

Stored XSS possible through saved Workspace query name

000045986 | Troubleshooting | Last updated 2026-09-11 | TotalAgility

ISSUE

A saved Workspace query name is not safely encoded when it is displayed.

If HTML/JavaScript is entered as the query name, the value is stored and subsequently rendered as HTML. This allows JavaScript to execute when the relevant event is triggered.

Example payload:

```
<h1 onmouseover=alert('XSS')>XSS</h1>
```

Repro steps:

Open the Work Queue and create a new query.

Set the query name to:

```
<h1 onmouseover=alert('XSS')>XSS</h1>
```

Save the query.

Open the area where the saved query name is displayed.

Move the mouse over the query name.

Observe that the JavaScript executes and an alert is displayed.

CAUSE

This was confirmed as a Bug 2263984:[2026.4] Stored XSS possible through saved Workspace query name

SOLUTION

Bug was fixed and verified on upcoming TA 2026.4 version

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/45986>