ctf web5 练习_CTF-攻防世界-WEB新手练习区 Writeup（12题入门题）

原创

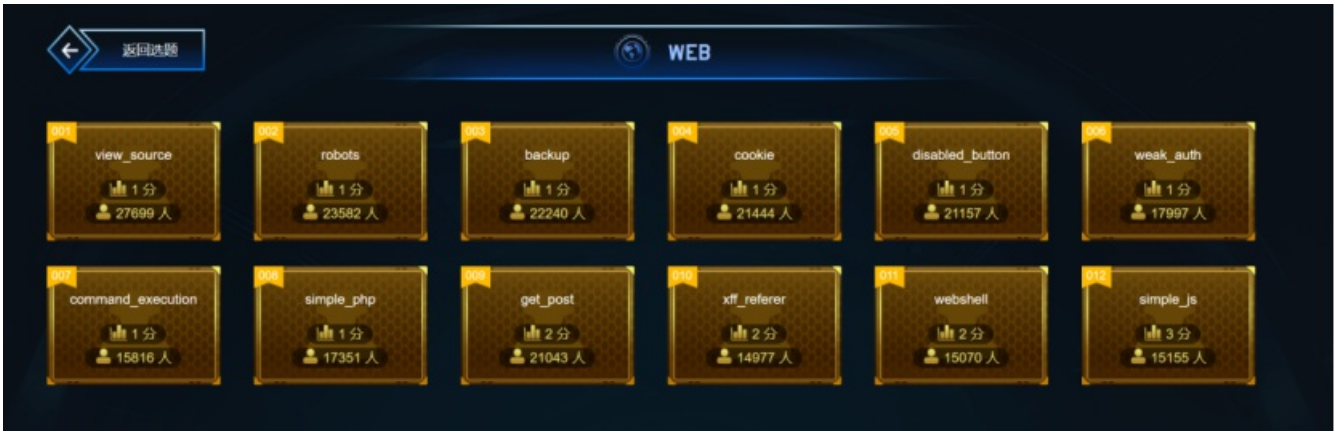
三盒草莓 于 2021-01-15 08:17:47 发布 2462 收藏 4
文章标签： ctf web5 练习

本文链接：https://blog.csdn.net/weixin_33603656/article/details/112994567

注：作者是CTF初学者，边学习边记录，如有错误或疏漏请批评指正，也请各位大佬多多包涵。

攻防世界-WEB新手练习区 12题入门题 Writeup

(注意：攻防世界WEB题每次生成场景后，有时flag会改变，因此flag不同不要在意，主要是学习解题思路和方法)

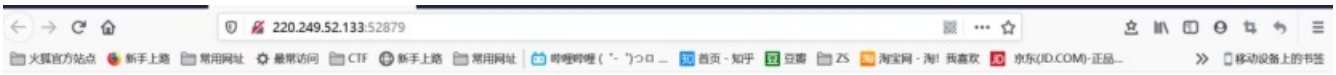


0X01view_source

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。

题目提示查看源码，鼠标右键不管用，用F12打开控制台

发现源码里有flag



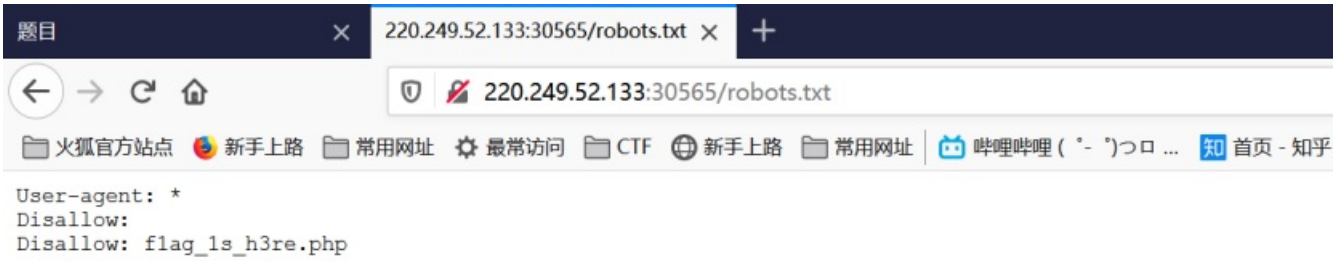
cyberpeace{d8e1850dd09cba974a8ad6de6eecbc1d}

0x02robots

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。

根据提示(也可用御剑后台扫描得到)，输入/robots.txt

发现提示跳转f1ag_1s_h3re.php



2.打开f1ag_1s_h3re.php，发现flag

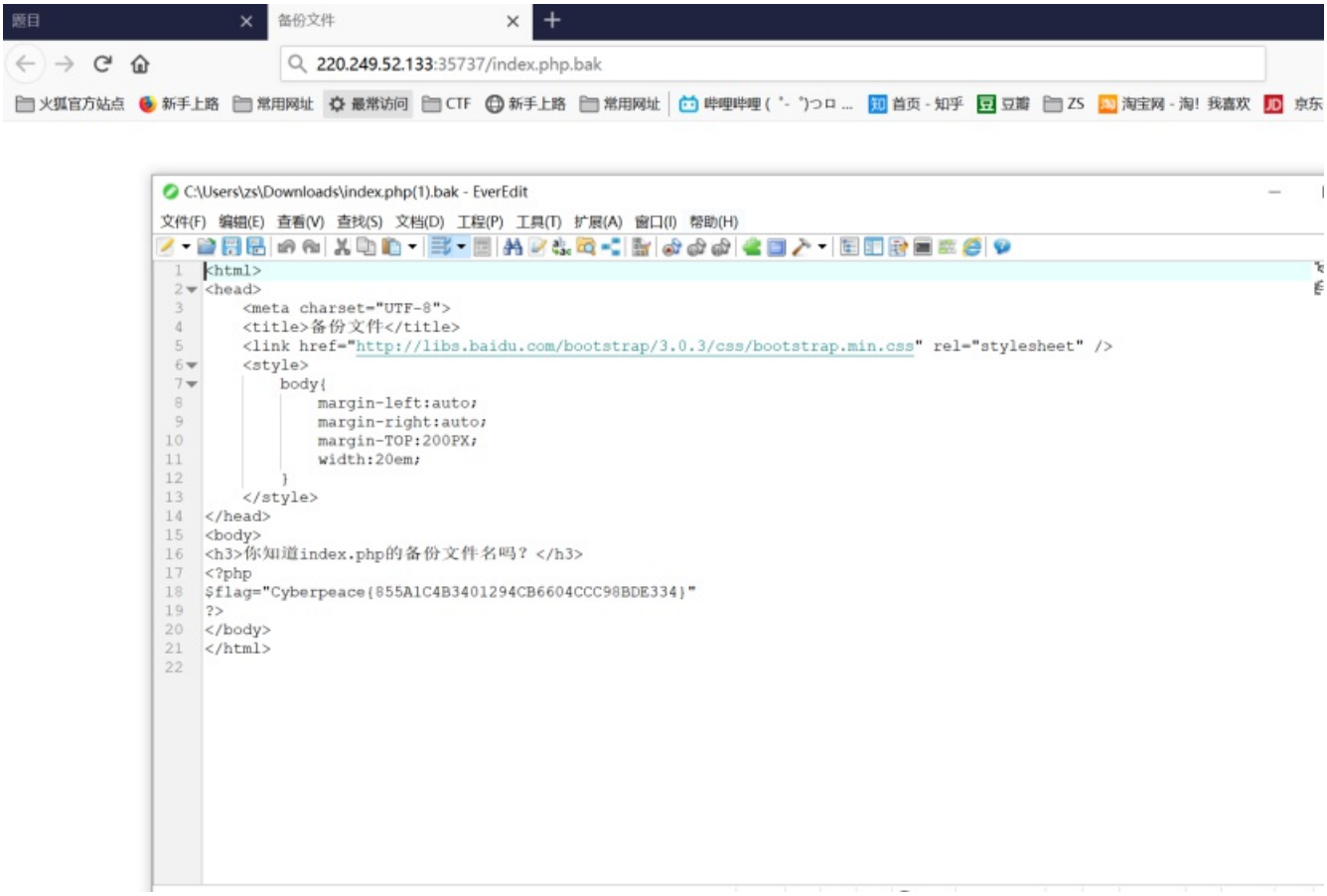
cyberpeace{c50a53cfa6c67eeeb1cc277eb928352c}

