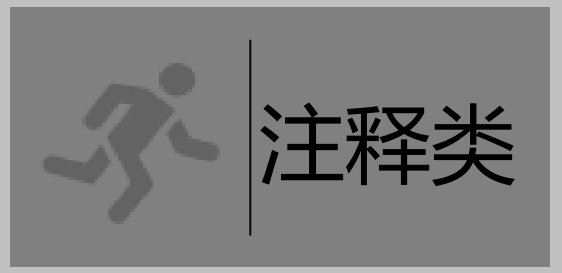
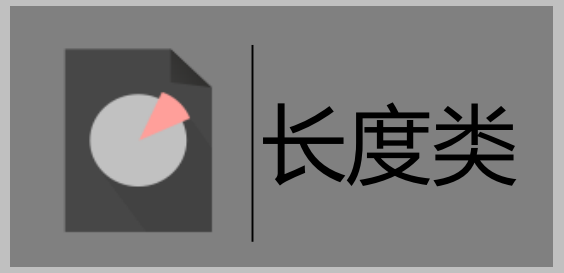
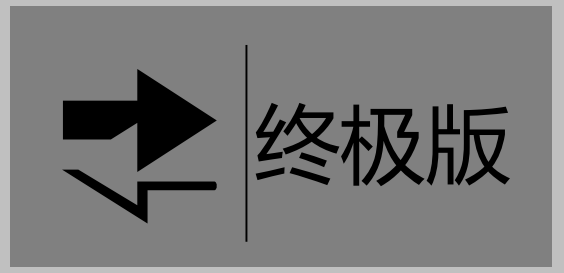
基于正则类sql注入防御的绕过技巧

