

BUGKU_CTF WEB(1-10)writeUP

原创

程序小黑 于 2018-10-19 16:00:52 发布 44871 收藏 1

分类专栏: [网络安全](#) [WEB](#) [网络空间安全](#) 文章标签: [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_27180763/article/details/83183836

版权



[网络安全](#) 同时被 3 个专栏收录

77 篇文章 3 订阅

订阅专栏



[WEB](#)

12 篇文章 1 订阅

订阅专栏

[网络空间安全](#)

41 篇文章 8 订阅

订阅专栏

第一题: WEB2

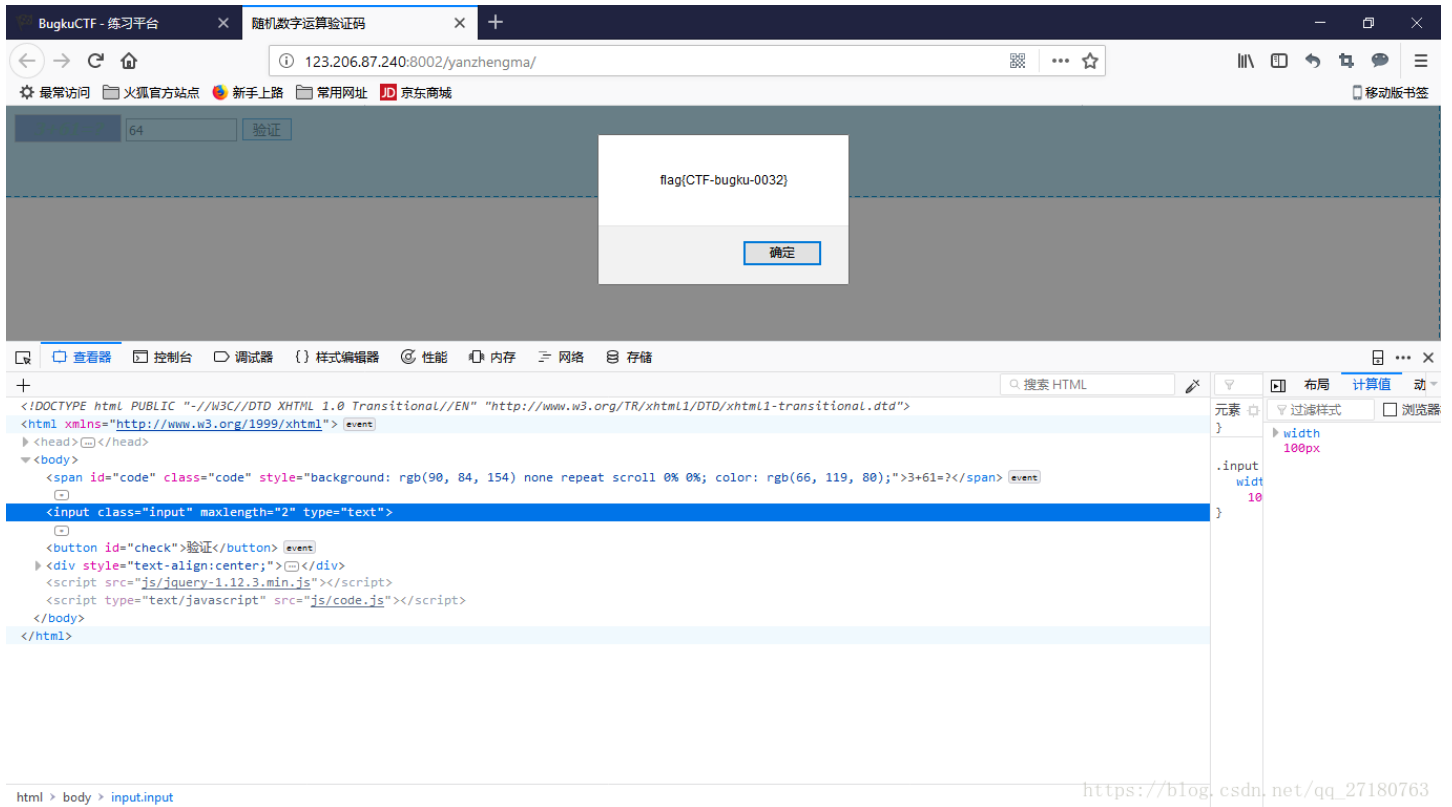
右击查看查看源代码或者直接F12审查元素就可以看到flag值了。

![Screenshot of a web browser showing a page with a background of yellow smiley faces. The browser's developer tools are open, showing the HTML source code. A comment in the code reads: <!--flag KEY(Web-2-bugKssNw1s9100)-->. The browser's address bar shows the URL 123.206.87.240:8002/web2/. The developer tools show the following HTML structure: <!DOCTYPE html PUBLIC](js/Snow.js)

```
<!--flag KEY(Web-2-bugKssNw1s9100)-->
```