0x03backup

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！

1.根据提示你知道index.php的备份文件名吗？

输入/index.php.bak



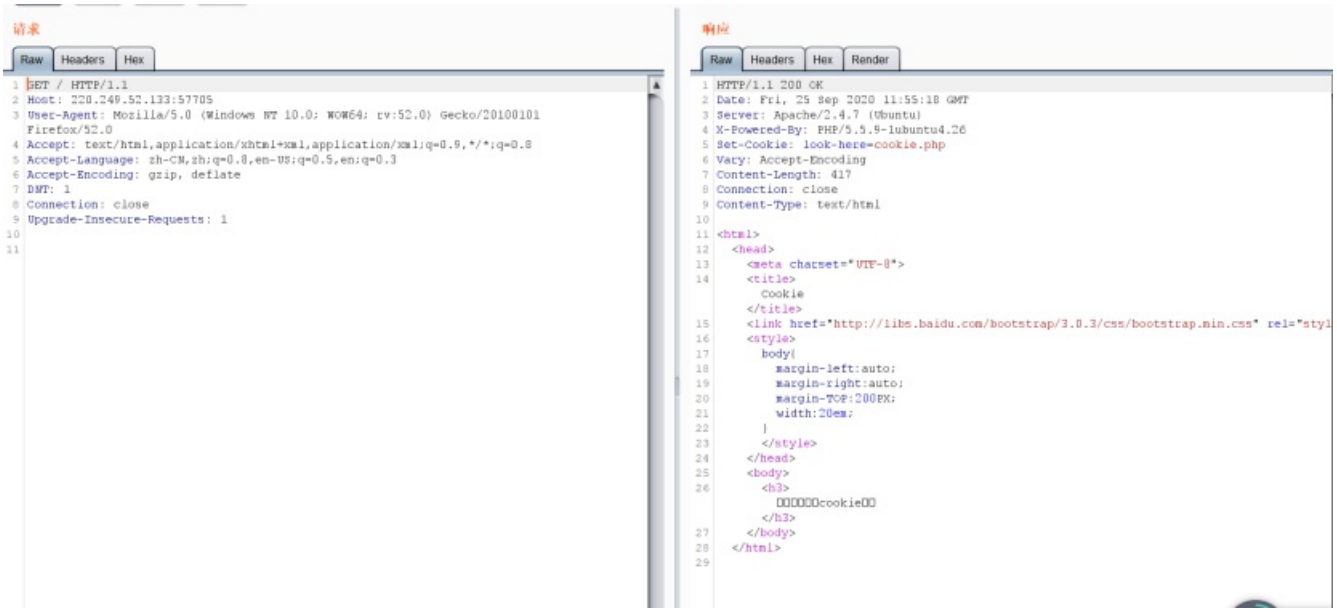
2.下载文件，打开发现flag

Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

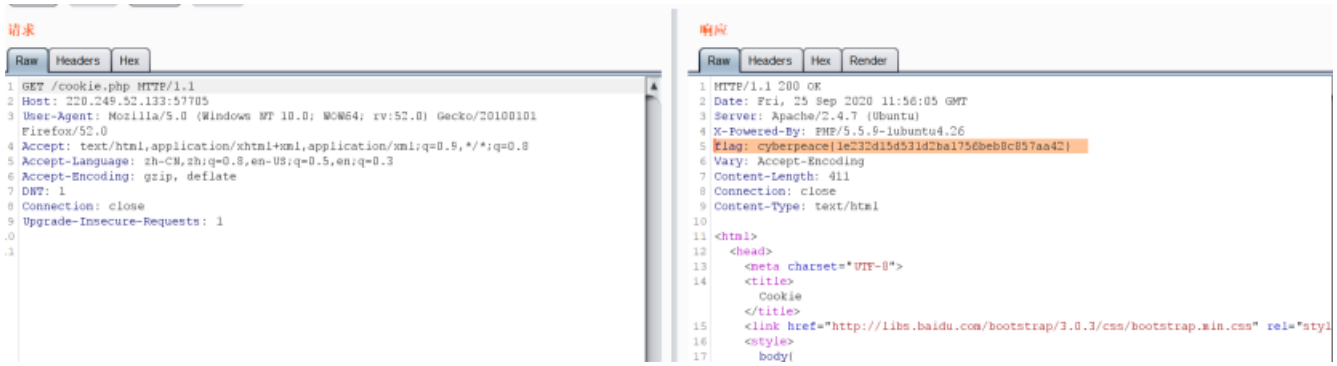
0x04cookie

