

New issue

[Jump to bottom](#)

File Upload #4

Closed

JuneRainBlog opened this issue on Jun 2, 2020 · 3 comments

JuneRainBlog commented on Jun 2, 2020 • edited

Describe the bug

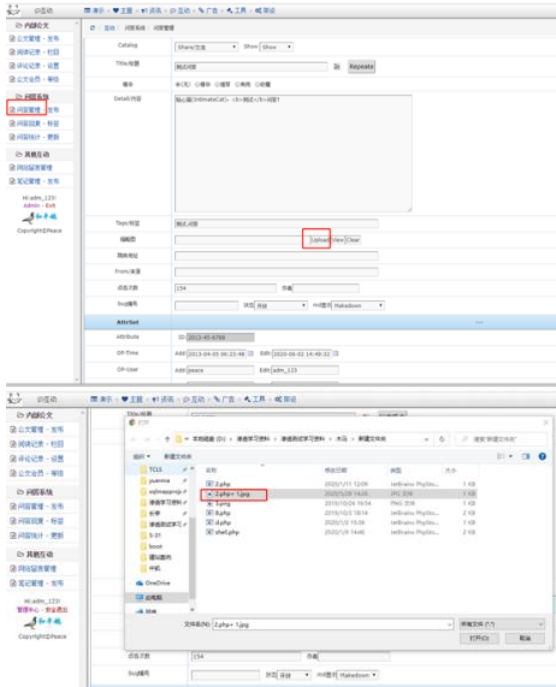
Upload php files to control the target server

Exploit vulnerability :

Upload malicious PHP file here:

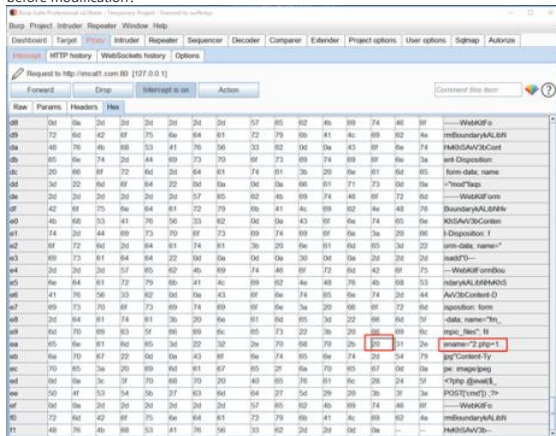
url:127.0.0.1/root/run/adm.php?

PHP file name: 2.php+ 1.jpg

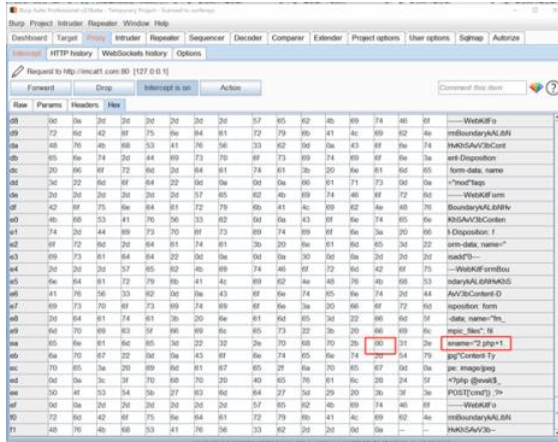


Use Burpsuite, modify Hex 20 -> 00:

before modification:



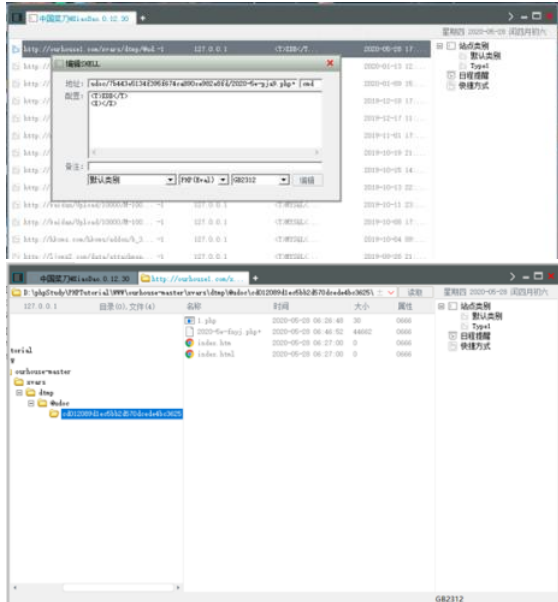
after modification:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	HTTP	1024	POST http://127.0.0.1:80/2020-5w-pja9.php+ HTTP/1.1
2	0.000000	127.0.0.1	127.0.0.1	HTTP	1024	200 OK

connect PHP file:

127.0.0.1/xvars/dtmp/@udoc/7b443e5134f395f674ca890ce982e8fd/2020-5w-pja9.php+



The Vuln-src-code:

imcat(core\clib\comUpload.php -> checkType() -> strpos()),because strpos() can not match .php+

imcat(core\clib\comUpload.php -> upEnd() -> in_array()), because in_array() is only used for checking filename whether or not have jpg. , so we can upload 1.php+ .jpg to bypass filtering.

```
private function checkType(){
    $ext = $this->getFileExt();
    $skips = 'asp,aspx,jsp,php,exe,sh,bat,com'; // www.cve.org,php3,php4
    if(strpos($skips, $ext)){ // 超管管理员都不给上传这些文件??
        $this->stateInfo = "Error '$ext'!";
        return false; //Error '$ext'!
    }
    $flag = $this->config['allowFiles'] === 'super' ? true : in_array($ext, $this->config['allowFiles']);
    return $flag;
}

private function upEnd() {
    $this->stateInfo = $this->stateMap[0];
    if(in_array($this->fileType, array('jpg', '.jpeg'))){
        comImage::compress($this->fullName);
    }
}
```

Credit: @chaitin Tech.

peacexie commented on Jun 4, 2020

Owner

Thanks!

Replace the file imcat\core\clib\comUpload.php as attachments;
Can it stop you from attacking?

[comUpload.zip](#)

JuneRainBlog commented on Jun 4, 2020

Author

Yes!already fixed.

peacexie commented on Jun 5, 2020

Owner

OK, I fixed it in the master branch already.



peacexie closed this as completed on Jun 5, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

