**WordPress插件（Drag and Drop File Upload 1.3.3.2 & Contact Form 7）- Remote Code Execution漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

# 二、机理分析

## 1、Remote Code Execution漏洞

**影响版本：**Drag and Drop File Upload 1.3.3.2

**漏洞编号：**无

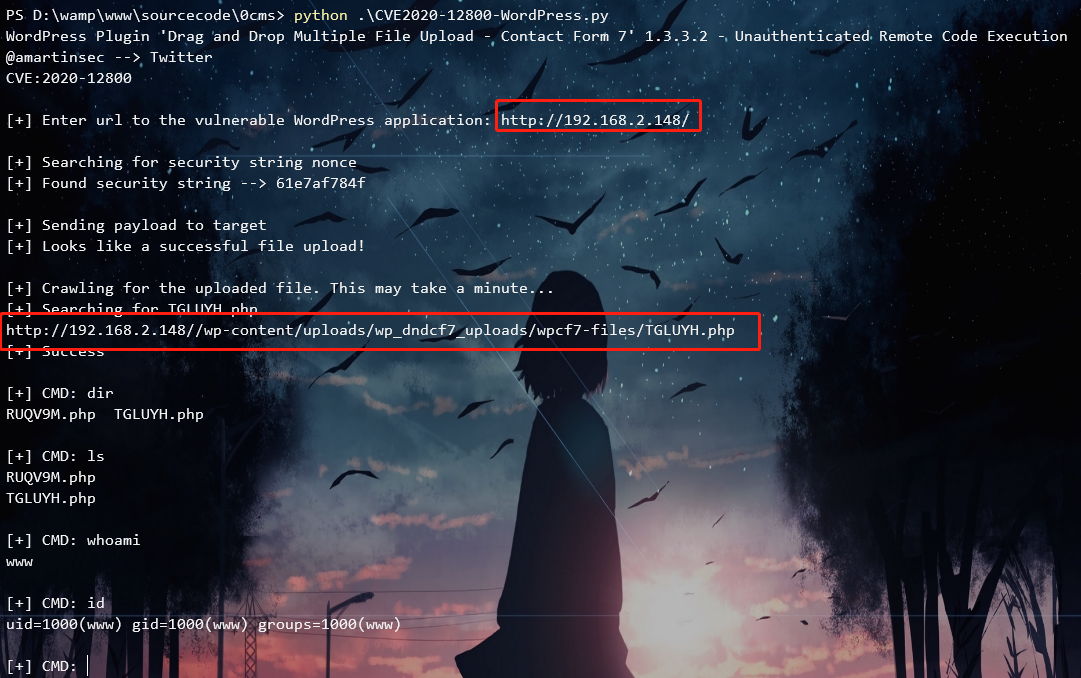
任何文件类型都可以添加到“supported\_type”参数中，这些上传的文件可以在wp-content/uploads/wp\_dndcf7\_uploads/访问，危险的文件类型（如php）在创建文本文件的末尾附加了“\_.txt”，可以通过在允许的文件类型结尾和文件名末尾添加“%”来绕过此问题。

例如“shell.php%”用于文件名

POC中的PHP payload可以很容易地修改以获得一个反向shell

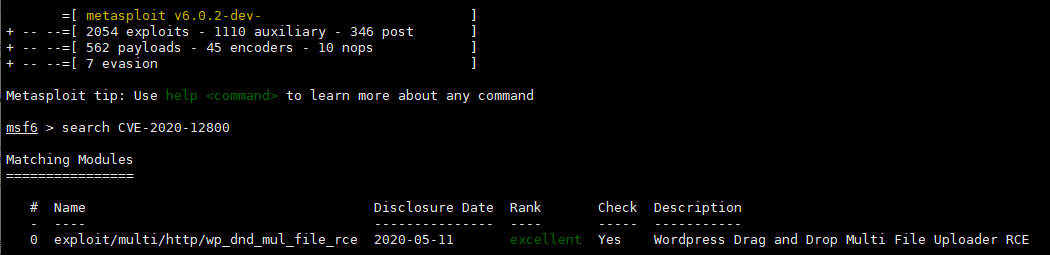
# 三、攻击路径

1. 使用修改后的poc来直接利用：



附上poc：

2. 使用msf来利用



exploit/multi/http/wp\_dnd\_mul\_file\_rce



# 四、防御方案

升级插件Drag and Drop File Upload版本