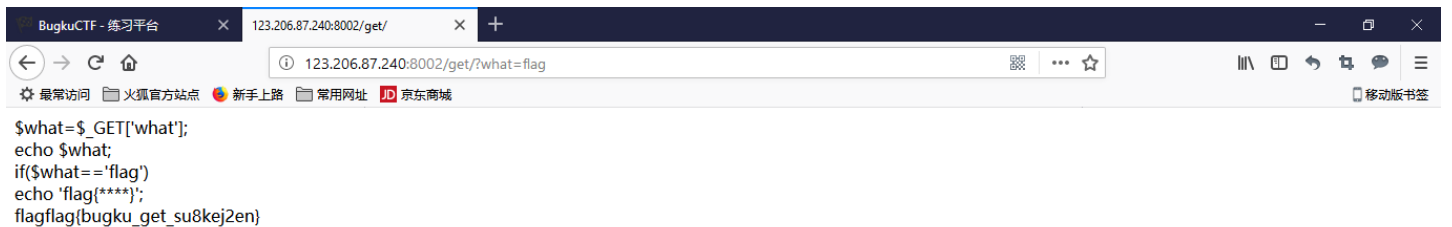
第二题: 计算器

右击审查元素，发现input表单里有一个maxlength属性。将属性值调大，就可以输入计算结果，从而拿到flag。当然burp抓包和自制表单也可以实现该功能。



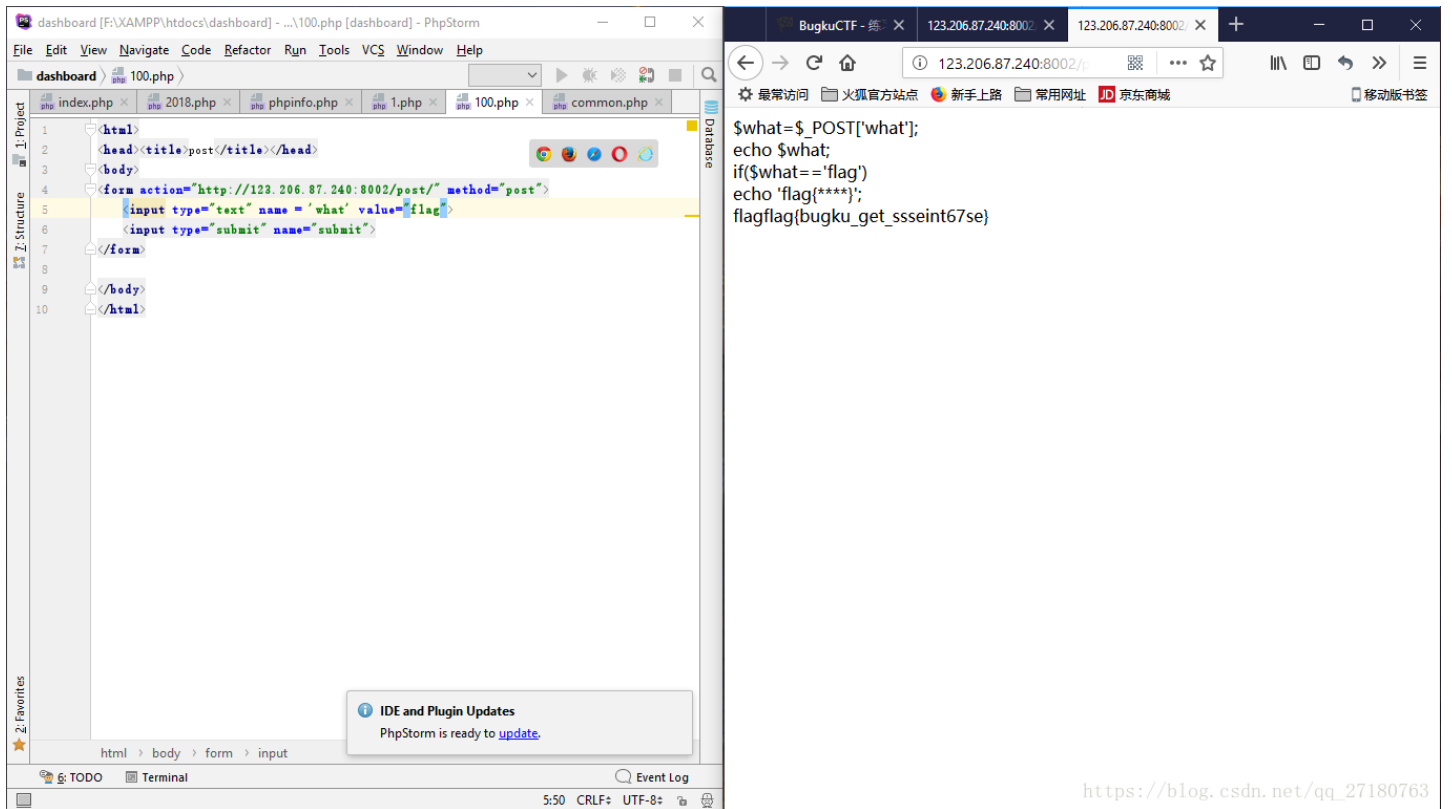
第三题：WEB基础\$_GET

可以通过查看给出源码直接传递GET参数。拿到flag



