File Inclusion inclusion

A **file inclusion vulnerabilityis a web application vulnerability that will arise due to dynamic linking or execute the files or code from web server.on the file inclusion vulnerability the application will bui;ds the path based on the user supplied input and it can be controlled by user input .by takking this as advantage the attacker will tries to gives input or inject payloads that will leads to remote code exection or loading confidential files from server.thera are two types of files inclusion vunlerablity**

1.local file inclusion(LFI)

Local File Inclusion (LFI) **allows** **an attacker**  **to retrive** files stored on web server. This vulnerability exists **in web**  applications that includes a file without **properly** sanitizing the input, **which allow an attacker to**  to manipulate input and inject path traversal characters or to retrieve the files from **the** server. The local file inclusion vulnerability will further lead to directory traversal, sensitive information disclosure, remote code execution or even cross site scripting also. Local file inclusion will commonly arises in php web applications.

based on functionality of application the LFI will leads to execute the file by the language parser,download the requested file or display the content of file on web page.the remediation of lfi is the web application should accept only character and numbers for file names and should be blacklisted all the special charcters,limit the access to allowed directory only

2.remote code exection(RFI)

Remote file inclusion (RFI) is an attack targeting vulnerabilities in web applications that dynamically reference external scripts. The perpetrator’s goal is to exploit the referencing function in an application to upload malware (e.g., [backdoor shells](https://www.imperva.com/learn/application-security/backdoor-shell-attack/)) from a remote URL located within a different domain.

The consequences of a successful RFI attack include information theft, compromised servers and a site takeover that allows for content modification.

Using Remote File Inclusion (RFI), an attacker can cause the web application to include a remote file. This is possible for web applications that dynamically include external files or scripts. Potential consequences of a successful RFI attack range from sensitive information disclosure and [Cross-site Scripting (XSS)](https://www.acunetix.com/websitesecurity/cross-site-scripting/) to [Remote Code Execution](https://www.acunetix.com/blog/articles/blind-out-of-band-remote-code-execution-vulnerability-testing-added-acumonitor/).

Remote File Inclusion attacks usually occur when an application receives a path to a file as input and does not properly sanitize it. This allows an external URL to be supplied to the include function.

## Remote File Inclusion

Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.

Almost all web application frameworks support file inclusion. File inclusion is mainly used for packaging common code into separate files that are later referenced by main application modules. When a web application references an include file, the code in this file may be executed implicitly or explicitly by calling specific procedures. If the choice of module to load is based on elements from the HTTP request, the web application might be vulnerable to RFI.

An attacker can use RFI for:

* Running malicious code on the server: any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise.
* Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, Javascript to steal the client session cookies).

PHP is particularly vulnerable to RFI attacks due to the extensive use of "file includes" in PHP programming and due to default server configurations that increase susceptibility to an RFI attack ([4,5]).

"PHP Runtime Configuration"

[4] <http://php.net/manual/en/filesystem.configuration.php>

"PHP Register Globals"

[5] <http://php.net/register_globals>