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？

1.用BP抓包，发现cook中有cookie.php



2.用bp打开，看响应包，发现flag

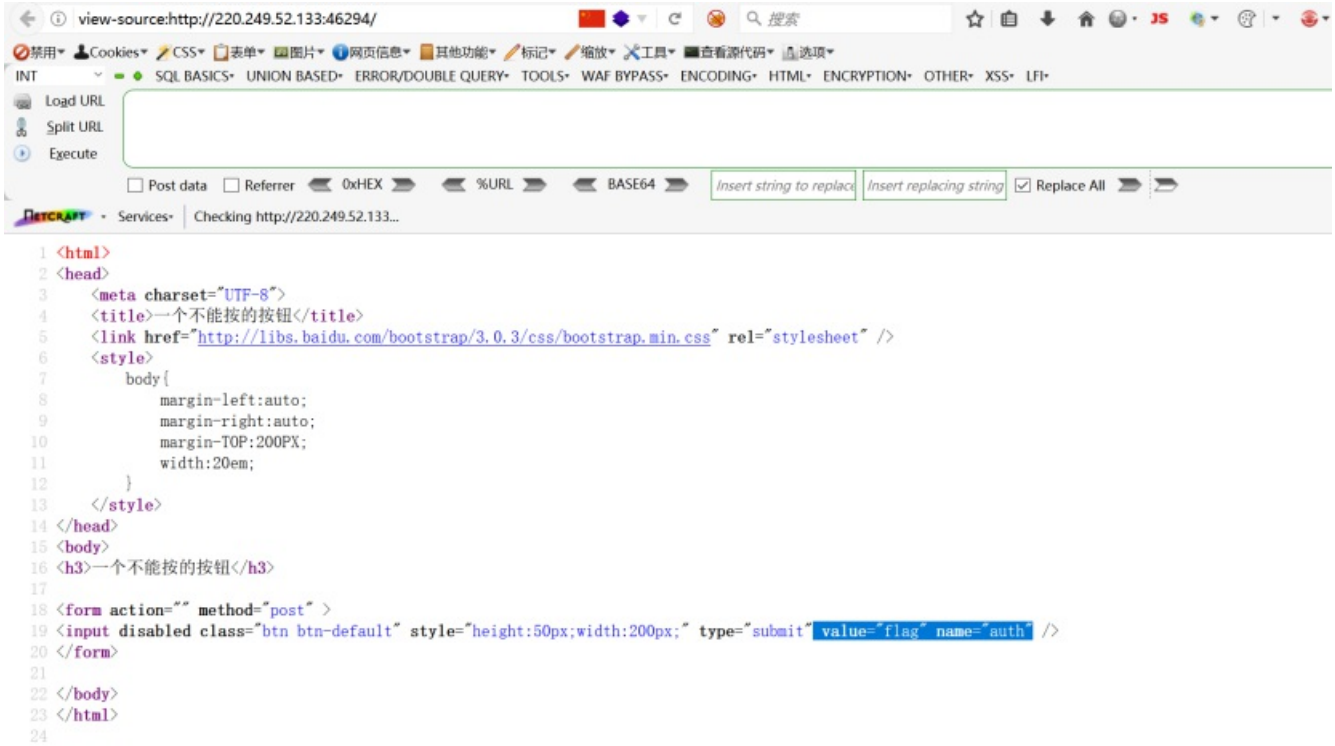


cyberpeace{1e232d15d531d2ba1756beb8c857aa42}

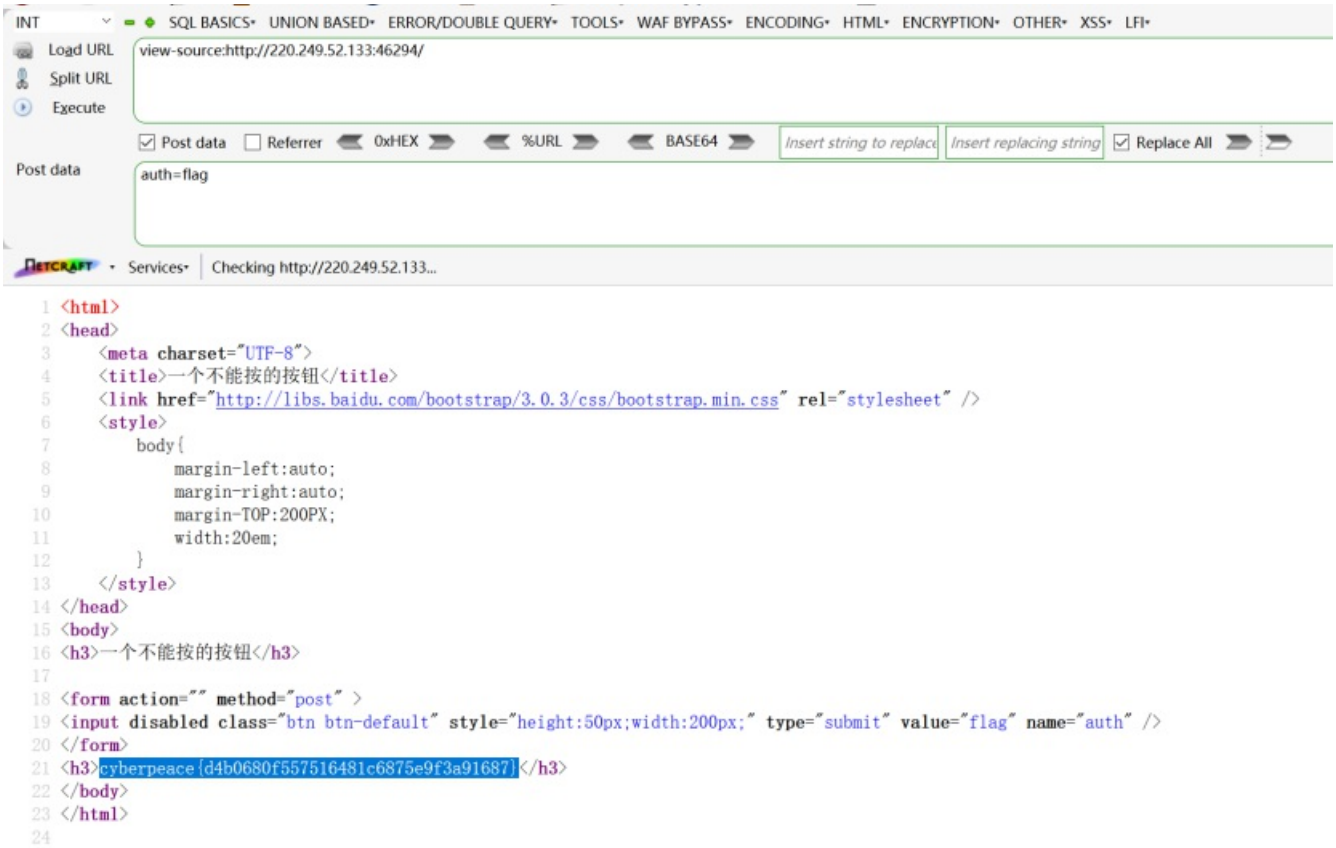
0x05disabled_button

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？

1.打开网页，发现无法按下，查看源码进行分析