第四题：WEB基础\$_POST

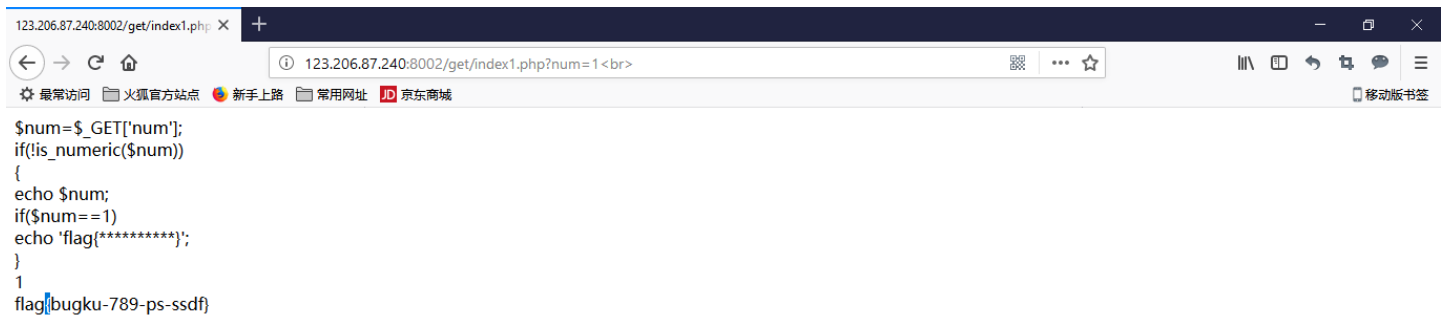
可以自己通过写一个表单进行传输传递从而实现拿到flag值



https://blog.csdn.net/qq_27180763

第五题：矛盾

通过源代码可以看到，题目用了is_numeric来判断传入参数是否为数字，这里php会进行类型判断。而在下面的\$num==1时，php会进行值判断，不进行类型判断。即字符串会被int型截断。



