# 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

```php
<?php

function HandleError($message)
{
    echo "-ERR " . iconv(MYOA_CHARSET, "utf-8", $message);
    exit();
}

include_once ("inc/session.php");
if (!empty($_POST["PHPSESSID"]) && isset($_POST["PHPSESSID"])) {
    @session_id($_POST["PHPSESSID"]);
}

session_start();
ob_start();
include_once ("inc/utility_all.php");
include_once ("inc/utility_file.php");
include_once ("inc/utility_folder.php");
include_once ("inc/utility_sms1.php");
include_once ("inc/utility_sms2.php");
ob_end_clean();

while (list($key, $value) = each($_GET)) {
    $$key = $value;
}

while (list($key, $value) = each($_POST)) {
    $$key = $value;
}

if (!isset($_FILES["Filedata"]) || !is_uploaded_file($_FILES["Filedata"]["tmp_name"]) || ($_FILES["Filedata"]["error"] != 0)) {
    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

```php
while (list($key, $value) = each($_GET)) {
    $$key = $value;
}

while (list($key, $value) = each($_POST)) {
    $$key = $value;
}
```

Line：23-29 典型的变量覆盖

```php
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。

```php
if ($FILE_SORT == 2) {
    $query = "SELECT FOLDER_CAPACITY from USER_EXT where UID='" . $_SESSION["LOGIN_UID"] . "'";
    $cursor = exequery(TD::conn(), $query);

    if ($ROW = mysql_fetch_array($cursor)) {
        $FOLDER_CAPACITY = $ROW["FOLDER_CAPACITY"];
    }

    if ($FOLDER_CAPACITY != 0) {
        include_once ("function.func.php");
        $USER_ID = $_SESSION["LOGIN_USER_ID"];
        $query = "select SORT_ID from FILE_SORT where SORT_TYPE=4 and USER_ID='$USER_ID' and SORT_PARENT=0";
        $cursor = exequery(TD::conn(), $query);
        $SORT_SIZE = 0;

        while ($ROW = mysql_fetch_array($cursor)) {
            $SORT_ID_TMP = $ROW["SORT_ID"];
            $SORT_SIZE += tree_size($SORT_ID_TMP);
        }

        $SORT_SIZE += tree_size_root();

        if (($FOLDER_CAPACITY * 1024 * 1024) < $SORT_SIZE) {
            handleerror(_("您的个人文件柜已超过容量限制($FOLDER_CAPACITY MB)! "));
        }
    }
}
```

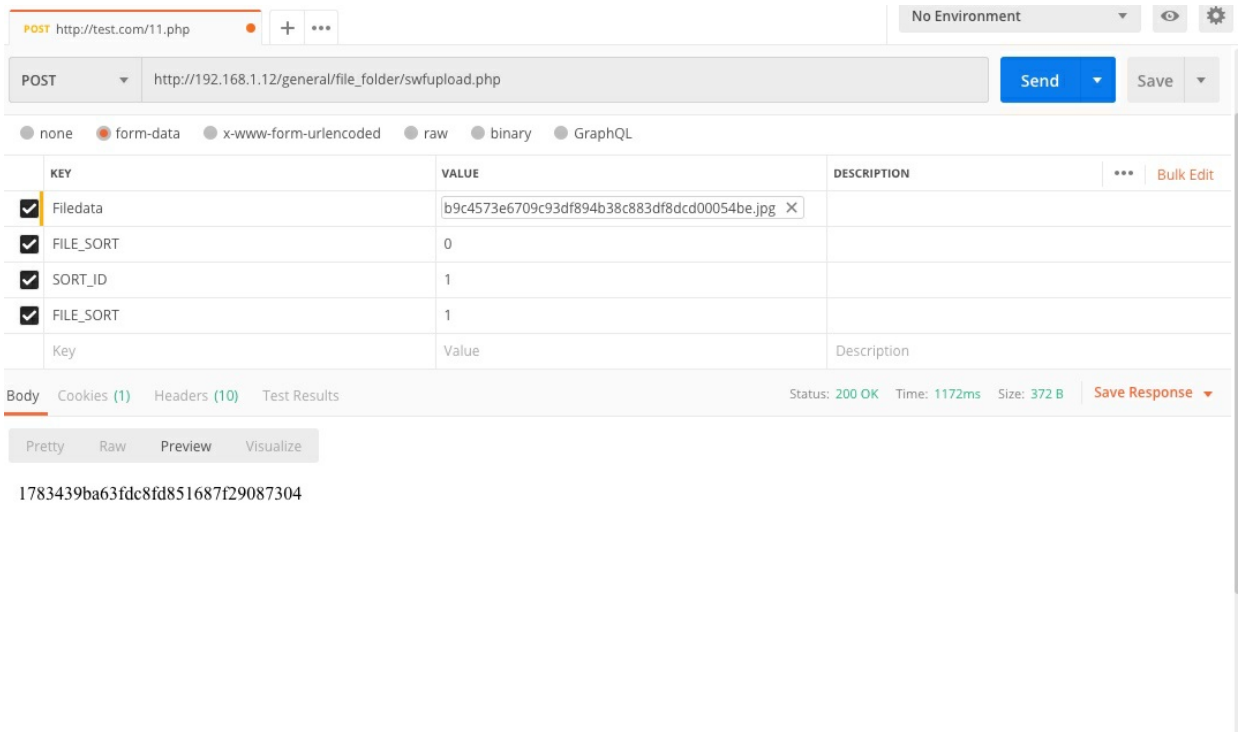
Line 35~61 需要传入参数 `FILE_SORT`，满足条件则会执行数据库查询当前用户的文件容量，这里看到了SQL语句中拼接了 `$_SESSION["LOGIN_UID"]` ,再结合上边的变量覆盖是不是可以导致注入呢？答案是不行的，因为在上文引用文件中引入了 `inc/common.inc.php`

```
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 $s_key => $s_value ) {
        $_COOKIE[$s_key] = strip_tags(securerequest($s_value));
        $$s_key = $_COOKIE[$s_key];
    }

    reset($_COOKIE);
}

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

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

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

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

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

    reset($_GET);
}
```

