Stored XSS on https://apps.topcoder.com/wiki/plugins/socialbookmarking/updatebookmark.action

3

Share:

State	Resolved (Closed)
Disclosed	**May 12, 2020 7:17pm +0530**
Reported To	Topcoder
Asset	apps.topcoder.com (Domain)
Weakness	Cross-site Scripting (XSS) - Stored
Severity	High (7.1)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

powerpuff submitted a report to **Topcoder**. May 6th (25 days ago)

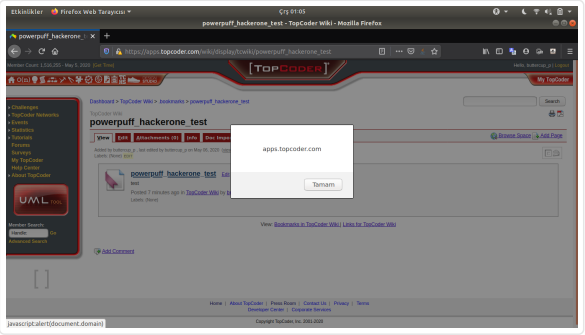
Summary:

Hi :) Adding javascript url causes to stored XSS when creating bookmark.

Steps To Reproduce:

Go to https://apps.topcoder.com/wiki/plugins/socialbookmarking/updatebookmark.action . Write `javascript:alert(document.domain)` on url input and fill other areas. After create, go `https://apps.topcoder.com/wiki/display/tcwiki/<TITLE>` and when you click the title on this page, XSS will execute.

PoC:
https://apps.topcoder.com/wiki/display/tcwiki/powerpuff_hackerone_test



Impact

XSS can use to steal cookies or to run arbitrary code on victim's browser.

1 attachment:
F816754: 2020-05-06_01-05-54_ekran_g_r_nt_s_.png

powerpuff posted a comment. May 6th (25 days ago)
Hi :) This only works to signed-in users. Because unauthorized users cannot create bookmarks. I think there is a mistake on https://apps.topcoder.com/wiki/login.action . If you encounter an error, you can login on main site (https://accounts.topcoder.com/member) then try.

dwan HackerOne triage posted a comment. Updated May 6th (25 days ago)

lugtag HackerOne triage updated the severity from Medium to High (7.1). May 6th (25 days ago)

lugtag HackerOne triage changed the status to **Triaged**. May 6th (25 days ago)
Hello @powerpuff,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
@lugtag

jwheeler closed the report and changed the status to ○ **Resolved**. May 11th (20 days ago)
The legacy topcoder wiki has been disabled. This is not longer reproducible.

powerpuff requested to disclose this report. May 12th (19 days ago)
Can we disclose this?

jwheeler agreed to disclose this report. May 12th (19 days ago)

This report has been disclosed. May 12th (19 days ago)