File Inclusion Vulnerabilities

File Path Traversal
A path traversal attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences it may be possible to access arbitrary files and directories stored on file systems.

File Inclusion
Occur when a web application allows users to submit input into files or upload files to the server. File Inclusion vulnerabilities allow an attacker to read and sometimes execute files on the victim server or, as is the case with Remote File Inclusion, to execute code hosted on the attacker's machine via the upload file functionality.

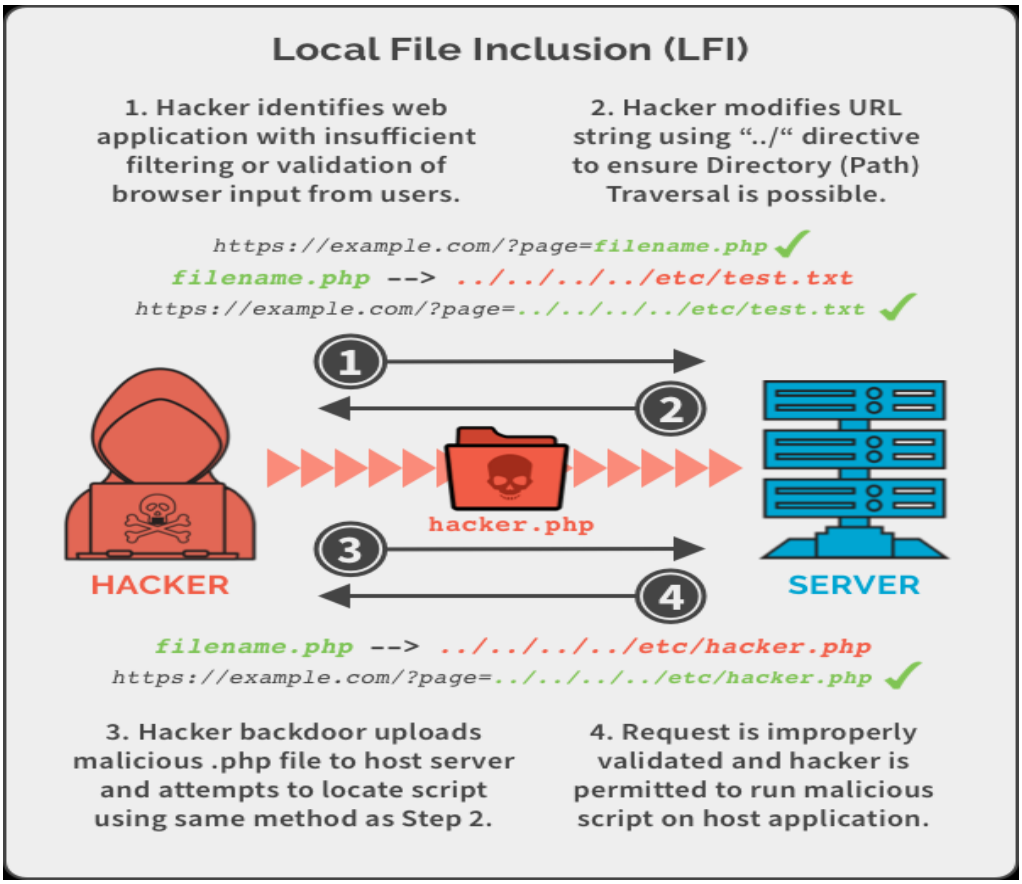
An attacker may use remote code execution to create a web shell on the server, and use that web shell for website defacement.

What is the difference between Path traversal and File Inclusion?
Path/Directory Traversal vulnerabilities only allow an attacker to read a file, while LFI and RFI may also allow an attacker to execute code.

Types
File inclusion vulnerabilities come in two types, depending on the origin of the included file:

– Local File Inclusion (LFI)
– Remote File Inclusion (RFI)

Local File Inclusion (LFI)
A Local File Inclusion attack is used to trick the application into exposing or running files on the server. They allow attackers to execute arbitrary commands or, if the server is misconfigured and running with high privileges, to gain access to sensitive data.



