Category:

Network

Name:

Can you spot the CVE#?

Message:

Find the flag from attached pcap file.

Objective:

Find CVE number of the vulnerability exploited in the attached pcap file.

Instructions:

The "network_challenge.pcapng" contains seriese of portscan (performed by nmap), and http requests & responds.
As network scan doen not exploit, those can be filtered and focus on HTTP packets.
In the series of HTTP packets a suspicious packet at 132445.

> POST /?-d+allow_url_include%3dON+-%64+safe_mode%3doFf+--define+suhosin.simulation%3d1+--define+disable_functions%3d%22%22+-%64+open_basedir%3dnone+-d+auto_prepend_file%3dphp://input+-%64+cgi.force_redirect%3doFf+-%64+cgi.redirect_status_env%3d0+-%6e HTTP/1.1 (application/x-www-form-urlencoded)

You should be able to find CVE number of above exploit.

Alternatively, if you look at like 131325, you will find string "metasploitable2".
CVE may also be speculated by finding PHP vulnerability with CVE number that works on Metasploitable2