<> Code   ⊙ **Issues** 23   ⑂ Pull requests 4   ▷ Actions   ⊞ Projects   ⊘ Security   •••

New issue   **Jump to bottom**

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

⊙ **Open**   **fuzzyap1** opened this issue on Feb 13 · 0 comments
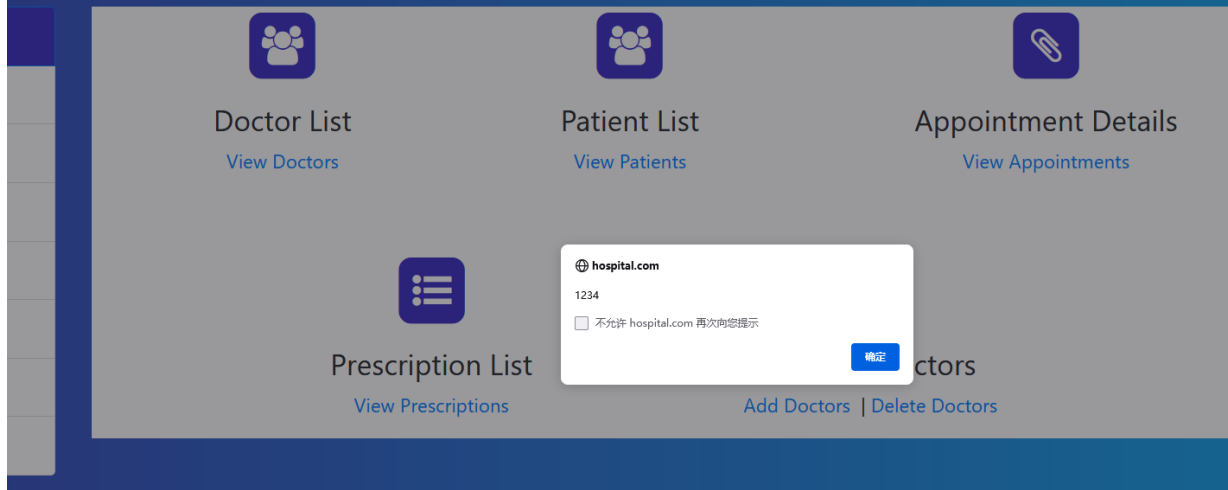
---

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 demail.

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

WELCOME RECEPTIONIST

Doctor List
View Doctors

Patient List
View Patients

Appointment Details
View Appointments

Prescription List
View Prescriptions

🌐 hospital.com

1234

☐ 不允许 hospital.com 再次向您提示

确定

ctors

Add Doctors | Delete Doctors

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