New issue

Jump to bottom

SQL Injection Vulnerabilities #261

Open **xiaoxianghuayu** opened this issue on Jul 3 · 2 comments

xiaoxianghuayu commented on Jul 3

There are 2 time-based SQL Injection Vulnerabilities, in /load_data_for_groups.php and /load_data_for_topusers.php respectively.

ENV:
ubuntu14.04
php 5.5.9
mysql 5.5.62

SQL Injection in /load_data_for_groups.php

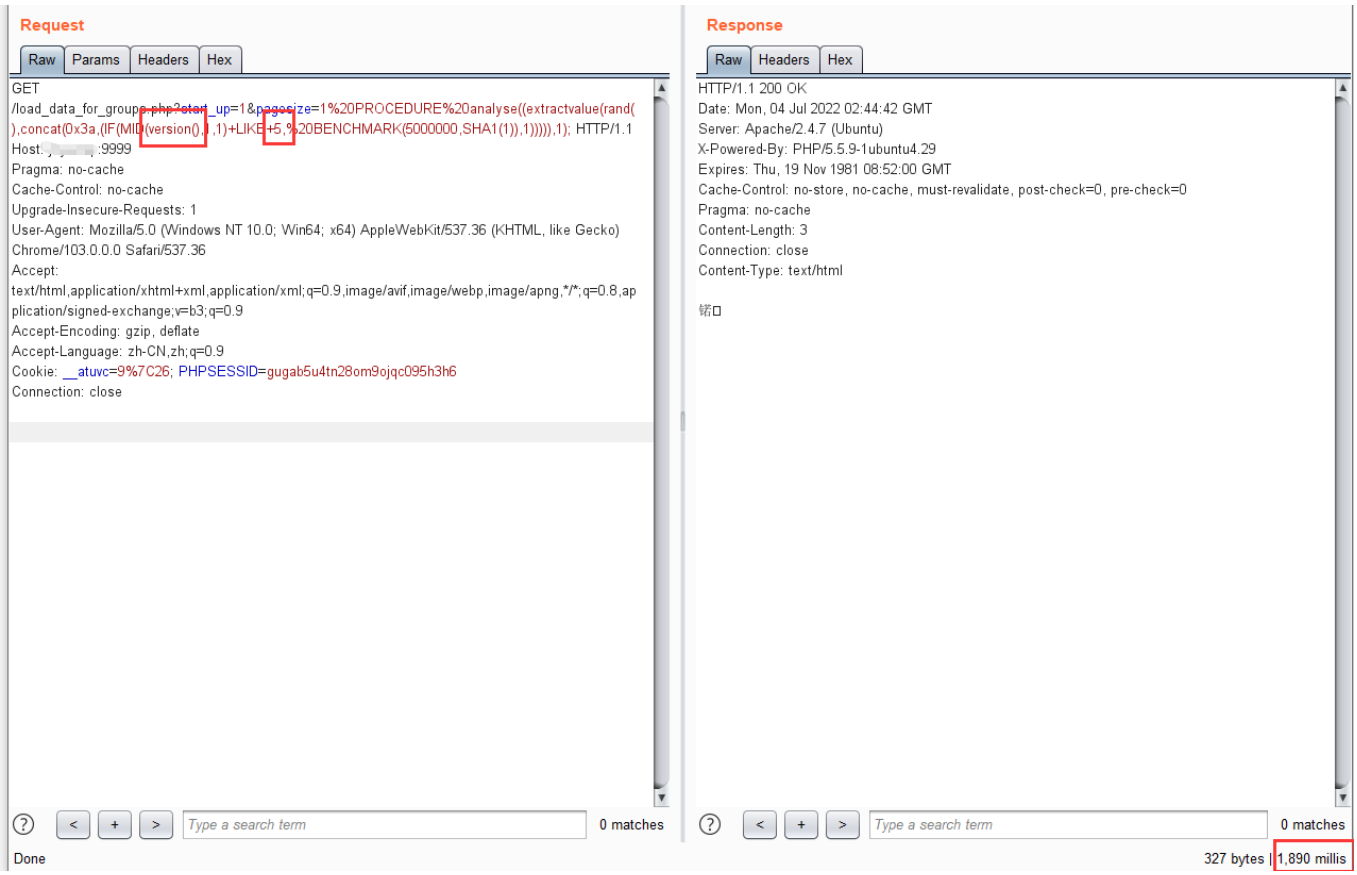
vulnerable code:

Line16: the $page_size is user controllable and directly used in sql statement which may cause a time-based sql injection

