

Secure Coding -Lab5

T.Venkata Sumanth
18BCE7271

24/02/21
L39 +L40

Questions :

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.

1. Reflected XSS

Querying for my registration number



Result

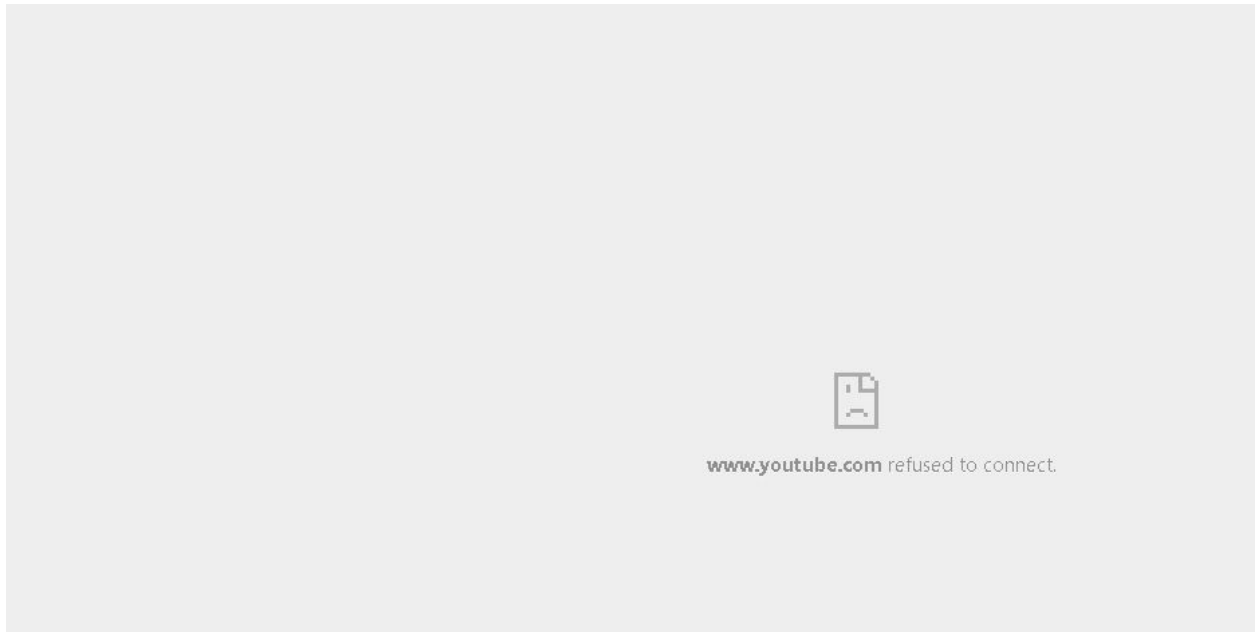


Sorry, no results were found for
18bce7271
. [Try again.](#)

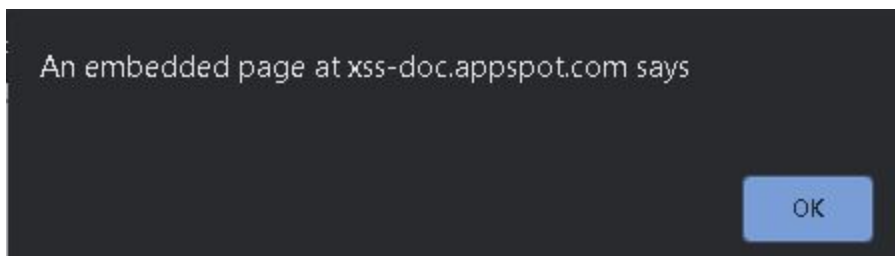


Sorry, no results were found for [vitap](#). [Try again.](#)

On clicking this site it will redirect you to given link



3.
Trying to get the cookies



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

4.



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



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

To get the cookies from payload we are now using advanced level xss which gives us cookies

2. Stored XSS

BlathrBox

Blabber with your friends



You

Fri Feb 26 2021 21:51:33 GMT+0530 (India Standard Time)

Welcome!

