Exploit Title: User Registration and Login System With Admin Panel Exploit - SQLi in user login page leads to account takeover

Date: 19-11-2020

Exploit Author: Hemant Patidar

Vendor Homepage: http://egavilanmedia.com

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

Version: 1.0

Tested on: Kali Linux and Windows 10

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

SQL Injection:

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

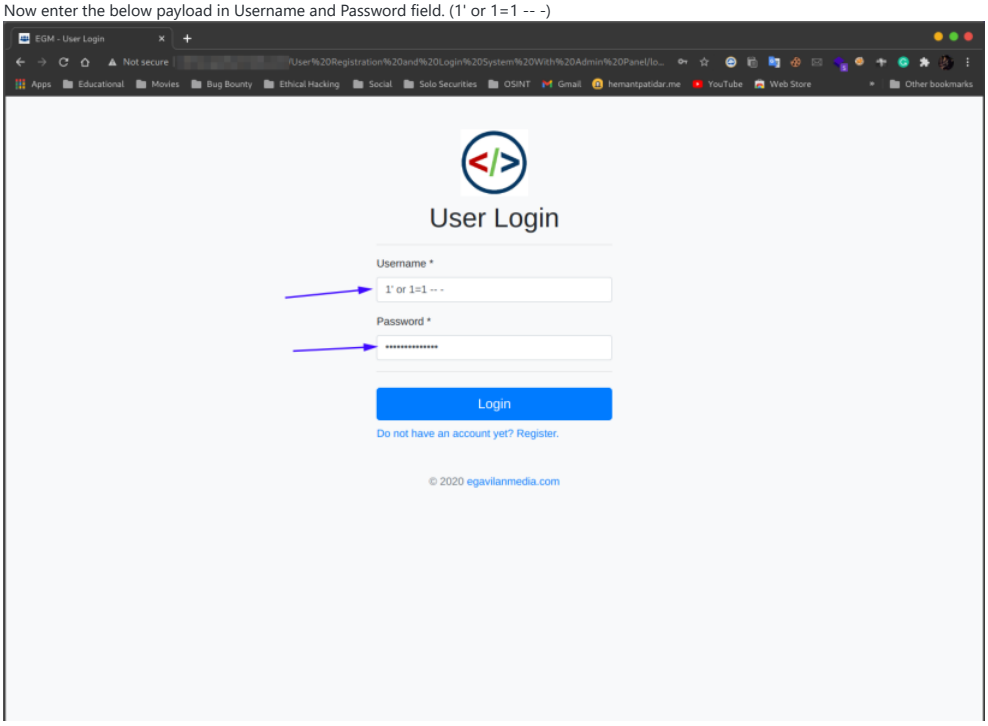
Attack Vector:

An attacker can gain any User's account login access using SQLi.

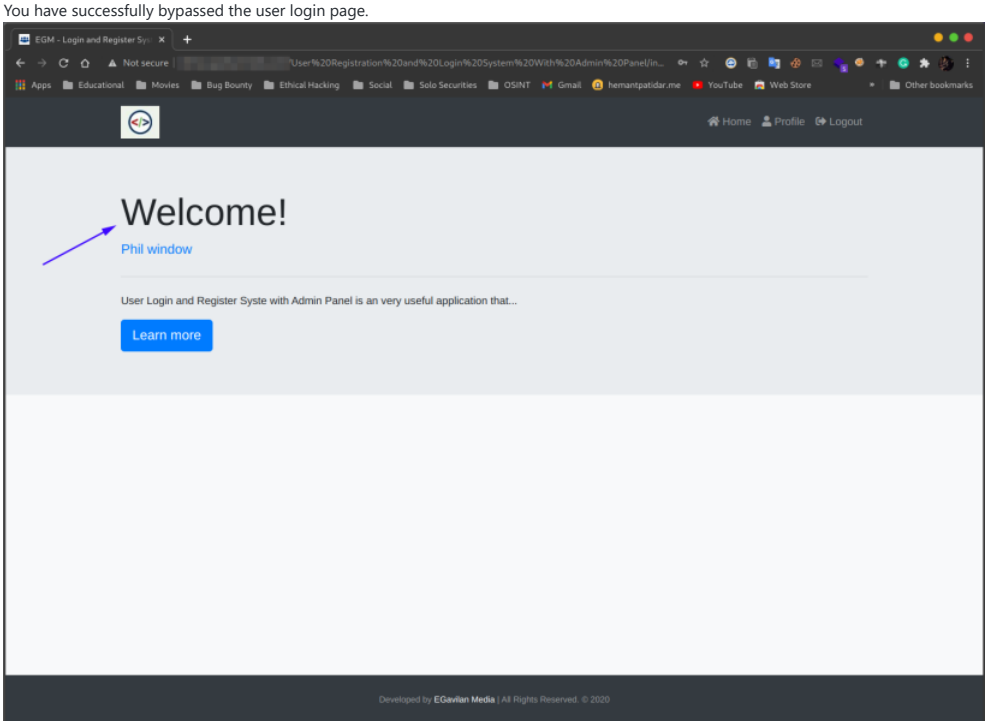
Steps to reproduce:

1. Open Userlogin page using following URI: ->
   http://localhost/User%20Registration%20and%20Login%20System%20With%20Admin%20Panel/login.html

2. Now enter the below payload in Username and Password field. (1' or 1=1 -- -)



3. You have successfully bypassed the user login page.



IMPACT:

If any attacker can gain user login access than they can alter the user's details.

Mitigation:

Option 1: Use of Prepared Statements (with Parameterized Queries) Option 2: Use of Stored Procedures Option 3: Whitelist Input Validation Option 4: Escaping All User Supplied Input