

攻防世界-MISC:wireshark-1

原创

LY613313 于 2021-12-15 21:14:37 发布 2996 收藏

分类专栏: [攻防世界](#) 文章标签: [安全](#)

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/m0_56161093/article/details/121961879

版权



[攻防世界 专栏收录该内容](#)

21 篇文章 1 订阅

订阅专栏

这是攻防世界高手进阶区的第五题, 题目如下:

wireshark-1

最佳Writeup由 [系统战队](#) • admin 提供

难度系数: ★ 1.0

题目来源: [广西首届网络安全选拔赛](#)

题目描述: 黑客通过wireshark抓到管理员登录网站的一段流量包 (管理员的密码即是答案)。 flag提交形式为flag{XXXX}

题目场景: 暂无

题目附件: [附件1](#)

CSDN @LY613313

点击下载附件一, 得到一个压缩包, 解压后得到一个流量包, 用wireshark打开, 分组字节流搜索字符串flag

No.	Time	Source	Destination	Protocol	Length	Info
						[Time since previous frame in this TCP stream: 0.000342000 seconds]
						TCP payload (809 bytes)
				Hypertext Transfer Protocol		
				HTML Form URL Encoded: application/x-www-form-urlencoded		
				Form item: "email" = "flag"		
				Key: email		
				Value: flag		
				Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"		
				Form item: "captcha" = "BYUG"		
11a0	6f 67 69 6e 0d 0a 43 6f	6f 6b 69 65 3a 20 5f 5f		ogin: Cookie:		
11b0	63 66 64 75 69 64 3d 64	34 37 33 64 62 34 37 39		cfduid=d 473db479		

password的值即是flag, 所以这道题的flag如下:

flag{ffb7567a1d4f4abdfdb54e022f8facd}

感觉进阶的题比新手的题要简单得多啊□□□

以上就是我对这道题的解法。因本人菜鸡一只，如果有什么不对的地方，实属正常。还请各位大佬予以指正，谢谢！