2.根据源码用post提交auth=flag，得到flag

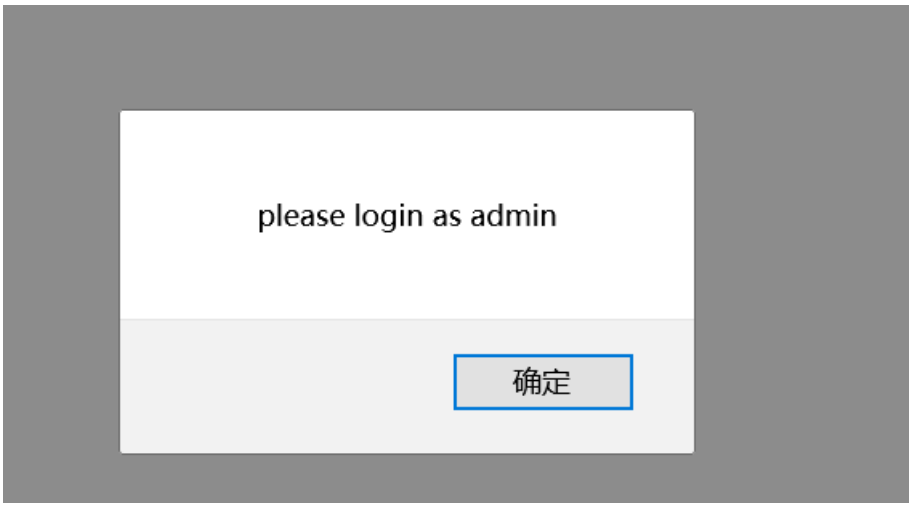


cyberpeace{d4b0680f557516481c6875e9f3a91687}

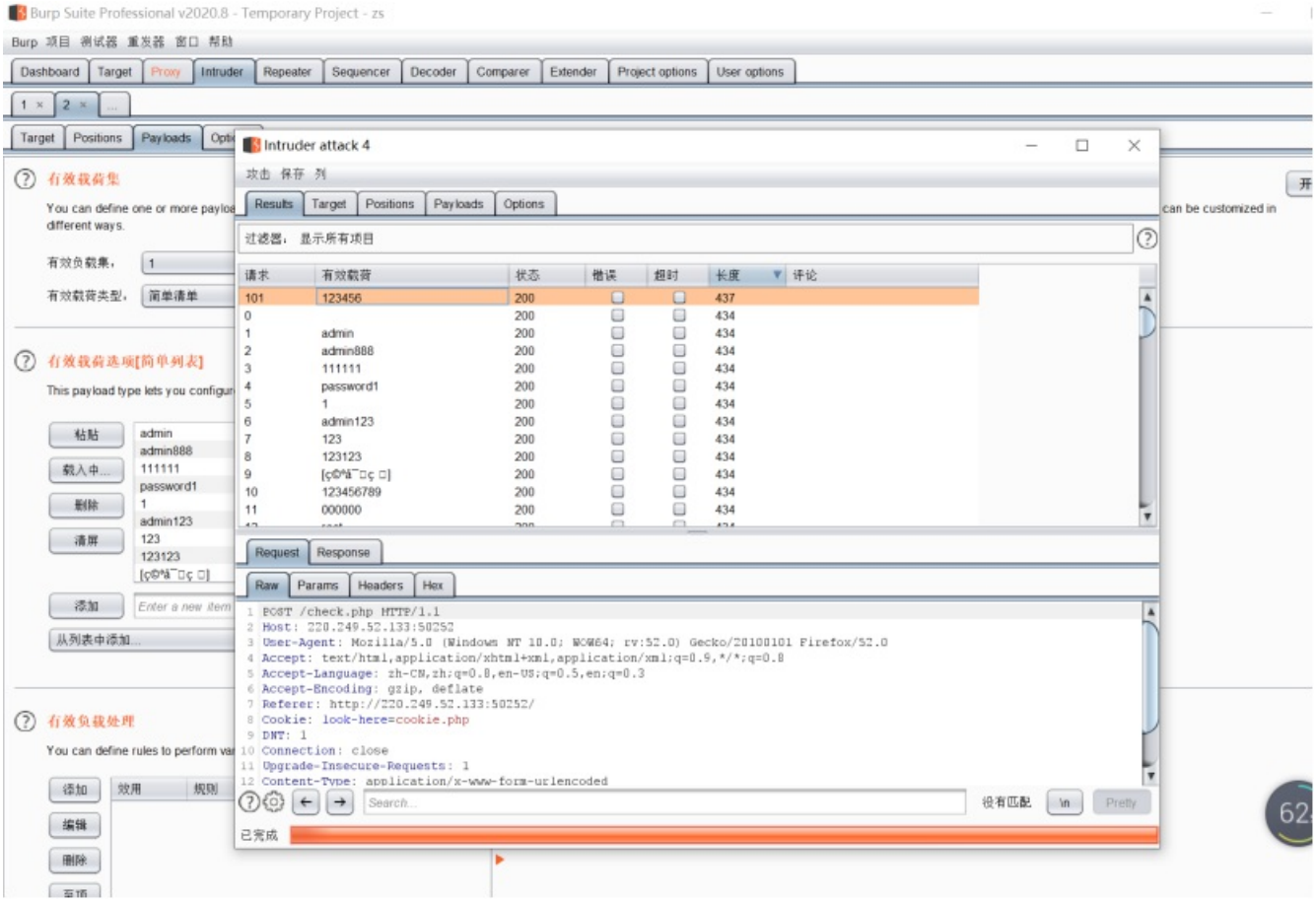
0x06weak_auth

小宁写了一个登陆验证页面，随手就设了一个密码。

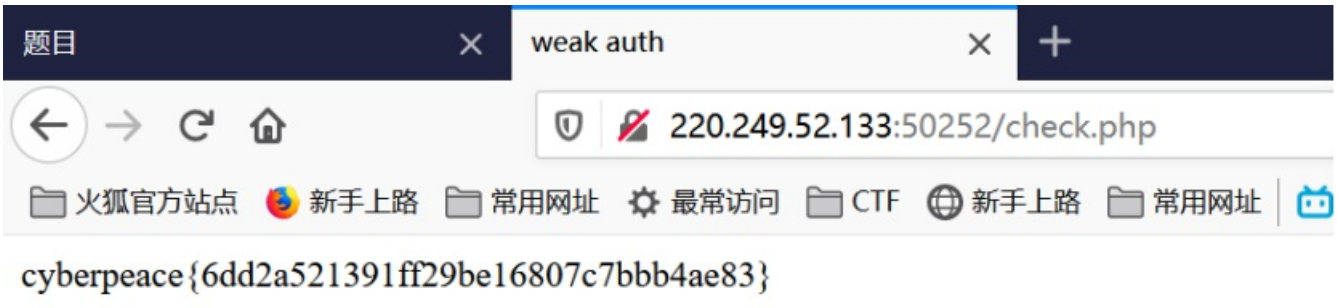
1.先测试用户名，提示用户名为admin



2.用bp暴破密码，密码为123456



3.登录得到flag

