Stored XSS in Tooltip in pimcore/pimcore

0

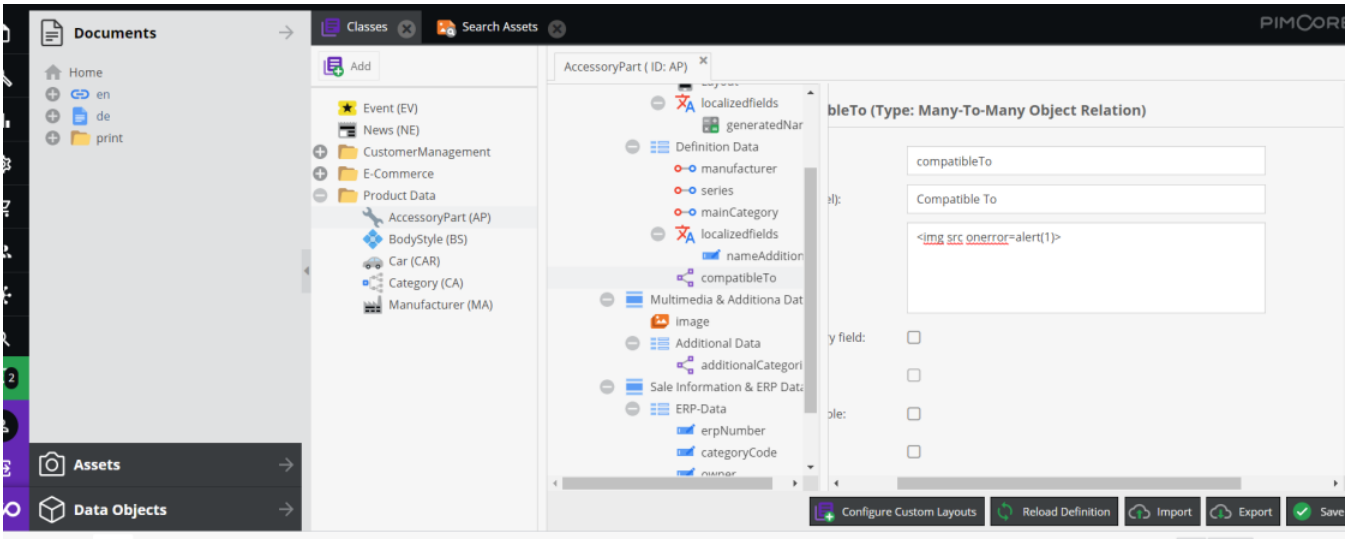
Valid Reported on Mar 23rd 2022

Description

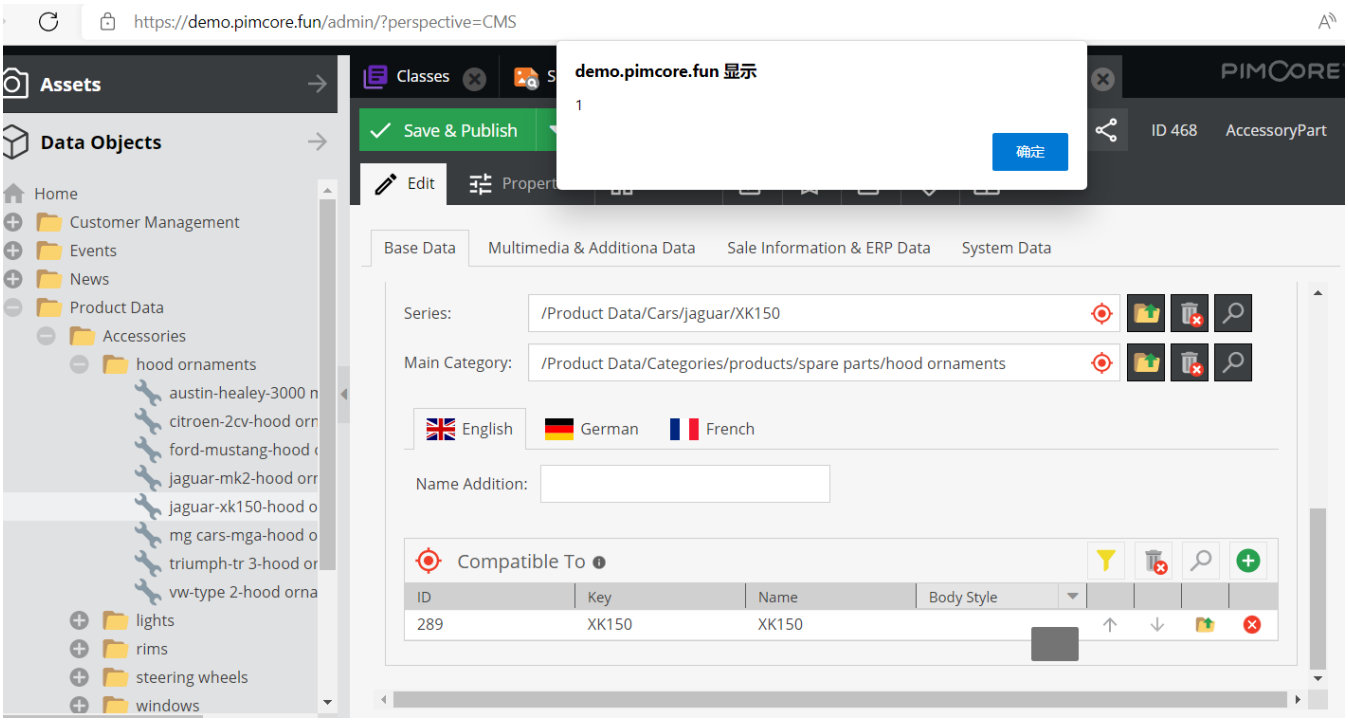
The Classes in Data Objects have the Tooltip field. It is vulnerable to XSS attack.