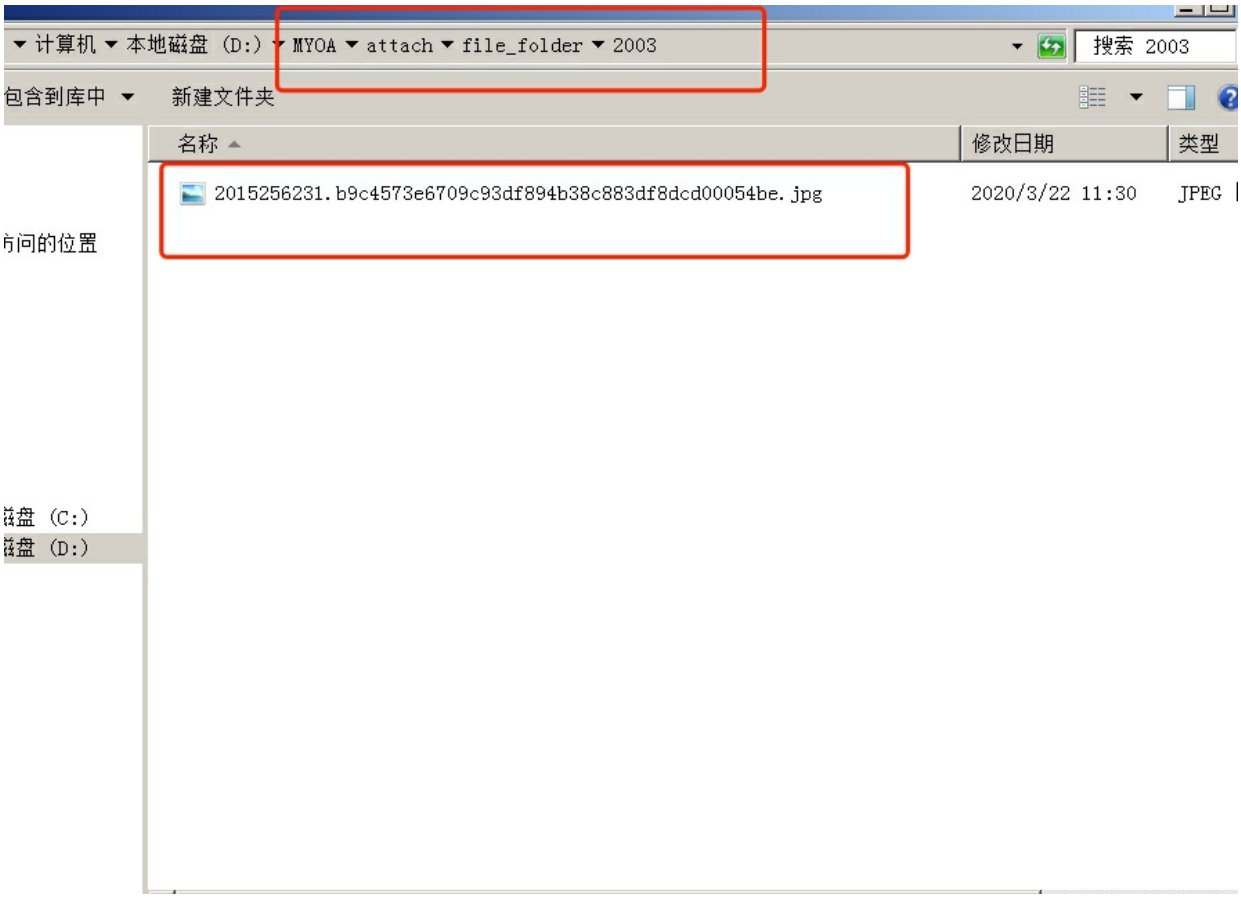
作用就是对传入进来的内容进行正则判断，如果存在`_COOKIE、_SESSION`等字符串则进行拦截，所以此处无法利用，继续向下看。


