**File Upload Vulnerability**

This vulnerability comes in two forms-

1. Local file upload vulnerability- When a malicious script is being uploaded by the user directly and executed.

One way this can happen is when there are no restrictions on the users who can upload the files. This can easily be fixed by adding authentication checks via restricting who can upload (eg- log in/sign ups) and authorization checks via checking what files are being uploaded.

Another way this can happen is when a file name/contents are not sanitized and the non-sanitized file can contain an extension which the attacker can use to execute a code accessed via web. This can be avoided with application which has features that allows it to sanitize files before uploading.

1. Remote file upload vulnerability- is when the users provide a site URL which is used to save a file from that site locally on a disk. If the file is malicious is then used by the attacker to cause harm.

This can be prevented by

1. Checking what kind of file is being uploaded.
2. The allowance of only specific types of file extensions
3. Only specific users being able to access this form of file upload.
4. Storing files in a directory that is only accessible to authorized users.
5. Making stored files non executable.

**Missing Authorization Vulnerability**

This takes place when an application does not do an authorization check when a user tries to use its resources or use it to do something. This allows users who should not have the privilege to access certain data or actions to do so.

This can create a whole host of problems like leaking of sensitive data, modification data by the attacker, attackers to execute codes on a targeted device, denial of service to users and attacker could grant themselves privileges by modifying critical data.

This can be prevented by having the architecture and design of the software being reviewed, alongside other detection methods.

# References

CyberSecurityTV. (2021, January 13). *File Upload Content-Type Validation Bypass | Web App Penetration E02*. Retrieved from Youtube: https://www.youtube.com/watch?v=v4gx9vTvmt4

*How to Prevent File Upload Vulnerabilities*. (2021, January 13). Retrieved from WordFence: https://www.wordfence.com/learn/how-to-prevent-file-upload-vulnerabilities/#:~:text=A%20local%20file%20upload%20vulnerability,Internet%20and%20store%20it%20locally.

Ltd., T. P. (2021, January 13). *Penetration Testing - File Upload Vulnerability*. Retrieved from Youtube: https://www.youtube.com/watch?v=jFRYPmCulh4

*Missing authorizations*. (2021, January 13). Retrieved from Common weakness enumerations : https://cwe.mitre.org/data/definitions/862.html