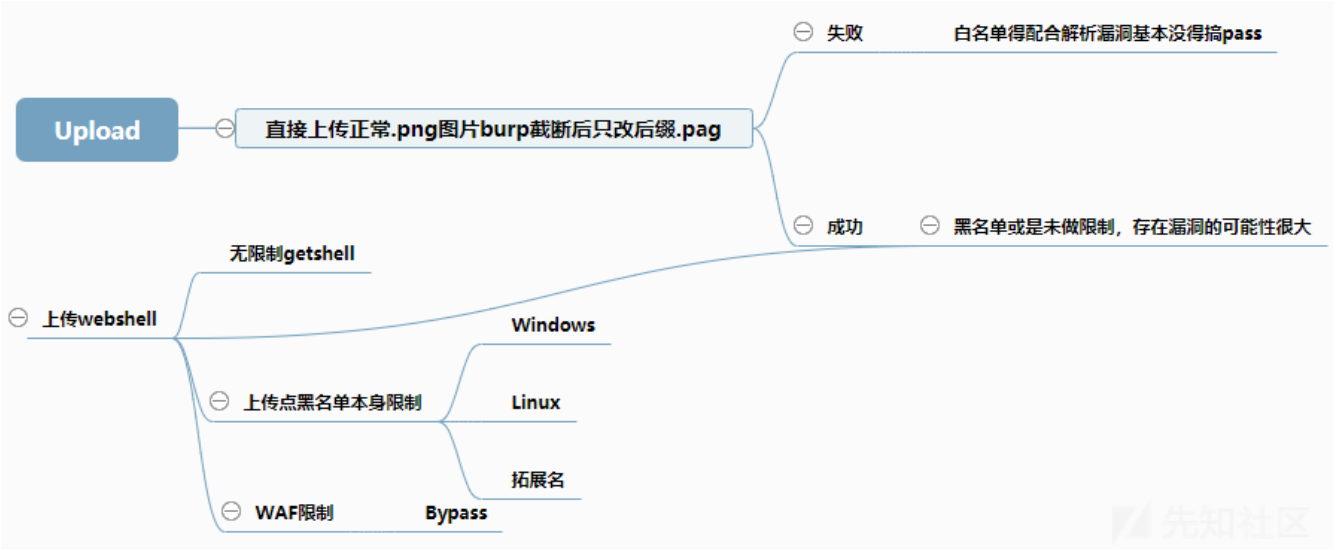
# 【转载】Upload与WAF的那些事

作者: ANONYMOUS | 时间: 2020-09-01 | 分类: ANONYMOUS

背景:去年实习的时候开始接触渗透，太菜，就偶尔在EDUSRC捡洞(资产多，WAF多，坑多)，主要是挖一些上传，逻辑，注入等基础漏洞，不建议拿一把梭工具扫，除非自己挖的通用洞或是对该漏洞原理理解深刻，不然成长不大。文件上传漏洞的介绍很多，就不废话了，下面讲讲如何快速判断文件上传漏洞是否客观存在与WAF绕过。

**Upload步骤**



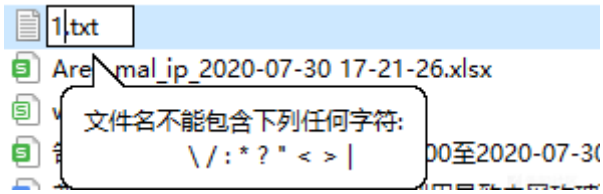

1.直接前端上传正常文件，burp截断只修改任意后缀判断黑白名单(略过content-type/前端js判断)。
2.传不上去就是白名单限制pass基本没得搞，传得上去就是黑名单或是未做限制。
3.webshell上传能落地，能拿到文件url，能web访问，能解析-->>getshell。
上面就是Upload漏洞的判断步骤。
下面来说说已经判断是黑名单后绕过上传点的限制与WAF的限制。

**判断程序本身限制与WAF限制**

1.程序本身黑名单限制：返回包通常会有上传文件格式不允许意思的字样
2.WAF限制：返回页面通常会是WAF的拦截页面或是该次请求被重置reset无响应包

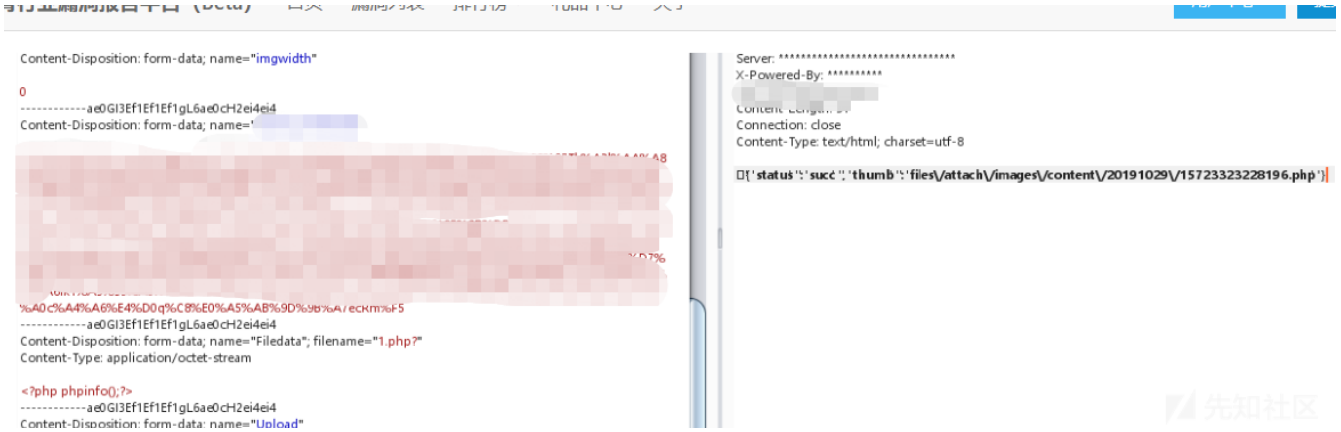
**后缀绕过黑名单的限制**

Windows：
大小写不敏感，[空格]，命名不允许的特殊字符，::$DATA。
命名不允许的特殊字符/?

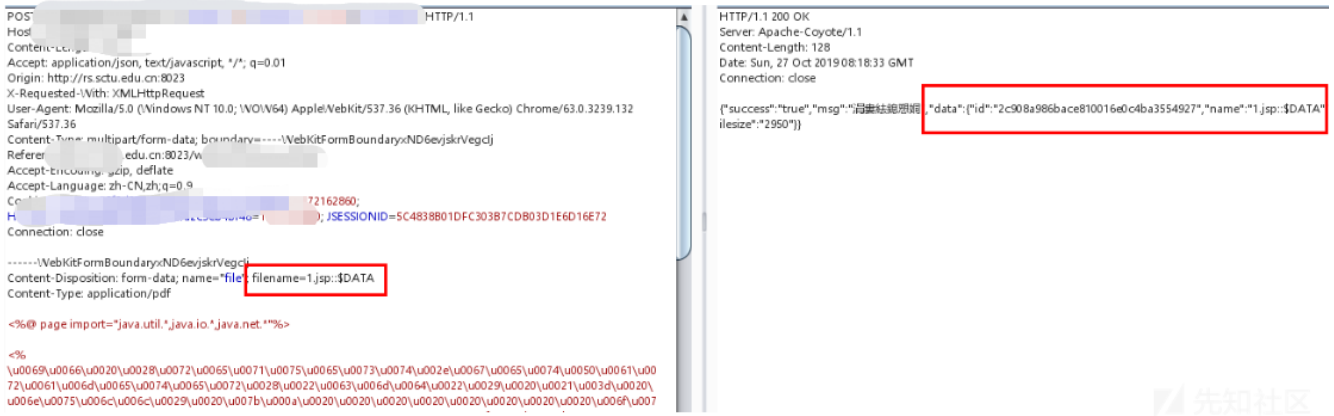




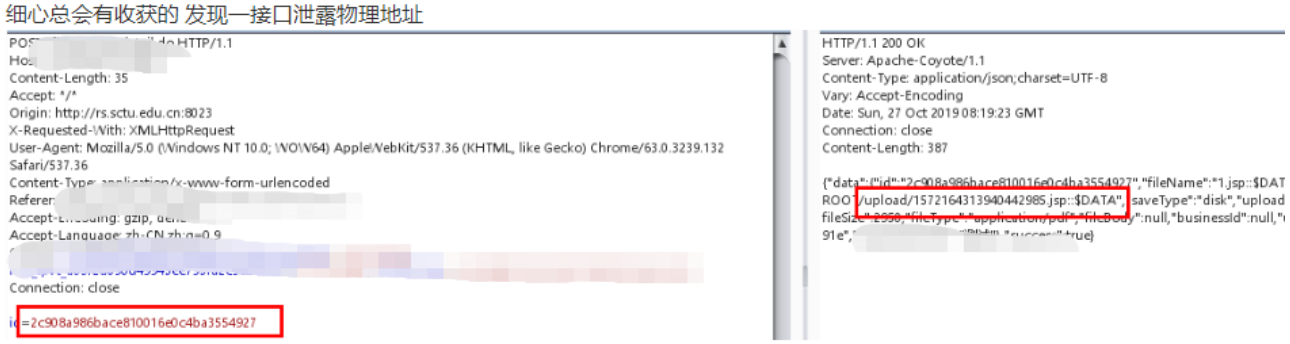
/uploadFiles/20191016012528457O8.jsp?cmd=whoami
访问webshell需带cookie

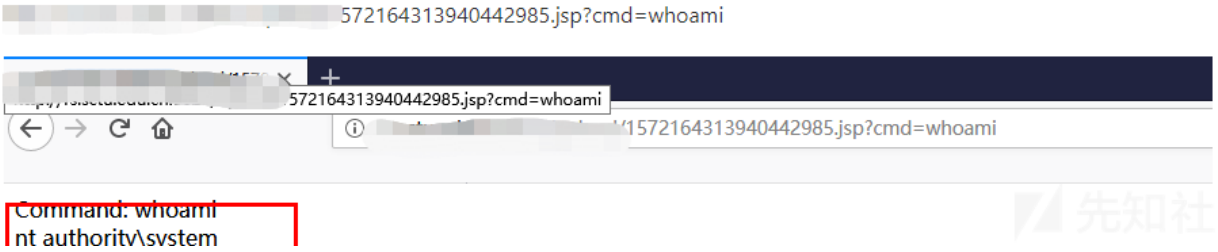



::$DATA

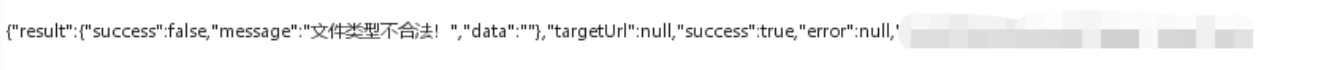


细心总会有收获的 发现一接口泄露物理地址

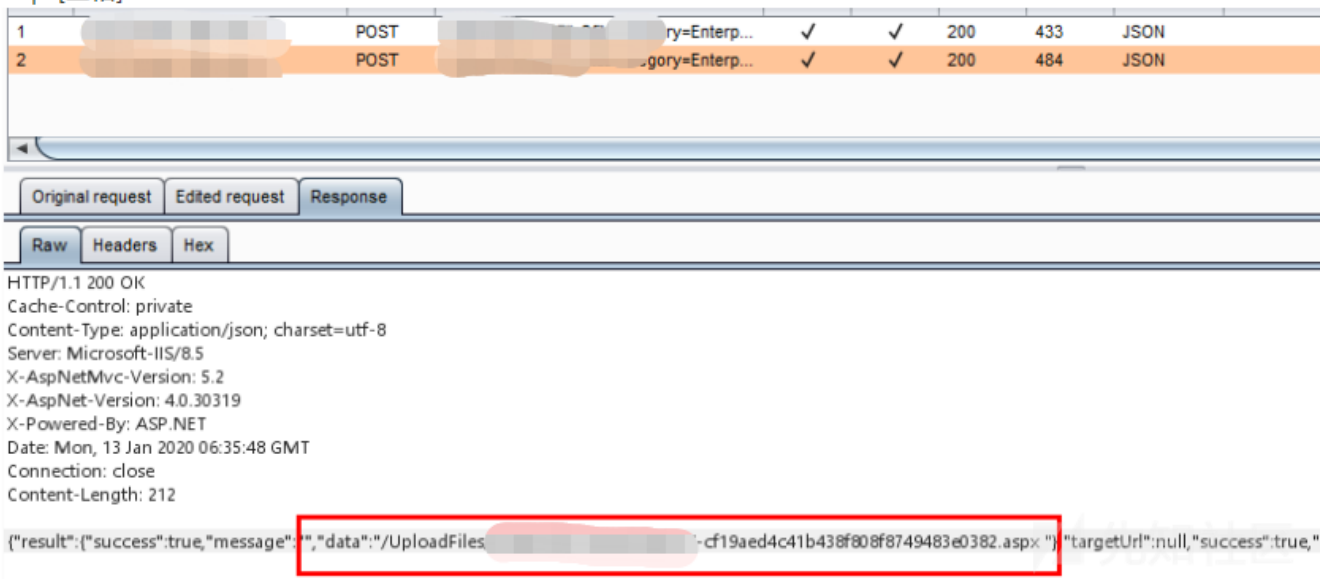



空格

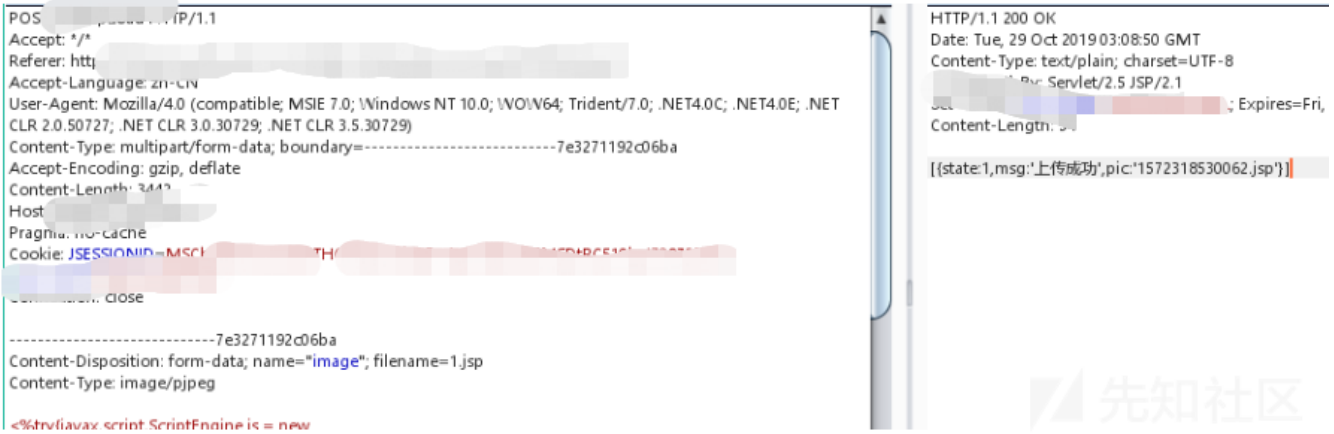



.aspx[空格]



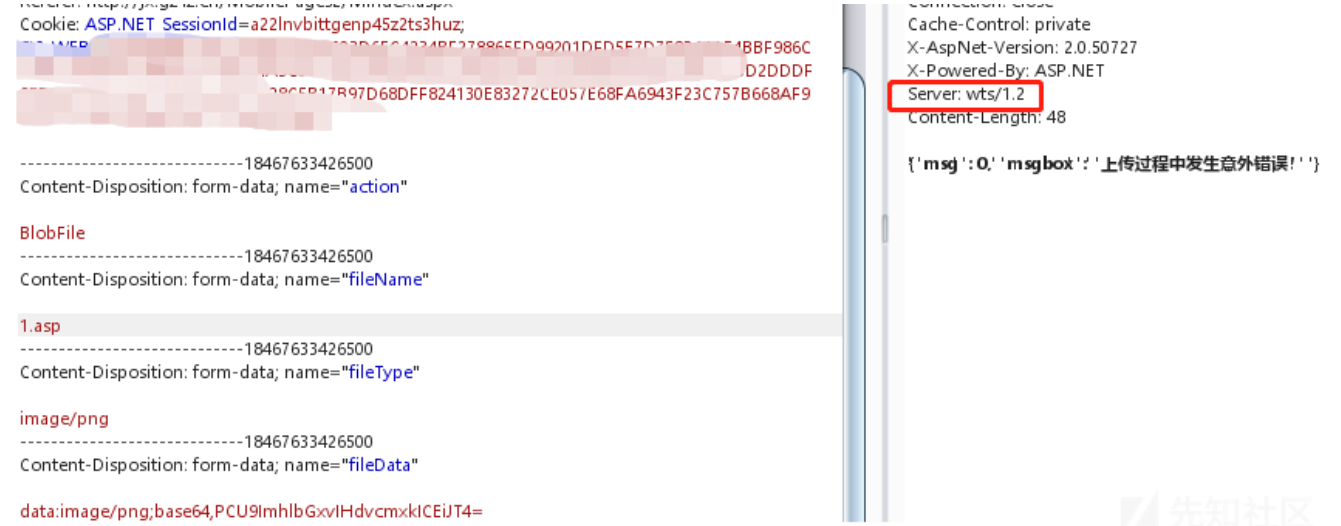

Linux：
可以试试/

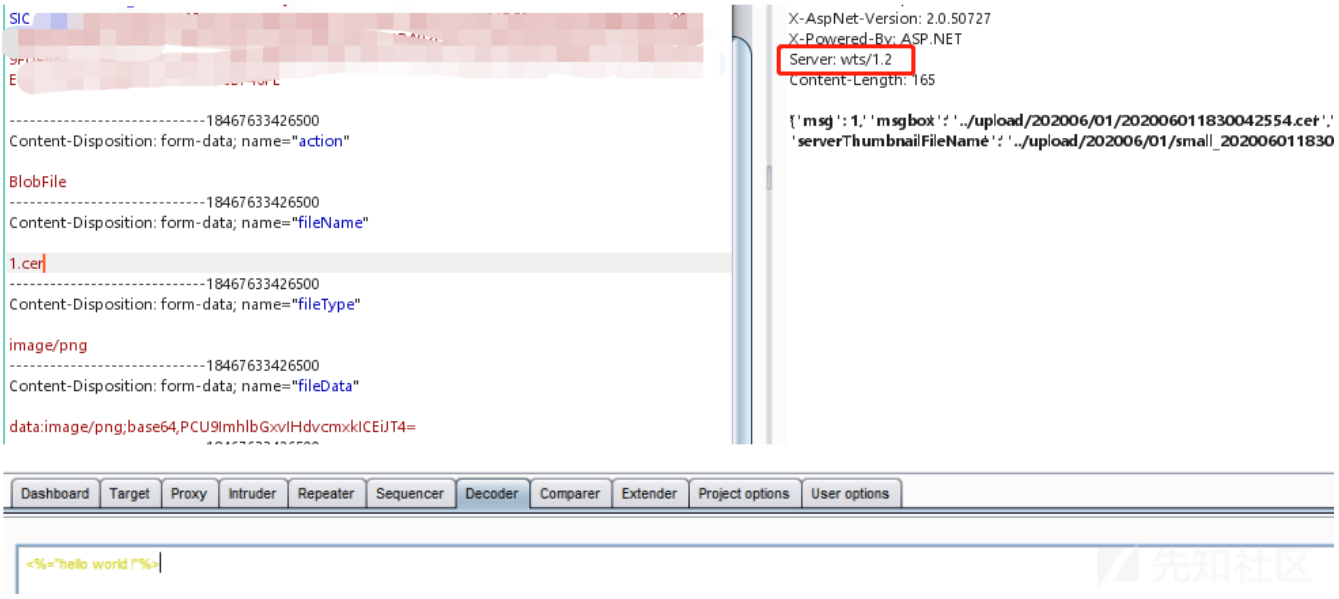

拓展名：
asp/cer/asa/cdx
aspx/ashx/asmx/svc... cshtml/vbhtml(.net4.0支持Razor)
jsp/jspx
php...
绕过WAF限制
维度：文件落地(后缀/内容)，能访问，能连接
这里主要讨论webshell后缀的落地
Content-Disposition: form-data; name="file"; filename="test.php"
通常检测就是这个字段，先说针对后缀绕过的方法：**构造当前能识别的正常文件的畸形包(.png)，然后再改后缀，反正是服务器能解析，WAF不认识。主要是对上述字段做畸形。**
我遇见的常见的WAF有安全狗，Yxlink-WAF，云锁，玄武盾，创宇盾，WTS-WAF，qianxin-WAF，WAF2.0
这些WAF都能在后缀落地的阶段绕过，每家WAF对后缀判断的具体的位置不同，就不一一说明了
例如某WAF：


filename参数去掉引号就可以过了，这里告警是因为内容免杀没过
Content-Disposition这一行可以动手脚的地方很多，师傅们可以自己试试，后缀都能bypass。

还有个有意思的：

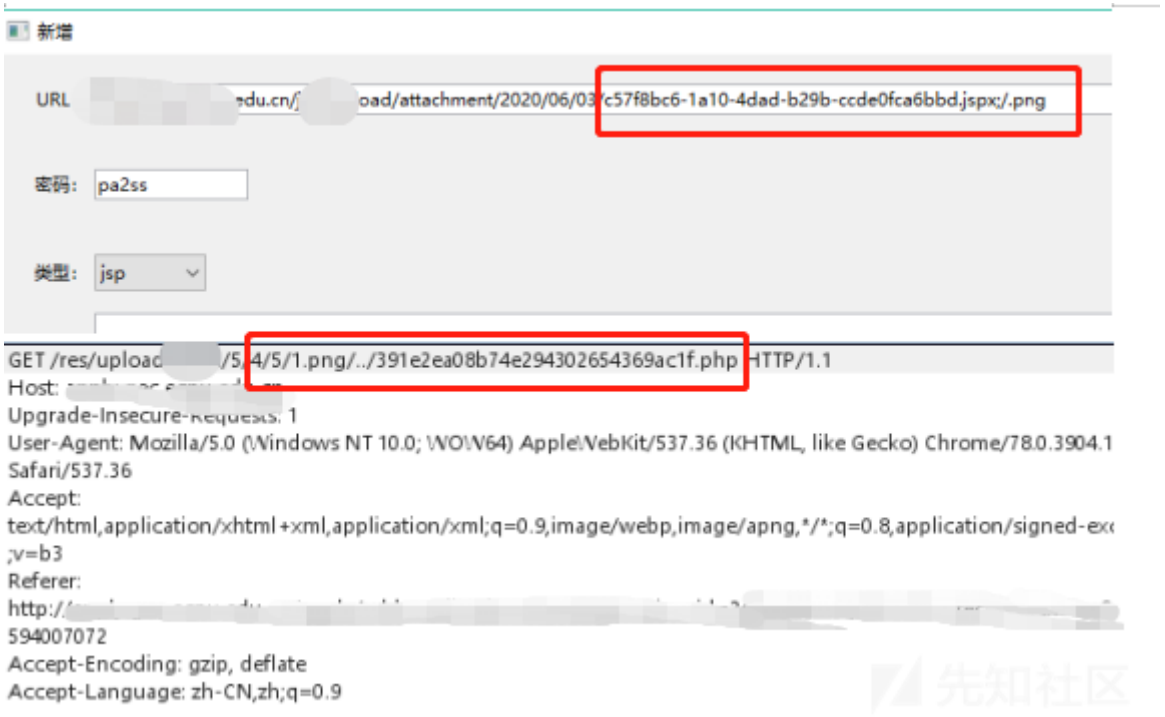






asp上传错误，cer成功，这个场景就是程序黑名单+WAF，可惜貌似WAF不认识Data URI Schema的文件上传，没找到后缀的可控点，所以WAF就没有拦。
有些WAF可能会阻止某些路径(upload)下访问脚本文件，可以试试这个




只是简单匹配URI的话，这个可以过
过内容的话，可以发大文件或是免杀的webshell...


过连接的话，自己改改通信的数据特征....

标签: Upload与WAF的那些事

---

## 添加新评论

**称呼** *

**Email** *

**网站**

http://

**内容** *

提交评论

上一篇: 【转载】内外网资产对应关系定位

下一篇: 没有了