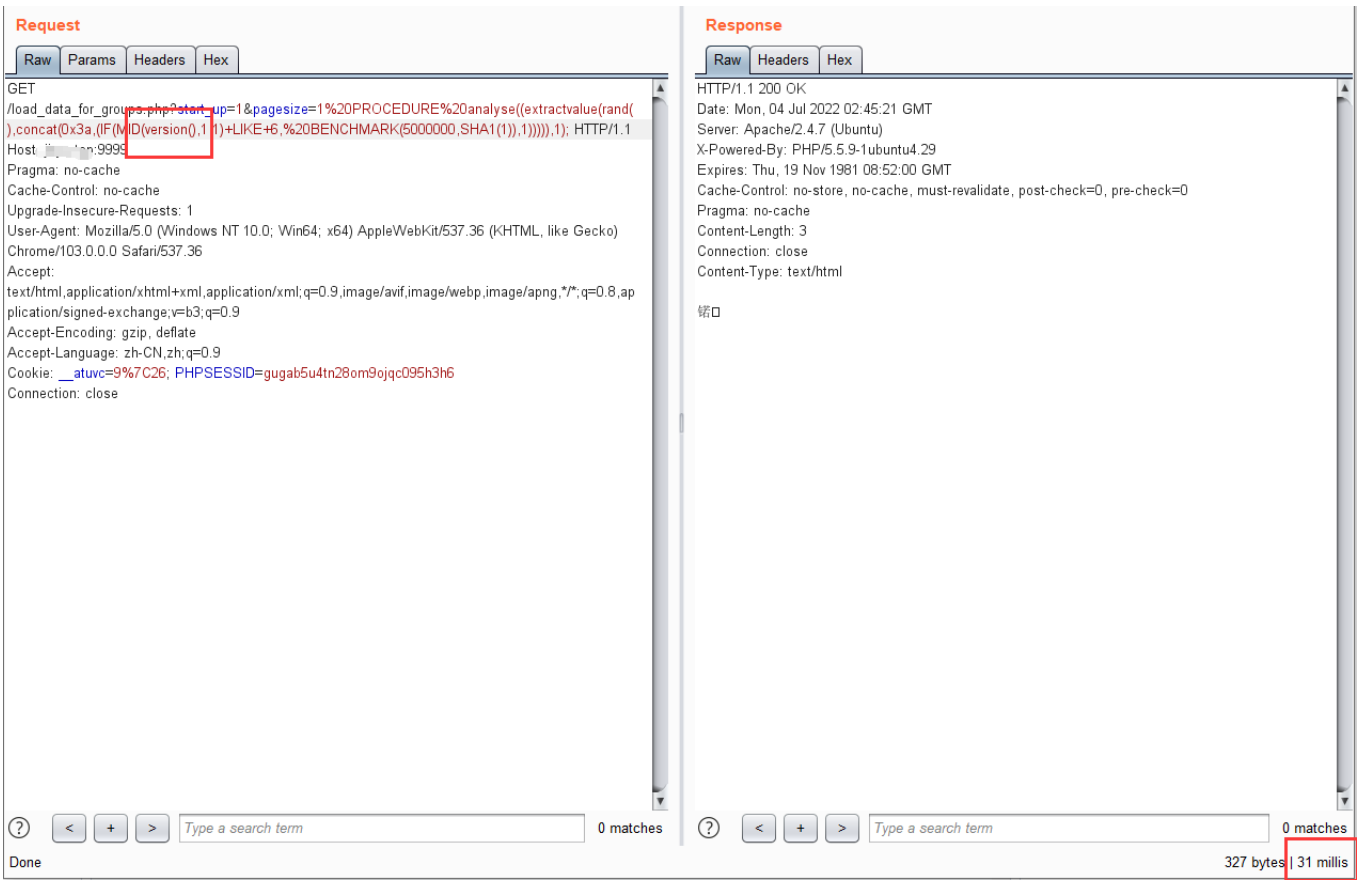
```
13          $start_up = isset($_REQUEST['start_up'])? $_REQUEST['start_up'] : "";
14          $page_size = isset($_REQUEST['pagesize']) ? $_REQUEST['pagesize'] : "";
15
16          $group = $db->get_results("SELECT * FROM " . table_groups . " WHERE group_status='Enable' ORDER BY group_status, group_date  DESC LIMIT $start_up, $page_size");
17
```

POC:

trigger the sql injection(my mysql version is 5.5.62):



do not trigger:



