

【墨者学院writeup】WebShell文件上传漏洞分析溯源(第2题) 题目思路

原创

iqiqiya 于 2018-05-23 16:37:23 发布 1481 收藏 1

分类专栏: [我的CTF之路](#) ----- [墨者学院CTF](#) [我的CTF进阶之路](#) 文章标签: [【墨者学院writeup】WebShell文件上传漏洞分析溯源\(第2题\)题目思路](#) [WebShell文件上传漏洞分析](#)

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/xiangshangbashaonian/article/details/80422077>

版权



[我的CTF之路](#) 同时被 3 个专栏收录

92 篇文章 5 订阅

订阅专栏



[-----墨者学院CTF](#)

3 篇文章 0 订阅

订阅专栏

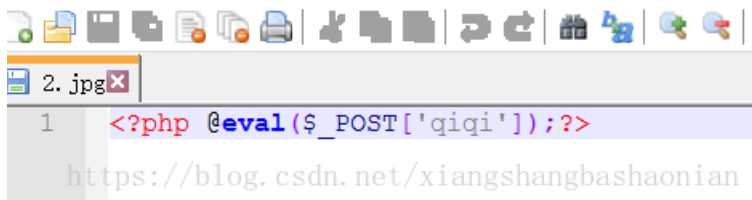
[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

这道题直接改后缀名先上传 burpsuit截包 再改回.php即可成功上传webshell

The screenshot shows a CTF challenge interface. At the top, there are buttons for '提交KEY' (Submit Key) and '放弃' (Give Up). Below that, the IP address is 219.153.49.228, port 47535, protocol http. The challenge title is '靶场介绍 解题思路 防御方案'. A progress bar shows the steps: 登录, 点击启动靶场环境, 访问靶场, 解题找到KEY, 提交KEY, 发表解题思路, 完成. The '背景介绍' (Background) section describes a security engineer finding a file upload vulnerability on a server. The '实训目标' (Practical Objectives) list six tasks: 1.掌握浏览器对JavaScript的禁用方法; 2.掌握表单数据通过POST提交数据时,对数据的修改方法; 3.了解WebShell是什么及其作用; 4.了解JavaScript基本语法; 5.了解JavaScript对文件扩展名的验证; 6.了解PHP程序的WebShell脚本的执行原理; The '解题方向' (Solution Direction) section suggests bypassing the file upload restriction using WebShell to retrieve source code. A URL is visible at the bottom: <https://blog.csdn.net/xiangshangbashaonian>



前提记得设置浏览器设置代理127.0.0.1:8080 打开burpsuit



将.jpg改成.php 点击forward即可上传成功

然后菜刀链接即可



得到KEY

