ctf 信息隐藏 html,ctf_web常见套路(一)

转载

阿瑜诶 于 2021-06-03 20:33:02 发布 732 收藏
文章标签： ctf信息隐藏 html

“感谢打赏”

8种机械键盘轴体对比

本人程序员，要买一个写代码的键盘，请问红轴和茶轴怎么选？

CTF_web出题常见套路(一)基础套路

1.查看源码

标志：

不用标志，每个网页都可能隐藏信息。

重要信息：

1.各种敏感词汇:

password,username,form,flag,key,tip等

2.包含的内容

都是重要提示信息

3.其他php，txt文件

index.txt,search_key.php等

4.隐藏的form表单

往往隐藏的表单可以获取变量名，方便post或get

2.修改ip头

标志：

题干中提到ip

常见ip头：1

2

3

4

5

6

7

8

9

10X-Forwarded-For: 127.0.0.1

Contact: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Real-IP: 127.0.0.1

X-Client-IP: 127.0.0.1

Referer: 127.0.0.1

From: 127.0.0.1

X-Wap-Profile: 127.0.0.1

True-Client-IP: 127.0.0.1

Client-IP: 127.0.0.1

后面的127.0.0.1根据题意修改。

实现方法：

burpsuite抓包改包，添加ip头.

特别：

可能让你ping ip,直接在网址栏Ping ip以及输入windows命令

3.修改UA(User-Agent)头

标志：

题干中提及浏览器

实现方法：

burpsuite抓包修改UA头，将浏览器改为题目所需

4.添加Referer

标志：

题干中提及网址来源于哪里

实现方法：

burpsuite抓包添加或修改Referer为来源

5.添加语言项Accept-language

标志：

题干中提及语言

实现方法：

burpsuite抓包添加或修改语言Accept-language: zh-CN,en 等，根据题目要求。

6.直接burpsuite直接发包

标志：

实现方法：

Burpsuite直接抓包后repeater->go

7.查看网络项中的Host头

标志：

每个页面都看一看

实现方法：

F12->网络->原始头

8.保存页面，修改html代码(maxlength等)

标志：

提交一个数满足要求

实现方法：

保存页面，修改html代码，再用浏览器打开

9.文件备份泄露，猜测存在的目录

标志：

题目未提示任何文件

常见文件备份格式：

index.php.txt

……..(待补充)

可以用脚本跑

10.文件包含伪协议查看源码

标志：

无法直接看到源码

实现：1?file=php://filter/read=convert.base64-encode/resource=需要查看源码的文件名.php

11.xss脚本

题干中提及XSS,具体操作查看另一篇文章

https://jinlanzhijiao.github.io/2018/05/15/xss%E7%BB%95%E8%BF%87%E5%A7%BF%E5%8A%BF/

12.正则绕过

13.hash长度扩展攻击

标志：准备了一个密文和一些数据构造成一个字符串里，并且使用了MD5之类的哈希函数生成了一个哈希值(也就是所谓的signature/签名)

让攻击者可以提交数据以及哈希值，虽然攻击者不知道密文

服务器把提交的数据跟密文构造成字符串，并经过哈希后判断是否等同于提交上来的哈希值

实现：

1.burpsuite抓包，得到length,verify

假设1$key 是密文，长度46，已知的是guest，签名是78cfc57d983b4a17e55828c001a3e781，我们需要加上的数据是admin

2.使用kali里的hashpump执行如下命令：1

2

3

4

5

6

7cd hashpump

//得到# hashpump

//继续依次输入：

Input Signature: 78cfc57d983b4a17e55828c001a3e781(原来的verify)

Input Data: guest(已知的数据)

Input Key Length: 46(抓取到的length)

Input Data to Add: admin(加上的数据)

得到新的签名，以及要post的值1

25f585093a7fe86971766c3d25c43d0eb

guestx80x00x00x00x00x98x01x00x00x00x00x00x00admin

在burppsuite里，把新的签名赋给verify，第二个是要post 的值，把x 改成%，提交

14.过滤字符串大小写或构造双层绕过

标志：

输入php得不到返回，可能是过滤了php。

绕过：

1.使用PhP等大小写可能绕过，具体看源码中如何过滤

2.构造pphphp，过滤了一层绕过后，拼接成php达到目的。

15.php反序列化漏洞

16.写python脚本

17.查看robots.txt文件

标志：

题干提到robots或者网络爬虫

解法：

查看robots.txt文件或者用御剑扫敏感目录

看禁止索引的有哪些文件，查看这些文件。