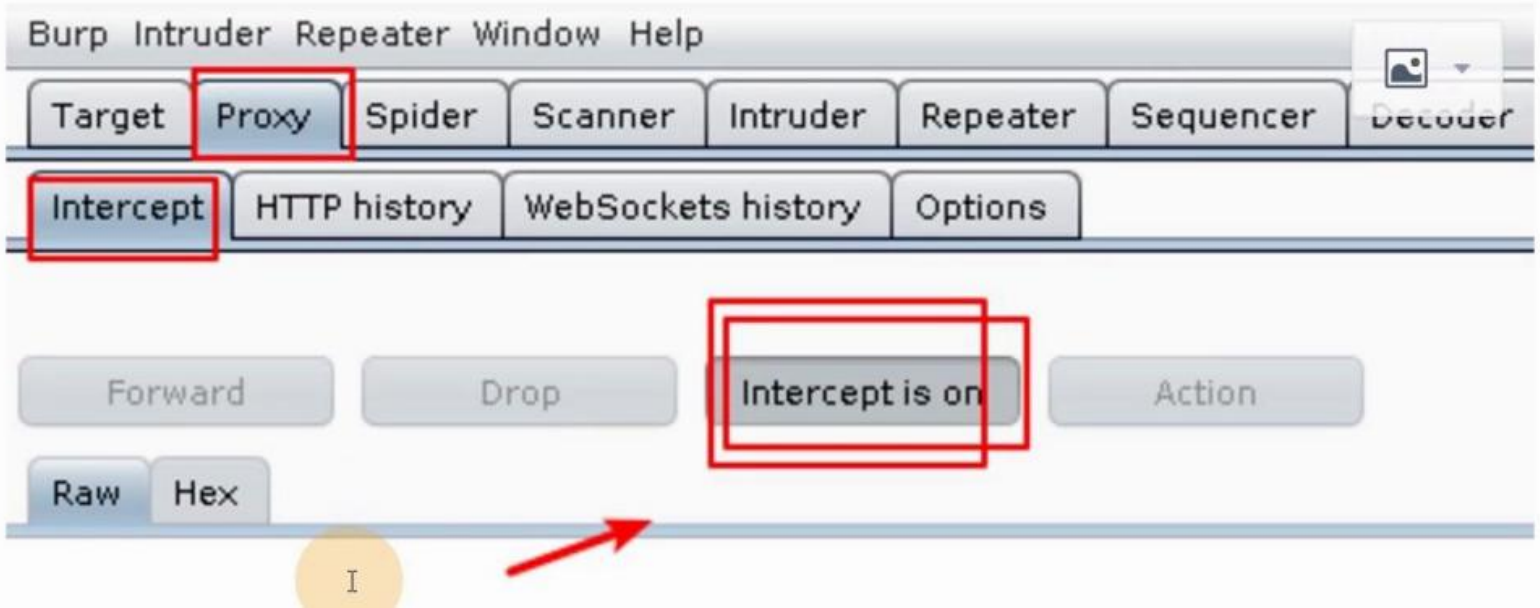
kali linux渗透测试

第25课 网站入侵，使用Burp拦截数据，抓取网络流量包

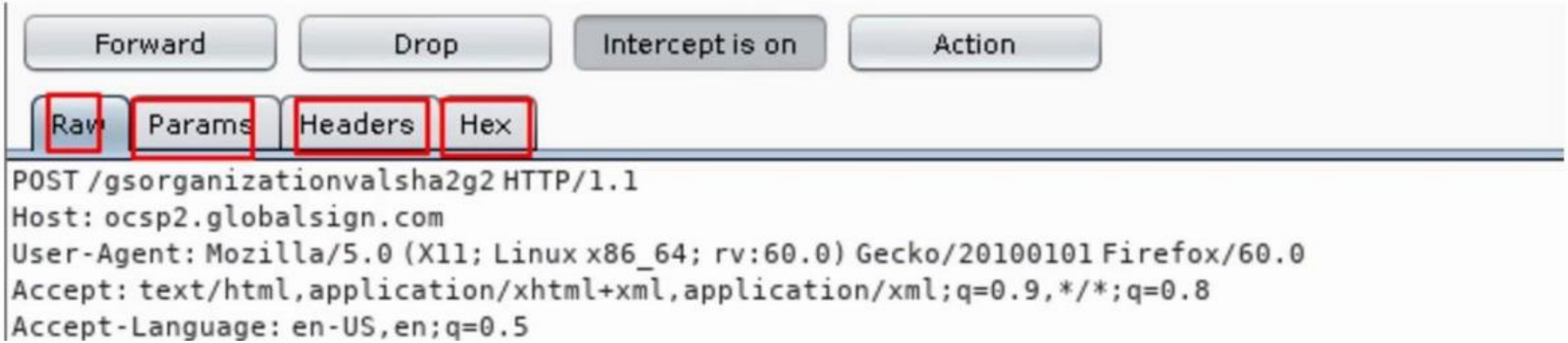
通过上一期视频的学习，我们对Burp Suite代理模式和浏览器代理设置有了基本的了解。Burp Proxy的使用是一个循序渐进的过程，刚开始使用时，可能并不能很快就获取你所期望的结果，慢慢地当你熟悉了它的功能和使用方法，你就可以用它很好地对一个产品系统做安全能力评估。

一般使用Burp Proxy时，大体涉及环节如下：

打开Proxy功能中的Intercept选项卡，确认拦截功能为“Interception is on”状态，如果显示为“Intercept is off”则点击它，打开拦截功能。



打开浏览器，输入你需要访问的URL并回车，这时你将会看到数据流量经过Burp Proxy并暂停，直到你点击【Forward】，才会继续传输下去。如果你点击了【Drop】，则这次通过的数据将会被丢失，不再继续处理。



Raw 这是视图主要显示web请求的raw格式，包含请求地址、http协议版本、主机头、浏览器信息、Accept可接受的内容类型、字符集、编码方式、cookie等。你可以通过手工修改这些信息，对服务器端进行渗透测试。

params 这个视图主要显示客户端请求的参数信息、包括GET或者POST请求的参数、Cookie参数。渗透人员可以通过修改这些请求参数来完成对服务器端的渗透测试。

headers 这个视图显示的信息和Raw的信息类似，只不过在这个视图中，展示得更直观、友好。

Hex 这个视图显示Raw的二进制内容，你可以通过hex编辑器对请求的内容进行修改。

```
POST /gsorganizationvalsha2g2 HTTP/1.1
//POST请求，HTTP协议的版本号
Host: ocsp2.globalsign.com
//接收请求的服务器
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/
//客户端软件的名称和版本号等信息
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
//客户端支持的数据类型，以MIME类型来表示
Accept-Language: en-US,en;q=0.5
 //客户端支持的语言，汉语为zh，英语为en
 Accept-Encoding: gzip, deflate
 //客户端支持的编码格式，一般来说表示的是数据的压缩格式
 Content-Length: 79
 //消息体的长度
```

```
Content-Type: application/ocsp-request
//消息体的数据类型
Connection: close
//发送响应之后TCP连接是否继续保持连接
```

谢谢观赏