

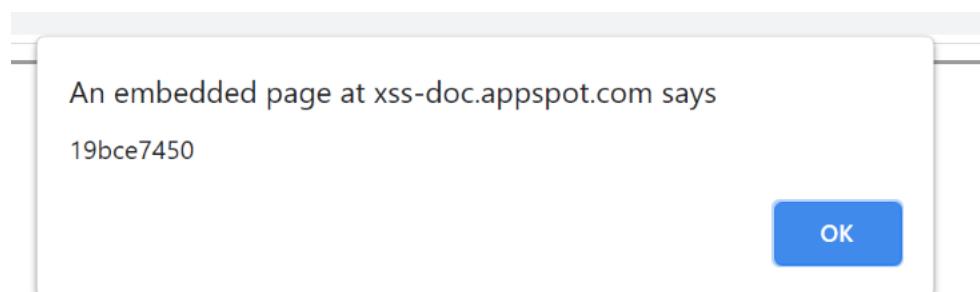
SIVN YASWANTH 19BCE7450

How Secure Coding is related to XSS?

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. By using this hackers can inject payload directly to websites, Database, users if they are vulnerable . In secure coding it is our job to write or test the code for vulnerabilities and to observe the patterns how hacker checking the vulnerable in websites .

(Q) Rxss on demo website?

here I directly searched the payload so that in reflex xss it will directly execute it .



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

Storedxss on demo website

Here as a host injected the payload so that it will stored in database and when users connect to database this payload will be executed .

An embedded page at xss-doc.appspot.com says
19bce7450

OK

You
Fri Apr 02 2021 11:34:31 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!

You
Fri Apr 02 2021 11:34:39 GMT+0530 (India Standard Time)
hi

You
Fri Apr 02 2021 11:52:46 GMT+0530 (India Standard Time)


You
Fri Apr 02 2021 11:52:57 GMT+0530 (India Standard Time)
hi

I loaded another page as a another user now when I entered the message the payload that I injected to database that will be excuted .

The screenshot shows a messaging interface with several messages from a user named 'You'. A tooltip is displayed over the third message, which reads: 'An embedded page at xss-doc.appspot.com says 19bce7450' with an 'OK' button.

- You**
Fri Apr 02 2021 11:34:31 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!
- You**
Fri Apr 02 2021 11:34:39 GMT+0530 (India Standard Time)
hi
- You**
Fri Apr 02 2021 11:52:46 GMT+0530 (India Standard Time)
.
- You**
Fri Apr 02 2021 11:52:57 GMT+0530 (India Standard Time)
hi
- You**
Fri Apr 02 2021 11:53:33 GMT+0530 (India Standard Time)
hi

(Q) DOM xss on demo website

Here I checked the page source code to find the vulnerables .

I found two where we can change the name , and let the user direct to another page when this website is loaded .

First vulnerable

The screenshot shows a browser window with the URL brutelogic.com.br/tests/sinks.html?name=19bce7450. The page displays the text 'Hello, 19bce7450!'.

Hello, 19bce7450!

← → C https://brutelogic.com.br/tests/sinks.html?redir=https://vitap.ac.in

Hello, 19bce7450!

The screenshot shows a browser window with two tabs. The active tab is titled 'DOM XSS' and contains the URL 'https://brutelogic.com.br/tests/sinks.html?redir=https://vitap.ac.in'. The content of the page is the Vit-AP homepage. The navigation bar at the top includes links for 'ADMISSIONS', 'ACADEMICS', 'PLACEMENT', and 'FACILITIES'. The main content area features the Vit-AP logo and some descriptive text.

(Q) Solution of alf.nu/alert1

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

Warmup

```
function escape(s) {
    return '<script>console.log("'+s+'");</script>';
}
```

Input 8

```
alert(1)
```

Output

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

Console output

```
alert(1)
```

Test iframe

