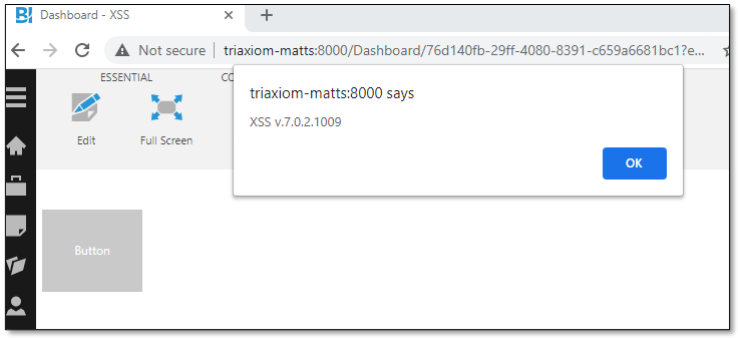
CVE-2020-28408 & CVE-2020-28409 – MULTIPLE PERSISTENT XSS DISCOVERED IN DUNDAS BI SERVER

POSTED ON NOVEMBER 10, 2020 BY RUMHAM



Content here will be expanded on upon later, for now this serves as a quick description and write-up.

Overview

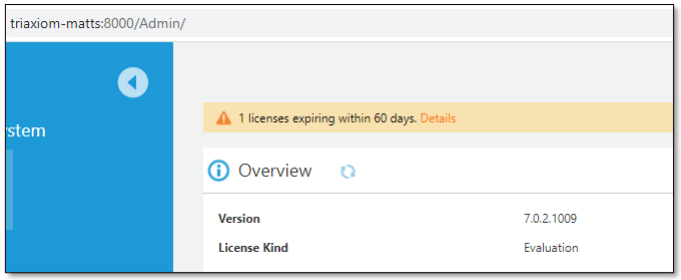
Dundas BI server has two stable release versions available for download for customers. Version 7.0.2.1009 and Version 8.0.0.1001. Both product versions contain persistent cross-site scripting (XSS) vulnerabilities in the same location.

Version 7.0.2.1009

HTML Label

An authenticated attacker may insert malicious Javascript code in an HTML label when creating or editing a dashboard. To do this:

1. User must be authenticated and have proper permissions to edit or create a dashboard.
2. In the dashboard editing screen, click on Components and select "HTML Label".
3. Insert code. PoC: <script>alert('XSS')</script>.



Version 7.0.2.1009

ABOUT ME

Matt Schmidt
Penetration Tester
B.S. Information Technology
OSCP, eWPT, eJPT, Security+

RECENT POSTS

(External Blog Post) XMPie, a Xerox Company, UStore Vulnerabilities Discovered

(External Blog Post) Web Application Weakness Trends

(External Blog Post) Android Penetration Testing After Nougat

TCM Security PNPT Exam / Certification Review (Updated: 2/1/2022)

Your IPv6 is Showing [CarolinaCon]

