**sql 注入是什么及如何预防 sql 注入？**

答：SQL 注入攻击指的是用户或者黑客通过构建特殊的输入作为参数传入我们的 Web 应用程序端，而这些输入大都是 SQL 语法里的一些组合，通过执行 SQL 语句进而执行攻击者所要的操作，其主要原因是程序员没有细致地过滤用户输入的数据，致使非法数据侵入系统而造成的。因此我们在做开发过程中一定要预防 sql 注入，主要从两方面着手：

1、占位符的方式，就是对 sql 语句进行预处理，然后执行 sql 语句

2、通过 addslashes 或者 mysql\_real\_escape\_string 这两个函数对用户输入的值进行

安思栏深思 艾斯给

转义处理，把一些特殊的字符转义掉。

**xss攻击怎么防止**

XSS 又称 CSS，全称 Cross SiteScript(跨站脚本攻击)， XSS 攻击类似于 SQL 注入攻击，

是 Web 程序中常见的漏洞，XSS 属于被动式且用于客户端的攻击方式，所以容易被忽略

其危害性。其原理是攻击者向有 XSS 漏洞的网站中输入(传入)恶意的 tHTML 代码，当用

户浏览该网站时，这段 HTML 代码会自动执行，从而达到攻击的目的。如，盗取用户 Cookie

信息、破坏页面结

常见的恶意字符 XSS 输入：

1. XSS 输 入 通 常 包 含 JavaScript 脚 本 ， 如 弹 出 恶 意 警 告 框 ：

<script>alert("XSS");</script>

2. XSS 输入也可能是 HTML 代码段，譬如：

(1) 网页不停地刷新 <meta http-equiv="refresh" content="0;">

(2) 嵌入其它网站的链接 <iframe src=http://xxxx width=250 height=250></iframe>

构、重定向到其它网站等。

方法：利用 php htmlentities()函数

php 防止 XSS 跨站脚本攻击的方法：是针对非法的 HTML 代码包括单双引号等，使用

htmlspecialchars()函数。

在 使 用 htmlspecialchars() 函 数 的 时 候 注 意 第 二 个 参 数 , 直 接 用

htmlspecialchars($string)的话，第二个参数默认是 ENT\_COMPAT，函数默认只是转化

双引号(")，不对单引号(')做转义。

所 以 ， htmlspecialchars() 函 数 更 多 的 时 候 要 加 上 第 二 个 参 数 ， 应 该 这 样 用 :

htmlspecialchars($string,ENT\_QUOTES) 。 当 然 ， 如 果 需 要 不 转 化 如 何 的 引 号 ， 用

htmlspecialchars($string,ENT\_NOQUOTES)。

另 外 ， 尽 量 少 用 htmlentities(), 在 全 部 英 文 的 时 候 htmlentities() 和

htmlspecialchars()没有区别，都可以达到目的。但是，中文情况下, htmlentities()

却会转化所有的 html 代码，连同里面的它无法识别的中文字符也给转化了。

htmlentities()和 htmlspecialchars()这两个函数对单引号(')之类的字符串支持不

好，都不能转化， 所以用 htmlentities()和 htmlspecialchars()转化的字符串只能防

止 XSS 攻击，不能防止 SQL 注入攻击。

所有有打印的语句如 echo，print 等，在打印前都要使用 htmlentities()进行过滤，这

样可以防止 XSS，注意中文要写出 htmlentities($name,ENT\_NOQUOTES,GB2312)