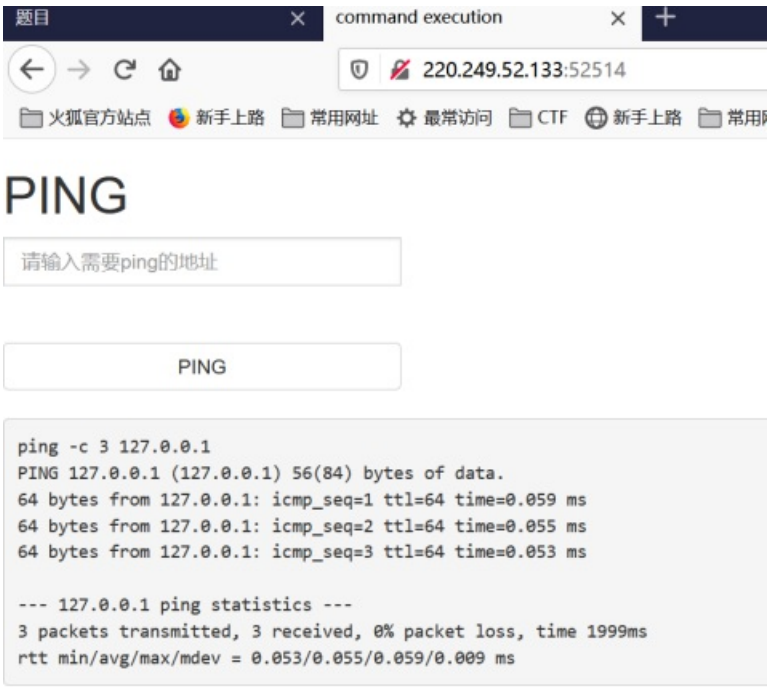


cyberpeace{6dd2a521391ff29be16807c7bbb4ae83}

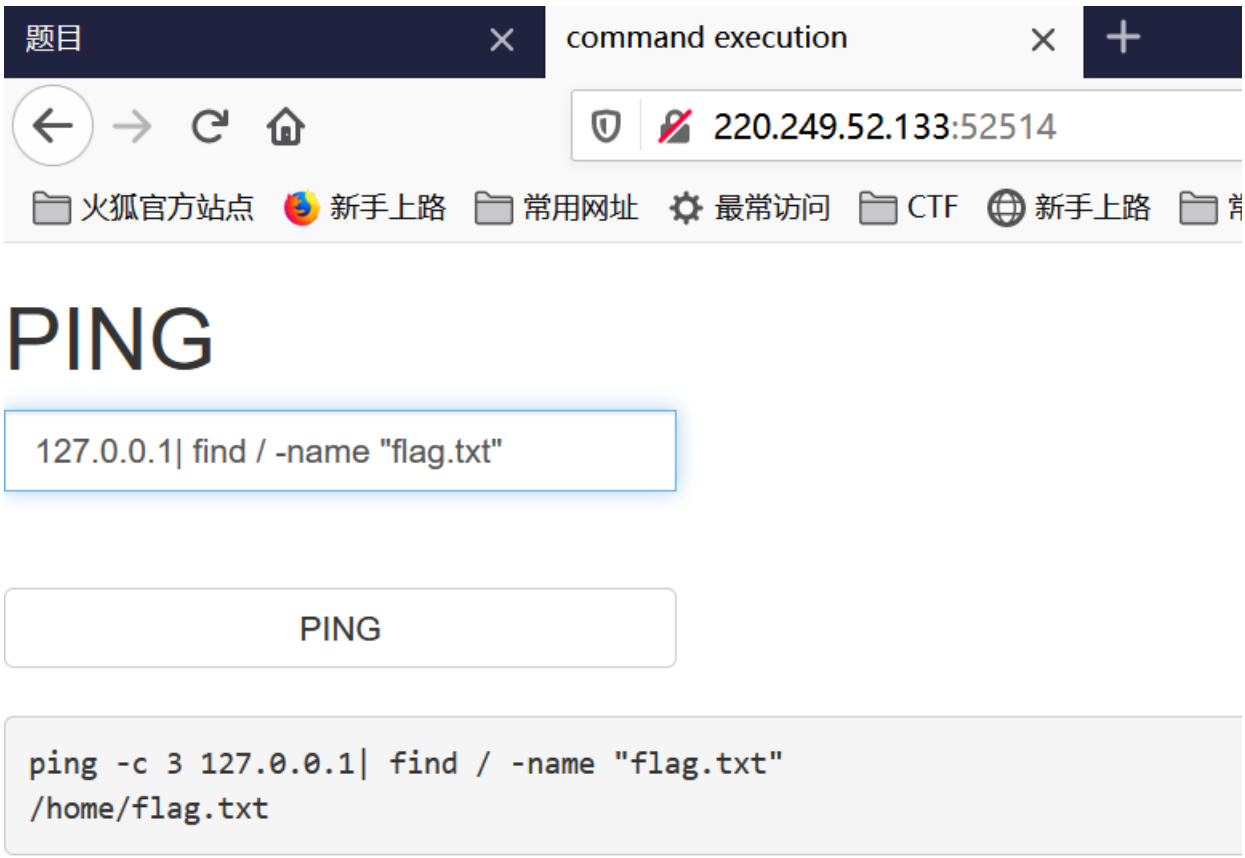
0x07command_execution

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。

1.可以ping127.0.0.1，测试常用命令

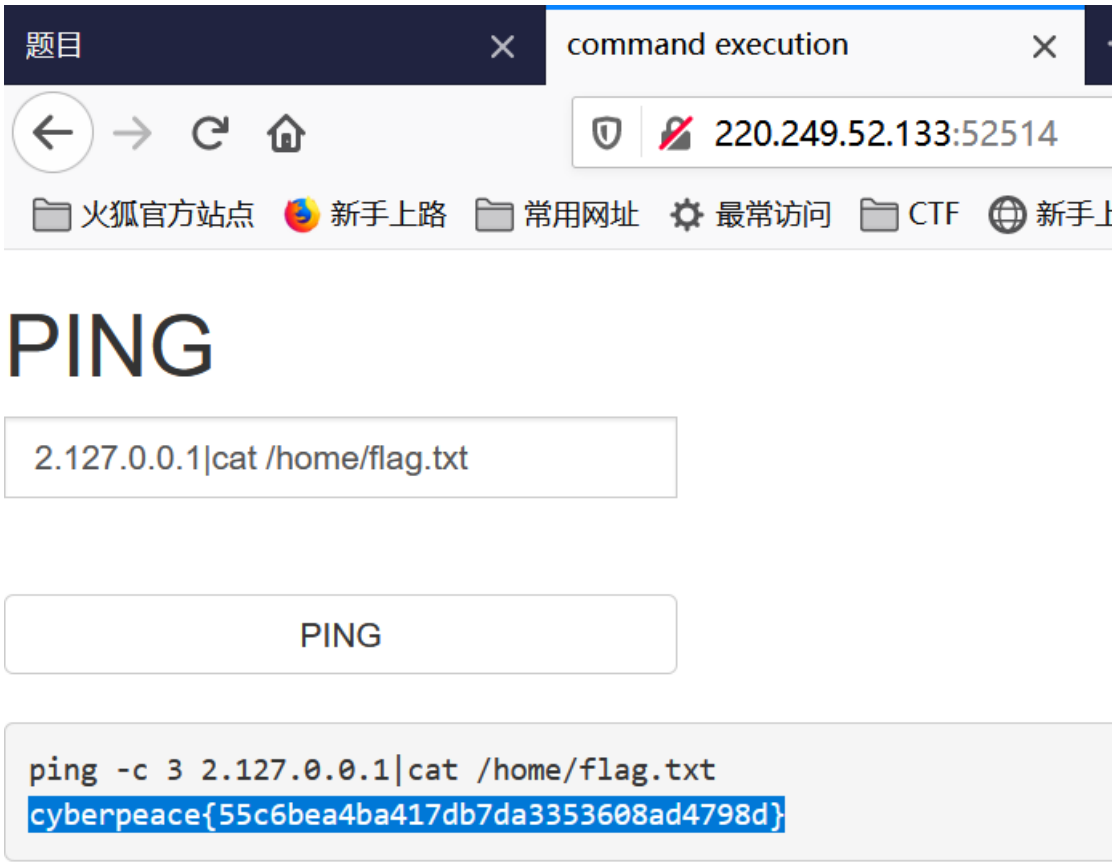


构造127.0.0.1| find / -name "flag*"