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 。

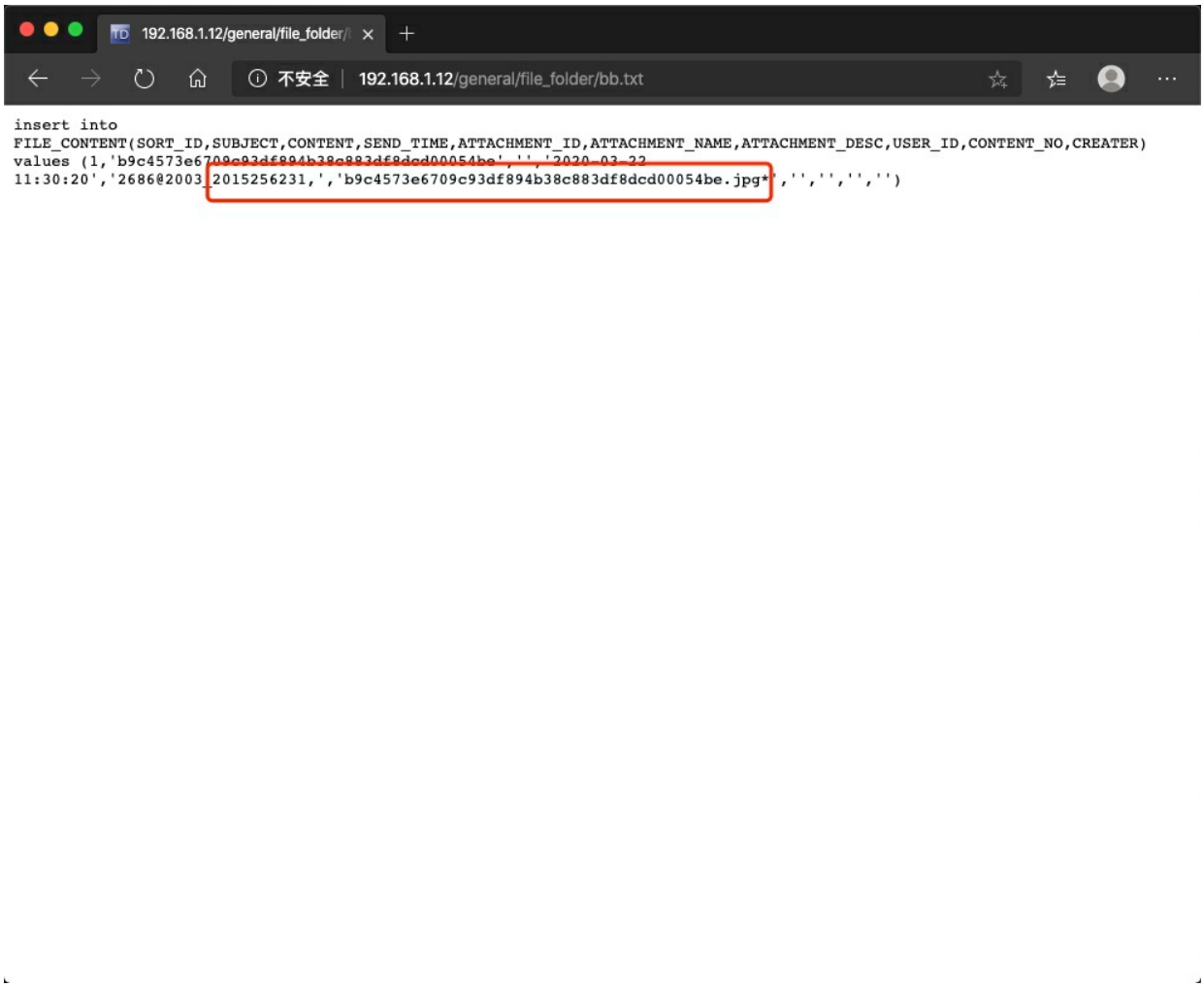
在流程的最后返回了一串md5加密的字符，那么上传文件的地址就需要从上文中的 aa.txt 和 bb.txt 来获得。
构造上传数据包：




