

## Stored Cross Site Scripting (XSS) via "properties" during creating new users in pimcore/pimcore

2



Valid

Reported on Sep 6th 2022

### Description

From demo url > login > click people icon at the left bar > click "Customers" > Click "New Customer" button from page > Fill up the "Edit" tab > Click "Save" button above > Click "Properties" tab > From "Add a custom Property" field , add "Test" on the first field > Click and select "text" on the second field > Click "+" button at the right of the field > On the table, click the key field to edit and add payload below:

```
mang"><img/src=x onerror=alert(/xss/)>
```

Then the XSS will triggered once the click any place in page.

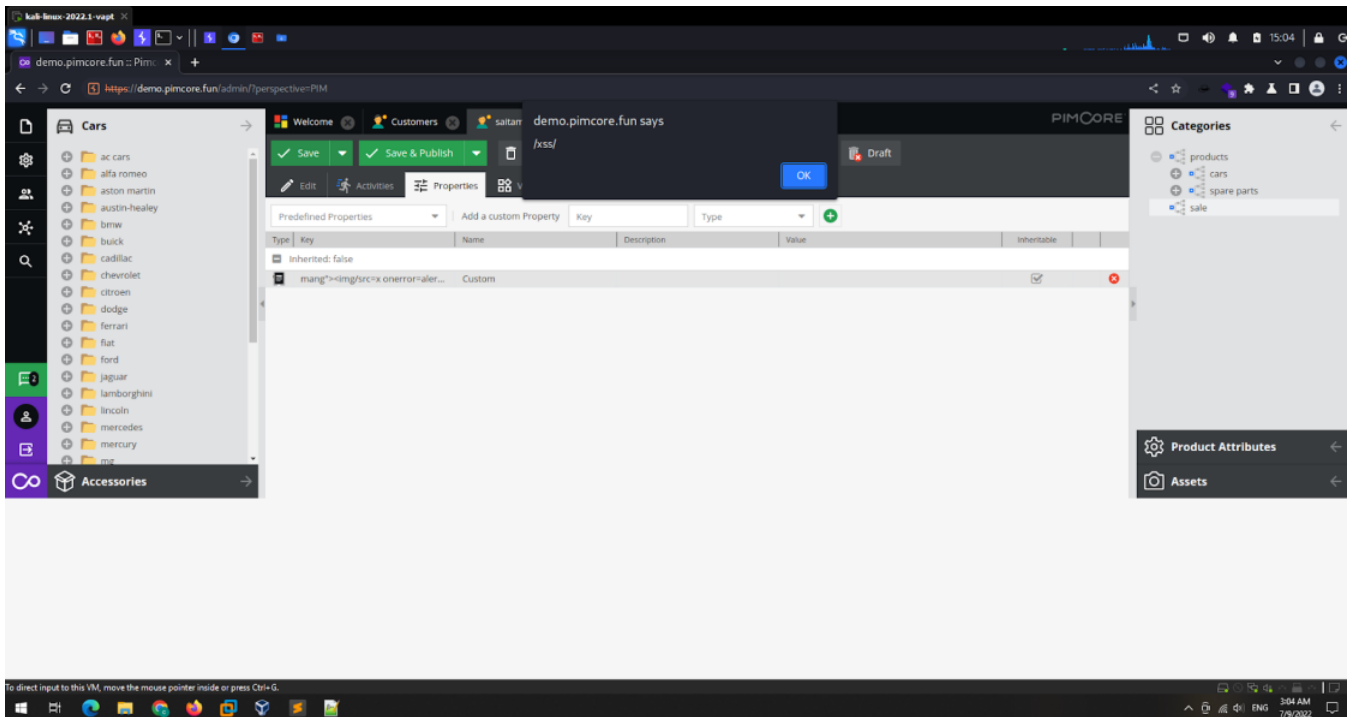
### Video Proof of Concept(PoC)

[https://drive.google.com/file/d/1sfuiGp\\_c0AqBth55aR5tEdmVNka\\_BG0x/view?usp=](https://drive.google.com/file/d/1sfuiGp_c0AqBth55aR5tEdmVNka_BG0x/view?usp=)



### Image PoC

[Chat with us](#)



## Impact

This vulnerability allows attackers to hijack the user's current session, steal relevant information, deface website or direct users to malicious websites and allows attacker to use for further exploitation.

## Occurrences

 UserController.php L277-L385

### CVE

CVE-2022-3211

(Published)

### Vulnerability Type

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

### Severity

Medium (5.8)

### Registry

Other

Chat with us

## Affected Version

10.5.5

## Visibility

Public

## Status

Fixed

## Found by



**Saitamang**

@saitamang

unranked ▼

## Fixed by



**Divesh Pahuja**

@dvesh3

maintainer

This report was seen 765 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 3 months ago

**Saitamang** modified the report 3 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 3 months ago

A **pimcore/pimcore** maintainer has acknowledged this report 3 months ago

**Divesh Pahuja** modified the Severity from High (7.7) to Medium (5.8) 2 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

**Divesh Pahuja** validated this vulnerability 2 months ago

**Saitamang** has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

Divesh Pahuja marked this as fixed in 10.5.6 with commit 0508c4 2 months ago

Divesh Pahuja has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

UserController.php#L277-L385 has been validated ✓

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us