Xercms 前台会员注入漏洞

Xercms 是一套 php 加 mysql 的 cms。

直接上 code 吧

XerCMS\Modules\member\index.php lines 29

```
class XerCMS_MODULE_index extends member
{
        public function pay() {
              X::$G['pay'] = htmlchars(g('pay'));
             include(tpl('member/pay_index.htm'));
       }

        public function message() {
               X::$G['d'] = g('d');
               if(X::$G['d'] == 'view') {
                      $id = int1(g('id'));
                      $message = rs('message')->view($id);
                      include_once(tpl('member/message.htm'));
               } else if (X::$G['d'] == 'rely') {
                      $id = g('id');                    //传入 id 上面套了一个 g（）函数
                      $rely = rs('message')->rely($id);   //29 行在这里调用了 rely（）函数
               } else if (X::$G['d'] == 'send') {
                      if(isset($_POST['message'])) {
                             $message = p('message');

sendmessage((int)$message['uid'],htmlchars($message['title']),htmlchars($message['content']));
                             showtips('message_send_finish','index.php?m=member&a=message');
                      } else {
                             X::$G['send'] = (int)g('send');
                             include_once(tpl('member/message.htm'));
                      }
```

我们看看 g（）函数是什么，在 XerCMS\Utils\XerCMS_base.php lines 796

```
function g($key,$default = '') {
      return isset($_GET[$key]) ? $_GET[$key] : $default;   //GET 方式传入，没有任何过滤。
}
```

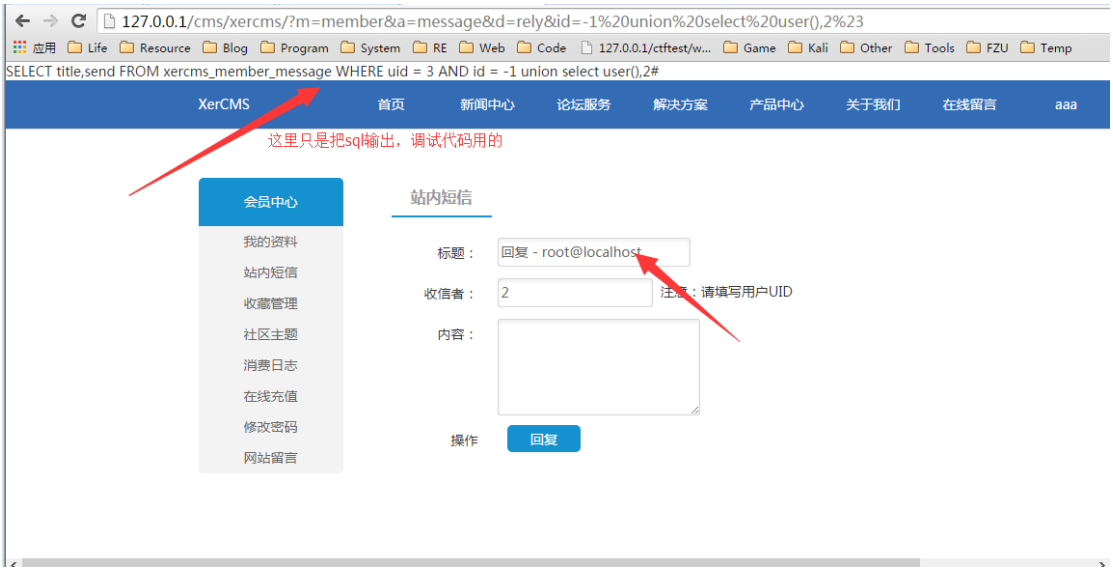
可以看出 id 是我们可以控制的。

接下来看看 rely()这个函数。在 XerCMS\Utils\tables\XerCMS_message.php lines 55

```
        function rely($id,$uid = 0) {
            $uid = empty($uid) ? X::$G['uid'] : $uid;
            return DB::result('SELECT title,send FROM xercms_member_message WHERE uid =
```

'.X::$G['uid'].' AND id = '.$id);
    }

综上所述，可以看出 id 是 get 方式传入，并且没有任何过滤直接带入查询。



前台注册一个会员，然后直接注入。（默认注册会员是开启的）

++

这个是最早申请 90sec 会员的　15 年的 cms ，那时候刚刚学习 php 审计。简单了一点，大牛勿喷