提示有 /home/flag.txt

2.构造127.0.0.1|cat /home/flag.txt

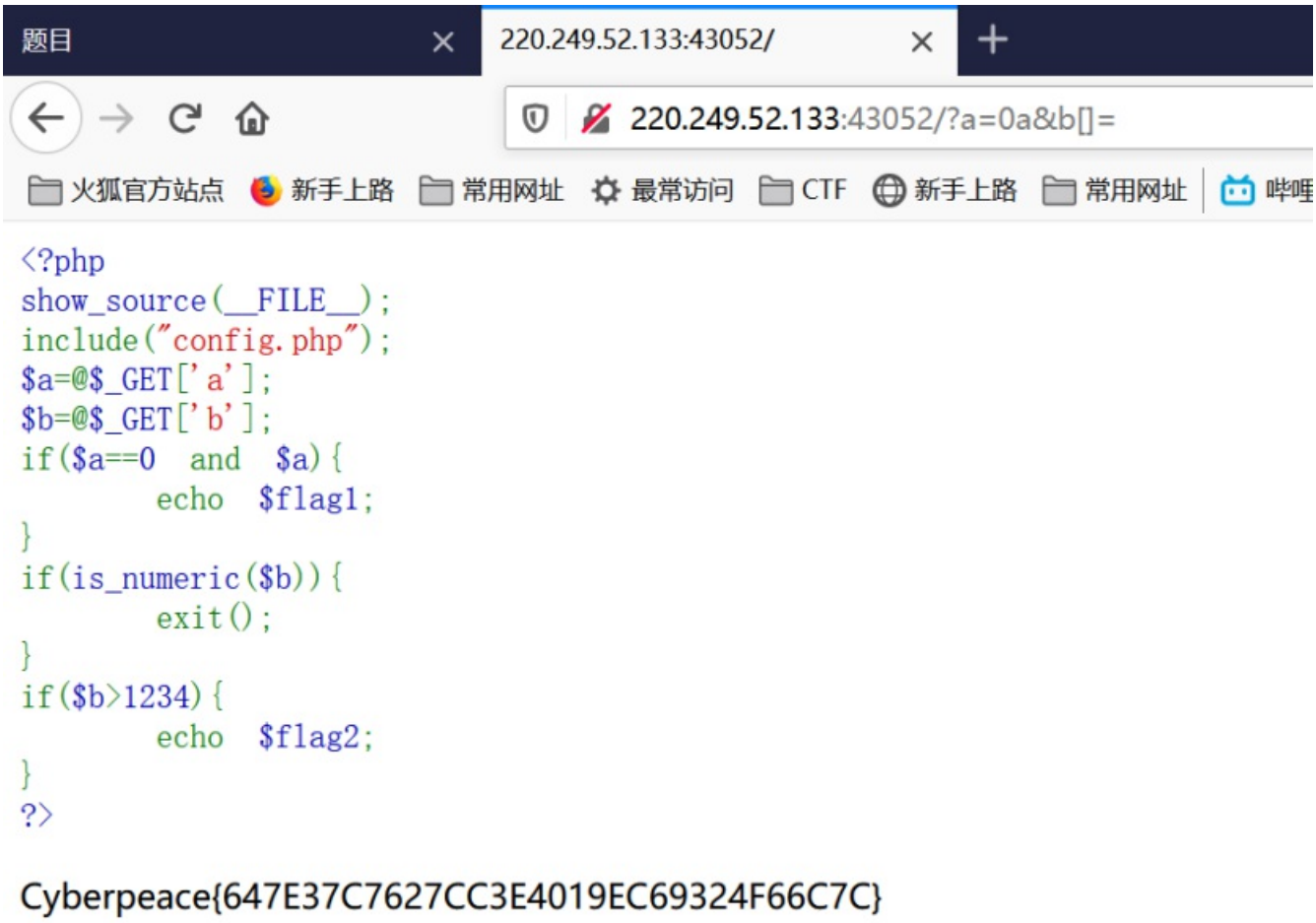


cyberpeace{55c6bea4ba417db7da3353608ad4798d}

0x08simple_php

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。

1.代码审计，根据源码，构造get请求 ?a=0a&b[]=



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

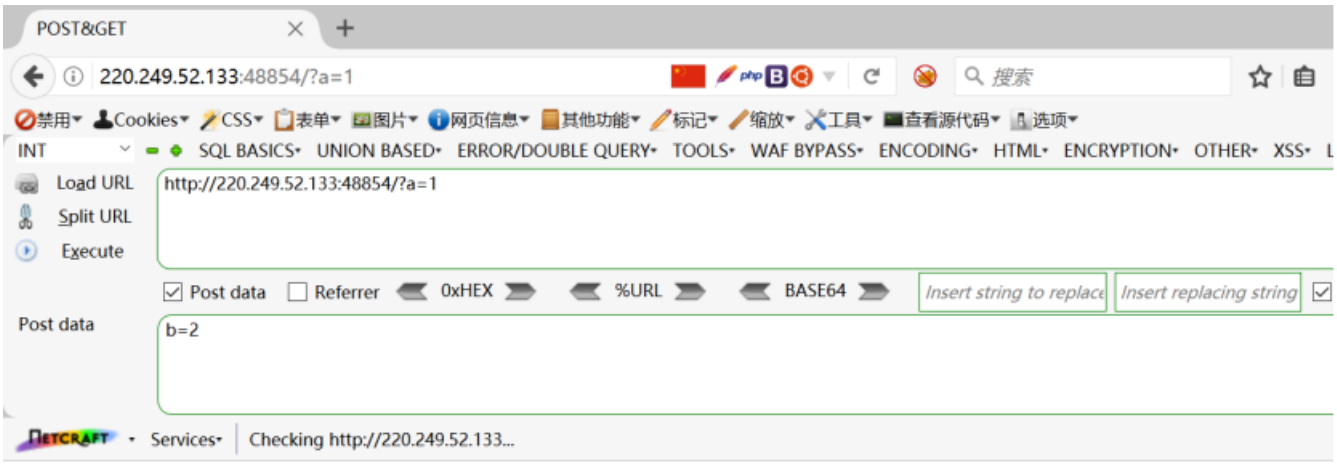
0x09get_post

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？

1.根据提示，请用GET方式提交一个名为a,值为1的变量。构造?a=1

2.根据提示，请再以POST方式随便提交一个名为b,值为2的变量。

用火狐浏览器提交post b=2



请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{fb23b6d776f7b36e25c9d2aa957ab3d5}

