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

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:

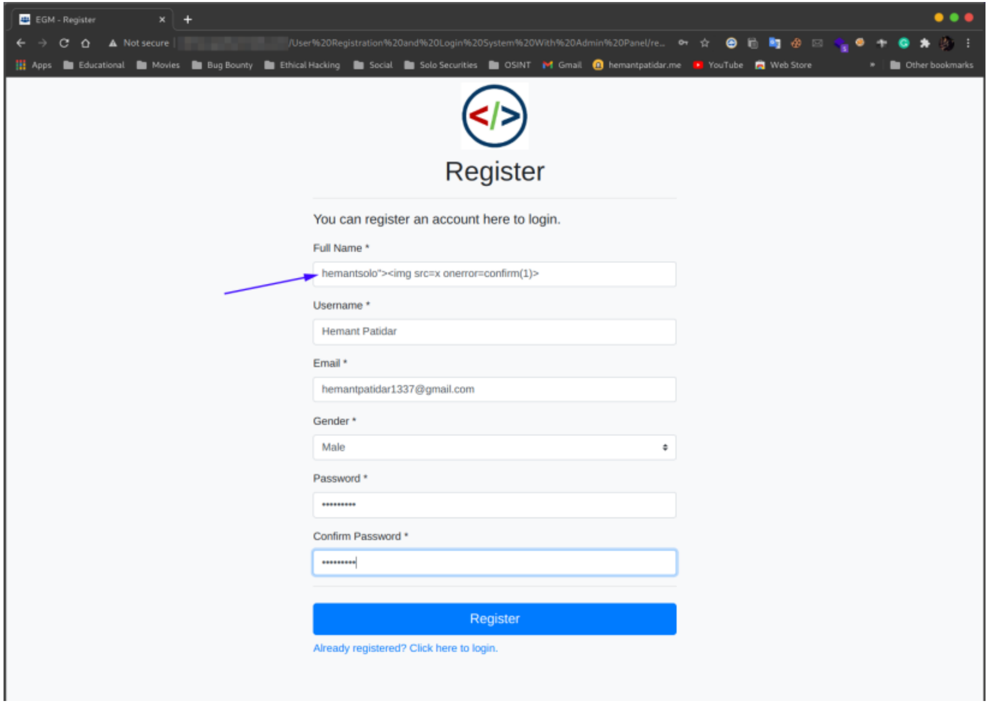
This vulnerability can results attacker inject the XSS payload in the User Registration section and each time when he will go to the dashboard, the XSS triggers, and the attacker can able to steal the cookie according to the crafted payload and can do malicious activities with the server.

Vulnerable Parameters: First Name, Last Name

Steps-to-reproduce:

1. Go to the user Registration page.

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



Register

You can register an account here to login.

Full Name *
hemantsolo"><img src=x onerror=confirm(1)>

Username *
Hemant Patidar

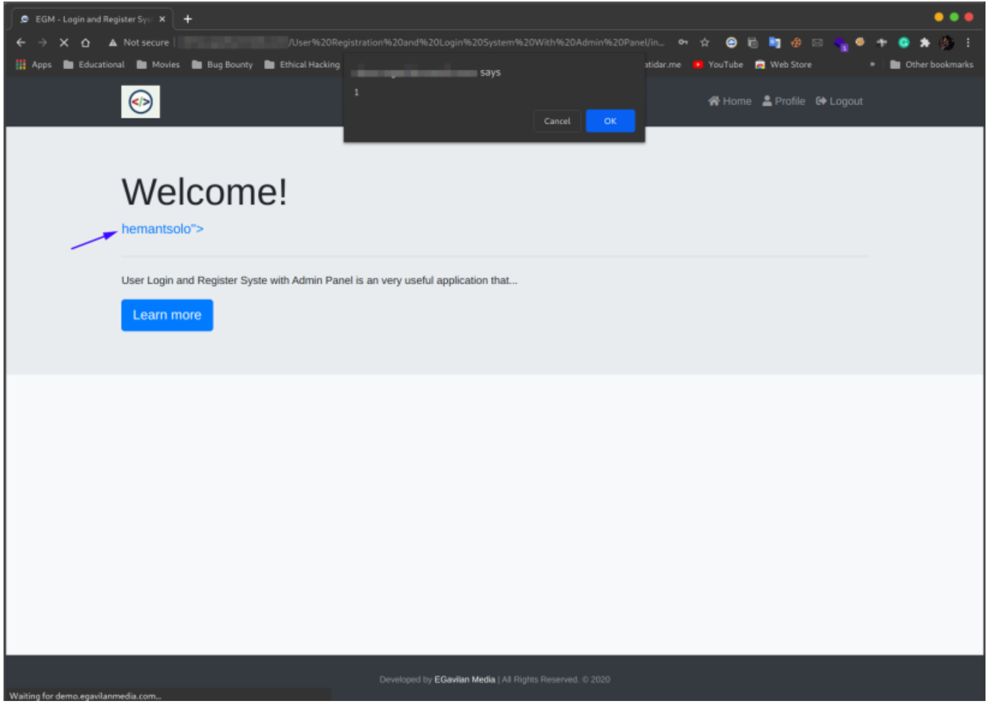
Email *
hemantpatidar1337@gmail.com

Gender *
Male

Password *
•••••••••

Confirm Password *
•••••••••

3. Now login your account and the payload will execute.


EGM - Login and Register Sys
Not secure
[redacted]/User%20Registration%20and%20Login%20System%20With%20Admin%20Panel/in...
Apps
Educational
Movies
Bug Bounty
Ethical Hacking
...tidar.me
YouTube
Web Store
Other bookmarks
Home
Profile
Logout

[redacted] says
1

Welcome!

hemantsolo">

User Login and Register Syste with Admin Panel is an very useful application that...

Learn more
Developed by EGavilan Media | All Rights Reserved. © 2020
Waiting for demo.egavilanmedia.com...