File Inclusion

File inclusion vulnerability is a web application vulnerability that will arise due to dynamic linking or execute the files or code from the web server and it is high-risk vulnerability. On the file inclusion vulnerability, the application will build the path based on the user-supplied input and it can be controlled by user input .by taking this as an advantage the attacker will try to gives input or inject payloads that will lead to remote code execution, loading confidential files from the server, deface the website, etc. There are two types of file inclusion vulnerability.

1. local file inclusion(LFI)

Local file Inclusion is an attack targeting in web application that exist in the input fields (id field, text boxes, text fields, URL parameters, etc) that dynamically reference file and scripts from server storage and does not sanitize input fields properly, which allow an attacker 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, and code execution or even cross-site scripting(XSS). Local file inclusion will commonly arise in PHP web applications but can in all kinds of web applications. Based on the functionality of the application the LFI will lead to executing the input(file or command) by the language parser, download the requested file or display the content of file on the 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 characters, limit the access of files by the web application from specific directories only.

2. Remote Code Execution (RFI)

Remote file inclusion is an attack targeting in the web application that exists in the input fields (id field, text boxes, text fields, URL parameters, etc) which dynamically reference external script and does not sanitize input fields properly. Using the remote file inclusion the attacker can include or load the file stored in a remote location. Almost all types of web applications support the file include but most commonly it will be found in a PHP web application because in PHP programming we will use file includes" extensive. By using the remote file inclusion the attacker can trick web application to load the malicious code stored in a remote location the malicious code will include backdoors, web shells, code execution at OS level, etc. By successfully exploiting the RFI the attacker can gain sensitive information from the server, take over the application or server, server hijacking, etc. The main causes for remote file inclusion are programming mistakes, misconfigurations of the respective programming language functionality. The best way to eliminate the RFI is to completely avoid the dynamically including the files based on user inputs or maintain the white list of filenames that can be included in user inputs.