File upload

- the things that programs check for are the following
  1. file name
  2. file content
  3. file type : programs checks for magic numbers (have bypass), the programs also in a form of validation use sandboxes (can be bypassed using race condition)
- the first target of file upload is reverse shell , then we try another thing (path traversal and others)

port swagger labs :

---

1. first lab : we start by sending a photo and then checking the request for the three checks above the file name(**we try making it malicious name and check**) and the file type(**we try to change it .php or anything else**) and the file content (**we try to change it to a php shell one liner and try to read the desired file or execute any command**) and then we make a new request that all is does is to read the uploaded files (the request is a get request for the path of the file while the file have the command injection the read of the get request will execute the code)
2. second lab : we start by checking the three again and then we do the same with file content we change it with a php shell that process a code such as : **ls or pwd or /etc/passwd**
3. third lab : we start checking for the same three and we can change the file name to the file we uploaded and we chain it with a path traversal so that the file name is (**../../filename**)then the file executed
4. forth lab: we start by checking the three ,then we find out that the blacklist is blocking all file extensions that are not jpg so we know that all filters are applied to this and we can't upload any php file or any alias for it because the file is uploaded but not executed so we upload a file to edit the configurations this file is (**.htaccess**) inside of it we get the code to edit this setting so to execute all the php files so that when we upload the file we want the code get's executed (**if there is an .htaccess file in the server we over ride it and execute ours**)
5. polyglot lab : we start checking the three , we upload our payload inside of the file content while keeping the header and the footer content because the server checks for the magic number of the content ,then we upload the file and send a get request to retrieve the file we uploaded that have our payload .