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




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     }
```

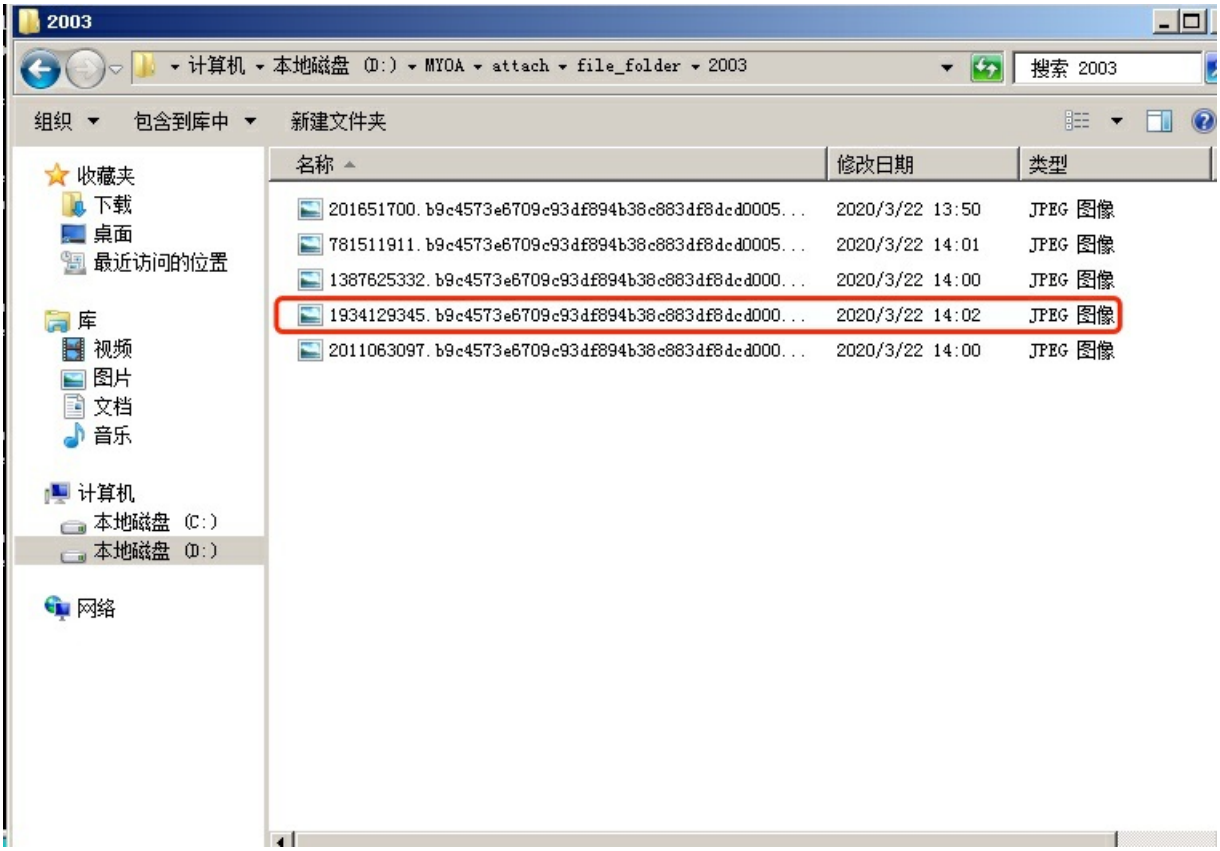
| KEY | VALUE | DESCRIPTION |
| --- | --- | --- |
| Filedata | b9c4573e6709c93df894b38c883df8dcd00054be.jpg | |
| FILE_SORT | 0 | |
| SORT_ID | 1+sleep()/ | |
| SMS_SELECT_REMIND | 1 | |
| SMS_SELECT_REMIND_TO_ID | 1 | |
| Key | Value | Description |

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

Pretty Raw Preview Visualize HTML

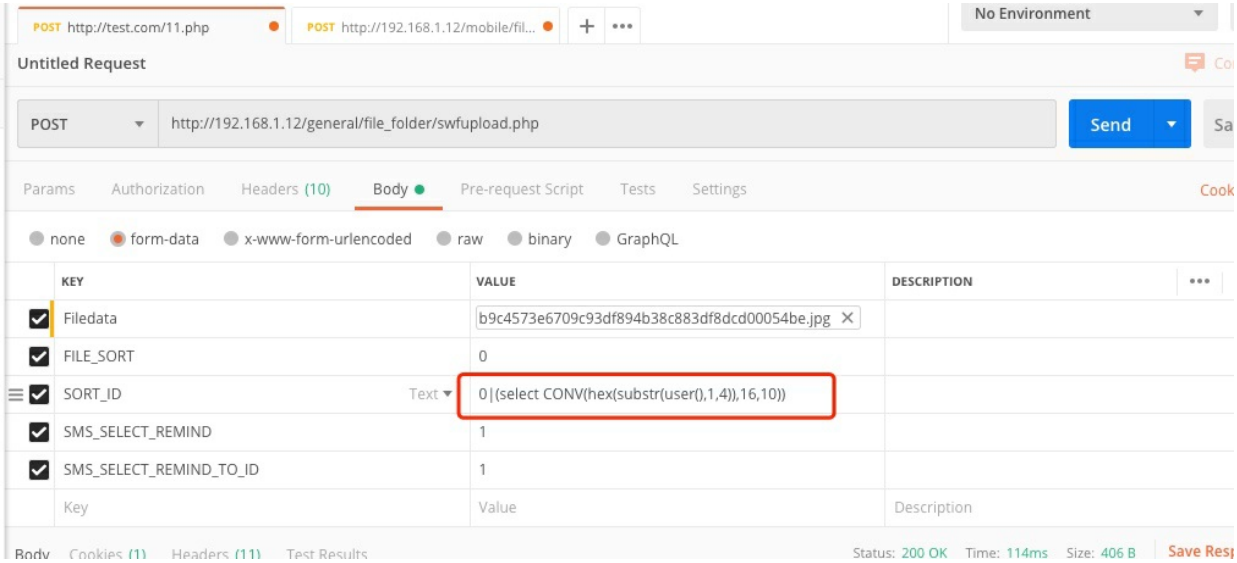
```
1  不安全的SQL语句: sleep<br />insert into FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,
       USER_ID,CONTENT_NO,CREATER) values (1+sleep()/,'b9c4573e6709c93df894b38c883df8dcd00054be1584856951','','2020-03-22 14:02:31',
       '266@2003_1934129345,','b9c4573e6709c93df894b38c883df8dcd00054be.jpg*','','','','')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