——range@bugscan


简介


注释类


长度类


终极版

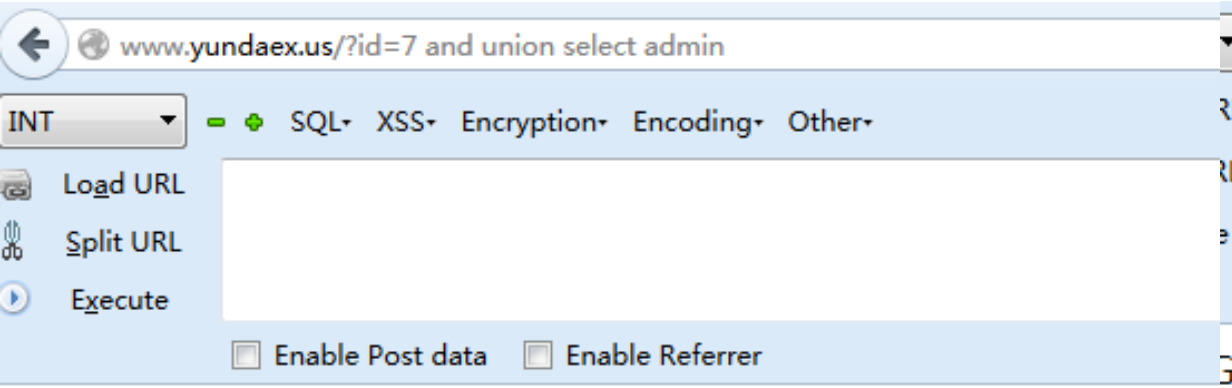
简介

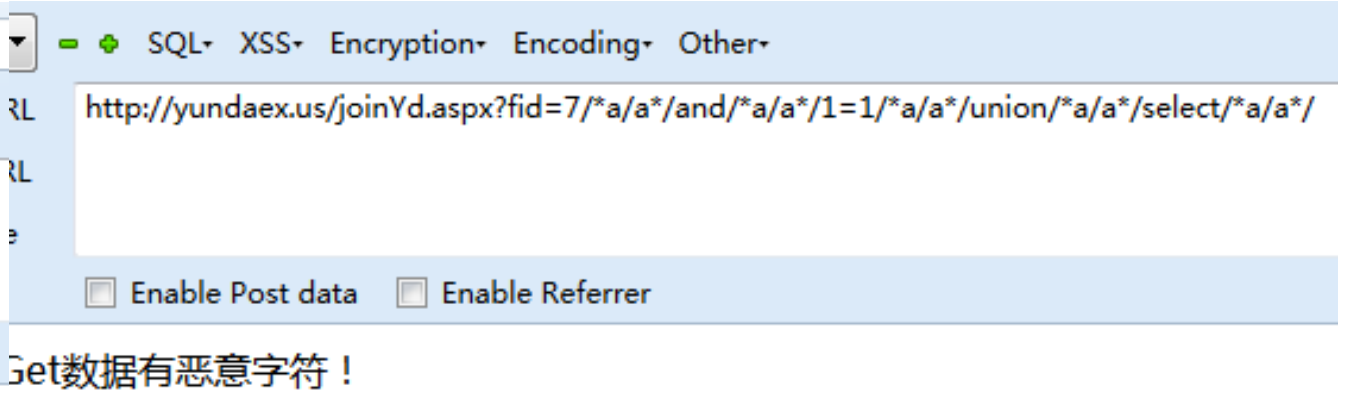
大多数waf对sql注入的防护是基于正则过滤的，因此只要绕过正则的匹配，即可绕过过滤继续注入，网络上也有很多关于这方面的资料，就不再赘述了，主要从个人经历过的绕过入手。

注释类

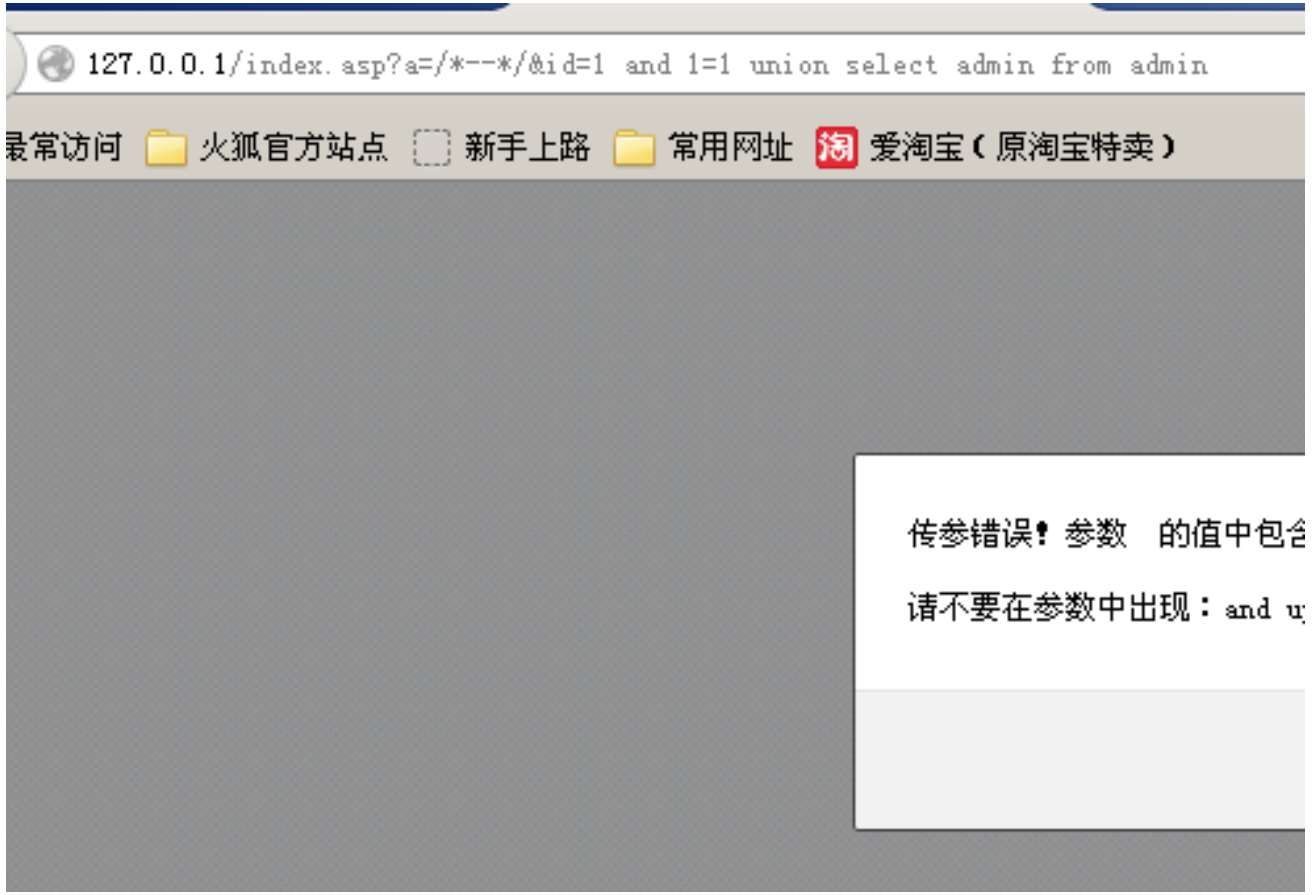
注释类

1. /*a/a*/ ， /***/ (安全狗最新版)





2. a=/*--*/& (安全狗3.5beta版)



长度类

网站防火墙

192.168.207.130/NewsType.asp?SmallClass=1 and 1=1

屏幕录像专家 未注册

INT

SQL· XSS· Encryption· Encoding· Other·

Load URL

Split URL

Execute

http://192.168.207.130/NewsType.asp?SmallClass=1%20and%201=1

管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>

半:

其他人怎么说？ 安全狗-网站安全专家

0KB/S 0.0KB/S 8%

20:23

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

恢复会话 | 南方数据- | 南方数据-

127.0.0.1/index.asp

百度 <Ctrl+K>

最常访问 火狐官方站点 新手上路 常用网址 爱淘宝(原淘宝特卖)

南方数据
WWW.SOUTHIDC.NET

企业邮局 联系我们 收藏本站 繁體中文

首 页 | 阿斯顿企业简介 | 新闻资讯 | 产品展示 | 下载中心 | 企业荣誉 | 营销网络 | 人才招聘 | 客户留言 | 会员中心 |

需要一个插件来显示此内容。
安装插件…

QQ Online
在线咨询
网站建设
点击客服QQ号码
即时交流或留言

用户登陆

用户名：
密 码：
登录 清除
新用户注册 忘记密码?

产品查询

产品名称
所有大类
所有小类
关键字 搜索

产品列表

联系我们:[QQ:240003933] [E-mail:onlinetrans@163.com]

新 闻 导 航->

公司新闻 | 业内资讯

asdf	[2008-8-17]
hellllllllllllllloooooooooooooo	[2008-8-14]
爱上对方	[2008-7-15]
请进老康博客	[2008-4-22]
南方数据企业网站管理系统V11新增功能	[2008-2-20]
南方数据企业网站管理系统V11.0 ACCESS版成功发布	[2008-2-18]
南方数据得到用户的一致好评	[2008-2-16]

