SQL injection in GridHelperService.php in pimcore/pimcore

0

Valid 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

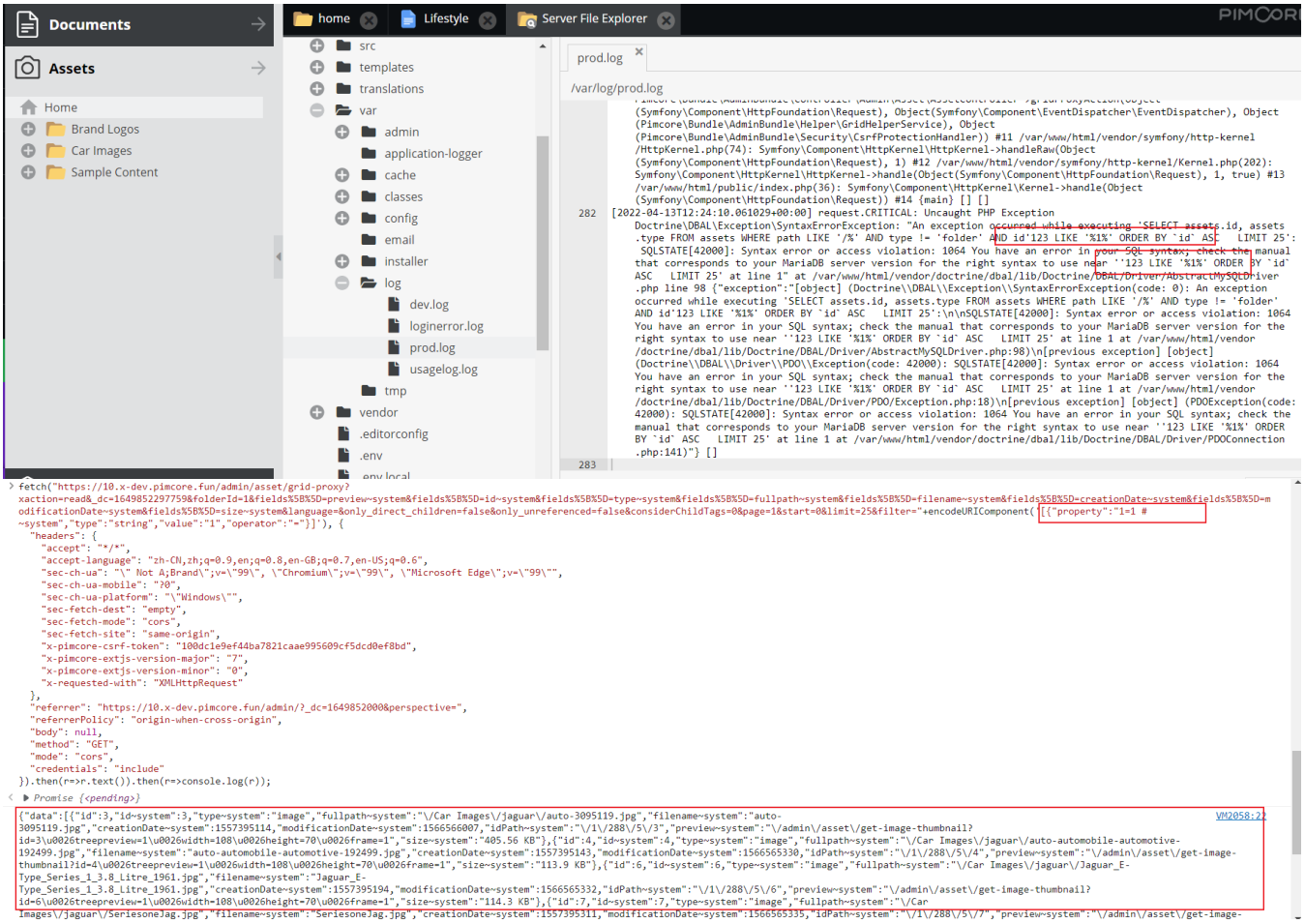
Proof of Concept

/grid-proxy

```
https://10.x-dev.pimcore.fun/admin/asset/grid-proxy?xaction=read&_dc=16498
```

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

the error log.



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

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 ✖

Sign in to join this conversation

Chat with us