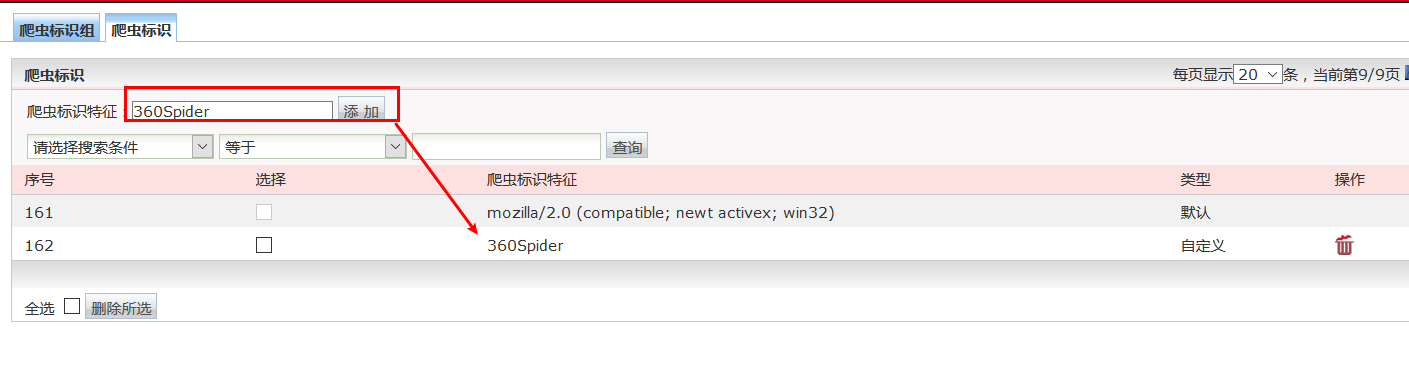
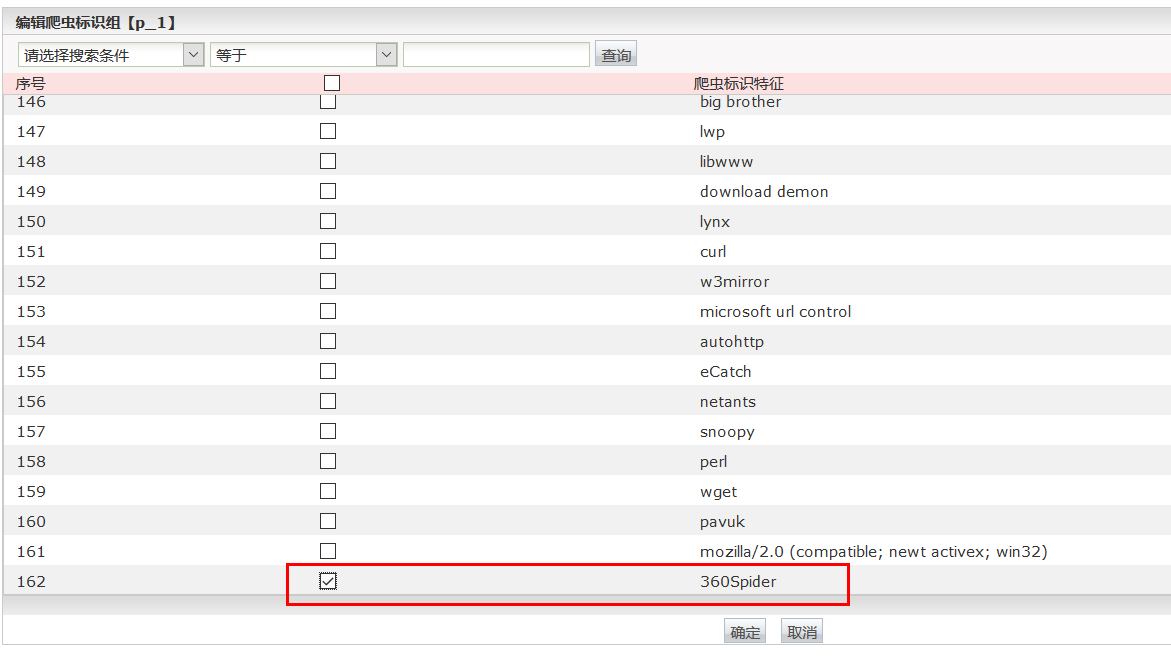
**28.WAF 上配置开启爬虫防护功能，当爬虫标识为 360Spider，自动阻止该行为；**

