# i春秋 第二届春秋欢乐赛 Web-Hello World

原创

xnudhi 于 2020-01-20 17:14:51 发布 977 收藏 1

分类专栏： ctf



本文链接：https://blog.csdn.net/qq_34106499/article/details/104054255






## 访问题目

http://106.75.72.168:9999/

## 解题过程

审查源码，抓包查看请求头及响应头，今发现flag.xmas.js，提示flag可能存在这个文件中，然而访问这个文件出现404。尝试访问flag.js出现flag.js源码，由于源码太长没看完就放弃了。。。

扫描后台目录没有收获，看来flag只能从flag.js找线索了。把flag.js放控制台运行无收获，就不会了。

查询资料后发现，这个题目考的是git泄露漏洞。使用大佬写的工具Git_Extract，可直接获取文件

【upload】

在beyond compare中将flag.js与flag.js.04bb09进行对比，如下：

【upload2】

可以看出开头即为`flag{`，挑出所有访问量不一样的地方，即可获得flag。

## 补充git泄露

漏洞原因：在运行git init 初始化代码库时，会在当前目录下产生一个.git的隐藏文件，用来记录代码的变更记录等。在发布代码得时候，没有吧.git这个目录删除，导致可以使用这个文件来恢复源代码。

git文件夹分析

文件夹：
hooks:存放一些sheel的地方
info：存放仓库的信息
**object**：存放所有git对象的地方
**refs**：存放提交hash的地方
config：github的配置信息
文件：
description：仓库的描述信息，主要给gitweb等git托管系统使用，无需关心
**HEAD**：映射到ref引用，能够找到下一次 commit的前一次哈希值

未完待续。。。

## 参考

ctf/web源码泄露及利用办法【总结中】
git源码泄露漏洞总结：这个总结的很全面