XSS in WP plugin Chamber Dashboard Business Directory

Aug 31, 2020 About 1 min

TOC

Issue Description

XSS in WordPress plugin Chamber Dashboard Business Directory.

Problem

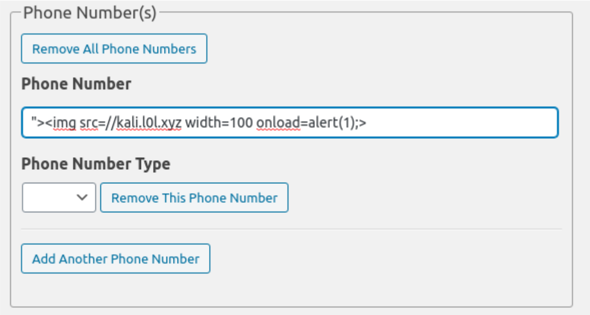
User entered input which contains HTML/JS is not properly encoded on output, resulting in XSS.

Affected versions

Tested on version 3.2.8 (latest)

Details

Enter payload into affected field (phone field in this example) and update company profile.

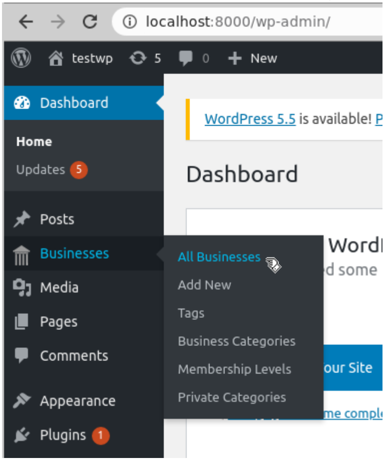


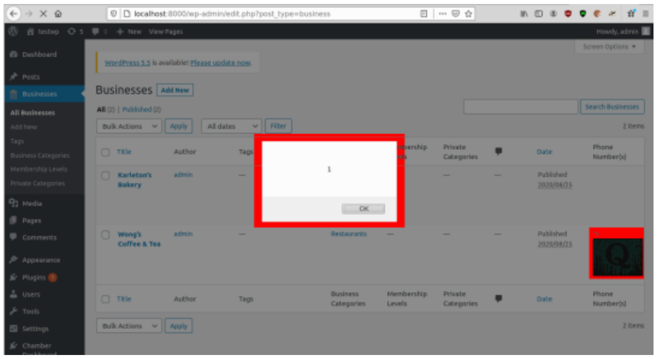
Phone Number

```
"><img src=//kali.l0l.xyz width=100 onload=alert(1);>
```

Phone Number Type

In WordPress admin choose Businesses -> All Businesses and entered payload is executed :)





WordPress 5.5 is available! Please update now.

Businesses

1

☐	Title	Author	Tags	Business Categories	Membership Levels	Private Categories	💬	Date	Phone Number(s)
☐	Karleton's Bakery	admin	—			—	—	Published 2020/08/25	
☐	Wong's Coffee & Tea	admin	—	Restaurants	—	—	—	Published 2020/08/25	
☐	Title	Author	Tags	Business Categories	Membership Levels	Private Categories	💬	Date	Phone Number(s)

Previous example was around *phone* field, because this is displayed in directory listing and therefore can be used as attack vector with less clicks requried from admin.

Other vulnerable fields include:

- Country
- State
- Social media url
- E-mail
- City
- Zip
- Address
- Location
- Hours

CVE-2020-24699 was issued

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-24699

‹ Pentester Academy - Python for Pentesters...

SSRF with root perms in Webdesktop... ›