--File Upload Vulnerabilities--

* what is file upload Vulnerabilities?
--File upload vulnerabilities are when a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size.

* impact
-- web-shell upload, reverse shell upload, remotly control, security loss, financial loss, file override

* information gathering
-- server name and version, which shell, limitation, web shell/ reverse shell, allow extention etc

1st directory searching:

dirb http://192.168.1.5/dvwa
wfuzz -c -W /usr/share/wfuzz/wordlist/dir/common.txt --hc 400,404,403 http://192.168.1.5/dvwa/FUZZ
./dirsearch.py –u http://192.18.1.5/dvwa -e php -f -x 400,403,404
dissearch -u http://192.168.1.5/dvwa -r 3

filtering:

client-side filtering
server-side filtering
blacklist filters
whitelist filters
limited file uploads

client-side validation:

1. check source code
2. delete filtering code
3. upload file and call uploaded file from uploaded directory

or

1. intercept code using Burp (response intercept)
2. delete .js file and forward
3. uplaod file and call the uploaded from uploaded directory

Extention Filtering:

1. BlackList Filtering >> php,pthm,php3 etc
2. Whitelist Filtering >> png, jpg,pdf etc

Extention Filtering Bypass:

1. intercept the request using burp
2. Brute force the extentions using burp intruder
3. upload shell using perfect extention
4. call uploaded file from upload perfect directory

content type filtering:
image/jpg, image/png, text/css, application/x-php

MIME-Type FIltering:

Multipurpose internet mail Extention(MIME) is an internet standard that determines the type of a file
determines the type of a file through its genaral format and bytes structure

need to change magic bytes of files or file signature

1. intercept code and check allow extentions
2. collect allow extention magic bytes
3. add allow extention magic bytes with webshell
4. upload file and call file uploaded from uploaded directory

Resources :

1. Hack the Box Academy
2. Port Swigger
3. THM
4. CTF