Wordpress

Content management system

tools
- wpscan ⎫
- CMS map ⎬ potential vuln (common vuln)
- Metasploit ⎭ wordpress user enumeration
      Brute force
      file uploading
      Vulnerable Thems & plugin

let's understand a wordpress have ⎧ plugin   which mean vulnerable.
we can have for the two.   ⎩ Thems

> wpscan --update   at   for thems enumeration ⎫
> wpscan --url any.com -e   ap   for plugins   ⎬ for enumerate plugins
            vt   for thems vuln ⎭
            vp   for plugins vuln

> wpscan --url any.com → will get all the list of vulnerabilities.

XML - RPC API

Mobile App ———
Desk app ——— Wordpress
others ——— website

It allows me to : → write a post
         → edit a post
         → edit a comment
         → write a comment
         → delete a post

Client
XMLRPC Request
```
<?xml version="1.0"?>
<methodCall>
<methodName>get_account_info</methodName>
<params>
<param>
<value><string>john</string></value>
</param>
</params>
</methodCall>
```

XMLRPC Response
Listener
```
<?xml version="1.0"?>
<methodResponse>
<params>
<param><value><struct>
<member><name>points</name><value><i4>64</i4></value></member>
<member><name>username</name><value><string>john</string></value></member>
<member><name>fullname</name><value><string>Joe Johnson</string></value></member>
</struct></value>
</param>
</params>
</methodResponse>
```
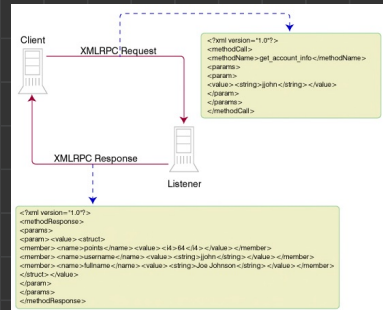
* CMSmap tool on github

→ this tool will give you the number of exploit + exploit name.

+ cmsscan

tool for CMS :

1. word press   wpscan, cmsmap, cmsscan
2. joomla   joommscan, cmsmap, cmsscan
3. drupal   cmsmap, cmsscan, drupwn, ubscan
4. vbulletin   vbullentin scanner, cmsmap, cmsscan
5. magento   magescanner
   and more ...