1. 请求方式混淆
   1. GET与POST的区别

Http定义了与服务器交互的不同方法，最基本的方法有4种，分别是GET，POST，PUT，DELETE。URL全称是资源描述符，我们可以这样认为：一个URL地址，它用于描述一个网络上的资源，而HTTP中的GET，POST，PUT，DELETE就对应着对这个资源的查，改，增，删4个操作。但是对waf而言，由于运算能力的限制，很可能存在检测上的区分。

检测时可以将请求包按不同格式发送，如将get包通过添加无用参数的方式改成post包。

* 1. 文件上传

某些WAF是通过Content-Type识别是否是文件上传数据包。假设我们将Content-Type更改，数据包也是正常提交过去的。这个就完成了一次bypass。

还有的时候就是Content-Disposition: form-data;，也有某些WAF是根据Content-Disposition匹配filename的（Safe Dog 3.5/4.0通杀），用于验证黑名单。我们经过混淆大小写也是可以bypass的。

1. 性能考量

由于云waf面临海量了请求，可能会对一些过大请求包或文件上传包直接放弃参数检测。

检测时可以通过添加干扰参数，增大请求包长度达到通过的目的。

1. Cdn waf

目前CDN服务的功能是越来越多，安全性也越加强悍，用户的每个请求都会被发送到指定的CDN节点上，最后转发给真实站点。这个过程就好像加了一道关卡，这个关卡提供了缓存、加速、防御的特点。

可以通过寻找真实ip，直接对真实目标发起检测，流量不经过cdn即可。