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

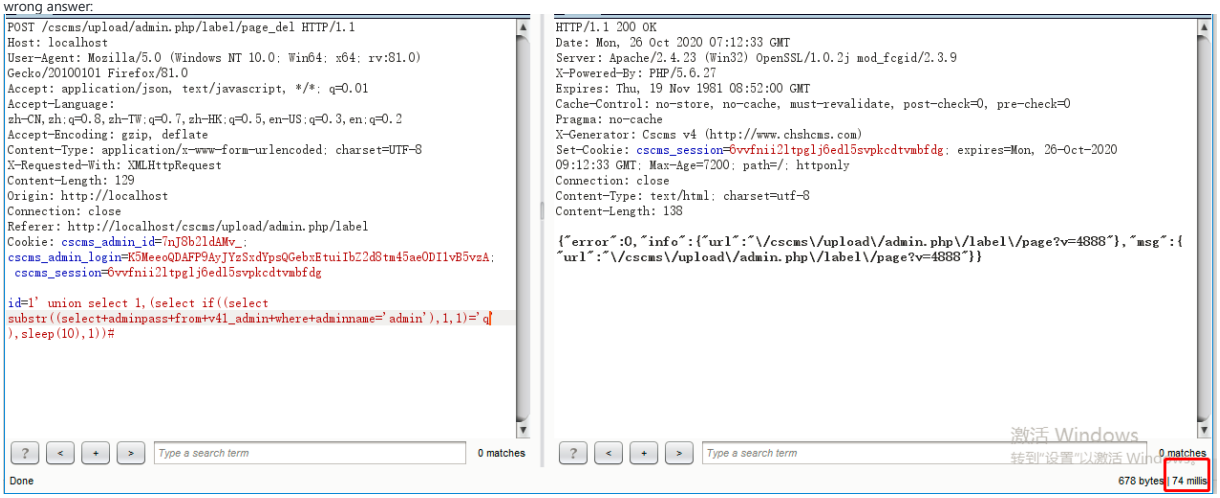
Vulnerability file:cscms4.1\plugins\sys\admin\label.php 197 lines-219 lines
Vulnerability function： js_del
Vulnerability param:id

```
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);
}
}
$this->Csdb->get_del('ads',$id);
$info['url'] = site_url('label/js').'?v='.rand(1000,9999);
getjson($info,0);
}
```

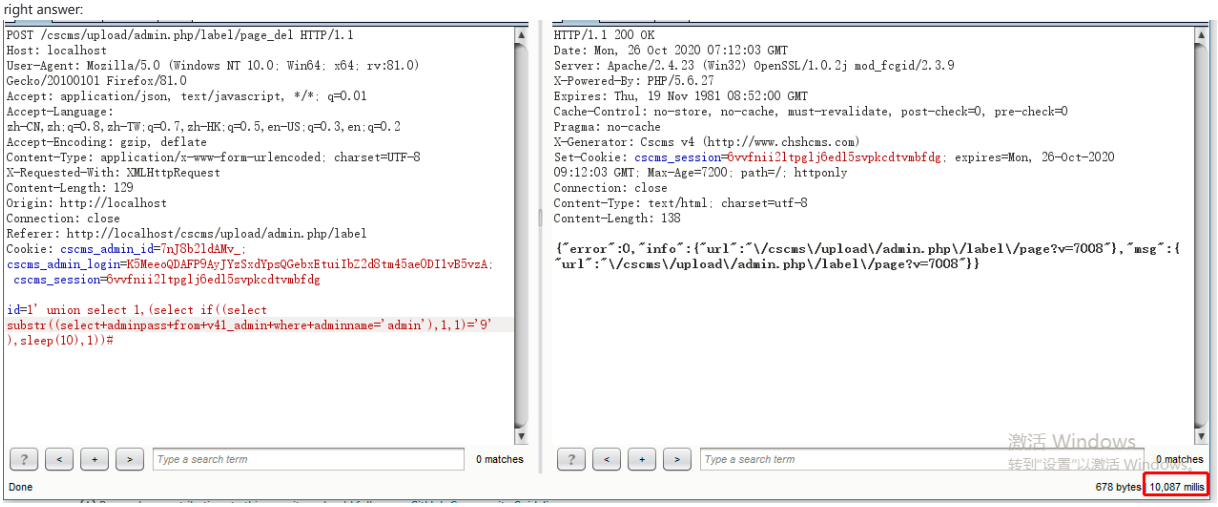
3.vulnerability exploitation

sql injection type：timebased-sqlinjection

wrong answer:



right answer:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant