

PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Source URL: https://gynvael.coldwind.pl/download.php?f=PHP_LFI_rfc1867_temporary_files_2021.pdf

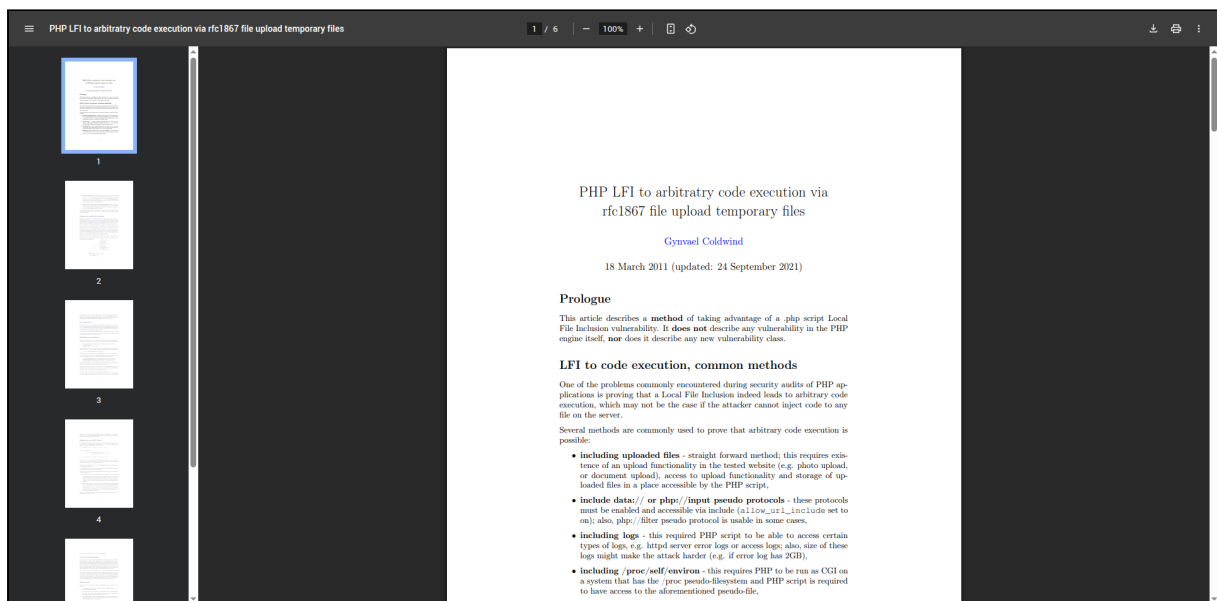
Archived Date: August 15, 2025 at 15:30

Published: September 24, 2021

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://gynvael.coldwind.pl/download.php?f=PHP_LFI_rfc1867_temporary_files_2021.pdf

Page Screenshot





1



2



3



4



5

PHP LFI to arbitrary code execution rfc1867 file upload temporary files

Gynvael Coldwind

18 March 2011 (updated: 24 September 2021)

Prologue

This article describes a **method** of taking advantage of a .php source File Inclusion vulnerability. It **does not** describe any vulnerability in the engine itself, **nor** does it describe any new vulnerability class.

LFI to code execution, common methods

One of the problems commonly encountered during security audits & applications is proving that a Local File Inclusion indeed leads to arbitrary code execution, which may not be the case if the attacker cannot inject a file on the server.

Several methods are commonly used to prove that arbitrary code execution is possible:

- **including uploaded files** - straight forward method; this requires the presence of an upload functionality in the tested website (e.g. photo or document upload), access to upload functionality and storing the file on the server.