通达OA任意文件上传并利用文件包含导致远程代码执行漏洞分析

aoteman / 2020-03-26 09:40:00 / 浏览数 8012

前言

初次投稿，代码审计新手，分析过程有问题大佬们多多指点

关于这个漏洞，利用方式大致有两种，一种是包含日志文件，一种是绕过身份验证文件上传然后在文件包含。第一种利用方式没什么说的，第二种绕过身份验证和上传以后文件的路径有点意思，写篇文章记录一下。

文件上传

入口文件/ispirit/im/upload.php

```
$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";
}
```

这里主要需要个参数P，P存在不为空然后获取session，否则的话进入auth.php身份认证

```
$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);
}
```

这里是第20行到第32行，这里说明需要DEST_UID参数，不能为空，这里涉及到td_verify_ids，大致意思是这个参数需要是0-9开头的任意字符串。

```
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();
    }
}
```

这段意思是，如果DEST_UID是0的话，那UPLOAD_MODE值必须是2，要不然就报错

然后继续往下

```
if (1 <= count($_FILES)) {

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

    $ATTACHMENT_ID = substr($ATTACHMENTS["ID"], 0, -1);
    $ATTACHMENT_NAME = substr($ATTACHMENTS["NAME"], 0, -1);
}
else {
    $dataBack = array("status" => 0, "content" => "-ERR " . _("无文件上传"));
    echo json_encode(data2utf8($dataBack));
    exit();
}
```

如果有文件上传进入upload，否则报错无文件上传

跟进upload函数，在utility_file.php第1665行，里面实现了一个上传功能，结果返回一个数组ATTACHMENTS

里面$ATTACHMENTS["id"]值是从add_attach函数返回。

跟进add_attach函数在第1854行

```
function add_attach($SOURCE_FILE, $ATTACH_NAME, $MODULE, $YM, $ATTACH_SIGN, $ATTACH_ID)
{
    $ATTACH_PARA_ARRAY = TD::get_cache("SYS_ATTACH_PARA");
    $ATTACH_POS_ACTIVE = $ATTACH_PARA_ARRAY["SYS_ATTACH_POS_ACTIVE"];
    $ATTACH_PATH_ACTIVE = $ATTACH_PARA_ARRAY["SYS_ATTACH_PATH_ACTIVE"];

    if (!file_exists($SOURCE_FILE)) {
        return false;
    }

    if ($MODULE == "") {
        $MODULE = attach_sub_dir();
    }

    if ($YM == "") {
        $YM = date("ym");
    }

    $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;
    }

    $AID = mysql_insert_id();
    $ATTACH_ID_NEW = $AID . "@" . $YM . "_" . $ATTACH_ID;
    return $ATTACH_ID_NEW;
}
```

可以看到返回值$ATTACH_ID_NEW有三部分组成$AID，$YM，$ATTACH_ID

这里注意一下，$ATTACH_ID_NEW只有文件名和一部分路径。完整的路径是$PATH，这里可以看到$PATH先拼接$MODULE然后拼接$YM，可以往上追溯到$SYS_ATTACH_PATH_ACTIVE

utility_file.php第403行

定义了$SYS_ATTACH_PATH_ACTIVE值

```
$SYS_ATTACH_PATH_ACTIVE = MYOA_ATTACH_PATH2;
```

跟踪到td_config.php 第134行

```
define("MYOA_ATTACH_PATH2", $ATTACH_PATH2);
```

这里定义常量MYOA_ATTACH_PATH2，内容是 $ATTACH_PATH2

往上翻第3行到第15行

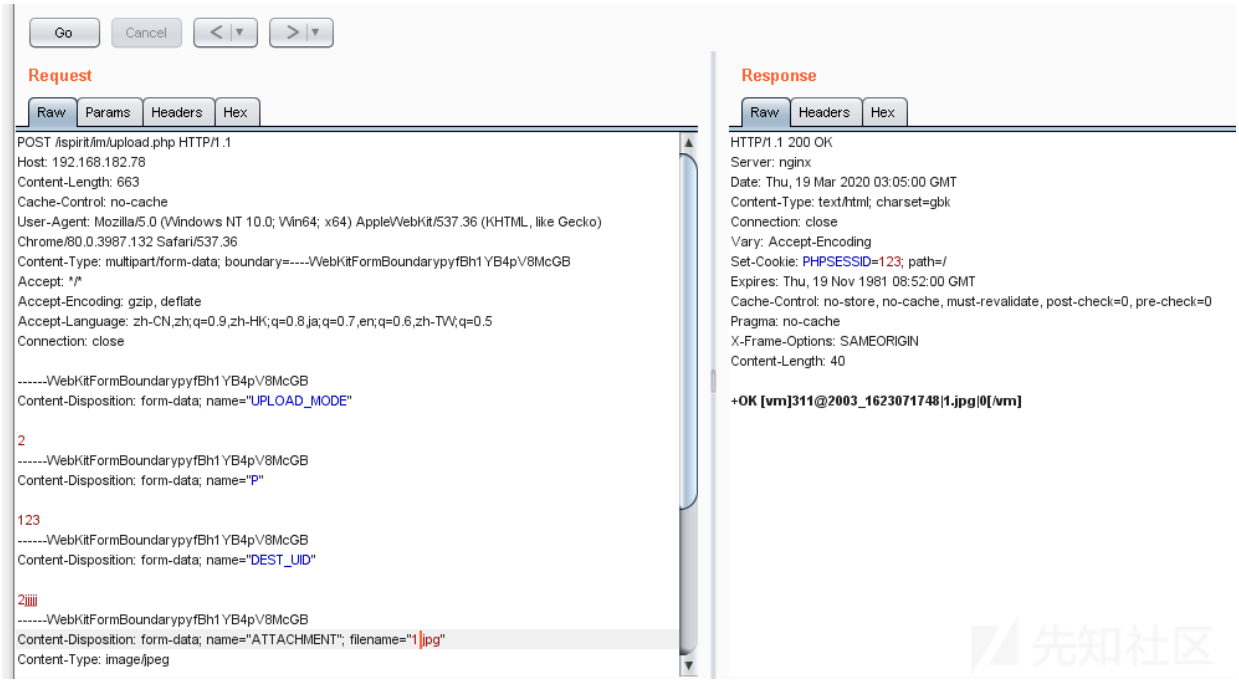
```
$ROOT_PATH = (isset($_SERVER["DOCUMENT_ROOT"]) ? $_SERVER["DOCUMENT_ROOT"] : "");

if ($ROOT_PATH == "") {
    $ROOT_PATH = str_replace("\\", "/", realpath(dirname(__FILE__) . "/../"));
}

if (substr($ROOT_PATH, -1) != "/") {
    $ROOT_PATH .= "/";
}
$ATTACH_PATH2 = realpath($ROOT_PATH . "../") . "/attach/";
```

这里跟到 `/inc/../../` 然后拼接 `/attach/`

然后UPLOAD_MODE值随便为1，2，3中的任意一个数字都可以返回文件名字和部分路径



文件包含漏洞

这部分比较简单

```
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/") !==
            include_once $url;
        }
    }

    exit();
}
```

$json参数接受一个json格式的值，然后转化为数组，当键值为url并且值不为空是include_once包含url

最后
感谢大佬分享的payload
附上大佬的GitHub https://github.com/jas502n/OA-tongda-RCE

关注 | 2　　点击收藏 | 0

上一篇： CVE-2020-2551: We...　　下一篇： 域渗透——基于资源的约束委派利用

0 条回复

动动手指，沙发就是你的了！