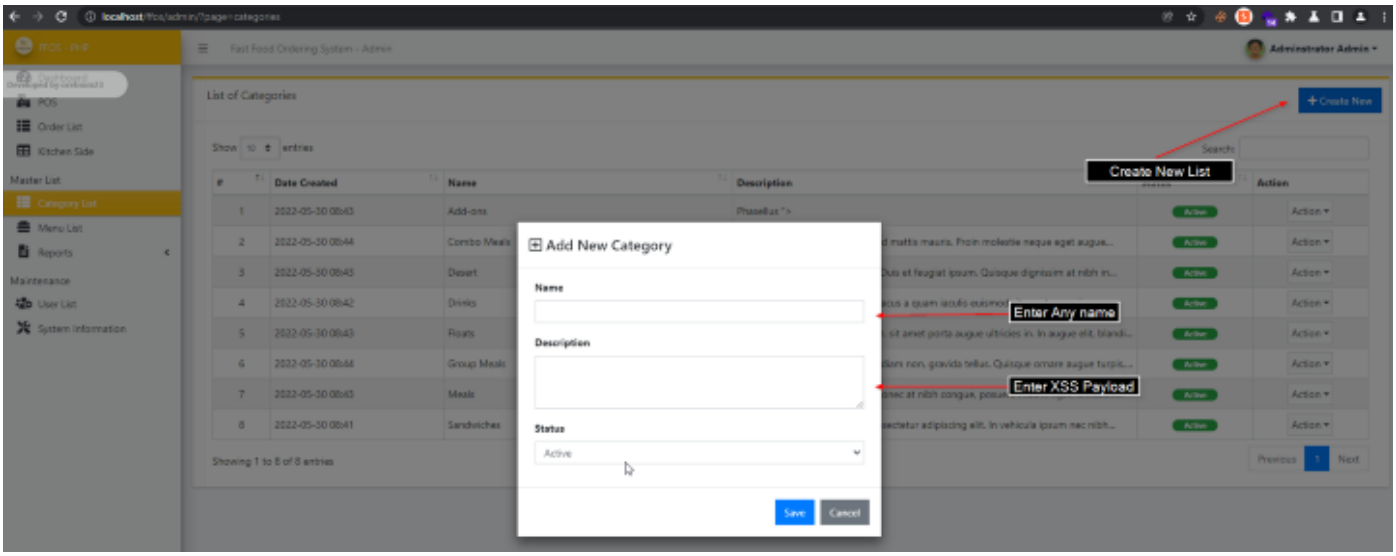
CYBERTHOTH Follow
May 30 · 2 min read · Listen

Fast Food Ordering System 1.0 Cross-Site Scripting

Vulnerable Parameters: Body.