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



You

Fri Feb 26 2021 21:52:03 GMT+0530 (India Standard Time)

hii



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

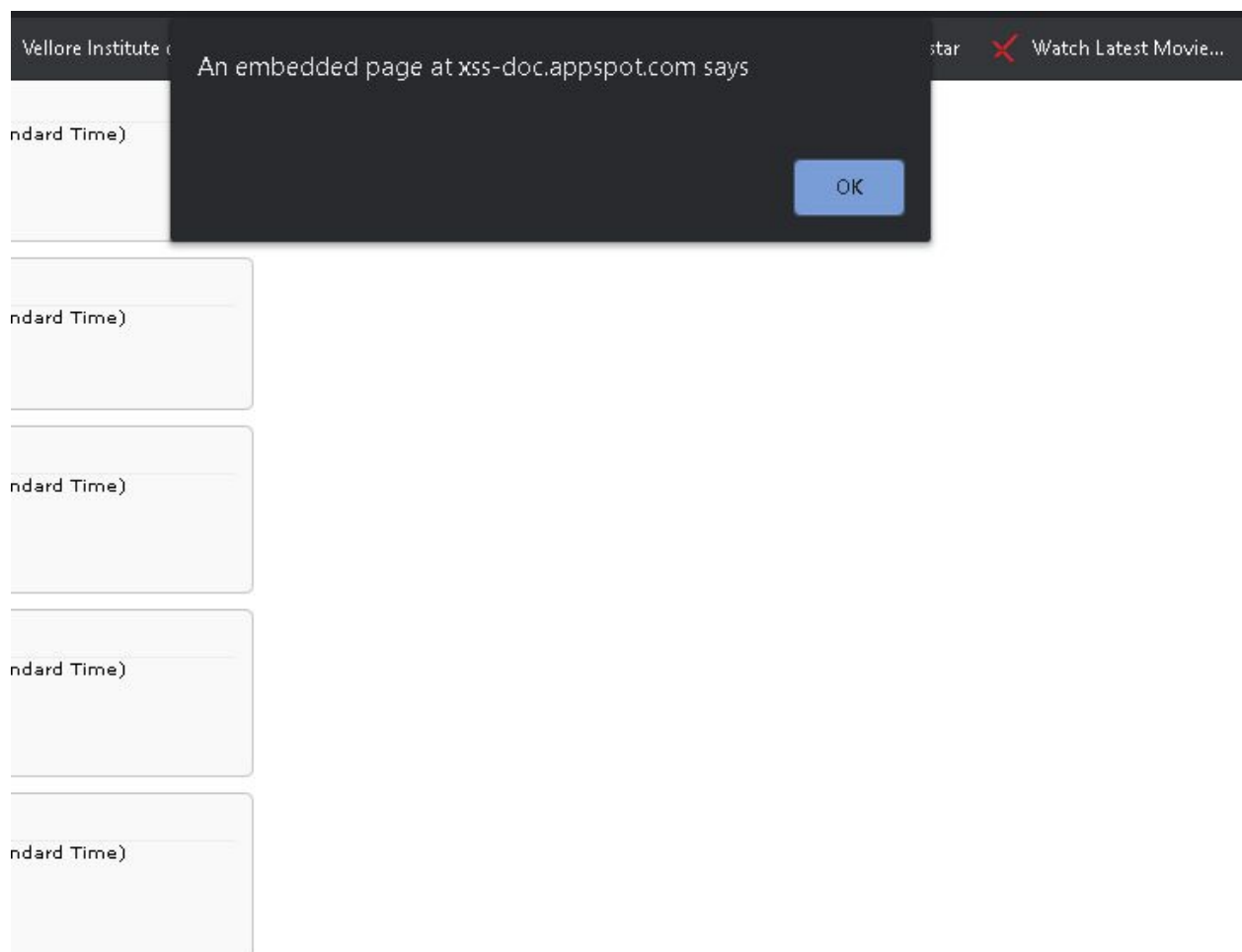
Share status!

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

OK

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

OK



It is not responding

3.Dom XSS

Hello, guest!

4. 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
7271	12	Chrome/88
ma	? 12	Chrome/88
Kyzer 12	? 12	Firefox/84