https://blog.csdn.net/qq_27180763

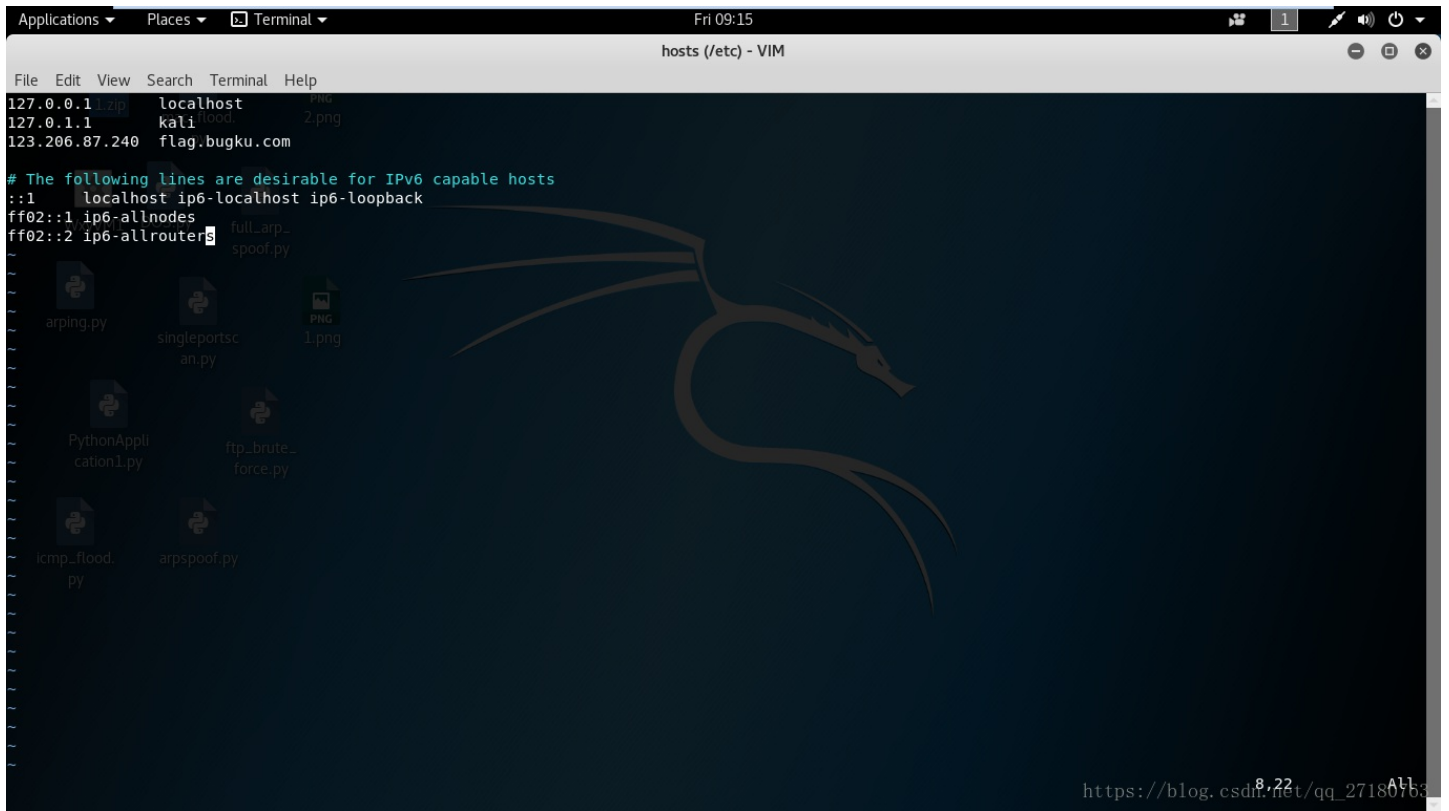
第六题：WEB3

打开页面可以看到页面不停的弹出对话框，我们通过审查元素查看源代码，可以发现被注释的unicode编码，使用unicode编码转义工具拿到flag。



第7题：域名解析

首先更改/etc/hosts下的域名解析文件:



```
File Edit View Search Terminal Help
127.0.0.1 localhost
127.0.1.1 kali
