 对于注入而言，错误提示是极其重要。所谓错误提示是指和正确页面不同的结果反馈，高手是很重视这个一点的，这对于注入点的精准判断至关重要。本问讨论下关于几类错误和他产生的原理，希望对读者有所帮助。 错误提示主要有逻辑错误和语法错误以及脚本运行错误三类。 一：逻辑错误 简单的例子是1=1 1=2这两个，1=1与1=2页面不同的原理是什么?以$sql = "0select * from news where id=$_GET[id]"为例。 0select * from news where id=1 and 1=2产生的结果集为NULL，然后程序取值得时候，就会去出空值，无法显示。当然有的程序发现SQL执行结果集为空，就立即跳转，效果就不显鸟。值得注意的是，有的如Oracle Postgresql的数据库在结果集为空情况下会再页面上表现字符型null字样，这算是个特点。如果使用or条件，比如 0select * from news where id=1 or 1=1 和and 1=2得结果正好相反，他的结果集十分庞大。如果SQL语句如此，再加上程序是循环读取结果集(一些编程上的陋习)那么会取出所有结果，结果可能运行很慢，在数据量巨大的Oracle上容易出现。这个例子会出现什么呢，一般程序取出结果集中的第一条结果，那么很可能已经不是id=1的那条新闻了，这就是由些小菜奇怪有时候or 1=1页面会发生变化的原因。 归根到底，都是结果集不同造成的，灵活掌握是关键，这并非单纯的经验问题。 二：语法错误 语法错误时比较熟悉的，比如对于sql server,PgSQL,Sybase的注入错误提示都很重要，因为利用它的

特性来获取信息很快速。语法错误造成的结果可能是SQL错误而中断脚本执行，但是脚本或服务器设置屏蔽错误的情况下，程序得到继续执行，但是结果集不存在，连NULL都算不上，反馈给攻击者的很可能就是结果集为空的情况，其实这是脚本的处理结果。当然Oracle PgSQL表现null。 三：运行错误不用说了，典型的就是利用MySQL注入benchmark让脚本运行超时得到物理路径，以及利用超时来获得不同的表征进行盲注入。 四：逻辑错误和语法错误的结合。 当表征极不明显的时候，利用类似iff这样的函数进行正确与否的区分有时候会成救命稻草。因为语法错误和逻辑错误的表征大多数情况都会有不同。 iff(1=1,1,no)这个会产生结果1 注意是数字，而iff(1=2,1,no)这个会产生no 是字符。那么 id=1 and 1=iff(1=1,1no)正确是必然成立的，而id=1 and 1=iff(1=2,1,no)会因为类型不同发生语法错误。不过可惜的是似乎支持iff函数的数据库不多，呵呵。 现在讲结果集在注入中的利用原理。 一：从or=开始 这是学习SQL注入的初级课程，登陆漏洞。我简略从SQL结果集上分析。 $sql = "0select top 1 * from admin where username=$username and password=md5($password)". 显而易见，or=的加入使SQL语句返回了一条记录，这才使验证通过。 二：再看现在的验证中的SQL $sql = "0select top 1 * from admin where username=$username". 结果集不为空才根据抽取的记录集中的密码值与用户提交的密码MD5值进行比对来进行验证。这样，你突然发现or=的计策失败鸟，但是后台明明有注入，这就是验证方法造成的。跟进这个验证过程，or=的确产生了一个结果集(admin表中的第一行记录)但是遗憾的事，后来的密码比对没法通过，验证无法成功。来源

：www.examda.com 思路很简单，网上有案例，我重在原理，利用union来产生想要的结果集。比如and(1=2)union 0select top 1 username,123456得md5值,id from admin where username=admin 这样产生了admin的记录信息，但是记录集中的密码那个位置的值被替换成了123456的md5值，这样，使用admin 123456通过验证并且继承他的权利。 更有甚者全部用xxx的方法来盲狙，这就很“过分”鸟。不过在sql2000 sybase这些严格要求类型匹配的数据库来说，这样不能撼动“管理员登陆”的，因为执行时发生了语法错误，结果集为NULL。另外以前 ewebeditor注入漏洞来上传马也是这个union操作结果集来达到目的的经典案例。 编辑特别推荐: oracle认证考试费用 Oracle的入门心得 使用Oracle外部表的五个限制 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com