PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot

1

2

3

4

PHP LFI to arbitratry 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 s
File Inclusion vulnerability. It **does not** describe any vulnerability i
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
plications is proving that a Local File Inclusion indeed leads to arbi
execution, which may not be the case if the attacker cannot inject
file on the server.

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

- **including uploaded files** - straight forward method; this re
tence of an upload functionality in the tested website (e.g. ph
or document upload), access to upload functionality and sto