New issue

Jump to bottom

there is a File upload attack vulnerability #8

Open **984231098** opened this issue on Aug 15, 2019 · 0 comments

984231098 commented on Aug 15, 2019

there is a File upload attack vulnerability,It can lead to arbitrary uploading of PHP script files.
The location of the vulnerability is in http://ip/public/admin,where the content editing function is.

Let's see the code:

```
public function ajaxUploadImage()
{
    $file = request()->file('image');
    /* 检查上传文件 */
    $file->validate([
        'size' => 1024000,
        'type' => 'image/jpeg',
    ]);
    if (!$file->check()) {
        return null;
    }
    /* 图像处理 */
    try {
        $upload = $file->move(ROOT_PATH . 'public/image');
        $image = \think\Image::open($upload->getRealPath());
        $image->thumb(620, 348, \think\Image::THUMB_CENTER)->save($upload->getRealPath());
    } catch (\Exception $e) {
        return null;
    }
    /* 拼接图像地址 */
    $path = str_replace(ROOT_PATH . 'public', '', $upload->getRealPath());
    return str_replace('\\', '/', $path);
}
```

There are two problems:

1. The uploaded file detection is not strict, only the content-type is detected, and even the file suffix is not detected, which causes us to modify the content-type when uploading to bypass the upload php file.
2. File processing logic vulnerabilities, although there is a file abbreviated processing, but when uploading a sentence Trojan with a jpg file header, the server will not return the address, but the file is already stored on the server, so the file upload can be achieved.

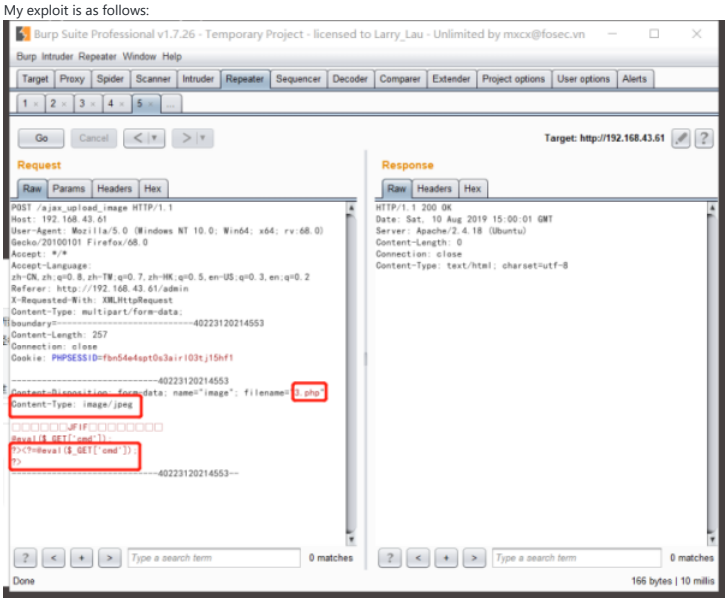
In addition, although the CMS detects and filters uploaded files, it will be automatically commented out if it matches **<?php** .
such as:

```
JFIF @eval($_GET['cmd']); ?>
<!--?php@eval($_GET['cmd']); ?-->
```

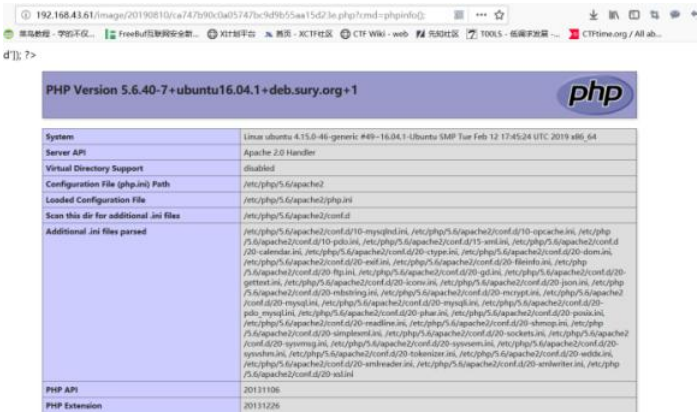
but We can bypass with short tags,such as:

1. Use **<?=** instead of **<?php**
2. Use **<script language='php'></script>** to bypass

My exploit is as follows:



Let's test it out.



as we can see,The PHP Trojan has been successfully uploaded and validated.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant