oracle手工报错注入,注入

转载

Adn无解 于 2021-04-10 09:26:44 发布 201 收藏
文章标签： oracle手工报错注入
Spring的常用注解2021-01-21 13:03:49

①　@Component:使用在普通java类上

②　@Service:使用在业务层类上

作用:声明一个类的对象为bean对象，相当于配置了bean标签。

注意:相当于使用的是无参数构造器来创建对象。

问题:

只使用@Service注解，和 A a=new A();的效果是相同的，创建的

是一个没有初始化数据的bean对象，但是在

sqlmap2021-01-20 22:32:44

文章目录

前言一、SQL注入二、SQLMAP1.GET注入2.POST注入3.Cookie注入

前言

sqlmap是sql注入的测试工具，优点是自动化和范围广，但是会有误报、漏报且测试方法有限。靶场我使用的是蚁景网安学院的sql入门靶场。

一、SQL注入

二、SQLMAP

官方网址：https://sqlmap.org

1.G

SQL注入-GET参数注入2021-01-20 15:30:18

CTF练习

第一次CTF练习

第一次CTF练习

1.拿到虚拟机后开启 一开始想用外部Xshell连接它，被老冯骂了一顿

2.开启kali用nmap扫描该机器 nmap 192.168.80.135 发现该机器开启了22和80端口 说明该机器开启了ssh和http服务

3.浏览器查看该机器的http服务 http://192.168.80.135

sql注入遇到的一些问题2021-01-19 23:30:05

一、字符型注入的思想是闭合引号： select 1,2 from tables where id='ID' ID: ' or 1=1' 、 ' or 1=1# 、' or 1=1– 步骤： 1、先判断当前表的字段数 ' order by 1(2,3,4,5…) #,直到出现错误，说明只有几个字段 2、知道了字段数之后，测试哪几个字段可以回显,比如有3个字段

Spring依赖注入2021-01-19 20:35:17

Spring依赖注入

创建对象的方式都是使用xml配置文件.

1.通过有参构造

dao层

package com.demo.dao;

public interface UserMapper {

}

package com.demo.dao.impl;

import com.demo.dao.UserMapper;

public class UserMapperImpl implements UserMapper {

}

service层

Da

SpringIOC的自动注入2021-01-19 17:03:13

问题:

SpringIOC的DI依赖注入后,我们可以根据对象之间的依赖关系的 责任链,让Spring容器对象帮我们创建有一个组装好的对象,比如A中有B,B 中有C,C中有D.将A,B ,C,D都创建为Bean对象,然后使用ref属性告诉Spring 对象之间的依赖关系的组装规则,假如依赖责任链特别长,使用ref注入就会

面2021-01-18 22:03:44

1. SQL注入类型及绕过方式

·注入分类：

1.数字型

2.字符型

3.报错注入

4.布尔型盲注

5.基于时间的盲注

2. 跨站脚本XSS类型及防御措施

·分类：

1.反射型

2.存储型

3.DOM型

·防御措施：

1.对输入进行严格的过滤和转义

2.针对输出点进行防御

3. XXE xml外部实体注入漏洞

·本质原理：

MYSQL 其他函数报错注入2021-01-18 12:04:21

都为空间数据储存函数，其余函数的报错原理与GeometryCollection()原理相同

MYSQL 中的空间数据存储

MySQL支持以下数据类型：

Geometry:可以存储所有的几何类型

Point:简单点

LINESTRING:简单线

POLYGON:简单面

MULTIPOINT：多点

MULITILINESTRING:多线

MUILITIPOLYGON：很多方面

GE

web安全之报错注入汇总2021-01-16 21:30:23

1 报错注入

MySQL 报错注入主要分为以下几类：

1. BigInt 等数据类型溢出；

2. Xpath 语法错误；

3. count() + rand() + group_by() 导致重复；

4. 空间数据类型函数错误。

1.1 floor()

rand(N) - 返回一个随机浮点数 v，范围是 0<=v<1.0；N 是可选提供的，如果提供了N，则会设定N为一个SEED

Web安全之SQL注入总结2021-01-16 20:32:19

本文会介绍POST注入、Head注入、报错注入、盲注、cookie注入、宽字节注入、堆叠注入、偏移注入、DNS注入、Access、Mssql、Oracle注入原理和手法。

联合注入：https://blog.csdn.net/xlsj228/article/details/105841168

按变量类型分：数字型和字符型

按HTTP提交方式分：POST注入、

cookie注入2021-01-16 19:03:06

SQL注入作为一种很流行的攻击方式被越来越多的人所知晓，很多网站都对SQL注入做了防护，用常规的手段去探测网站的SQL注入漏洞时会被防注入程序阻挡，一般的防注入程序都是基于“黑名单”的，根据特征字符串去过滤掉一些危险的字符。一般情况下，黑名单是不安全的，它存在被绕过的风险。比如有

SQL 注入2021-01-16 18:32:20

SQL 注入

文章目录

SQL 注入注入攻击原理什么是SQL？什么是SQL注入？SQL注入是怎么样产生的？

万能密码原理实例[极客大挑战 2019]easySQL

联合查询前提原理实例[极客大挑战 2019]LoveSQL[GXYCTF2019]BabySQli

堆叠注入原理实例[强网杯 2019]随便注方法一 预编译方法二 修改表

Spring中的注解配置2021-01-16 16:30:59

写在前面

注解配置和xml配置所实现的功能是一样的，即降低程序之间的耦合，只是配置的形式不一样。解析配置文件时就会创建容器进而创建对象。

曾经的xml配置

工厂类

class BeanFactory {

public static UserDao getUserDao(String id) {

// String className = 解析配置文件xml 拿到id对应的class

// 反射

1.1 Bug场景：

1.1 启动Spring Boot项目时报 NoSuchBeanDefinitionExpetion 没有找到bean的实例，即spring没有实例化对象，也就无法根据配置文件执行依赖注入依赖错误

2.1 Bug原因：

假设模块A需要引入模块B的依赖，并且需要注入模块B中的TestService对象。

第一步，需要在A的pom文件中

对一个BeesCMS网站的渗透测试2021-01-10 15:57:17

前言

自己刚开始接触渗透测试，于是想找一些综合型的靶场来练练手，自己搭建没有那种感觉，于是找到了一个叫墨者学院的网站，上面的靶场还是很多的，而且大多数贴合实战，我喜欢！ 今天，我们来玩一个BeesCMS网站。

文章如有抄袭或不足，请指出，我会继续改进的。

话不多说，直接开始

普普通通的

1.依赖注入 (Dependency Injection)

1.1 面向接口编程

public interface Drivable {

void drive();

}

public class Bike implements Drivable {

@Override

public void drive() {

System.out.println("骑车");

}

}

public class Car implements D

解决 SQL 注入2021-01-09 14:58:27

SQL注入是什么？

看一下百度百科的定义：

啊，好长一大段文字，些许不想看，下面通过一个例子，来说明一下什么是SQL注入：

新建一个数据库，再建一个表，添加两行数据：

use db1;

create table user(

id int primary key auto_increment,

username varchar(32),

password varchar(32)

);

in