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

CVE-2020–35396

#Exploit Author : Nikhil Kumar

#vendor : EGavilan Media

#Application Link : http://egavilanmedia.com/barcodes-generator-using-php-mysql-and-jsbarcode-library/

#Version: 1.0

#Exploit Link : https://www.exploit-db.com/exploits/49227

CVE Link : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35396

#CVE: CVE-2020–35396

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:

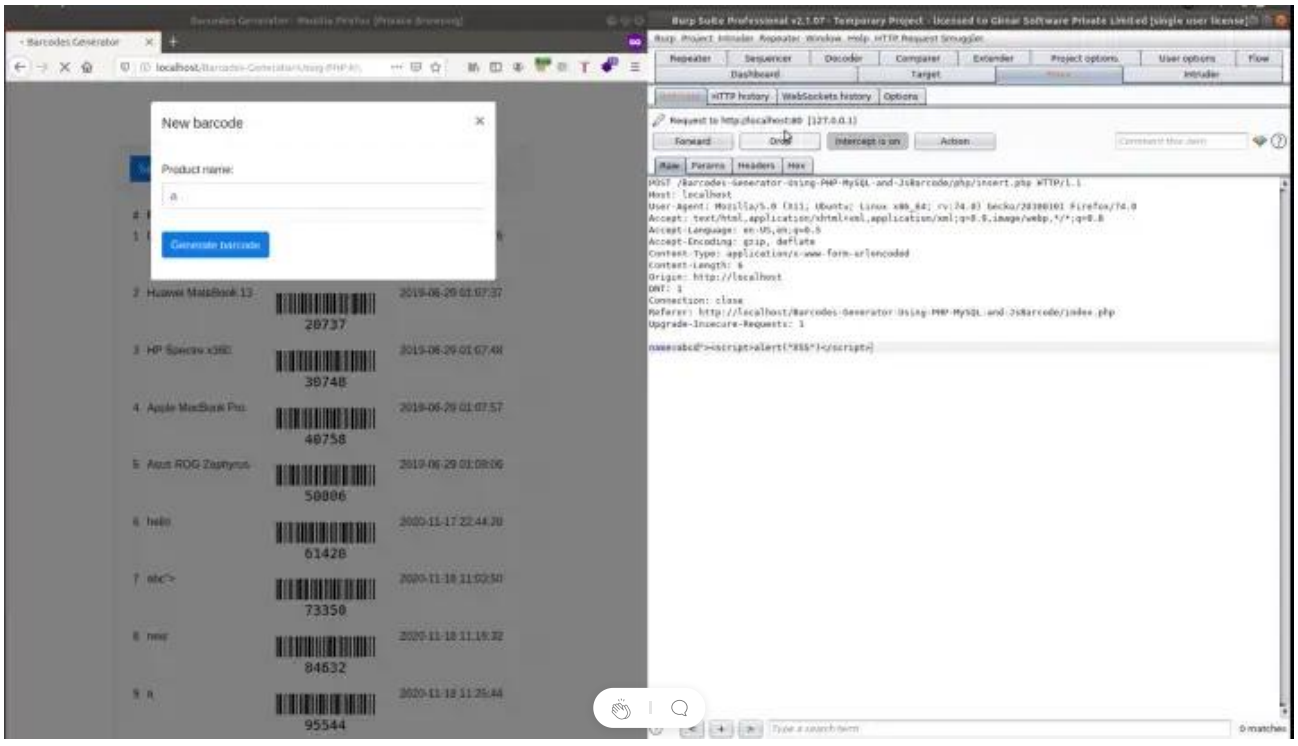
An attacker to inject the XSS payload in the Barcode Generator Area and each time user's visit application the XSS triggers and Attacker can able to redirect to some malicious or phishing webpages according to the crafted payload.

Vulnerable Parameter: "name="

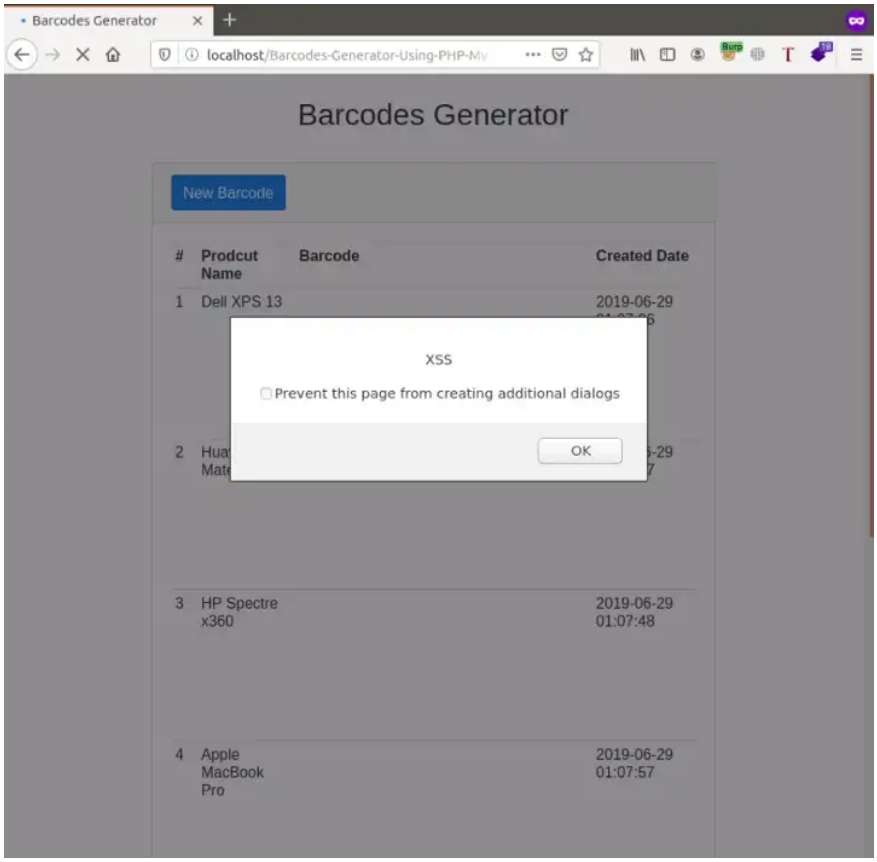
Steps to Reproduce:

1. Go to New Barcode Generator Page

2. Fill the details and Intercept the request through Burp Suite
Put a payload on "name=" parameter
abc"><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 Cve 2020 35396 Bug Bounty Writeup Cybersecurity