Offensive Approach to Hunt Bugs

File Uploading

Background Concept about File Uploading

- Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.
- The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and especially where it is stored.

Hunting of File Uploading

- Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.
- The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and especially where it is stored.

Hunting of File Uploading

Its not necessary for bug bounty hunting to upload web shell only if you will able to upload any of these files on web application then you will get bounty

- Malicious Files Link - https://github.com/fuzzdb-project/fuzzdb/tree/master/attack/file-upload/malicious-images

Another way of Hunting for File Uploading

- Sometimes you wont able to bypass there fitter
- In this case you can try automation of file uploading
- Tool Link - https://github.com/almandin/fuxploider