SQL Injection in /load_data_for_topusers.php

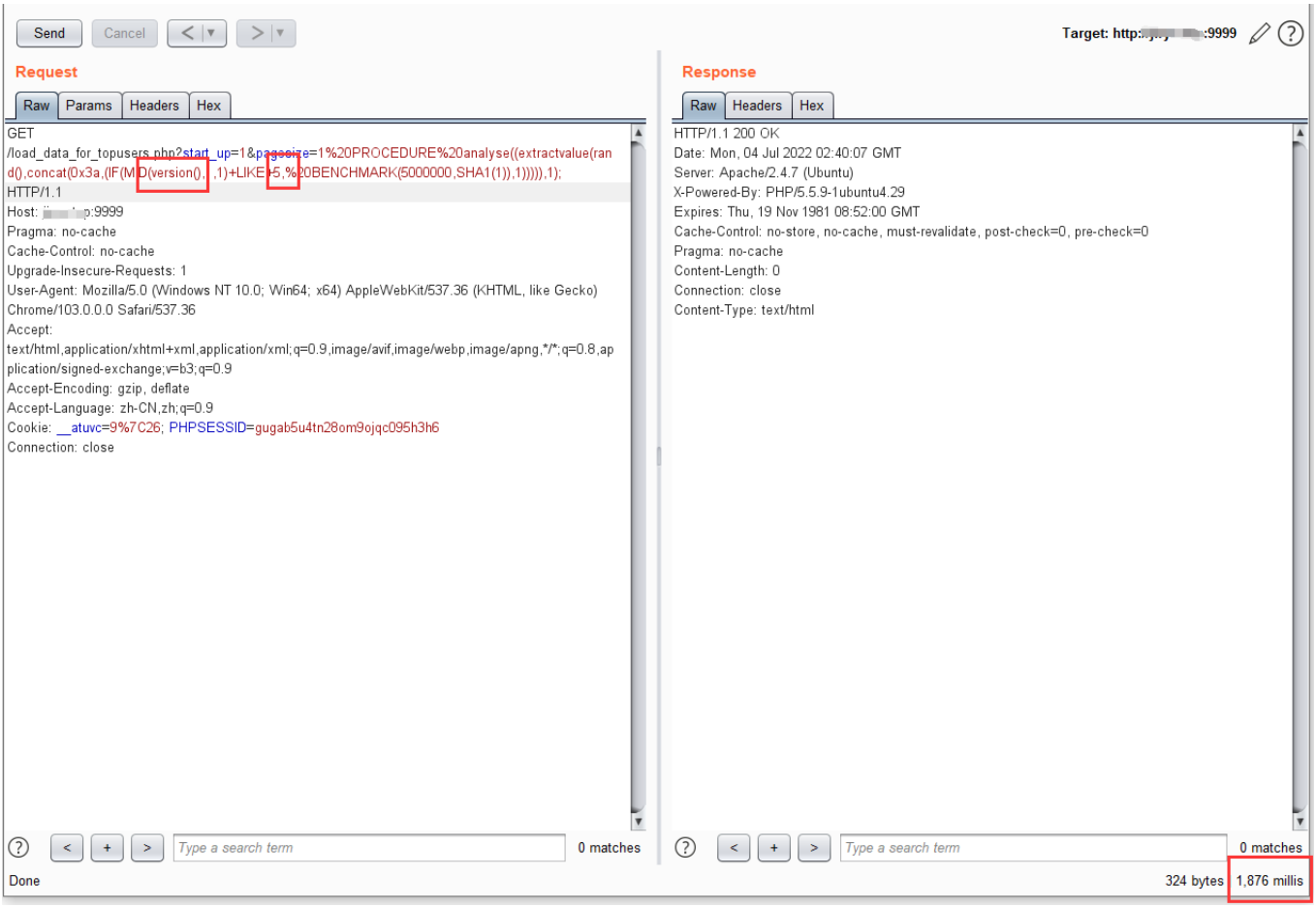
vulnerable code:

Line30: the $page_size is user controllable and directly used in sql statement which may cause a time-based sql injection

