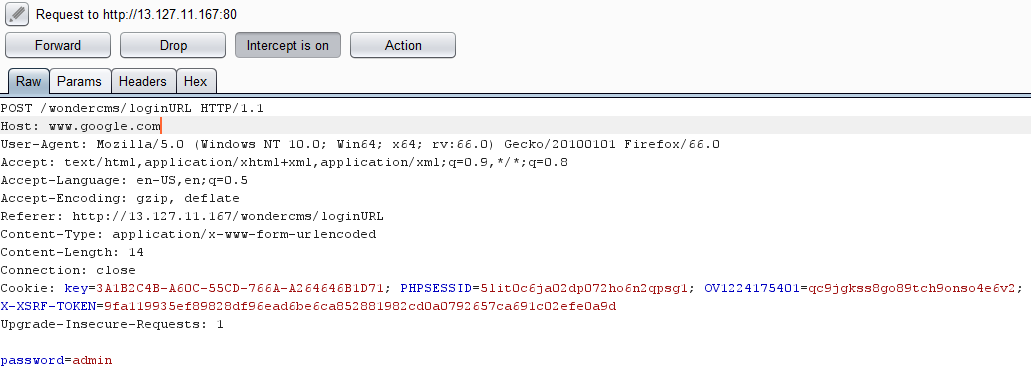
The Wonder CMS application allows illegitimate host header manipulation and leads to arbitrary web page re-direction. This can also lead to severe attacks such as password reset or web cache poisoning

CVE : CVE-2017-14523



In the CodoForum component the reply and search functionalities are both vulnerable to Stored XSS due to improper filtration in displaying the content of replies.

Steps to reproduce the vulnerability:

1. Login to your account.

2. look for any topic and add a reply .

3. in the reply textbox add a widely used common keyword within xss

payload for example : (keyword"><svg/onload=prompt(document.cookie)>)

4. while any user surfing the topic and started to search for specific

keywords the javascript code will be executed.