**Cockpit CMS Official Release**

**Persistent Cross Site Scripting (XSS)**

**Assigned CVE Number:**

***CVE-2018-11471***

**Proof-of-Concept**

**Submitted by:**

**Author: Nikhil Sahoo**

**Website:**  **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Cockpit CMS Official Release, which can be exploited to perform persistent Cross-Site Scripting (XSS) attacks.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source; the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

------------------------------------------

Vulnerability Type:

Cross Site Scripting (XSS)

------------------------------------------

Vendor of Product:

Cockpit CMS Official Release

------------------------------------------

Affected Product Code Base:

https://github.com/agentejo/cockpit/issues/766

------------------------------------------

Affected Component:

http://localhost/cockpit\_stable/

------------------------------------------

Attack Type:

Remote

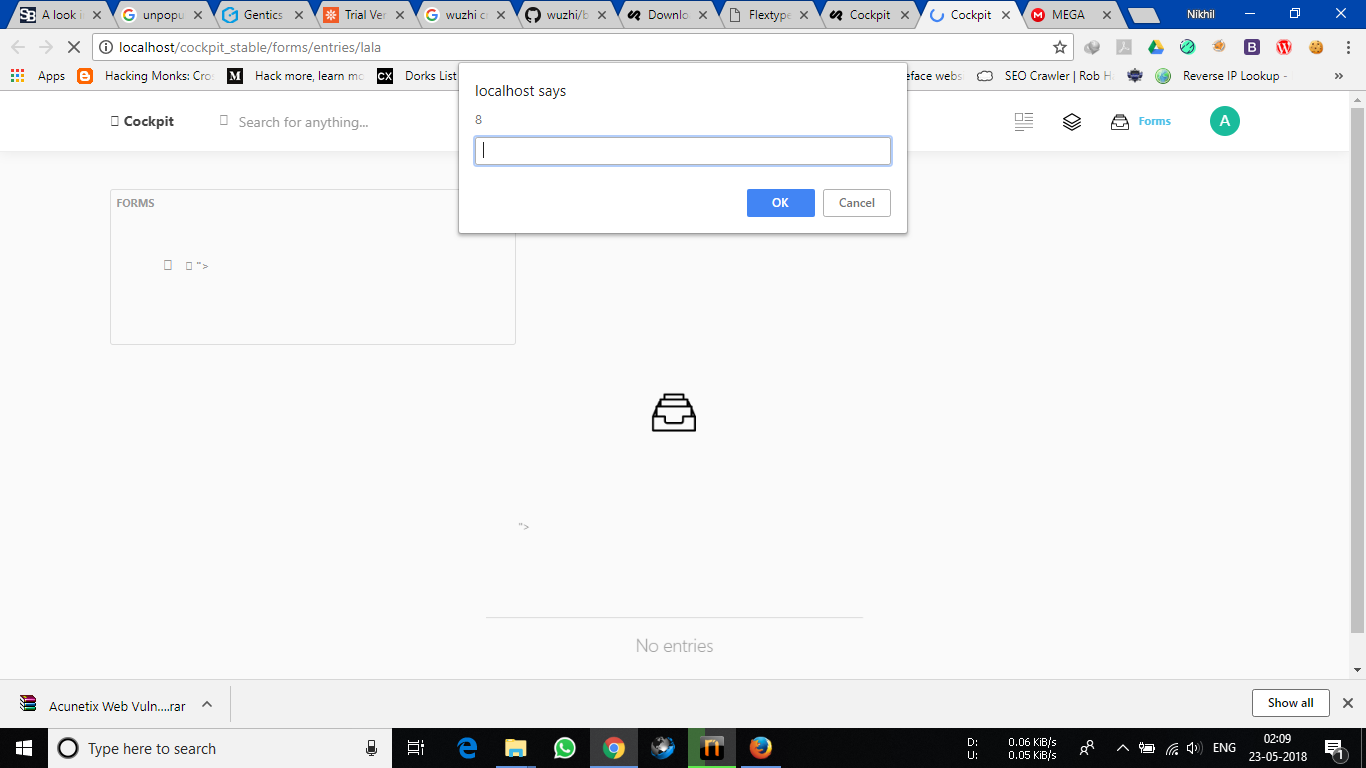
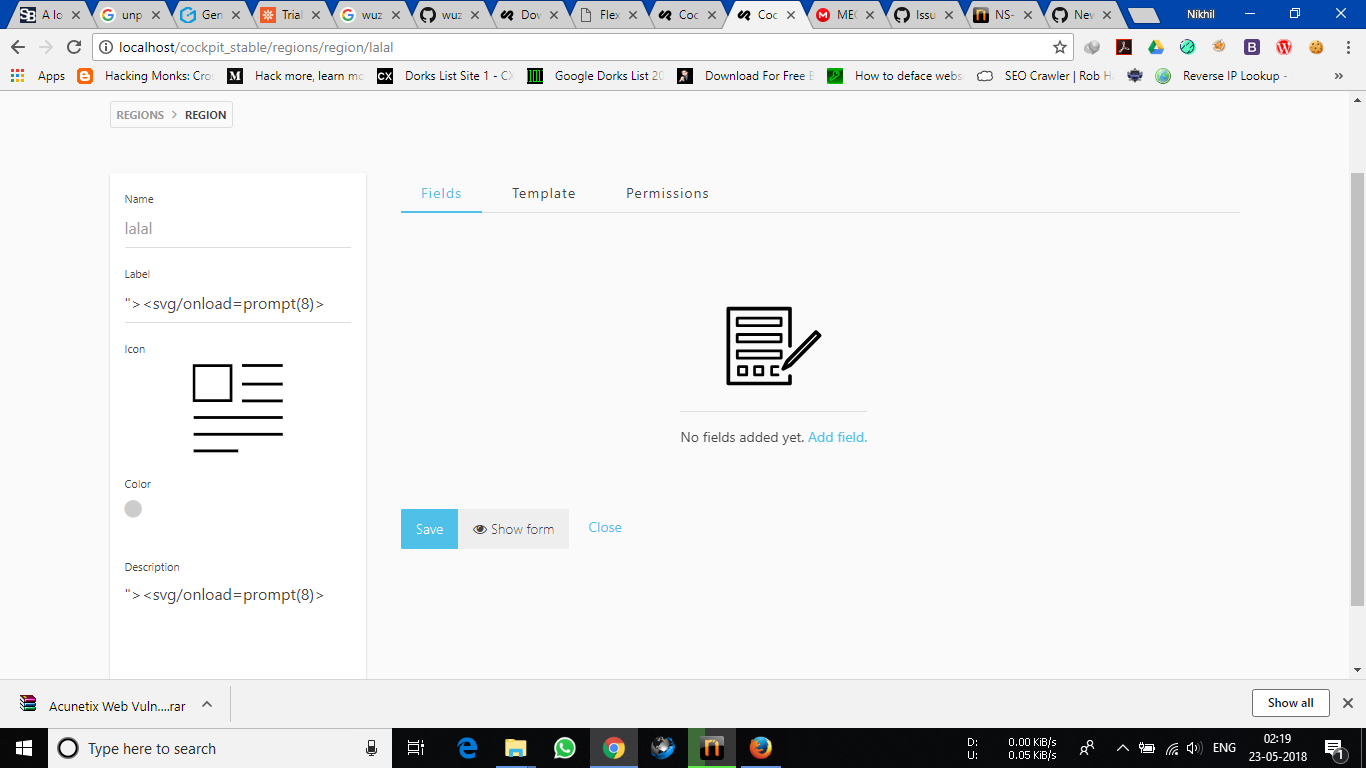
------------------------------------------

Attack Vectors:

Steps:

1)Click on either create regions or collection or form  
2)Now we need to fill up the form  
3)In place of name write whatever you want  
4)In place of form and description put the following payload:- "><svg/onload=prompt(8)>  
5)click on save and now go to the collection/form/region that you recently created  
6)You will get a pop up

POC are:



------------------------------------------

Reference:

https://www.owasp.org/index.php/Cross-site\_Scripting\_(XSS)

------------------------------------------

Discoverer:

Author: Nikhil Sahoo

Website: **https://www.linkedin.com/in/nikhil-sahoo-87204b106/**