Proof of Concept

STEP1: login https://demo.pimcore.fun/admin/ STEP2: Settings->Data Objects->Classes. Then choose an item, like product Data->AccessoryPart (AP)->compatibleTo。 STEP3: add payload in tooltip field. <img src onerror=alert(1)> .then save.



STEP4: Open a AccessoryPart type Data Objects, and move the cursor on the Compatible To filed to trigger the event.



all the item contains tooltip field is vulnerable to the attack.

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

CVE
CVE-2022-1351
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by
mylong

@mylong

unranked

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 707 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 8 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 8 months ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 8 months ago

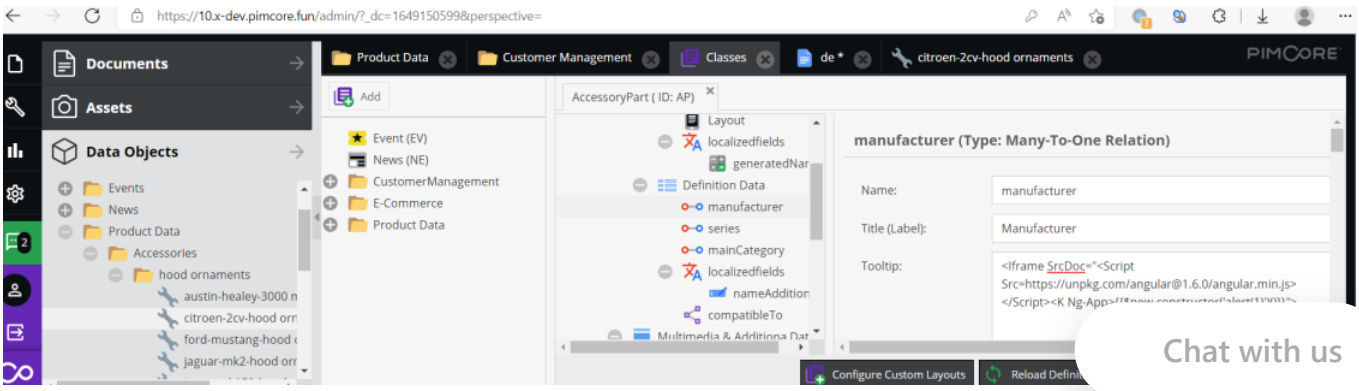
A **pimcore/pimcore** maintainer has acknowledged this report 8 months ago

Divesh Pahuja 8 months ago Maintainer

@mylong Hi, Pimcore comes with generic XSS protection handler, which is implemented on https://10.x-dev.pimcore.fun/admin. please try to reproduce the problem on master demo instance.

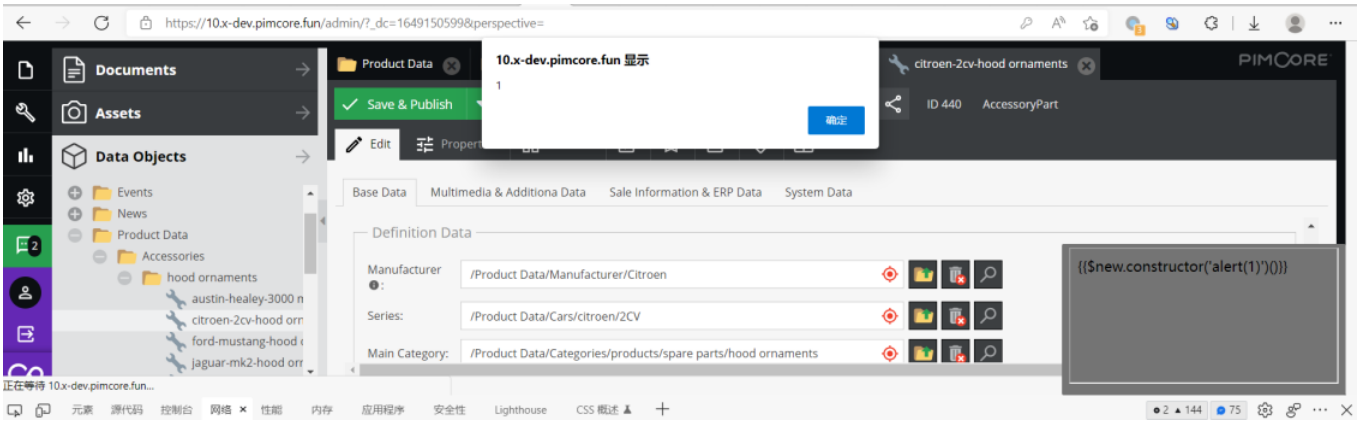
mylong 8 months ago Researcher

seems the csp works. since unpkg is in the whitelist. I can temporary use the following way to bypass the csp.
STEP1:



STEP2:

STEP2:



POC: <Iframe SrcDoc="<Script Src=https://unpkg.com/angular@1.6.0/angular.min.js></Script><KNg-App>{{$new.constructor('alert(1)')()}}">

Divesh Pahuja validated this vulnerability 7 months ago

mylong has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Divesh Pahuja marked this as fixed in **10.4** with commit **8c39a8** 7 months ago

Divesh Pahuja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

home
hacktivity
leaderboard
FAQ
contact us
terms
privacy policy

company
about
team