# [绕过WAF、安全狗知识整理](http://blog.csdn.net/hxsstar/article/details/24771085)

市场上WAF分3种：

1.以安全狗为代表的软件WAF

2.百度加速乐，安全宝等部署在云端的WAF

3.硬件WAF

WAF是有一个白名单的，在白名单内的客户请求将不做检测

### (1)伪造搜索引擎

早些版本的安全狗是有这个漏洞的，就是把User-Agent修改为[**搜索引擎**](http://lib.csdn.net/base/searchengine)，便可以绕过，进行sql注入等攻击推荐一个谷歌插件，可以修改User-Agent，叫User-Agent Switcher

### (2)伪造白名单特殊目录

360webscan脚本存在这个问题，就是判断是否为admin dede install等目录，如果是则不做拦截

比如

详细的见

wooyun-2014-049051

wooyun-2014-049161

wooyun-2014-050576

### (3)直接攻击源站

这个方法可以用于安全宝、加速乐等云WAF，云WAF的原理通过DNS解析到云WAF，访问网站的流量要经过指定的DNS服务器解析，然后进入WAF节点进行过滤，最后访问原始服务器，如果我们能通过一些手段（比如c段、社工）找到原始的服务器地址，便可以绕过，

# 0x03 WAF数据包解析阶段的绕过

### （1）编码绕过

最常见的方法之一，可以进行urlencode

### （2）修改请求方式绕过

我想玩渗透的都知道cookie中转注入，最典型的修改请求方式绕过，很多的asp，aspx网站都存在这个问题，有时候WAF对GET进行了过滤，但是Cookie甚至POST参数却没有检测。

还有就是参数污染，最近的一个典型例子就是wooyun社区给出的multipart请求绕过，在POST请求中添加一个上传文件，绕过了绝大多数WAF。

详情看<http://zone.wooyun.org/content/11423>

### （3）复参数绕过

例如一个请求是这样的

GET /pen/news.[**PHP**](http://lib.csdn.net/base/php)?id=1 union select user,password from [**MySQL**](http://lib.csdn.net/base/mysql).user

可以修改为

GET /pen/news.[**php**](http://lib.csdn.net/base/php)?id=1&id=union&id=select&id=user,password&id=from%20mysql.user

很多WAF都可以这样绕，

### （1）特殊字符替换空格

用一些特殊字符代替空格，比如在[**mysql**](http://lib.csdn.net/base/mysql)中%0a是换行，可以代替空格，这个方法也可以部分绕过最新版本的安全狗，在sqlserver中可以用/\*\*/代替空格

### （2）特殊字符拼接

把特殊字符拼接起来绕过WAF的检测，比如在Mysql中，可以利用注释/\*\*/来绕过，在mssql中，函数里面可以用+来拼接

比如

### （3）注释包含关键字

在mysql中，可以利用/\*!\*/包含关键词进行绕过，在mysql中这个不是注释，而是取消注释的内容。