Search …
Search

ARCHIVES

February 2022

May 2021

April 2021

February 2021

November 2020

September 2020

March 2020

January 2020

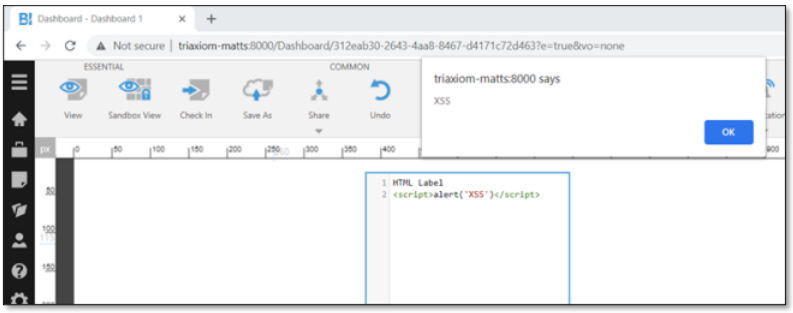
December 2019

July 2019

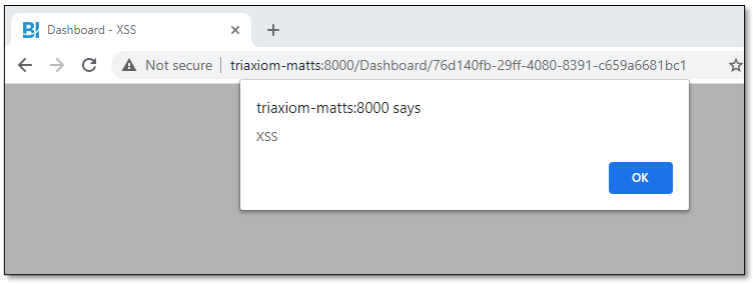
June 2019

May 2019

April 2019

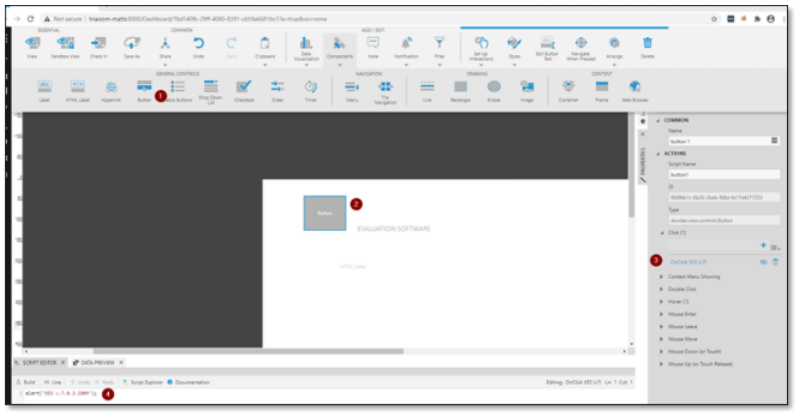


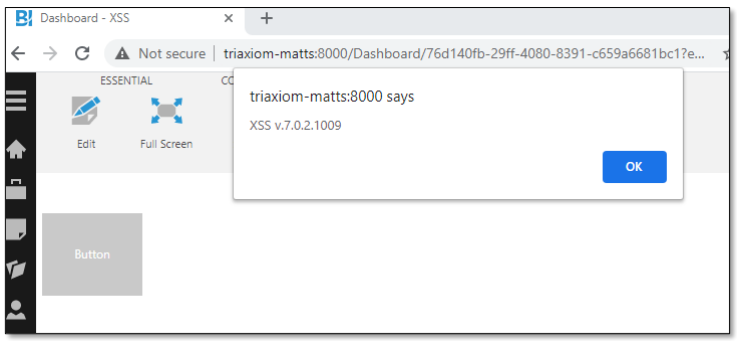
XSS will immediately execute after clicking out of label editor.



View from dashboard as any user.

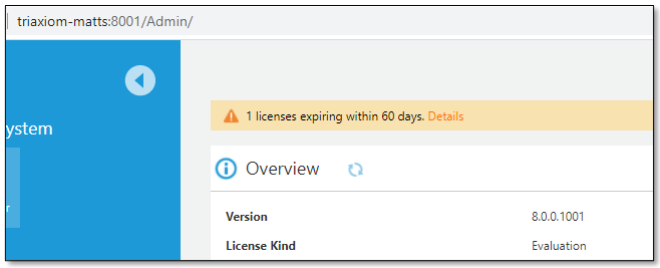
Button XSS





Version 8.0.0.1001

The same vulnerabilities exists within the latest deployment of Dundas.



March 2019

January 2019

November 2018

CATEGORIES

Achievement

CTF

External Blog Post

Meetup

Misc.

Non-Technical

Tutorial

Uncategorized

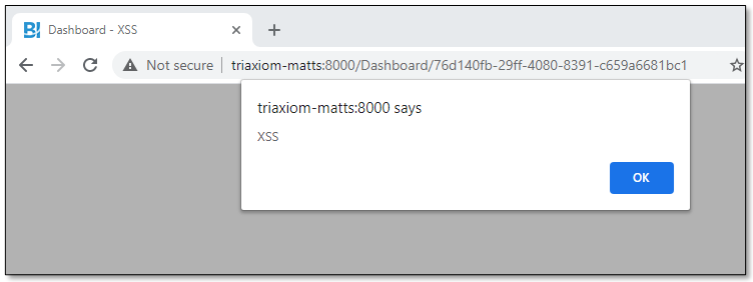
Web Applications

Writeup

Version 8.0.0.1001

HTML Label XSS

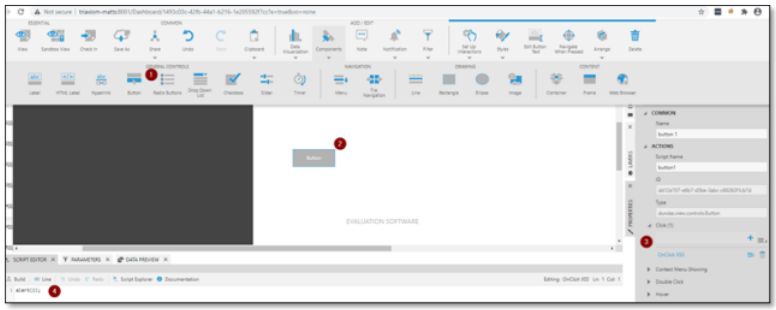
Version 8.0.0.1001 PoC



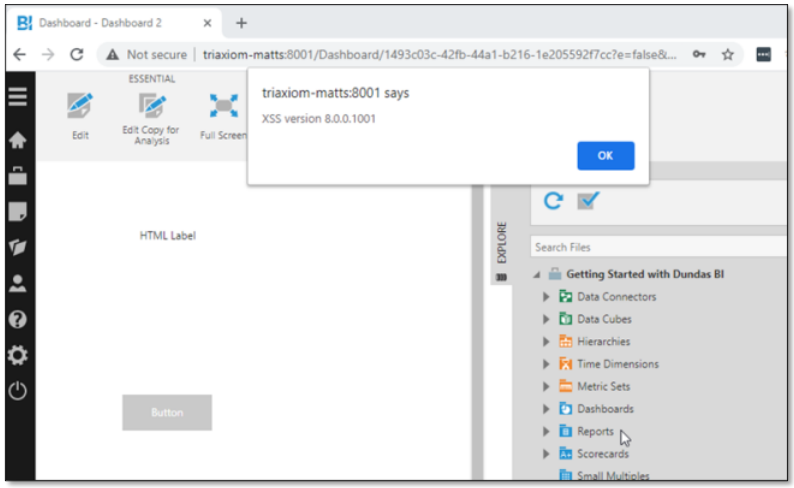
Version 8.0.0.1001 XSS executing

Button XSS

1. Click Components and add a button.
2. Select the button.
3. Click properties and select Click (or another action such as “Double Click”, “hover”, etc.)
4. Insert script and click “Build”.



Button XSS.



POSTED IN WRITEUP

RELATED POST

TCM SECURITY PNPT EXAM / CERTIFICATION REVIEW (UPDATED: 2/1/2022)

POSTED ON MAY 4, 2021 BY RUMHAM

THE CVE PROCESS

POSTED ON NOVEMBER 19, 2020 BY RUMHAM

REVIEW BOARD XSS DISCOVERED

POSTED ON APRIL 14, 2021 BY RUMHAM

PORTSWIGGER WEB ACADEMY REVIEW

THE CVE PROCESS