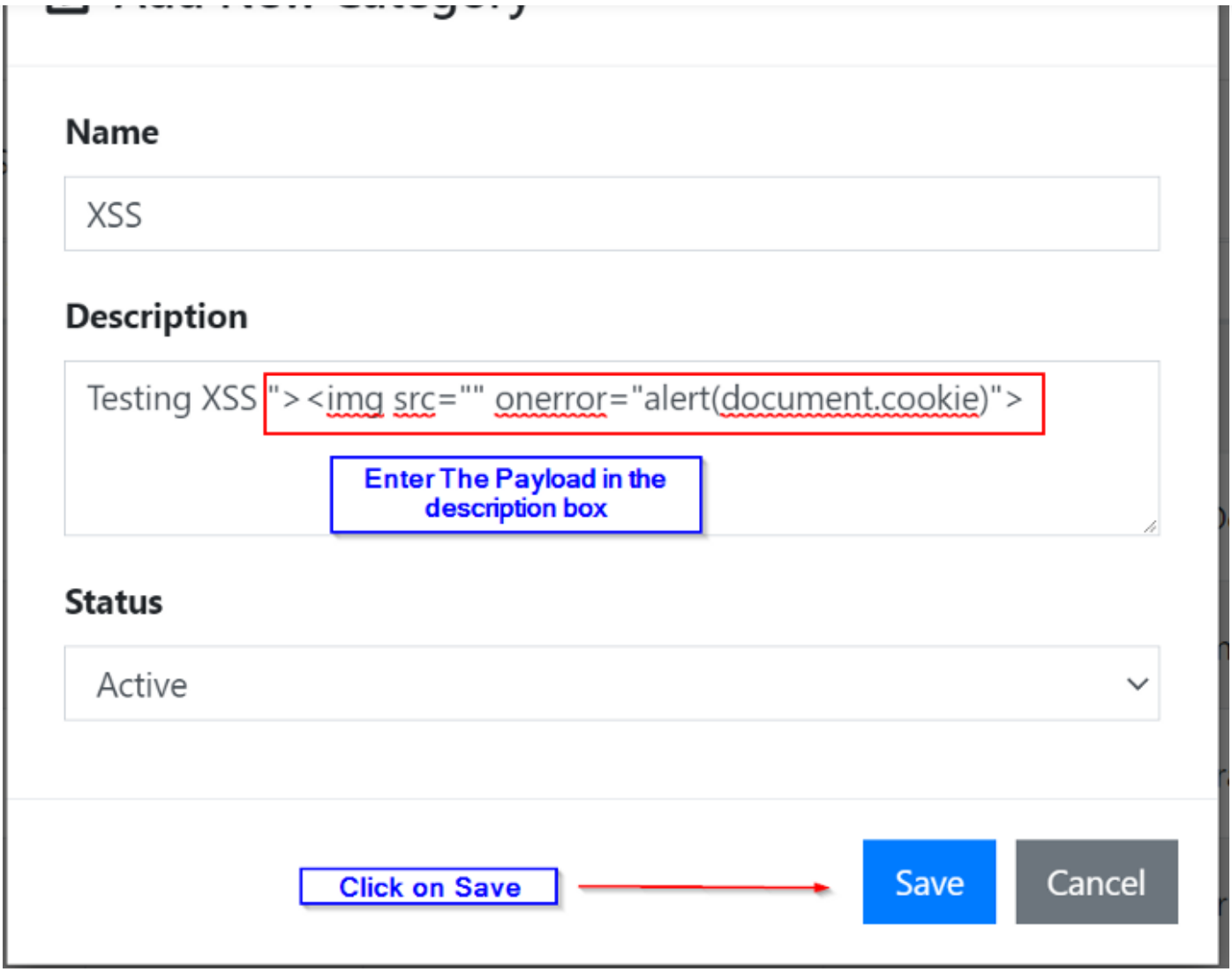
Create a New List

Attack Vector:

This vulnerability can results attacker to inject the XSS payload into the Description box and each time

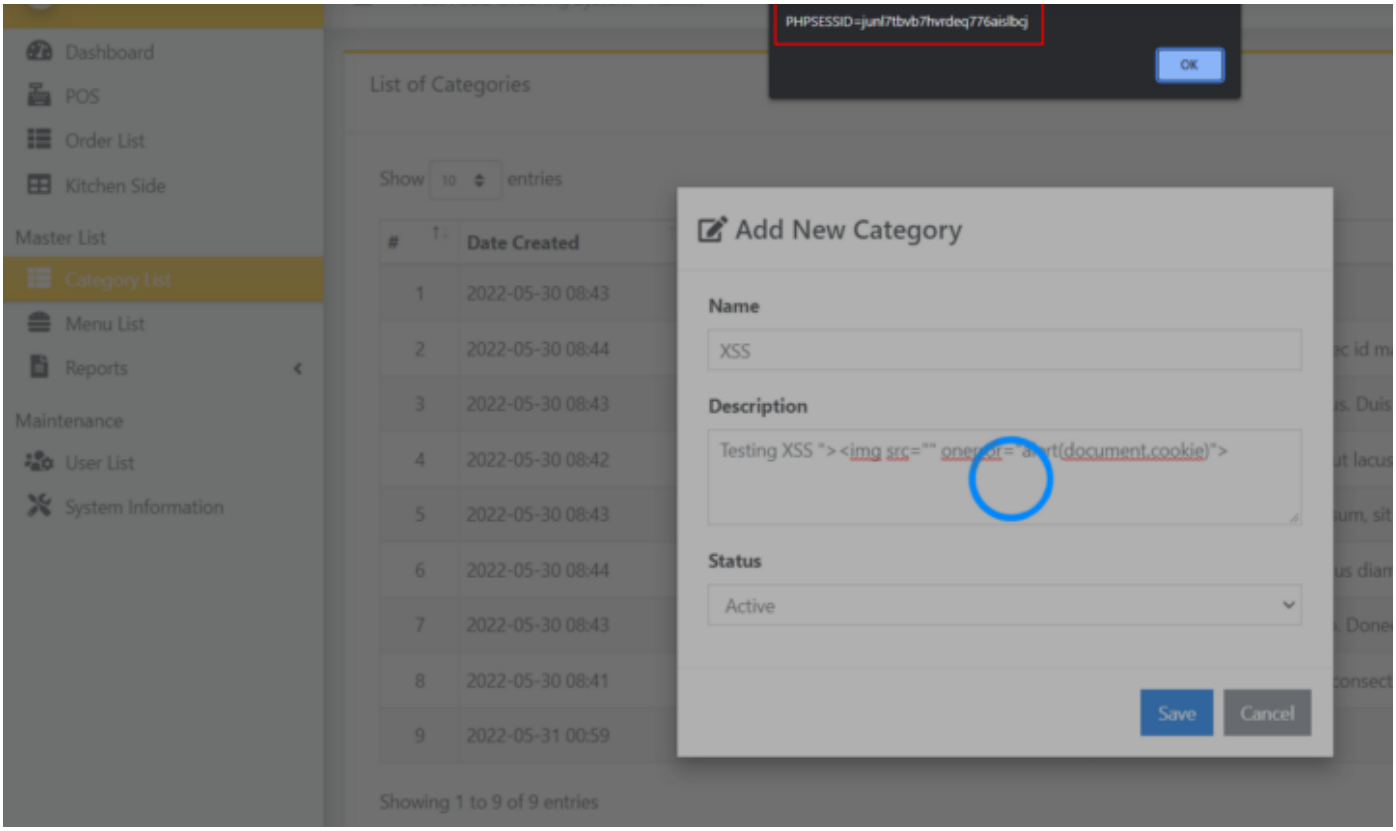
any user will go to that LIST, the XSS triggers, and the attacker can able to steal the cookie according to the crafted payload.

POC :



Enter the payload and save it

2



Payload trigger and it pops up the PHP cookie as shown in the evidence

Steps-To-Reproduce:

1. Login into Fast Food Ordering System CMS admin panel.
2. Now go to the Master List > Category List> Create New.
3. Now paste the below payload in the Description field.

Ashish “><img src=”” onerror=”alert(document.cookie)”>

4. Now click on the save button.
5. The XSS will be triggered.

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.