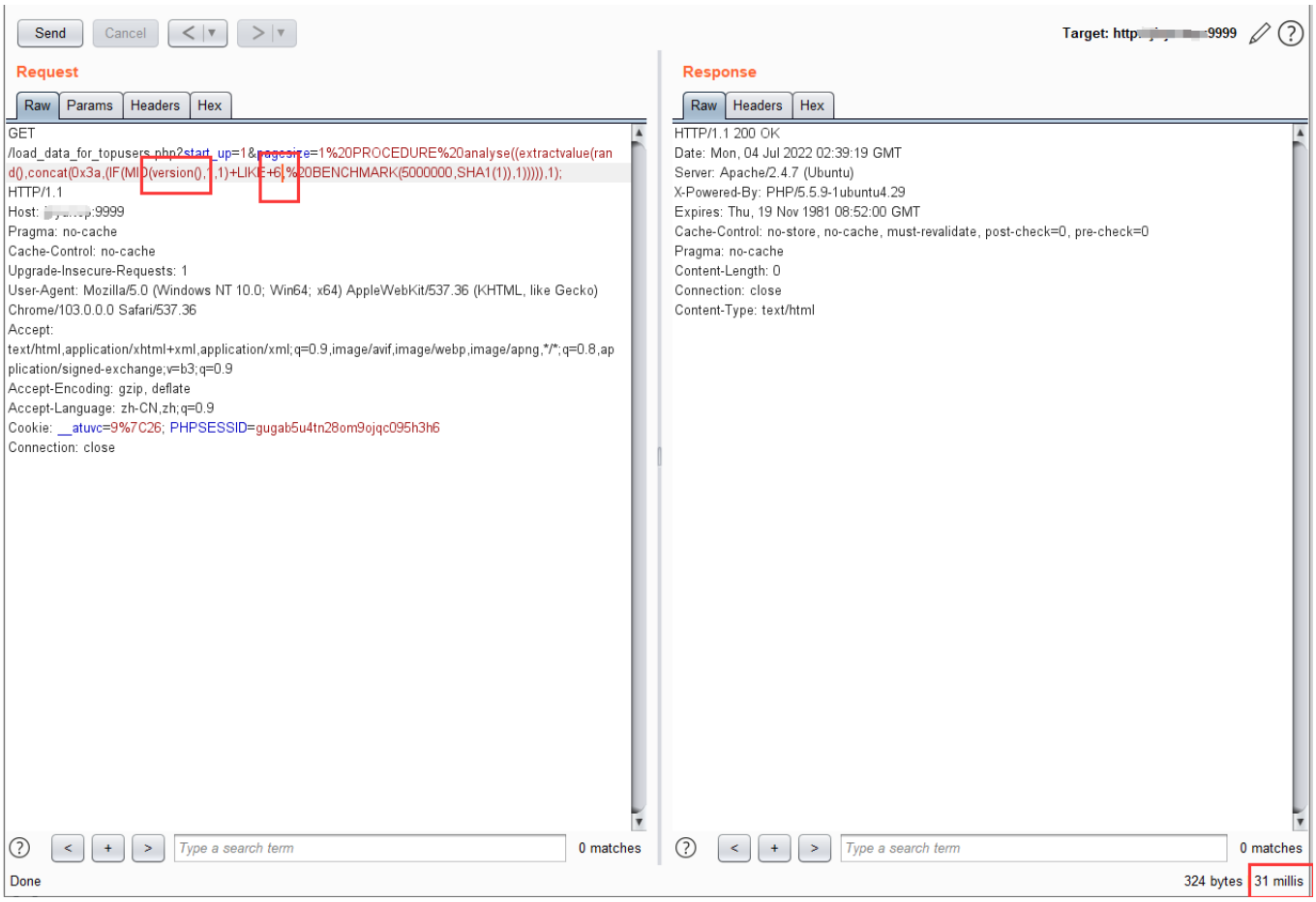
```
13
14      $start_up = isset($_REQUEST['start_up'])? $_REQUEST['start_up'] : "";
15      $page_size = isset($_REQUEST['pagesize']) ? $_REQUEST['pagesize'] : "";
16
17
18  $users = $db->get_results("SELECT user_karma, COUNT(*) FROM " . table_users . " WHERE user_karma > 0 $whether_to_show_user GROUP BY user_karma ORDER BY user_karma DESC", ARRAY_N);
19
20      $ranklist = array();
21      $rank = 1;
22      if ($users)
23          foreach ($users as $dbuser)
24          {
25              $ranklist[$dbuser[0]] = $rank;
26              $rank += $dbuser[1];
27          }
28
29
30      $users = $db->get_results("SELECT user_id FROM pligg_users WHERE user_karma > 0 AND user_enabled = 1 AND user_level <> 'Spammer' AND (user_login != 'anonymous' OR user_lastip) ORDER BY user_karma DESC LIMIT $start_up, $page_size");
31
32      $user = new User;
```

POC:

trigger the sql injection(my mysql version is 5.5.62):



do not trigger:



1

sqrtZeroKnowled... commented on Jul 19

I confirm, It's blind SQL INJECTION.

redwinefireplace commented on Sep 23

Kliqqi has been discontinued since 2018. I wouldn't recommend using it.

Assignees

No one assigned

Labels

None yet

Projects

None yet

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants