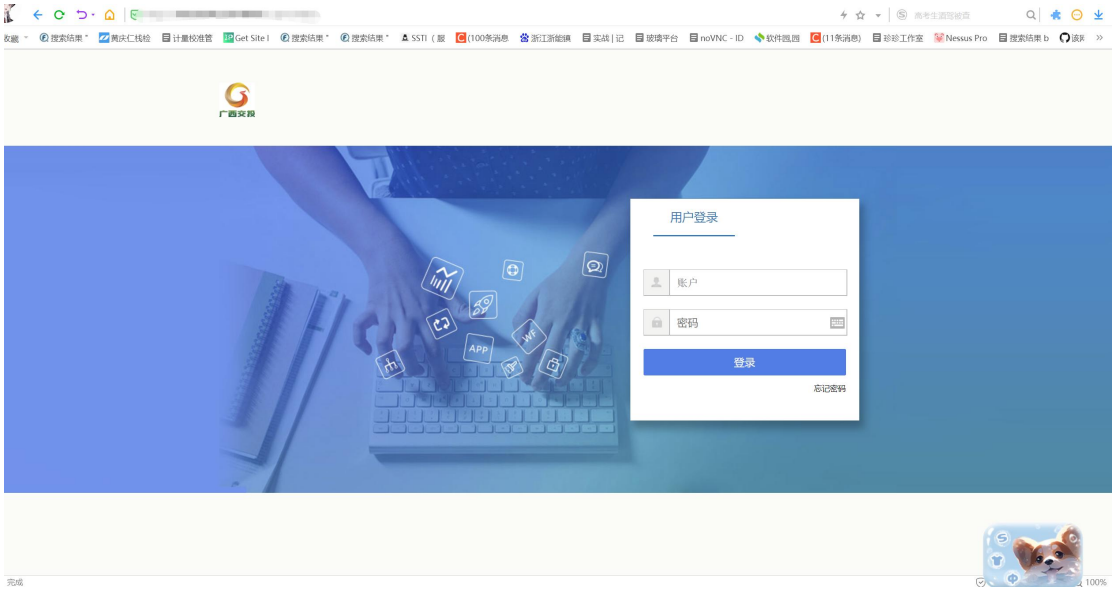
基于某狗 WAF 情况下的 ueditor.net 的绕过

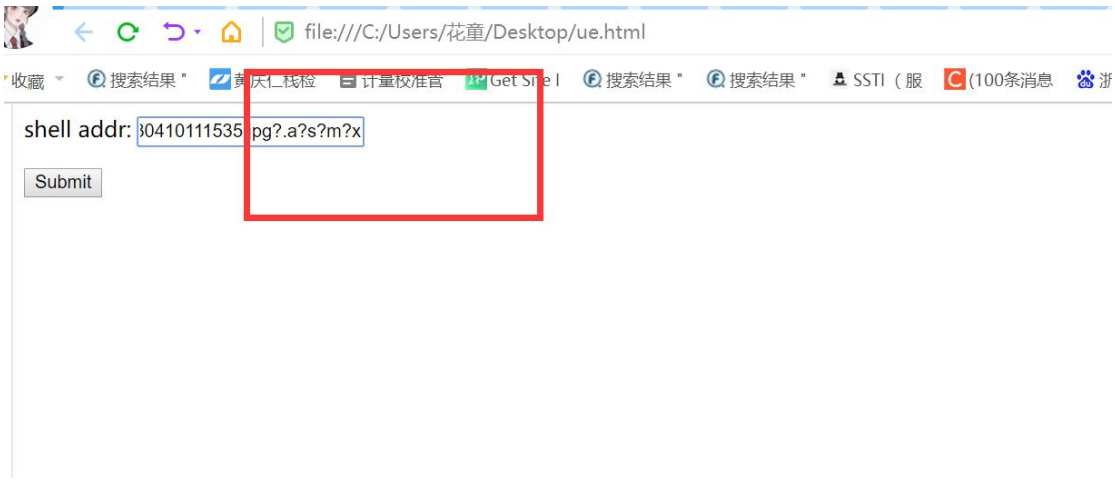
广西省 HW 案例



该站点的 WAF 为最新版安全狗

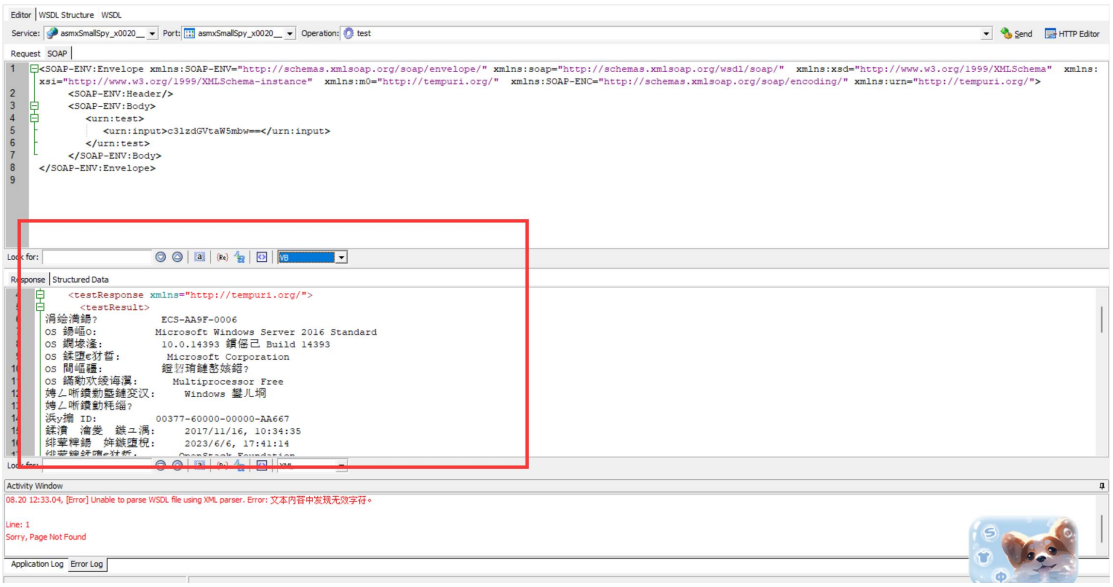
Aspx　ashx　asmx 秒死传不了

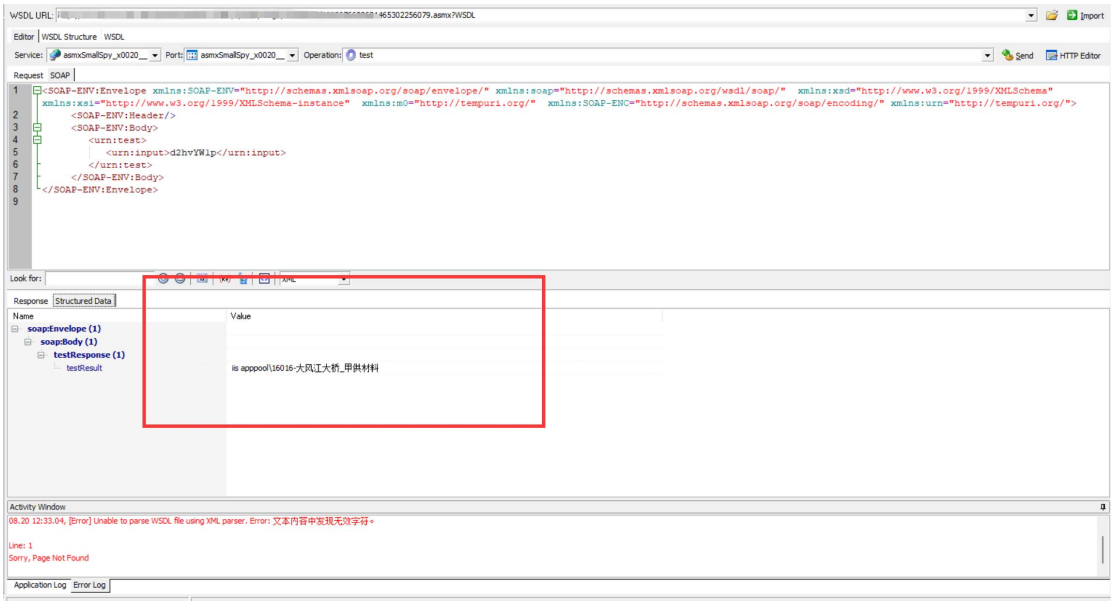
这个时候也差不多不用试其他后缀了，因为安全狗封的后缀比你想得到的更多
这个时候可以考虑 asmx 这类型木马，asmx 和 aspx ashx 本质不一样，asmx 是 asp.net 通过 SOAP 协议生成发送消息的功能。大概率能绕过正则
可以尝试将 asmx 变形为 a?s?m?x



