Exploit Title: EGavilanMedia - User Registration and Login System With Admin Panel - Persistent Cross-Site Scripting on admin Manage User tab

Date: 19-11-2020

Exploit Author: Hemant Patidar (HemantSolo)

Vendor Homepage: http://egavilanmedia.com/

Software Link: http://egavilanmedia.com/user-registration-and-login-system-with-admin-panel/

Version: 1.0

Tested on: Windows 10/Kali Linux

Contact: https://www.linkedin.com/in/hemantsolo/

Stored Cross-site scripting(XSS):

Stored XSS, also known as persistent XSS, is the more damaging of the two. It occurs when a malicious script is injected directly into a vulnerable web application. Reflected XSS involves the reflecting of a malicious script off of a web application, onto a user's browser.

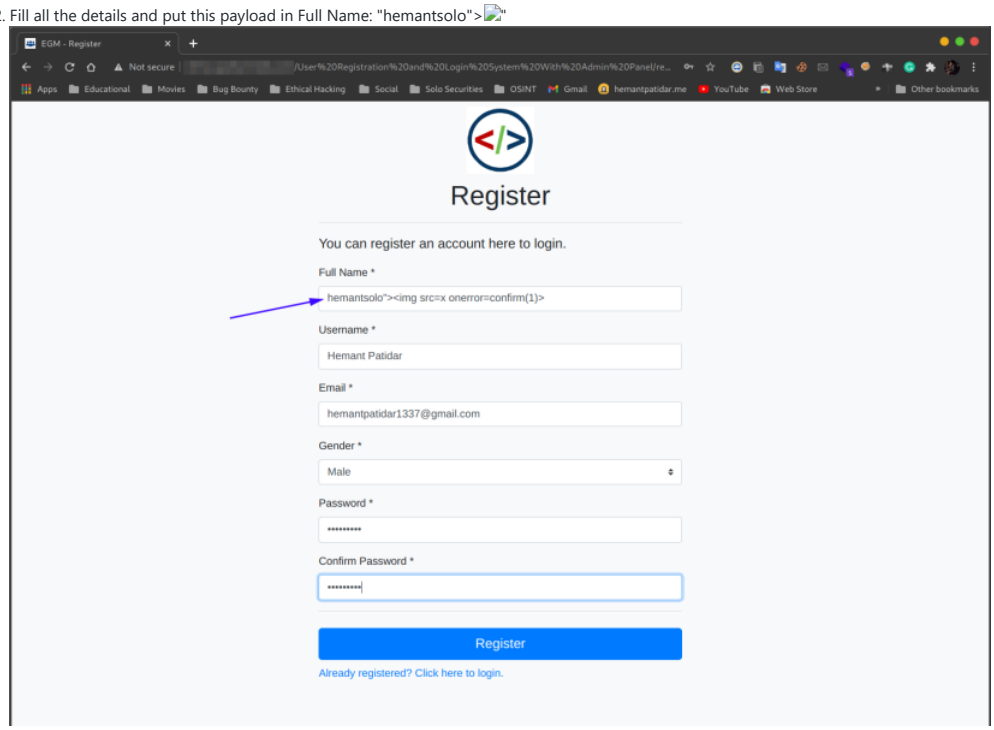
Attack vector:

This vulnerability can results attacker to inject the XSS payload in User Registration section and each time admin visits the manage user section from admin panel, the XSS triggers and attacker can able to steal the cookie according to the crafted payload.

Vulnerable Parameters: Full Name.

Steps-To-Reproduce:

1. Go to the registration page.

2. Fill all the details and put this payload in Full Name: "hemantsolo"> 

3. Now go to the admin panel-manage user tab and the XSS will be triggered.