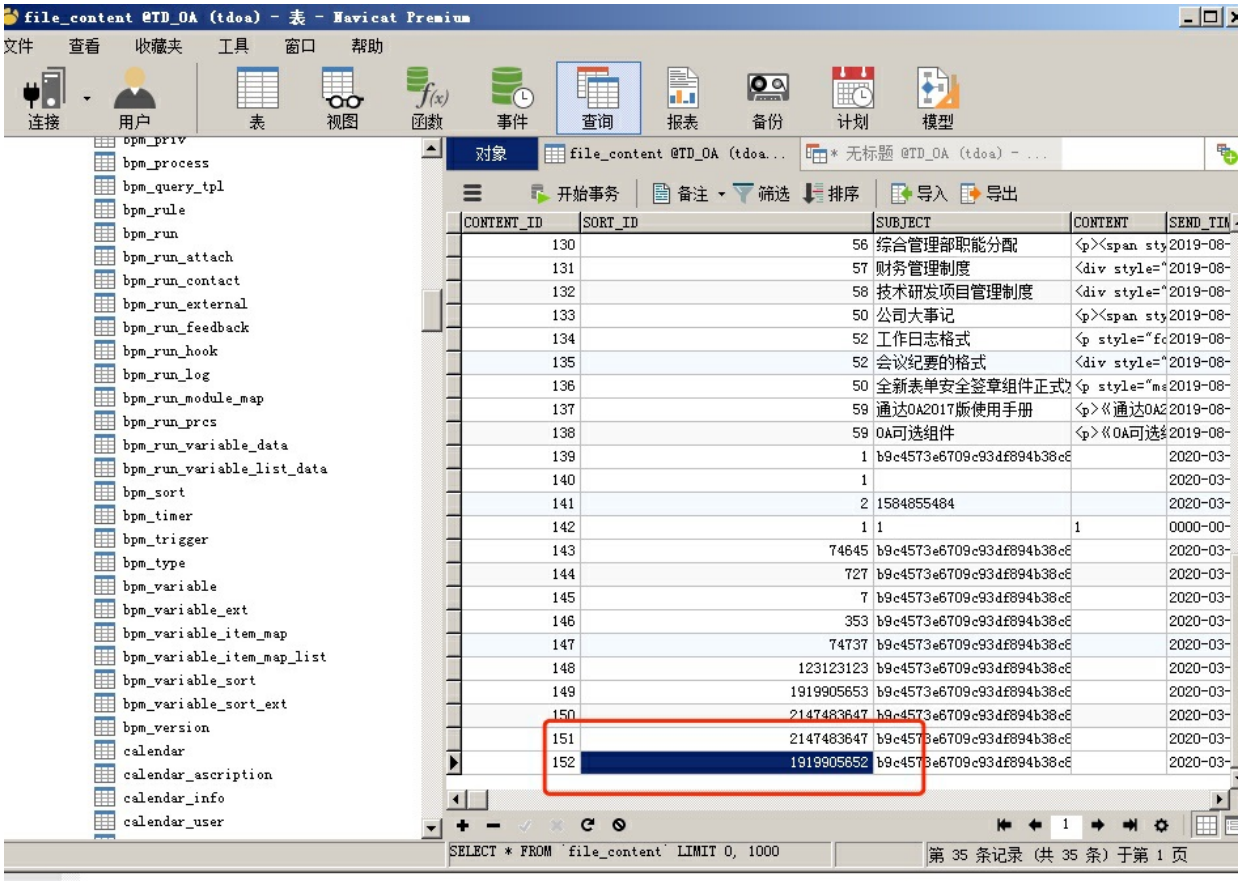
因为在执行sql语句之前文件已经上传成功，所以语句的错误并不妨碍文件上传。

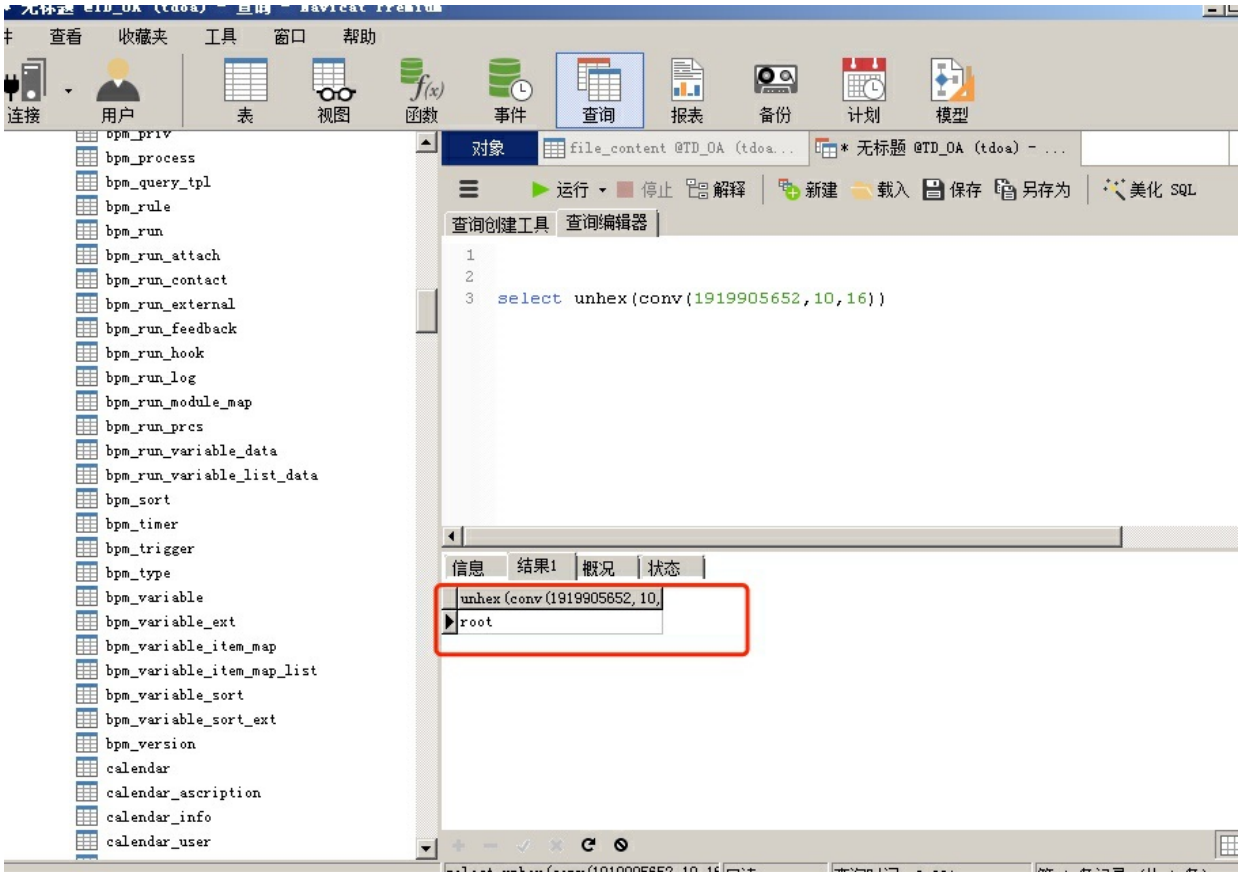


```
$query = "insert into
FILE_CONTENT(SORT_ID,SUBJECT,CONTENT,SEND_TIME,ATTACHMENT_ID,ATTACHMENT_NAME,ATTACHMENT_DESC,USER_ID,CONTE
values ($SORT_ID,'$SUBJECT','','$SEND_TIME','$ATTACHMENT_ID','$ATTACHMENT_NAME','$ATTACHMENT_DESC','','$CONTENT_NO','" .
$_SESSION["LOGIN_USER_ID"] . "')";
```

sort_id可控所以这里也是一个insert注入





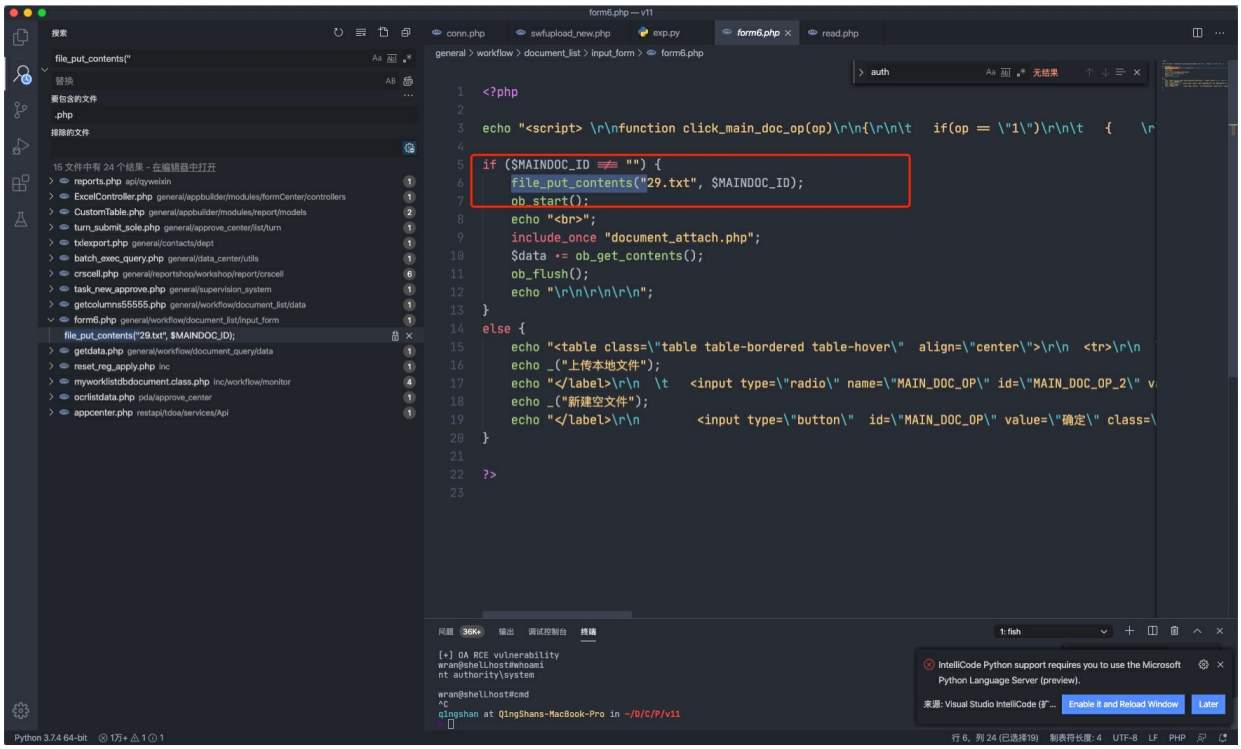

在 file_content 表中 sort_id 的是 int(11)，所以要使用字符截断控制长度，但是由于没有回显和过滤了一些函数，需要找到二次注入点或者找到一个可以显示 sort_id 的地方，由于还要写论文（毕业重要），时间问题就没有继续寻找。

## 失败的文件写入

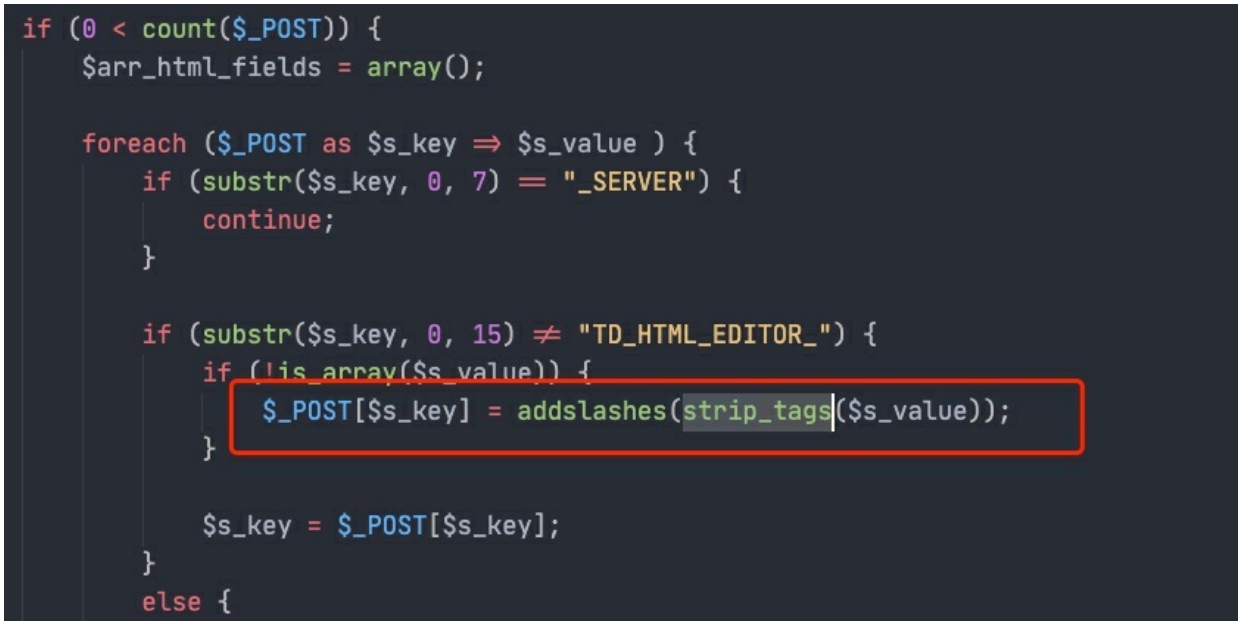
搜索 file_put_contents，文件 general/workflow/document_list/input_form/form6.php 没有校验权限，并将 $MAINDOC_ID 写入到29.txt

