-AP ADVANTAGE VIT Campuses. The main headline reads "Placements shine on our 1<sup>st</sup> Graduating Batch". Below this, a grid of logos for "OUR RECRUITERS" is displayed, including Amazon, Microsoft, Google, IBM, Oracle, SAP, and many others. To the right of the logos is a photograph of a group of students standing in front of a large, modern university building. At the bottom of the banner, there is a dark blue bar with the text "Announcement" and navigation links for "neering Courses", "Ph.D Programme ( Mathematics, Physics, Chemistry )", and "B.Sc & M.Sc Admissions 2020 -21".

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

Current market index is 3.

---