XCTF---web

原创

空の城 于 2020-10-27 14:41:46 发布 124 收藏
文章标签： unctf web 网络安全 js

本文链接：https://blog.csdn.net/qq_43779787/article/details/109310705

1. view_source

题目描述：X老师让小宁同学查看一个网页的源代码，但小宁同学发现鼠标右键好像不管用了。
打开页面后右键查看不了源代码，从题目中可以知道小宁想要看源代码，所以按F12查看发现flag

1. robots

题目描述：X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。
根据题目提示，找到网站目录下的robots.txt

直接访问即可获得flag

1. backup

题目描述：X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！
如果网站存在备份文件，在地址栏最末加上/index.php~或/index.php.bak，即可得到备份文件

下载下来查看源代码即可

1. cookie

题目描述：X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’
首先在浏览器中找到cookie信息

访问cookie.php根据提示用bp抓包发现http的请求头中的flag

1. disabled_button

题目描述：X老师今天上课讲了前端知识，然后给了大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？
这不是so easy直接审查flag 元素

在控制台中修改按钮的标签去掉disable即可

1. weak_auth

题目描述：小宁写了一个登陆验证页面，随手就设了一个密码。

遇到这样的题目怎么办，上图说的很清楚了

有手就行，直接手撕admin/123456

1. simple_php

题目描述：小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。
=== 会同时比较字符串的值和类型

== 会先将字符串换成相同类型，再作比较，属于弱类型比较

比较简单的绕过

.is_numeric() 函数会判断如果是数字和数字字符串则返回 TRUE，否则返回 FALSE,且php中弱类型比较时，会使('1234a' == 1234)为真，所以当输入a=a&b=1235a，可得到flag2，如图所示。

1. get_post

题目描述：X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？
知识补充：两种HTTP请求方法：GET和POST在客户机和服务器之间进行请求-响应时，两种最常被用到的方法是：GET和POST。{

GET-从指定的资源请求数据。

POST-向指定的资源提交要被处理的数据

}

直接传递参数即可

1. xff_referer

题目描述：X老师告诉小宁其实xff和referer是可以伪造的。
不多比比直接抓包改请求头X-Forwarded-For: 123.123.123.123

一看事还挺多，还需要Referer: https://www.google.com

1. webshell

题目描述：小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。
用菜刀连接，这个小宁比较无脑

1. command_execution

题目描述：小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的，你知道为什么吗。
掌握有关命令执行的知识windows或linux下:

command1 && command2 先执行command1，如果为真，再执行command2

command1 | command2 只执行command2

command1 & command2 先执行command2后执行command1

command1 || command2 先执行command1，如果为假，再执行command2命令执行漏洞（| || & && 称为管道符）

构造127.0.0.1 && find / -name "flag.txt"查找flag的位置

直接查看flag即可

1. simple_js

题目描述：小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx})
本题目参考https://blog.csdn.net/qq_41617034/article/details/91490695
这大佬讲的很好

个人博客空の城.