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



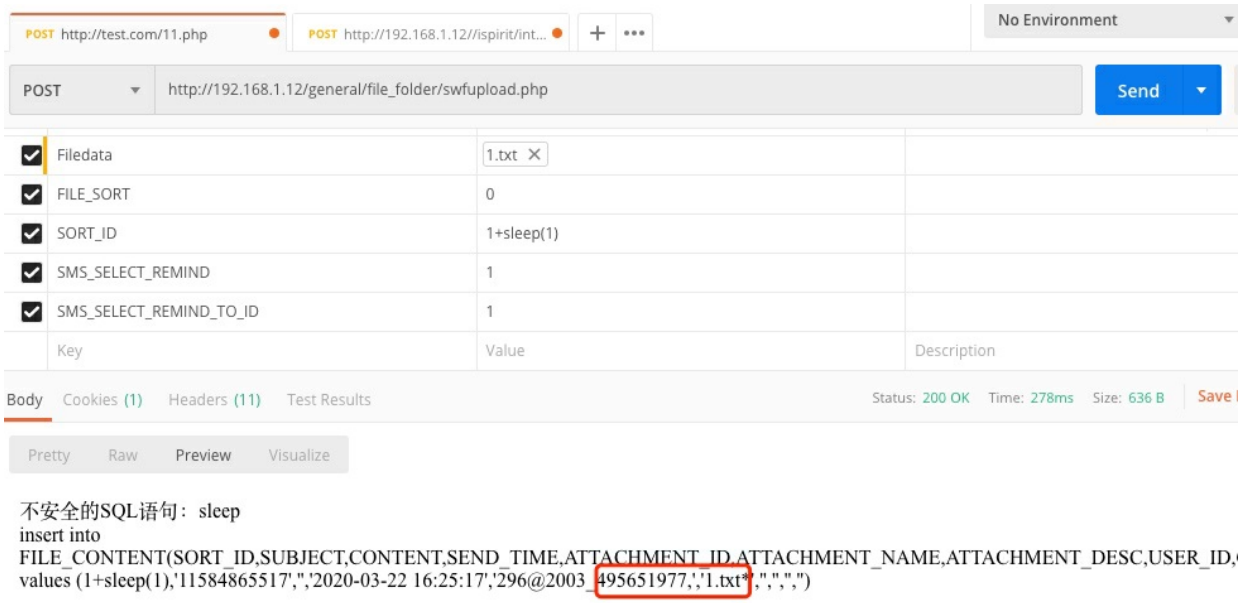

# 文件包含

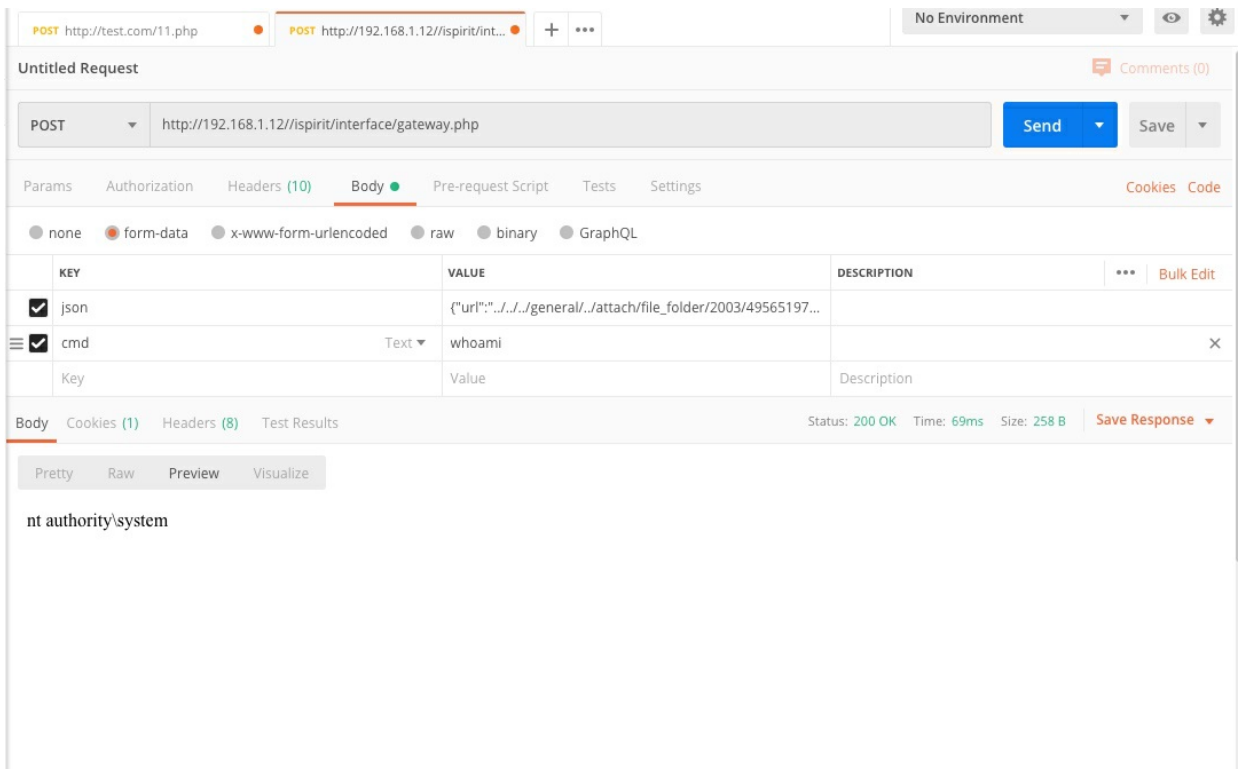
```php
<?php

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

?>


?>
```

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：




# 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。

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