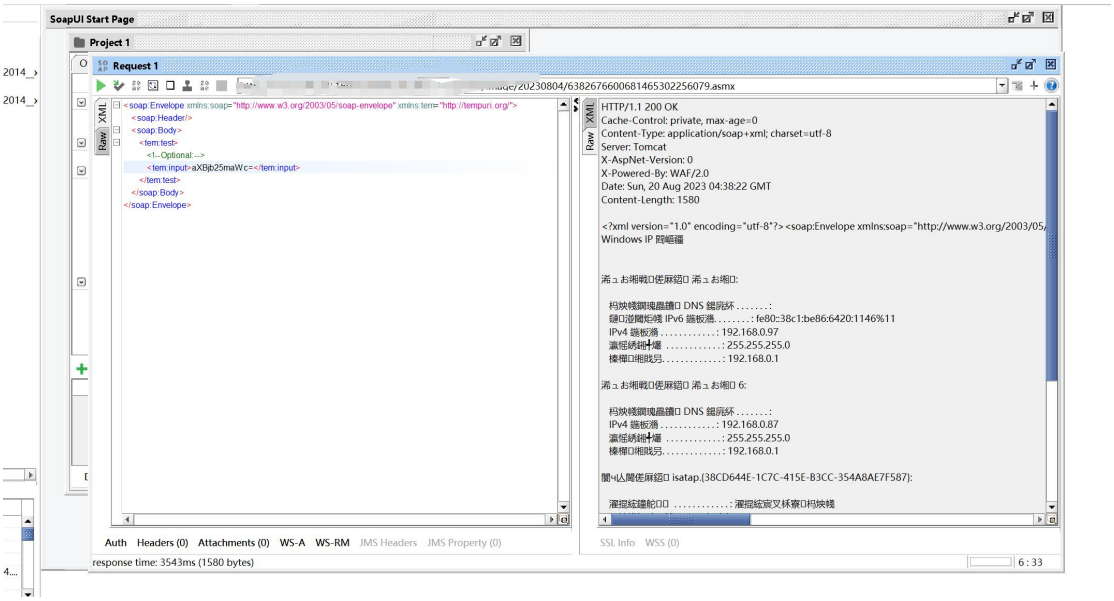
这里可以看到是成功上传了 asmx

然后就可以用哥斯拉工具进行连接
这个时候又会出现一种情况 连接失败
那么你的马可以换成其他类型的 asmx 的马，直接发包的那种
使用发包机制过 asmx 的马我就不发出来了
不建议直接用 burpsuite 进行发包，不太专业，而且也不规范，很容易报错
推荐使用 AWVSscaner soapui wsdler 三种工具
这里我使用 AWVSscaner 演示
成功 getshell





SOAPUI 效果图



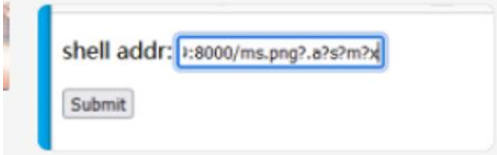
安远老哥试了直呼 NB

a? s? m? x

什么杀毒这么猛

这样

这个方法只对asmx有用



你需要用老版的awvsscaner那个客户端软件
发送soap包来激活asmx

上去了

牛逼

但是低权限

asmx?

还不快感谢我?