注水漏洞的利用和防范 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/353/2021_2022__E6_B3_A8_E6_B0_B4_E6_BC_8F_E6_c97_353590.htm 参加IT认证考试前，笔者习惯到网上去搜搜。乱逛之余，不小心就来到了PROMETRIC的中文站。笔者发现整个站点都是ASP程序，况且刚才还有个考场的登录界面，要是能发现什么漏洞就好了。 探测漏洞 随手找了个页面(http://www.promet.ric.com.cn/openpage.asp?page_id=0)，在参数0后面加上个单引号。返回的页面显示：500服务器内部错误。在IE的“ Internet选项→高级 ”中有一个“ 显示友好HTTP错误信息 ”的选项，取消前面的钩。现在，我们可以看到详细的错误信息：Microsoft OLE DB Provider for ODBC Drivers 错误 80040e14[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near ./audit.asp，行18原来PROMETRIC用的是MSSQL，看来存在严重的注入漏洞(由于涉嫌攻击步骤，此处不详细叙述)。漏洞原理SQL注入的漏洞通常是由于程序员对它不了解，设计程序时某个参数过滤不严格所致。就拿刚才测试用的链接中的page_id这个参数来讲，肯定就没有进行过滤检查，源程序中的查询语句如下所示：Select * From Table Where page_id=0当我们提交http://www.prometric.com.cn/openpage.asp?page_id=0 and 1=1时，查询语句就变成了：Select * From Table Where page_id=0 and 1=1当我们提交其他的查询语句时，程序也会进行执行判断，如：http://www.prometric.com.cn/openpage.asp?page_id=0 and user>0查询语句变成了：Select * From Table Where

page_id=0 and user>0user是MSSQL的一个内置函数，指的是当前连接数据库的用户名，是一个nvarchar值。当它与整型量0进行大小比较时，MSSQL会试图将user的值转换成int类型，于是MSSQL就会报错：[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value web to a column of data type int.错误信息的后面显示的是库名、表名、数据等。如果对方屏蔽了错误信息呢？这时，我们就要利用Unicode、Substr等函数通过条件判断来进行猜测了。如何利用大家可以利用小竹开发的NBSI2 MSSQL(以下简称“ NBSI2 ”)工具。不过大家要注意，工具永远只是工具，只能用来提高效率和准确性，自己一定得了解原理。通过NBSI2，我们顺利地导出了PRO METRIC中文站数据库中的表名和数据，这里面包括各个考场的登录用户和密码。通过跨库查询，笔者还发现BALANCE表中的BALANCE字段存放了考场预付款的余额信息，只要进行跨库更新，这个金额完全可以改变。这时候，笔者突发奇想，既然可以得到考场程序，我们是不是可以私设一个考场……心动不如行动，马上开始安装考试系统。安装过程非常复杂，需要config.dts文件(网站上没有)。正当笔者不知怎么办的时候，突然发现了企业邮箱服务，PROMETRIC为每一个考场都开设了新浪企业邮箱。这些考场会不会为了方便没有改默认密码呢？果然很多考场没有更改默认密码，笔者很轻松地就进入了这些邮箱。经过一番搜索，终于在一个考场的邮箱中找到了PROMETRIC发过来的config.dts文件……到这里，本次安全测试算是告一段落了。试想一下，如果私自安装了考场程序，我们是不是可以随意修改考生信息？如果更改预付金，是不是还可以免费报

名考试？而且利用考场ID和密码，我们在网站上可以更改任何一个考场的注册信息，然后通过社会工程手段，克隆出一个虚假的考场是完全有可能的。后记不知大家还记不记得上期《电脑报》上有关Oracle注入漏洞的文章。虽然两者在技术实现手段、危害上都不一样，但它们有一个共同点从一个小小的地方撕开缺口，从而造成极大的危害。在笔者所探测的网站中，有些网站只注意过滤地址栏中提交的非法字符，却忽视了搜索功能中提交的字符，这样网站依然会存在注入漏洞。网络安全是一项非常重要的、整体性很强的工作，每一个地方都需注意，否则造成的损失难以估计。