

[New issue](#)[Jump to bottom](#)

Persistent cross-site scripting (XSS) targeted towards web admin through /admin-panel1.php at via the parameter detail. #20

[Open](#) fuzzyap1 opened this issue on Feb 13 · 0 comments

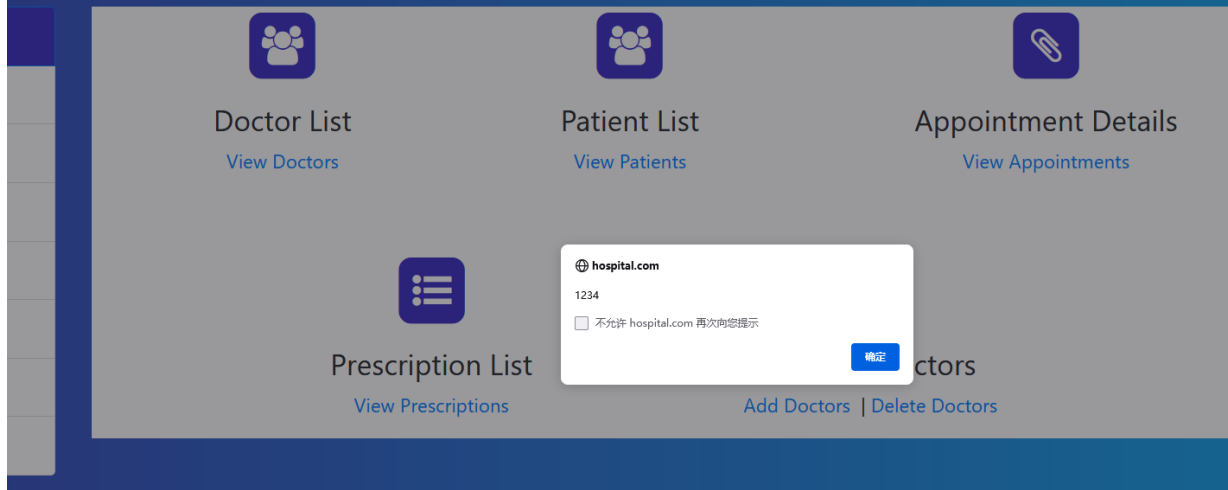
fuzzyap1 commented on Feb 13

Persistent cross-site scripting (XSS) in Hospital Management System v4.0 targeted towards web admin through /admin-panel1.php at via the parameter detail.

Add Doctor info payload to Doctor Name of Add Doctor page to target /admin-panel1.php ,then use burpsuite get requests datas,change the 'detail' parameter to xss payload: `<script>alert(5555)</script>`

The image shows a screenshot of the 'Add Doctor' form in the Hospital Management System v4.0. The form has a blue header with the text 'WELCOME RECEPTIONIST'. The form fields are: Doctor Name (www), Specialization (Select Specialization), Email ID (www@123.com), Password (*****), Confirm Password (*****), and Consultancy Fees (5555). There is an 'Add Doctor' button at the bottom. To the right of the form is a screenshot of the Burp Suite HTTP history. The selected request is a POST to /admin-panel1.php. The request body is: `doctor=www&detail=www@123.com<script>alert(5555)</script>&password=qqqq&consultancy=5555&docid=AddDoctor`. The Burp Suite interface shows the request details, including the URL, headers, and body.

WELCOME RECEPTIONIST



Proof of concept (Poc)

<sCrIpT>alert(5555)</ScRiPt>

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

