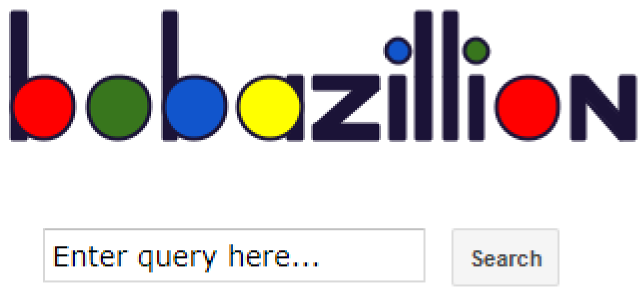
Secure Coding Lab - 5

Name: Charitha Bodapothula
Reg.No: 19BCN7005
Slot: L23+24

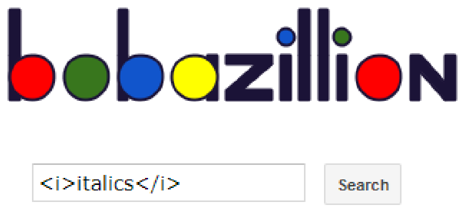
XSS

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different user.
The attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access cookies, session tokens or other sensitive information retained by the browser and used with that site.

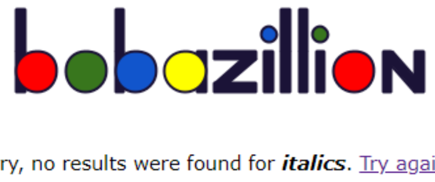
Reflected XSS on
https://devijagannadh.in/xss/reflected



Italic search

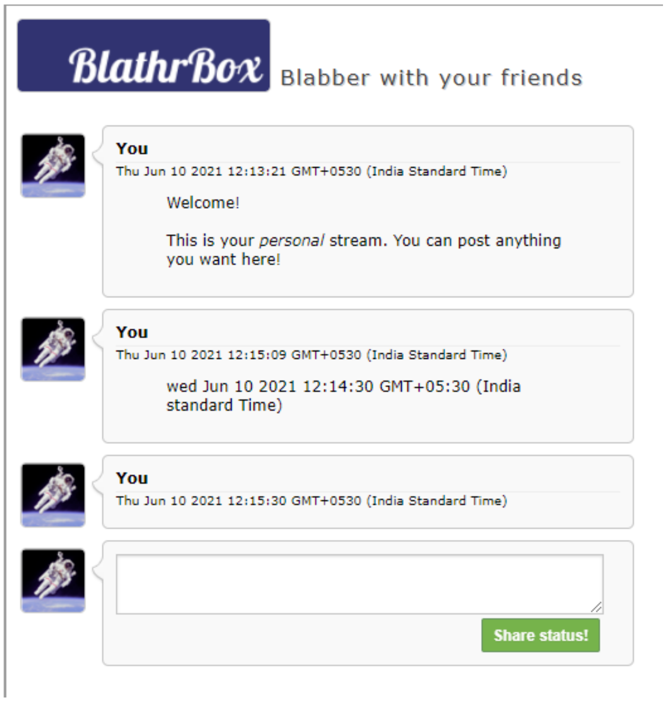


<i>italics</i>



Sorry, no results were found for ***italics***. Try again.

Stored XSS
https://devijagannadh.in/xss/stored



You
Thu Jun 10 2021 12:13:21 GMT+0530 (India Standard Time)

Welcome!

This is your *personal* stream. You can post anything you want here!

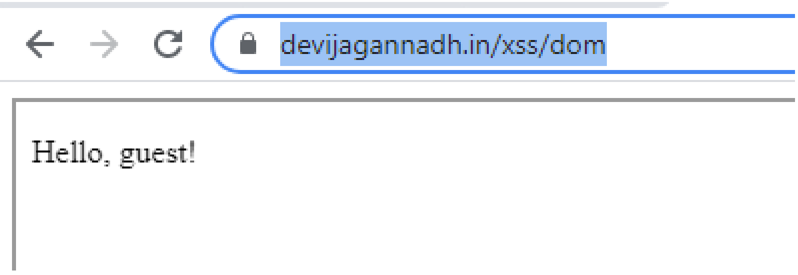
You
Thu Jun 10 2021 12:15:09 GMT+0530 (India Standard Time)

wed Jun 10 2021 12:14:30 GMT+05:30 (India standard Time)

You
Thu Jun 10 2021 12:15:30 GMT+0530 (India Standard Time)

DOM XSS

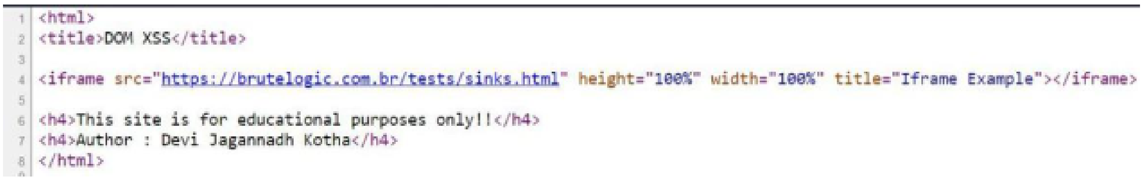
https://devijagannadh.in/xss/dom



devijagannadh.in/xss/dom

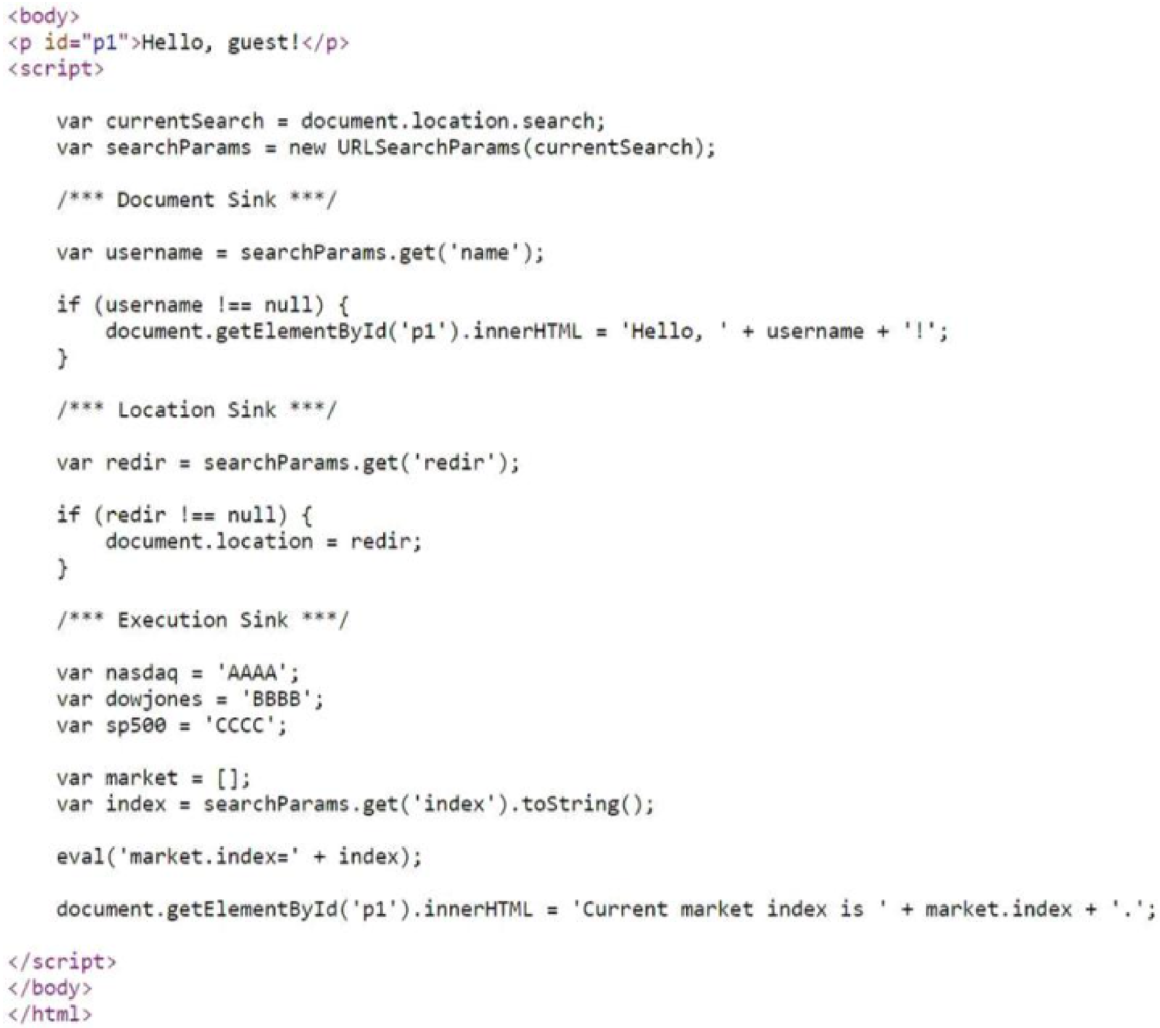
Hello, guest!

