README.md

CVE-2021-38149

Chikitsa Patient Management System 2.0.0 Stored Cross-Site Scripting (XSS)

An instance of stored cross-site scripting (XSS) exists in multiple pages on version 2.0.0 of Chikitsa Patient Management System that allows for arbitrary JavaScript to be executed in a user's browswer that could potentially allow for a user to escalate privileges.

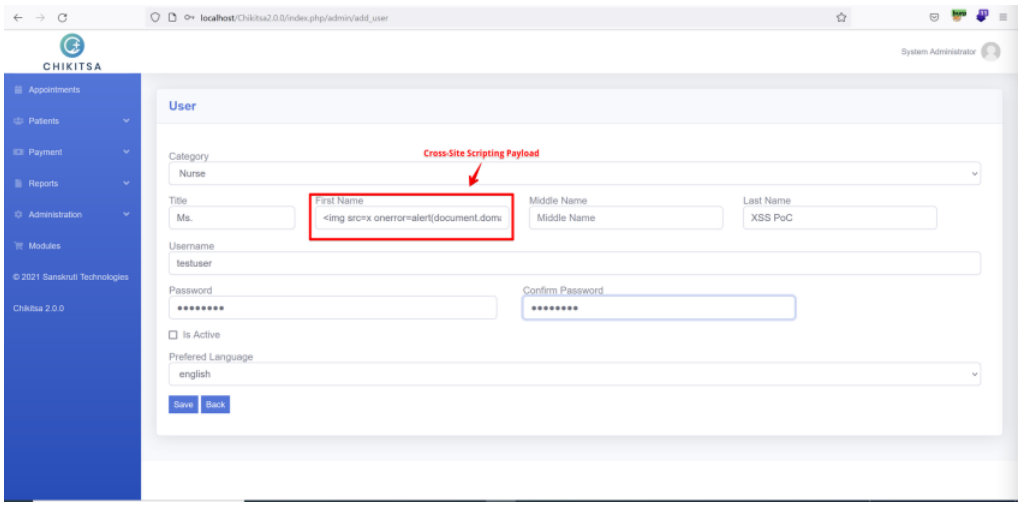
Vulnerable Pages:

- /index.php/admin/add_user
- /index.php/appointment/todos
- /index.php/appointment/insert_patient_add_appointment/(hr of apppointment)/(minute of appointment)//Appointments//0/

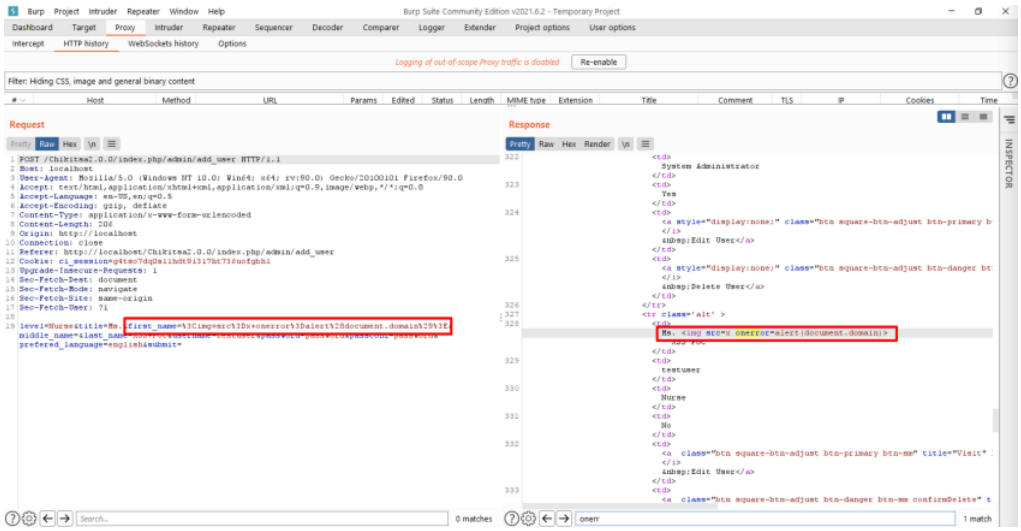
Known Cross-Site Scripting Payloads That Work:

- `<script>alert('xss');</script>`
- `<img src=x onerror=alert(document.domain)>`

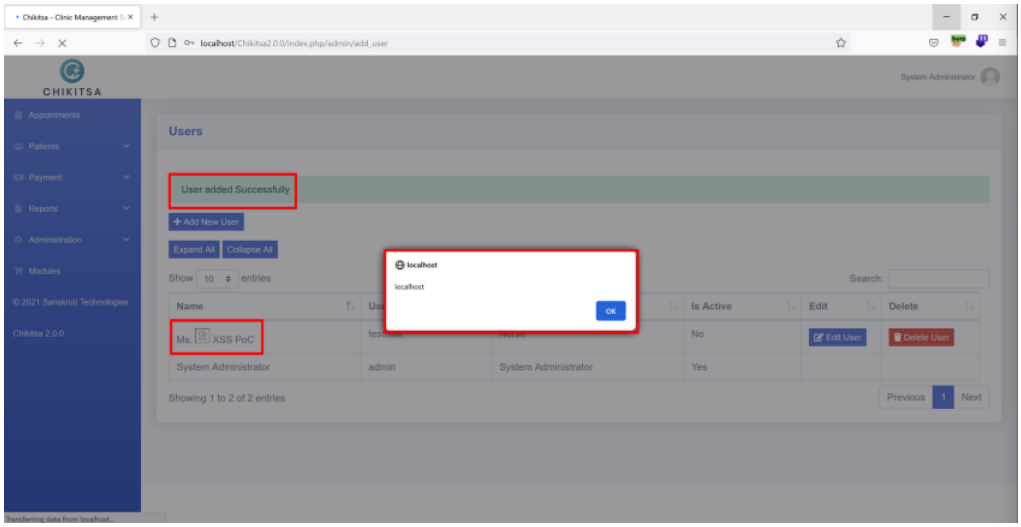
Proof of Concept:



A user with privileges to create other users has the ability to create users can input a XSS payload into any of the user's name fields shown above.



Observing the application's response reveals that the JavaScript is being reflected.



The created user containing the malicious XSS payload has successfully been created and will execute the JavaScript everytime a user visits the users the application contains.

Discovered By: Joe Aguilar Jr.

Releases

No releases published

Packages

No packages published