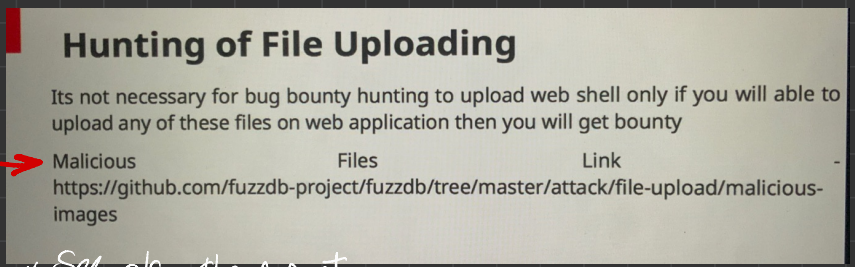
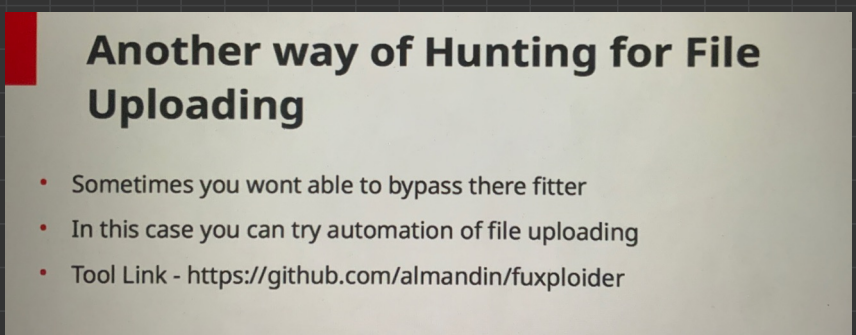
File Upload

* if you can't upload, intercept request change Content-type: image/jpeg



* See also the report



Setup lab

-> install wamp server if you use windows.
-> download upload-lab from Github and put it in wamp-server directory.

pass-01:

-> you need to disable js on your Browser.

pass-02 (Content-Type Bypass)

-> capture request with Burpsuite
-> Change in Content-type: the value text/php to image/png

pass-03 (Suffix Blacklist Bypass)

-> Capture
-> try this in the file name → try one by one

php parser: ← need some search
- .php* class -> .php2-7 (.php3 .php4 .php5 ...)
- .ph* class -> .pht .phtm . phtml
- .php.gif - .jpg%00.php

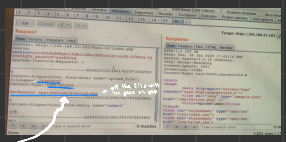
pass-05 (file parsing Rules bypass):

→ every possible php parsing is not allowed

→ see if .htaccess is not filter, so that you rewrite the file parsing rules into .htaccess.

→ try to upload the .htaccess with the content

→ Now try to upload your payload with any extension the site will take it as a .php because of this



pass-06 (not unified case of suffix)

try to manipulate the extension like try Php .phP .PhP .pHp ...

for more secure they should to convert the letter to small letters.

-> capture with burpsuite.

pass-06 (Blacklist bypassing windows features)

Windows file does not allow spaces, if spaces exists windows will remove the spaces.

Assum: server is hosted on a windows platform.

1. capture
2. add space to the end of the file name
3. upload will seccessed.

pass-07 (Blacklist bypassing windows features)

window file name suffix is not allowed to exist dot (.) if it exists windows will automatically remove the dot.

1. capture
2. change file name = 07.php to 07.php.
3. upload seccessed

↳ windows will remove the dot

pass-08 (Blacklist bypassing windows features)

Data is the default attribute for storing data streams in the NTFS file system.

abc.php::$DATA → abc.php

↑ This is appreciating NTFS file system

1. capture
2. change filename = 08.php to 08.php::$DATA
3. upload seccessed

pass-09 (Blacklist bypassing windows features)

just mix between all above and try.

try 09.php. . .

09.php. .

pass-10 (Double write Bypass method)

they will filter .php , so → .pphphp

they will filter .pphphp → .php

pass-14 (Picture prefix bypass)

1. capture
2. add a picture prefix in the code "GIF89a"
3. upload seccessed
4. go to → targ-ip/include.php?file= uploaded_path-image.

second way (picture Trojan horse)

> copy 1.png/ b + shell.php/a output.png

then go to → targ-ip /include.php?file= —

pass-15 (Getimagesize functionality bypass)

→ same as pass-14

1. capture
2. add in the code GIF89a
3. use include function.

→ second way

same as pass-14

use copy command

pass-16 (php_exif module bypass)

Same as pass-14 and 15

pass-17 (Coprehensive picture Horse Example)

here you need to use picture horse

and then use the include method

pass-18 (Conditional Race to delete File Time Difference bypass)

from uploaded file to a temporary file and detect, if match.

Case is, When you upload something, it moved, if does not match, then delete and change the name if match.

pass-19 (Condition Race)

1. upload your php file
2. capture
3. change Filename = any.gif
   Content_Type: image/gif
   add GIF89a
4. use include directory

pass-20 (Nullbyte)