Page source:



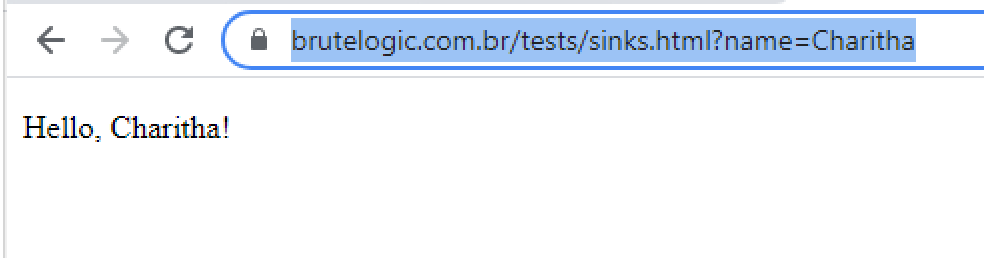
```
<html>
<title>DOM XSS</title>

<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
https://brutelogic.com.br/tests/sinks.html?tests/sinks.html



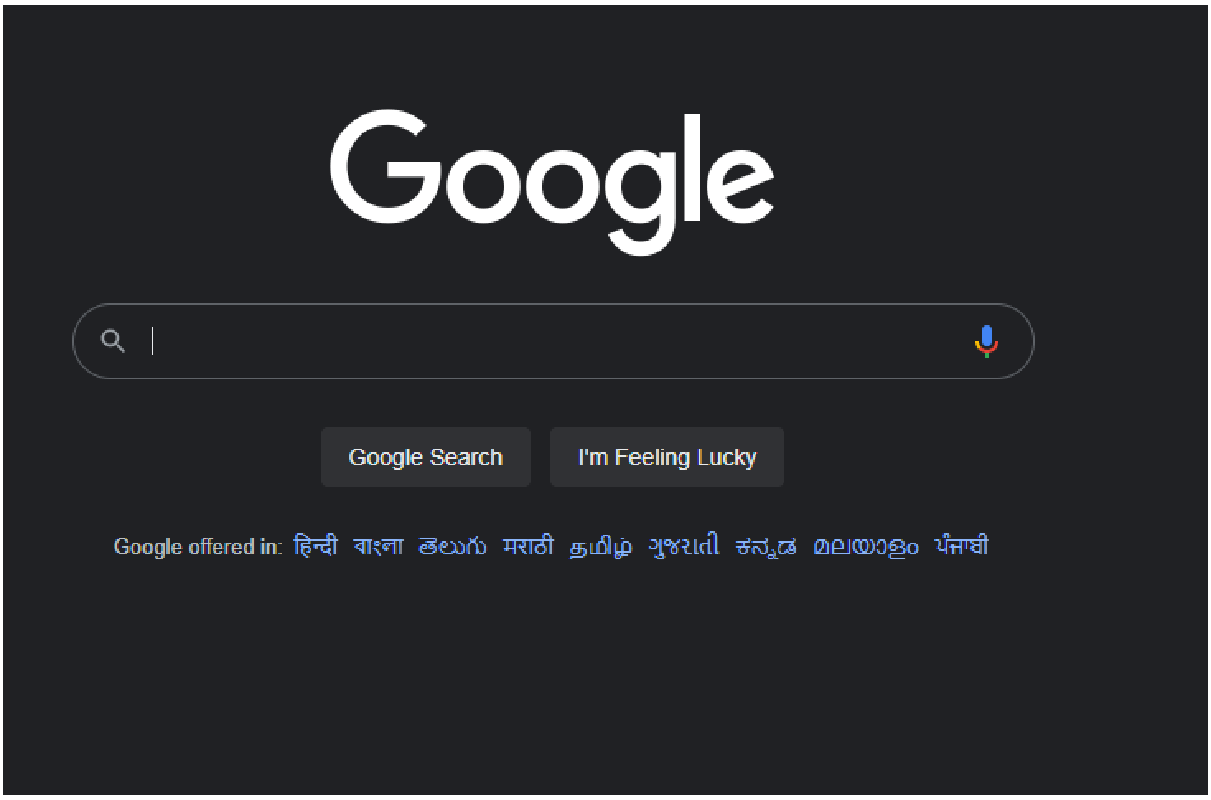
```
<body>
<p id="p1">Hello, guest!</p>
<script>

    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=Charitha



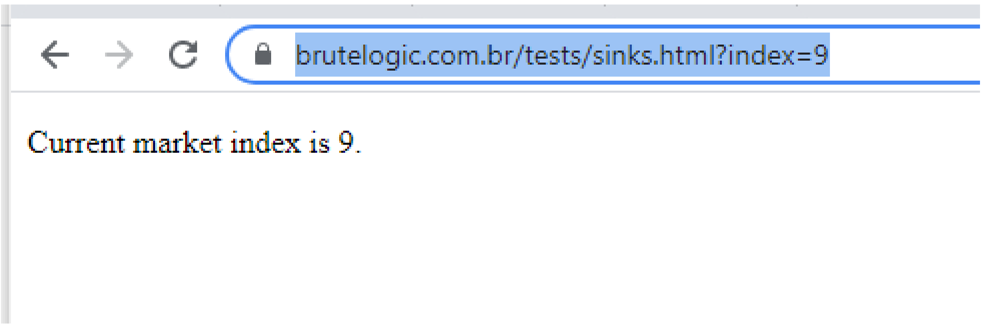
Hello, Charitha!

https://brutelogic.com.br/tests/sinks.html?redir=https://google.com/



Google
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ

https://brutelogic.com.br/tests/sinks.html?index=9



Current market index is 9.