产 品 导 航->

推荐产品 | 产品分类



新品推荐 >>

需要一个插件来显示此内容。
安装插件…

网站公告 >>

2008年9月1日

开始 | 南方数据- - Mozilla... | 网站安全狗 | 新建 文本文档.txt -... | 17:24

终极方法

终极类

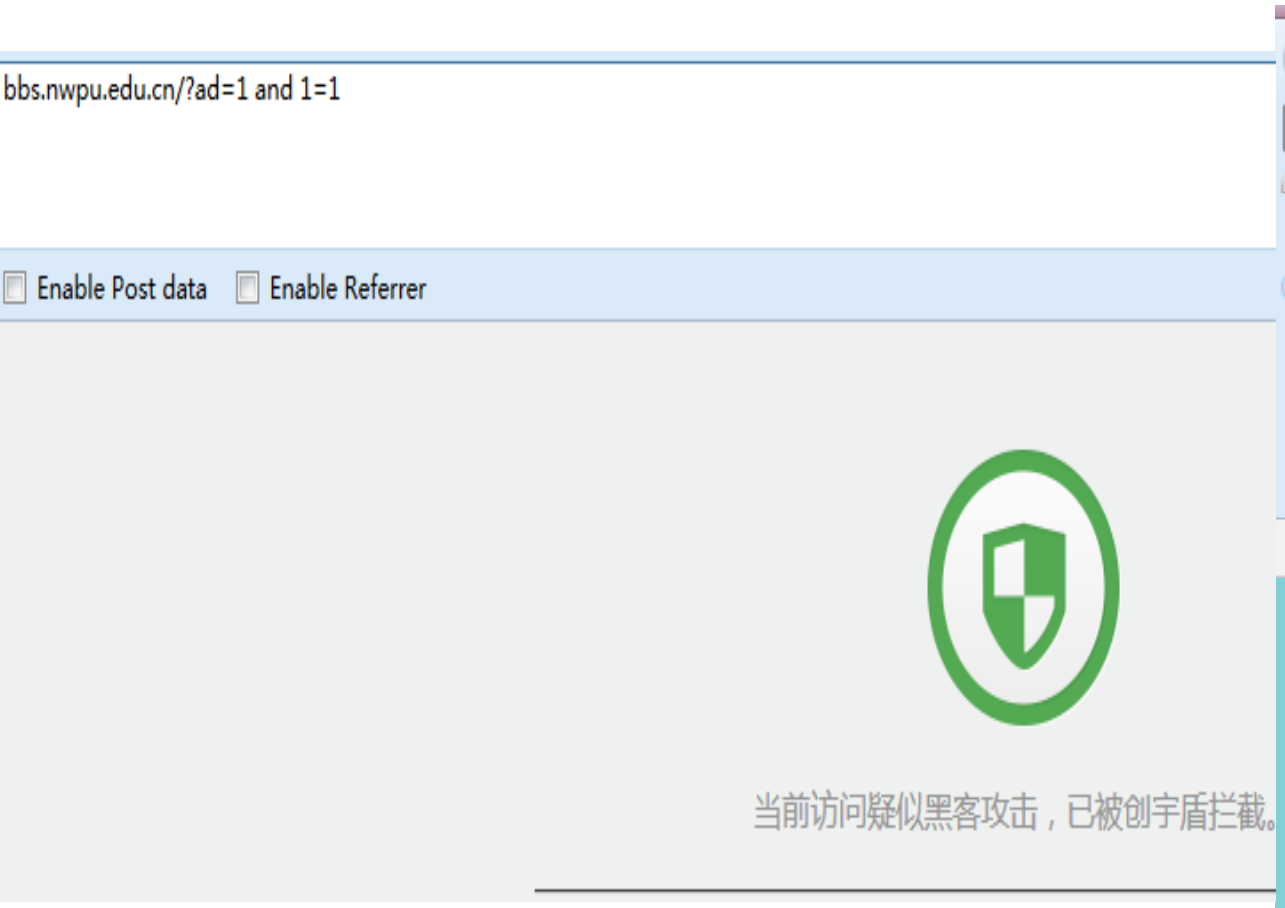
POST注入绕过安全狗，云锁，创宇盾

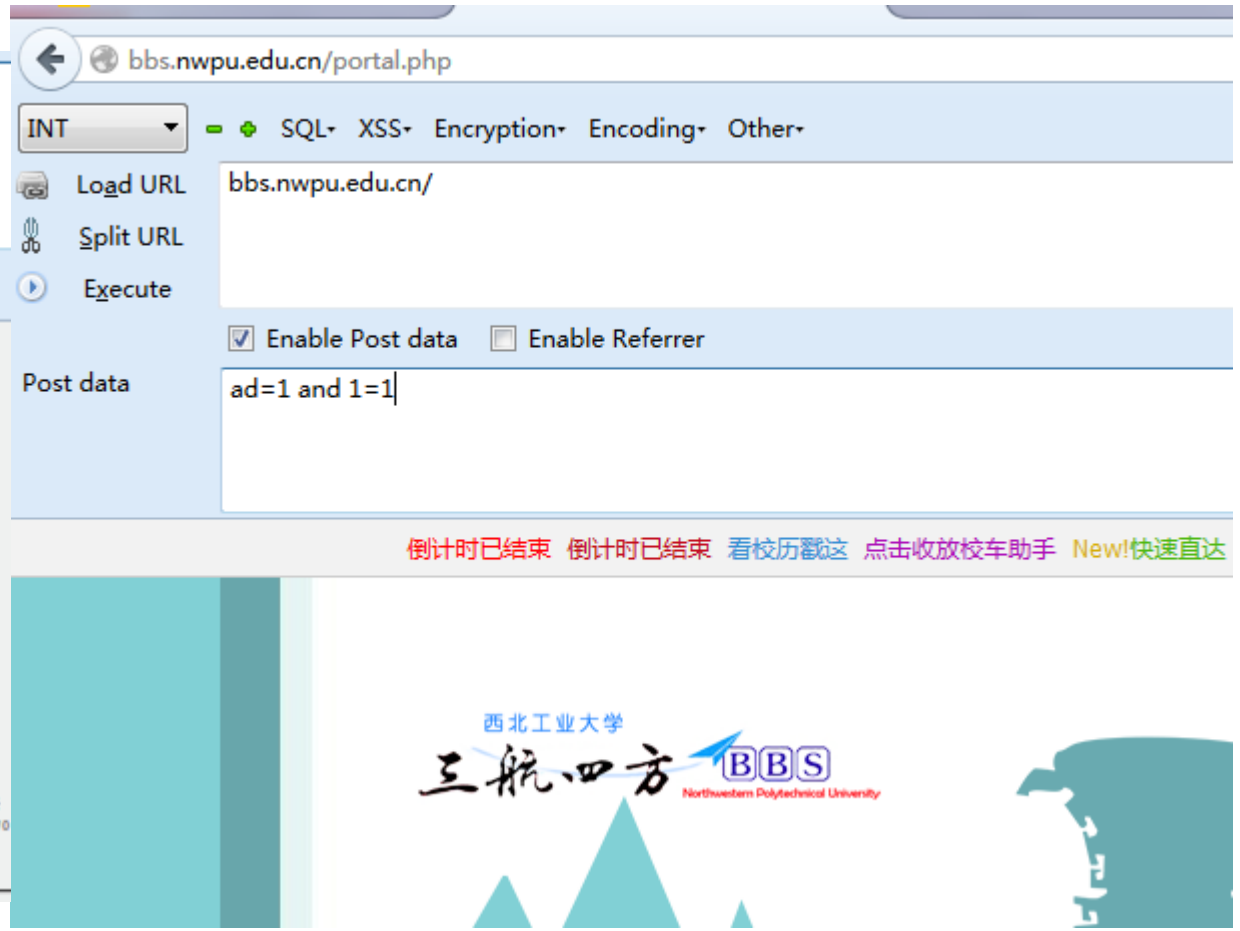
官方规则	SQL注入拦截规则	防止创建或者删除函数	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止创建或者删除Mysql用户	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止对数据库进行创建、删除、备份操作	开启	开启	开启
官方规则	SQL注入拦截规则	防止对数据库进行删除、创建表操作	开启	开启	开启
官方规则	SQL注入拦截规则	防止SQL联合查询	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止将本地或远程的数据文件批量导入到SQL Server数据库中	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止修改数据库	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止文件复制	开启	关闭	关闭
官方规则	SQL注入拦截规则	防止数据库系统的存储过程被执行	开启	开启	关闭
官方规则	SQL注入拦截规则	防止注入存储过程	开启	开启	关闭
官方规则	SQL注入拦截规则	防止对数据库进行数据删除操作	开启	开启	开启

新增 修改 删除 白名单

POST注入绕过安全狗，云锁，创宇盾等

POST注入绕过安全狗，云锁，创宇盾等






THANK YOU!