Ex:

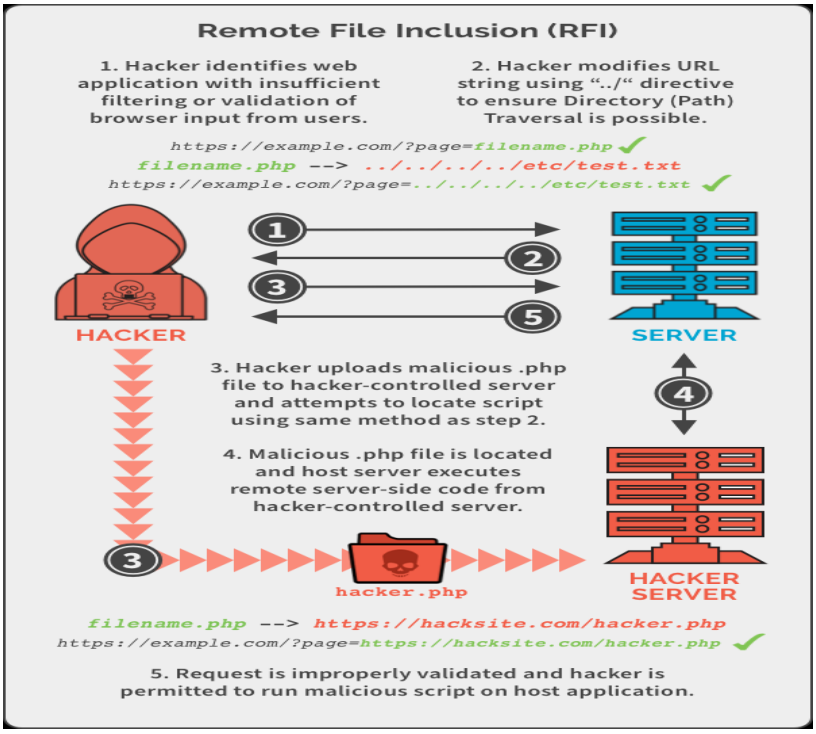
```
/**
* Get the filename from a GET input
* Example - http://example-website.com/?file=filename.php
*/
$file = $_GET['file'];

/**
* Unsafely include the file
* Example - filename.php
*/
include('directory/' . $file);
```

In the example above the attacker's intent is to trick the application into executing a PHP script, such as a web shell

http://example-website.com/?file=../../uploads/malicious.php

Once a user runs the web application, the file uploaded by the attacker will be included and executed. This will allow the attacker to run any server-side code that he wants.

Remote File Inclusion (RFI)
An attacker who uses Remote File Inclusion targets web applications that dynamically reference external scripts. The goal of the attacker is to exploit the referencing function in the target application and to upload malware from a remote URL, located on a different domain.



The results of a successful RFI attack can be information theft, a compromised server and a site takeover, resulting in content modification.

Mitigation

Make sure you restrict execution permissions for the upload directories, maintain a whitelist of acceptable files types, and restrict upload file sizes.

Impact
The consequences of a PHP file inclusion may differ depending on the type of attack. Successful file inclusion attacks may result in information disclosure, XSS, remote code execution and complete compromise of the system.

Preventions:

1. Proper input validation and sanitization.
2. Regularly scan applications for potential vulnerabilities.
3. Blacklist approach.
4. Whitelist approach.
5. Enable code reviewing for identifying vulnerabilities in the code

File Upload Vulnerability
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. Failing to properly enforce restrictions on these could mean that even a basic image upload function can be used to upload arbitrary and potentially dangerous files instead. This could even include server-side script files that enable remote code execution.

Impact
If the file's type isn't validated properly, and the server configuration allows certain types of files (such as .php and .jsp) to be executed as code. In this case, an attacker could potentially upload a server-side code file that functions as a web shell, effectively granting them full control over the server.

References
https://owasp.org/www-community/attacks/Path_Traversal

https://www.whitehatsec.com/glossary/content/path-traversal

https://portswigger.net/web-security/file-path-traversal#:~:text=Directory%20traversal%20(also%20known%20as,and%20sensitive%20operating%20system%20files.

https://www.offensive-security.com/metasploit-unleashed/file-inclusion-vulnerabilities/

https://brightsec.com/blog/file-inclusion-vulnerabilities/

https://spanning.com/blog/file-inclusion-vulnerabilities-lfi-rfi-web-based-application-security-part-9/

https://beaglesecurity.com/blog/vulnerability/file-inclusion-vulnerabilities.html

https://portswigger.net/web-security/file-upload#:~:text=File%20upload%20vulnerabilities%20are%20when,type%2C%20contents%2C%20or%20size.

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
https://blog.intigriti.com/hackademy/file-upload-vulnerabilities/