首先，默认只有一个DefaultRobots标识组，如果题目有特殊指定，我们应该去添加爬虫标识。

添加之后就会有爬虫标识特征了：

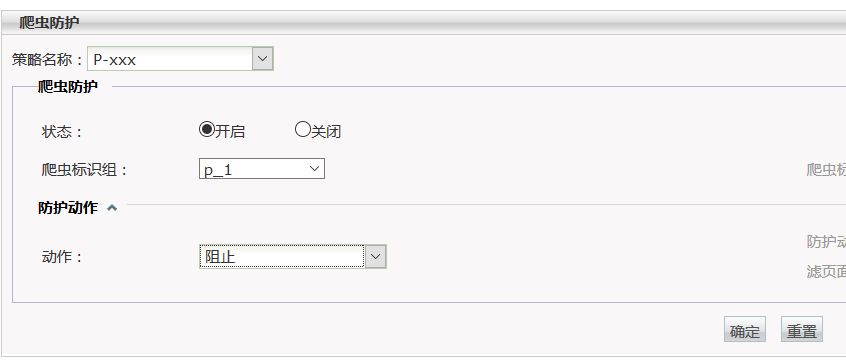


将爬虫规则添加到爬虫标识组：





然后应用爬虫防护：

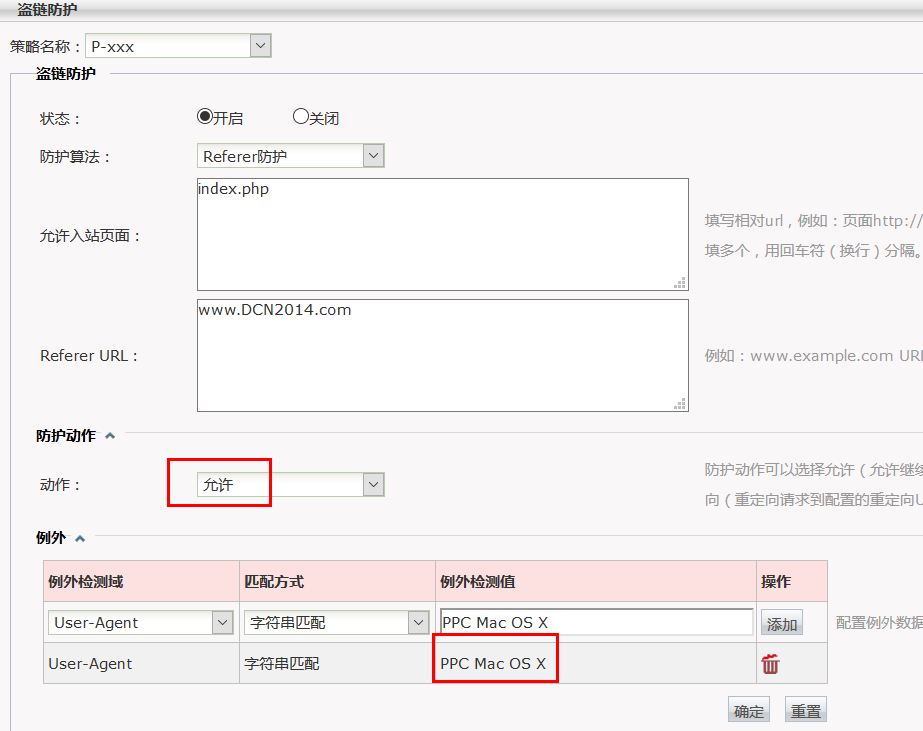


**29.WAF 上配置开启防护策略，将请求报头 DATA 自动重写为 DATE;**

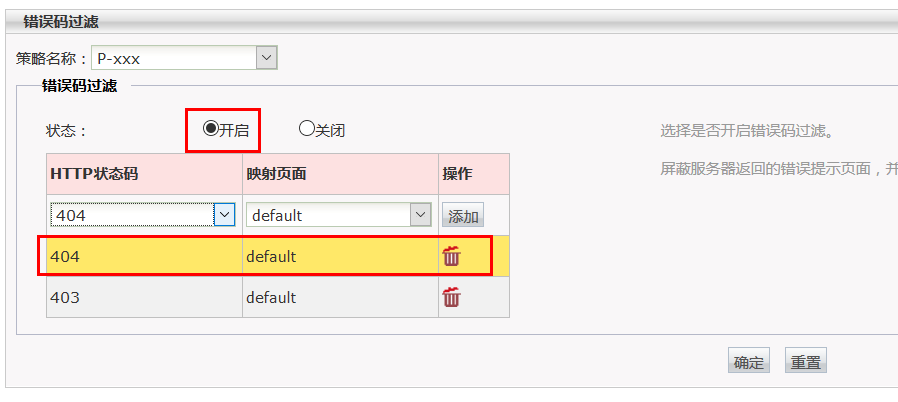
这个在题目上并不能获得关键字，只能根据经验了，通过站点转换，可以重写报文。



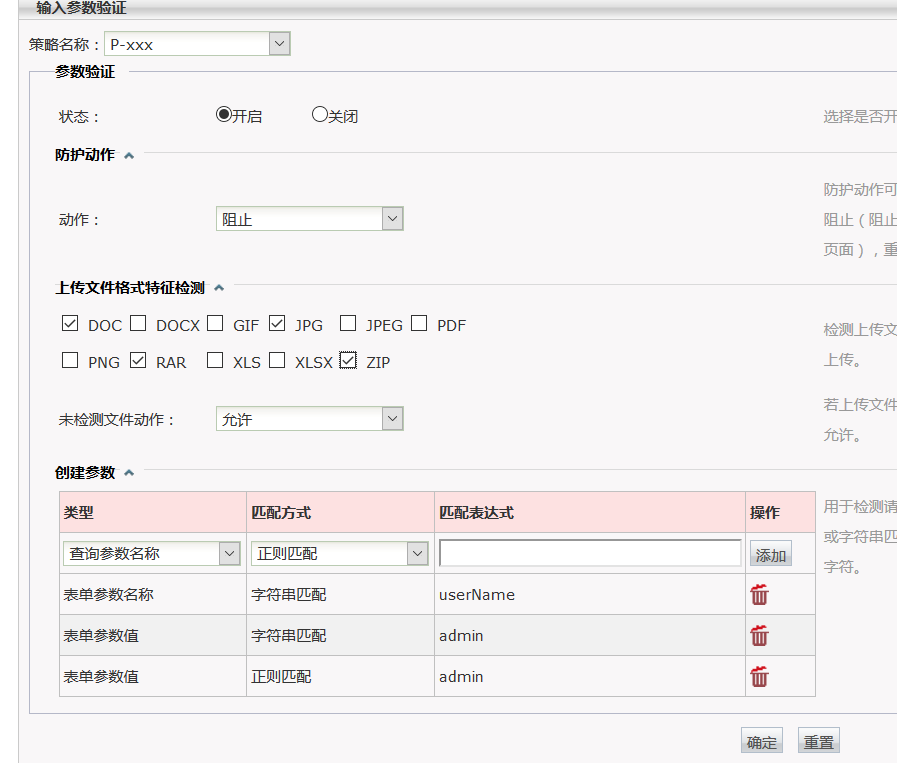
**30.WAF 上配置开启盗链防护功能，User-Agent 参数为 PPC Mac OS X 访问 www.DCN2014.com/index.php 时不进行检查;**



**31.WAF 上配置开启错误代码屏蔽功能，屏蔽 404 错误代码;**



**32.WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件;**



**33.WAF 上配置开启基本防护功能，阻止 SQL 注入、跨站脚本攻击；**



**34.WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问\*.bat 的文件;**

禁止xxx，就可以联系到黑名单

