Cross site scripting in Remote Clinic v2.0

Multiple cross-site scripting vulnerabilities are present in Remote Clinic 2.0. The following is detailed information about these vulnerabilities:

There are multiple Cross-Site Scripting vulnerabilities via the parameters in /patients/register-patient.php are vulnerable due to the _POSTs not being sanitized properly for XSS despite being sent through the friendly function.

File: /patients/register-patient.php

Parameters: Contact, Email, Weight, Profession, ref_contact, address

There is Stored Cross-Site Scripting and no sanitization for the parameters when retrieved by _POST in /patients/register-patient.php to be sent to the database. Attack can be made by changing the values in the dropdowns in the inspect menu.

File: /patients/register-patient.php

Parameters: gender, age, serial

In patients/edit-patient.php, the parameters being edited are not sanitized for Cross-Site Scripting when they are retrieved by _POST.

File: patients/edit-patient.php

Parameters: Contact, Email, Weight, Profession, ref_contact, address

In patients/edit-patient.php, the serial, age, and gender dropdowns values are unsanitized and is prone to XSS attacks via inspect menu

File: patients/edit-patient.php

Parameters: serial, age, gender

In staff/edit-my-profile.php, the parameters sent by _POST to be put in the database, is unsanitized and prone to Cross-Site Scripting (XSS)

File: staff/edit-my-profile.php

Parameters: Title, First Name, Last Name, Skype, Address

In clinics/settings.php, most of the parameters being passed into the database are sanitized insufficiently.

File: clinics/settings.php

Parameters: portal_name, guardian_short_name, guardian_name, opening_time, closing_time, access_level_5, access_level_4,access_level_ 3, access_level_2, access_level_1, currency, mobile_number, address, patient_contact, patient_address, patient_email

Submitted issue: https://github.com/remoteclinic/RemoteClinic/issues/17[https://github.com/remoteclinic/RemoteClinic/issues/17]

Above vulnerabilities are published at CVE-2021-39416[https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39416]

This vulnerability was detected as part of the DARPA CHESS program[https://www.darpa.mil/program/computers-and-humans-exploring-software-security]