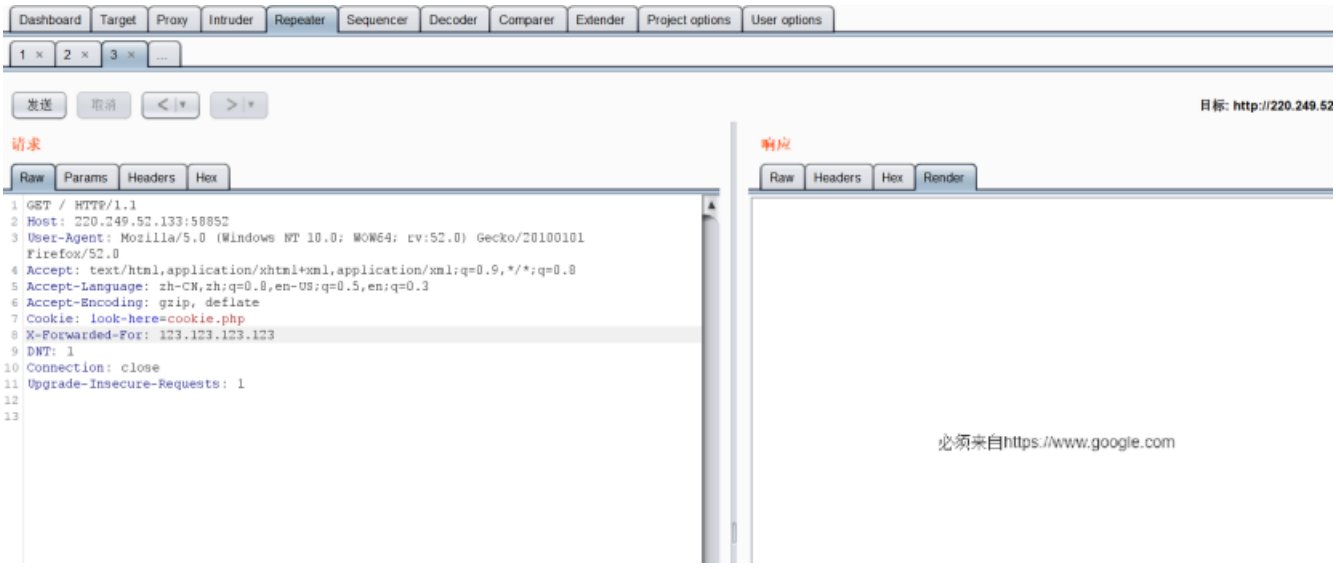
3.得到flag

cyberpeace{fb23b6d776f7b36e25c9d2aa957ab3d5}

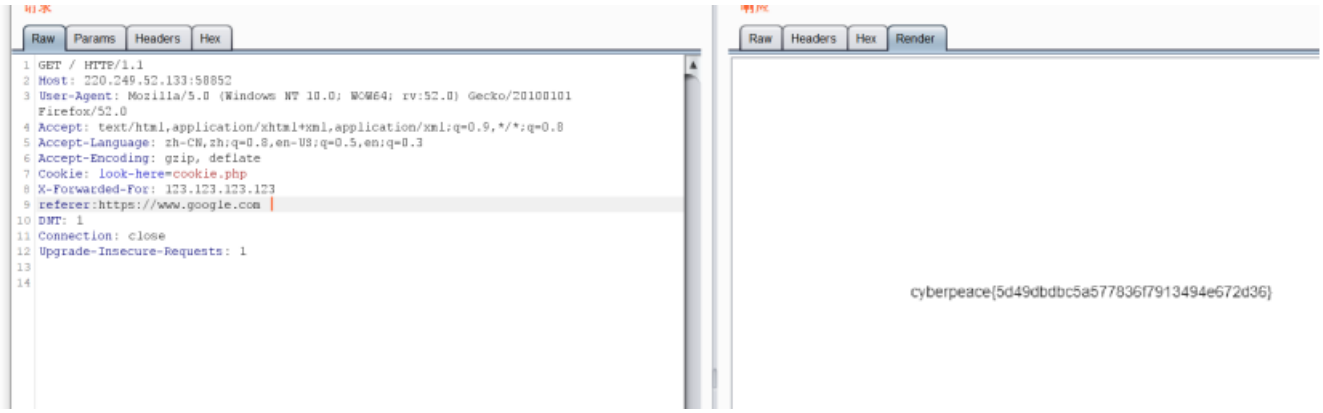
0x0axff_referer

X老师告诉小宁其实xff和referer是可以伪造的。

1.根据提示ip地址必须为123.123.123.123，在bp里添加XFF



2.根据提示必须来自https://www.google.com，BP添加referer参数



3.Flag为：

cyberpeace{5d49dbdbc5a577836f7913494e672d36}

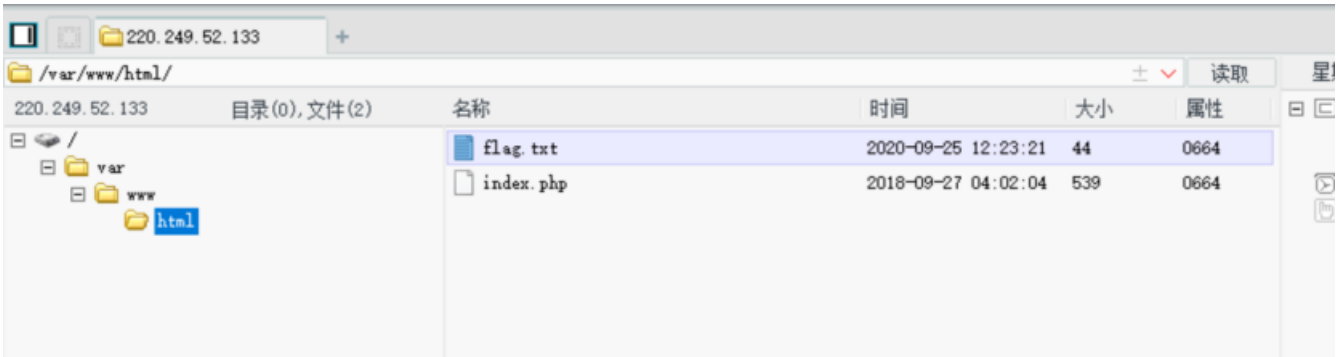
0x0bwebshell

小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

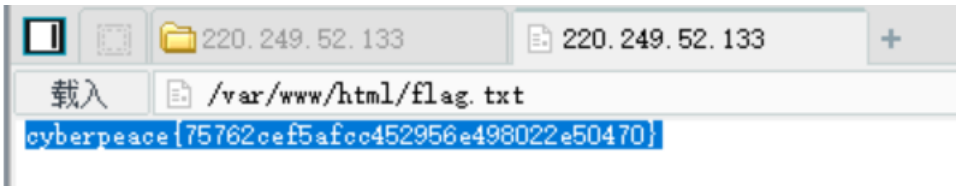
