

KANKANWAR DEVASHISH SANGAM
18BCN7022
SECURE CODING LAB 5

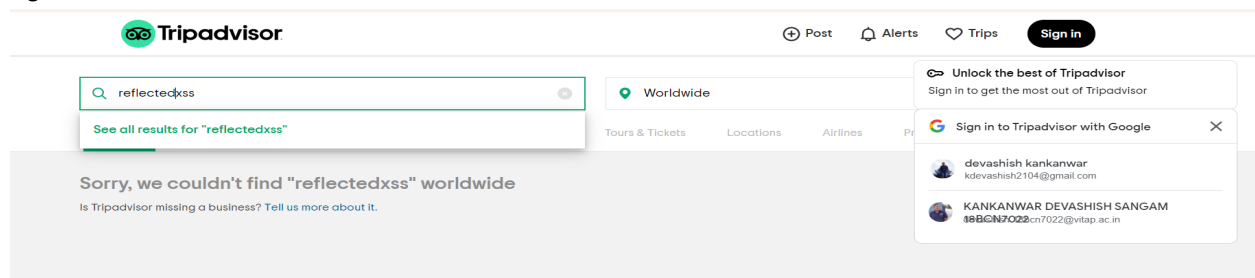
XSS

1.What is XSS attack?

Cross-site Scripting (XSS) is a client-side code [injection attack](#). The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.

2.Reflected XSS attack

Eg.



```

Blur="placementEvCall('taplc_srp_dual_search_0', 'handlers.whereFocused', event, this)" onfocus="placementEvCall('taplc_srp_dual_search_0',
andlers.whatFocused', event, this)" onkeydown="if (ta && (event.keyCode || event.which) === 13){ta.setEvtCookie('SRP_Search',
ction','Search | enter | EnterKey', 0, '/Search');}" onkeyup="placementEvCall('taplc_srp_dual_search_0', 'handlers.searchInputKeyUp',
ent, this)" autocorrect="off" spellcheck="false" value="reflectedxss" placeholder="Search TripAdvisor"/><span id="CLEAR_WHAT"
ass="clear-text ui_icon times-circle-fill hidden"></span><span class="input_highlight"></span></div></div></div><div
="GEO_SCOPE_CONTAINER" class="geoScopeContainer ui_column is-5"><div class="input_box"><span class="typeahead icon where_neighbor ui_icon
p-pin-fill"></span><span><div class="where with highlight"><input id="GEO_SCOPED_SEARCH_INPUT" type="text" class="text geoScopeInput "
Blur="placementEvCall('taplc_srp_dual_search_0', 'handlers.whereFocused', event, this)"
focus="placementEvCall('taplc_srp_dual_search_0', 'handlers.whereFocused', event, this)"
keyup="placementEvCall('taplc_srp_dual_search_0', 'handlers.searchInputKeyUp', event, this)" value="Worldwide" autocorrect="off"
ellcheck="false" placeholder="Enter a destination"/><span id="CLEAR_WHERE" class="clear-text ui_icon times-circle-fill
idden"></span><span><span class="input_highlight"></span><span><div><span class="hidden geoExample">Enter a destination</span><span>
ass="where_neighbor without dropdown ui_icon caret-down"></span></div></div></div><div><div class="ui_column is-2
arch_line_block"><button id="SEARCH_BUTTON" class="search_button" type="submit" onclick="if (ta && event.clientY) {
gment.gettlementById('global_nav_search_form').elements['pid'].value=3825; jta && ta.setEvtCookie('SRP_Search', 'Action', 'Search | ' + (
ent.detail === 0? 'Enter' : 'Click') + ' | SearchButton', 0, '/Search');return placementEvCall('taplc_srp_dual_search_0',
andlers.submitClicked', event, this);}" name="sub-search"><div id="SEARCH_BUTTON_CONTENT"><div class="inner">Search</div>
div></div></div><input id="TYPEAHEAD_GEO_ID" type="hidden" name="geo" value="1"><input id="TYPEAHEAD_LATITUDE" type="hidden"
me="latitude" value=""><input id="TYPEAHEAD_LONGITUDE" type="hidden" name="longitude" value=""><input id="TYPEAHEAD_NEARBY" type="hidden"
me="searchNearby" value=""><input id="AUTO_SCOPED" type="hidden" name="autoScoped" value=""><input type="hidden" name="pid"

```

