

**SQL** Injection Vulnerabilities #261

Open

New issue

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

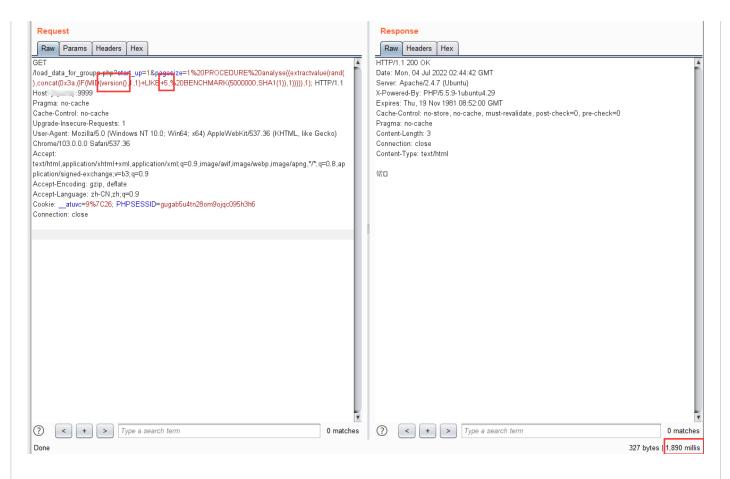
vulnerable code:

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

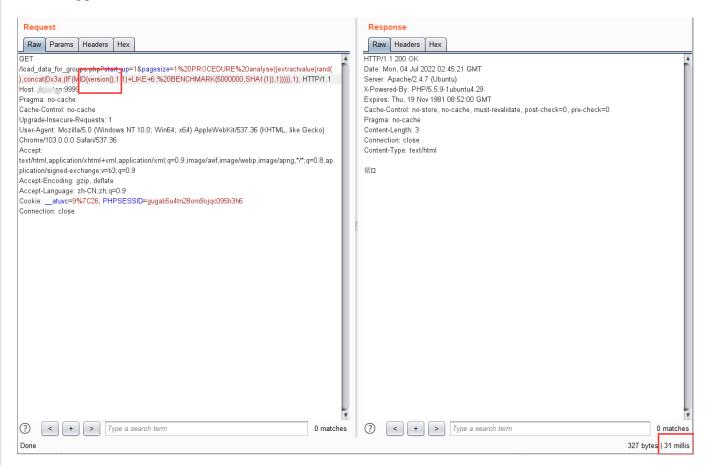
```
13
             $start_up = isset($_REQUEST['start_up'])? $_REQUEST['start_up'] : "";
            $page_size = isset($_REQUEST['pagesize']) ? $_REQUEST['pagesize'] : "";
15
             $group = $db->get_results("SELECT * FROM " . table_groups . " WHERE group_status='Enable' ORDER BY group_status,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

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:

Line 30: the \$page\_size is user controllable and directly used in sql statement which may cause a time-based sql injection

```
Start_up = |sset($_REQUEST['start_up'])? $_REQUEST['start_up'] : "";

| Spage_size = |sset($_REQUEST['start_up'])? $_REQUEST['pagesize'] : "";

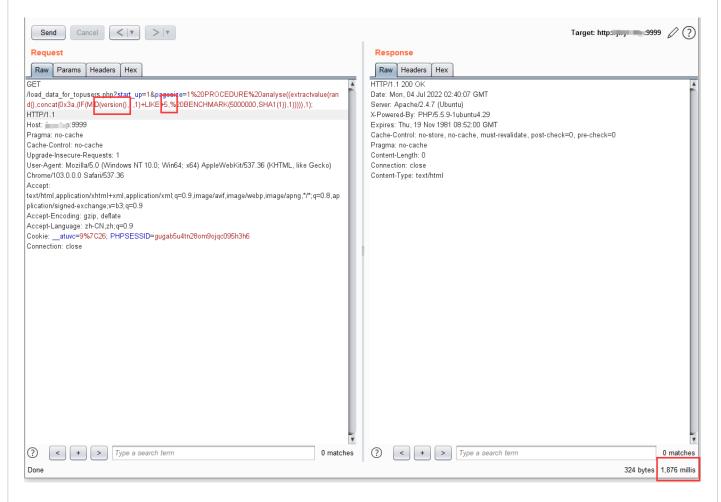
| Susers = $db-yet_results("SELECT_user_karma, COUNT(*) FROM " . table_users . " MHERE user_karma > 0 $whether_to_show_user GROUP BY user_karma ORDER BY user_karma DESC", ARRAY_N);

| Sranklist = array();
| Frank = 1;
| if (susers) |
| foreach (busers as $dbuser) |
| foreach (busers as $dbuser[0]] = $rank;
| $rank + $$dbuser[0]] = $rank;
| $rank + $$dbuser[0]] = $rank;
| $srank + $$dbuser[1];
| Susers = $db-yet_results("SELECT_user_id FROM pligg_users MMERE 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");

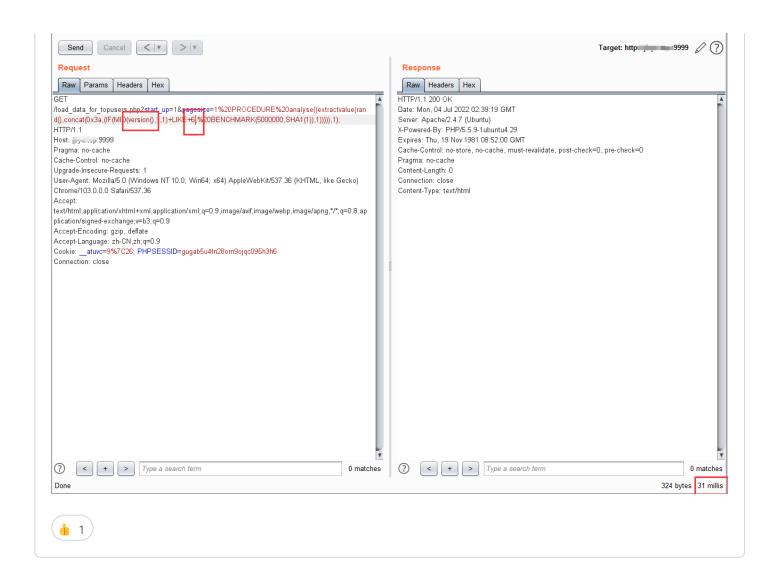
| Suser = new User;
```

POC:

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



do not trigger:



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 vet

ı	NUI	ı	ycι

Milestone

No milestone

Development

No branches or pull requests

## 3 participants





