

main

...

CVE-Reference / CVE-2020-29230.md



hemantsolo Update CVE-2020-29230.md

History

1 contributor

23 lines (19 sloc) | 1.48 KB

...

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">

EGM - Register

Not secure | /User%20Registration%20and%20Login%20System%20With%20Admin%20Panel/ve...

Apps Educational Movies Bug Bounty Ethical Hacking Social Solo Securities OSINT Gmail hemantpatidar.me YouTube Web Store Other bookmarks

Register

You can register an account here to login.

Full Name *
hemantsolo">

Username *
Hemant Patidar

Email *
hemantpatidar1337@gmail.com

Gender *
Male

Password *

Confirm Password *

Register

Already registered? Click here to login.

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

EGM - Admin Panel

Not secure | /User%20Registration%20and%20Login%20System%20With%20Admin%20Panel/admin/...

Apps Educational Movies Bug Bounty Ethical Hacking atidar.me YouTube Web Store Other bookmarks

1 says

Cancel OK

Create New User

Show 10 entries

Search:

ID	Full Name	Username	Email	Status	Update
91	Div Ananda	div	Divananda370@gmail.com	Active	
92	asdad	1234test	123@test.com	Active	
93	Ranjodh	shineinfomedia1	shineinfomedia@gmail.com	Active	
94	REGAN RICAFORT	DEMON	demon@gmail.com	Active	
95	Jimmy Rich	jimmy57000	jimmy.rich@outlook.com	Active	
96	god	godsky	godsky@godsky.com	Active	
97	MD SABIR	user123	sabir62290@gmail.com	Active	
98	hemantsolo">	testhacker	bad123bb123@gmail.com	Active	
99	hemantsolo	testacc	bad123bb123@gmail.com	Active	

Showing 91 to 99 of 99 entries

Previous 1 ... 6 7 8 9 10 Next

Developed by EDevlan Media | All Rights Reserved. © 2020