根据提示你会使用webshell吗？<?php @eval($_POST['shell']);?>

使用菜刀连接，密码为shell。

3.连接后在文件内找到flag.txt。

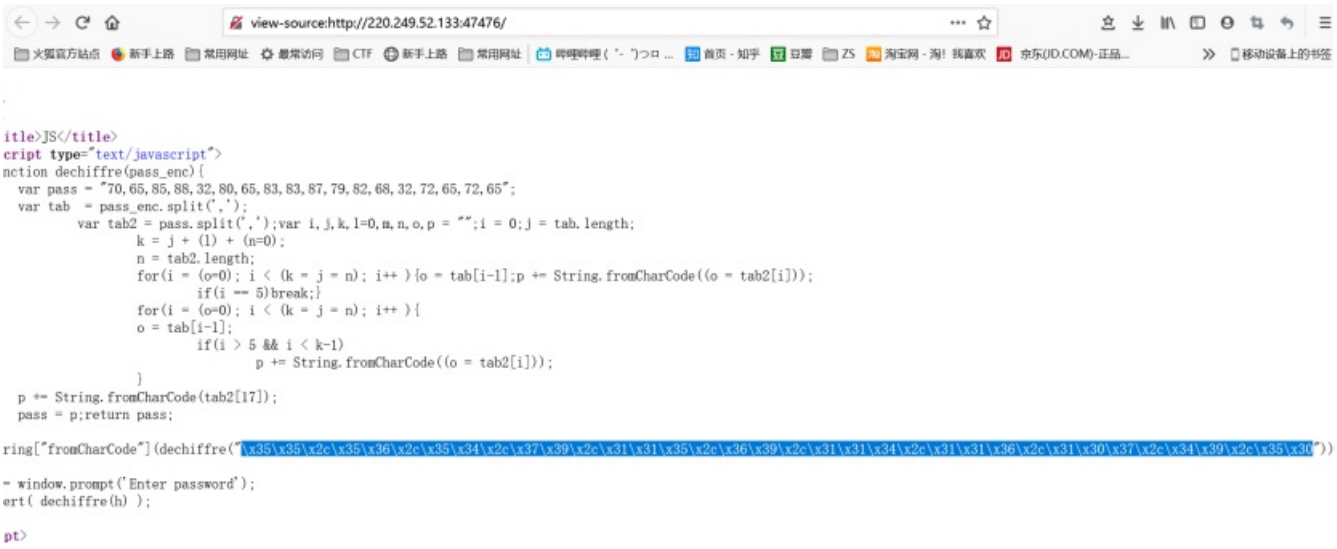


cyberpeace{75762cef5afcc452956e498022e50470}

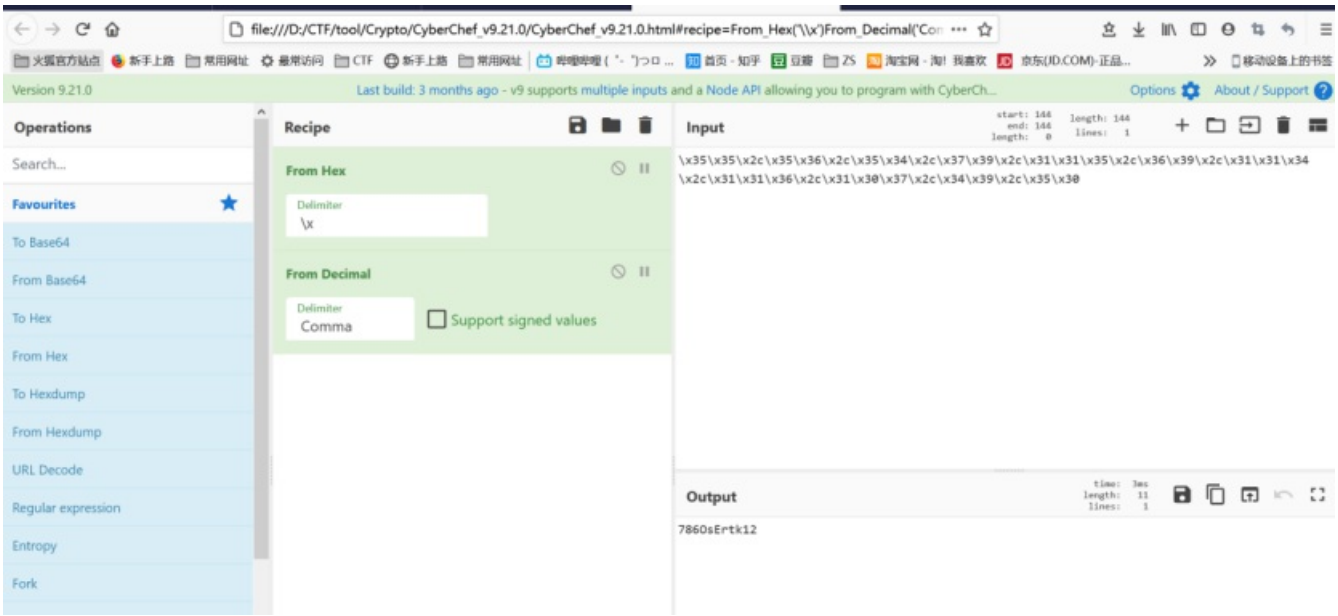


0x0csimple_js

小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxxx})



对话框点完后，右键查看源码，发现字符串(上面那串是假密码)cyberchef解码后得到密码786OsErtk12



Flag为 Cyberpeace{786OsErtk12}

感谢阅览，希望本文对您的学习有所帮助。欢迎关注、点赞、评论、收藏、转发、引用，分享请注明原作者和来源，谢谢！

作者：zs[CTF初学者]