Nikhil kumar Follow
Dec 15, 2020 · 2 min read · Listen

CVE-2020–35395

 # Exploit Title : XSS in Add Expense Component in EGavilan Media Expense Management System 1.0 allows attacker to permanently store the malicious JavaScript code via the 'description' field

#Exploit Author : Nikhil Kumar

#vendor : EGavilan Media

#Application Link : http://egavilanmedia.com/expense-management-system/

#Version: 1.0

Exploit Link : https://www.exploit-db.com/exploits/49146

CVE Link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35395

 # CVE: CVE-2020–35395

What is Stored XSS :

XSS is Stand for Cross-Site Scripting. Stored XSS is a type of XSS. In Which an attacker permanently inject the malicious java script in database of the target server. A common impact of XSS are that the attacker can steal the cookies of users , deface the web application and redirect the user's to phishing pages.

Stored XSS is also known as Persistent XSS.

Attack Vector:

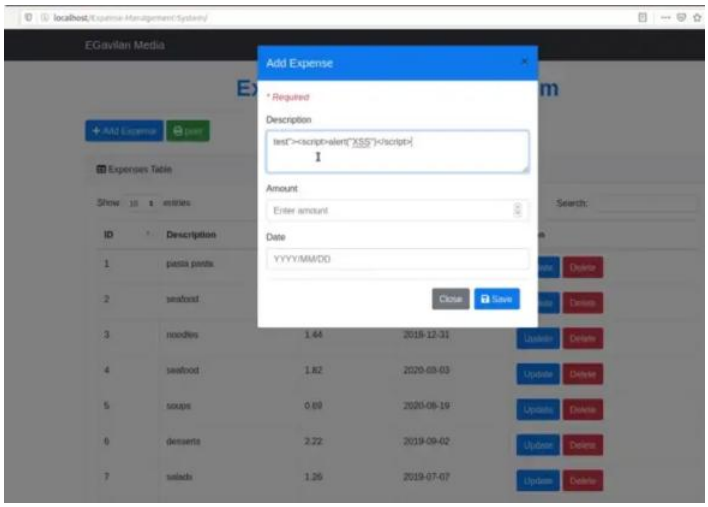
An attacker to inject the XSS payload in the Barcode Generator Area and each time user's visit application the XSS triggers and Attacker can able to redirect to some malicious or phishing webpages according to the crafted payload.

Vulnerable Parameter: "description="

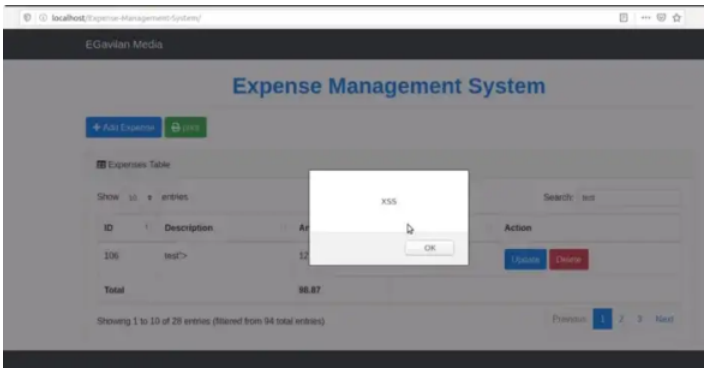
Steps to Reproduce:

1. Go to Add Expense Function
2. Fill the details and Put a payload on "description=" parameter

test"><script>alert("XSS")</script>



3. Web Server accept our Payload and we can see that our payload gets executed



Author: Nikhil Kumar

https://www.linkedin.com/in/nikhil-kumar-4b9443166/

Cve Bug Bounty Writeup Cybersecurity Infosec Cve 2020 35395