123.206.87.240 flag.bugku.com

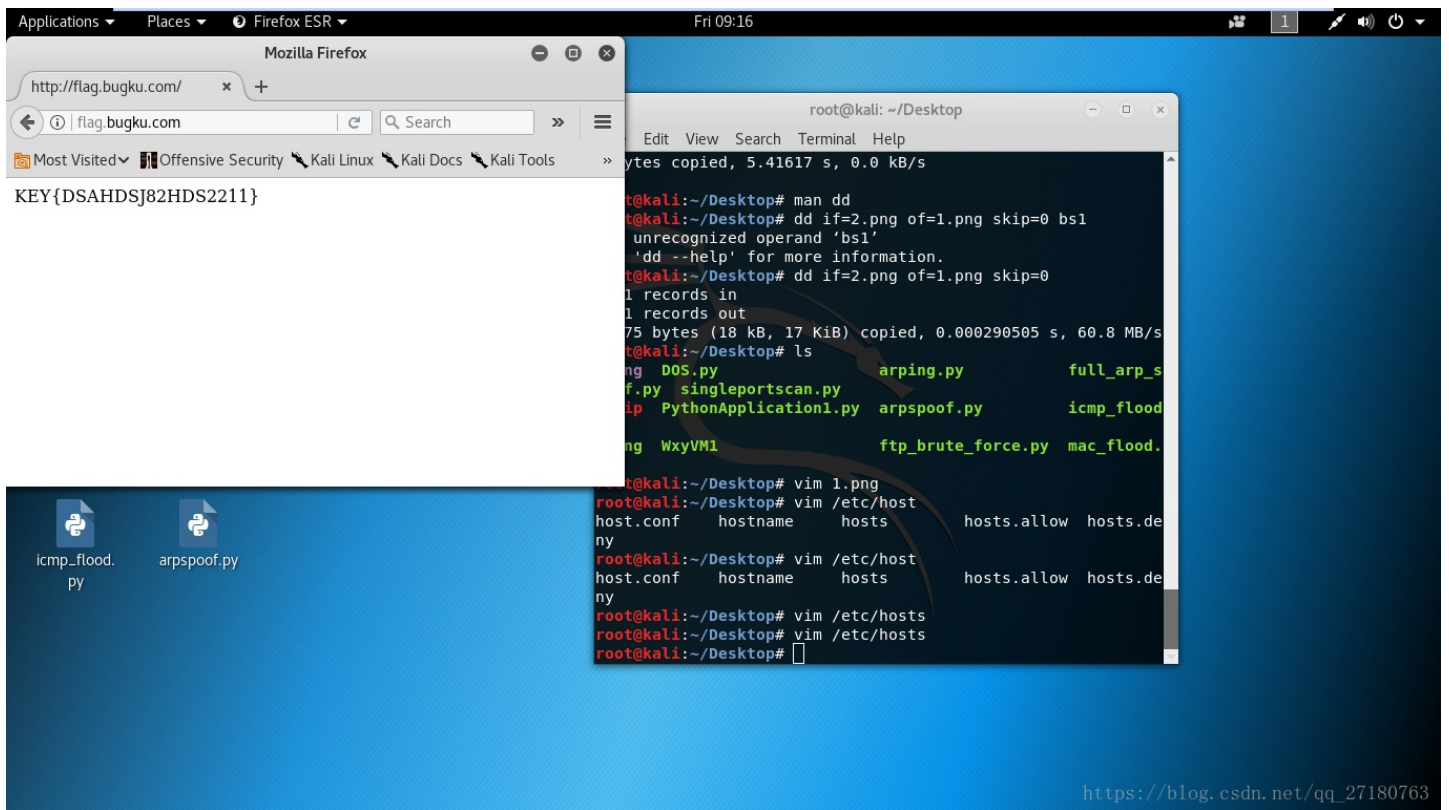
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

arping.py singleportscan.py 1.png
PythonApplication1.py ftp_brute_force.py
icmp_flood.py arspooft.py

8.22 All

https://blog.csdn.net/qq_27180763

然后直接访问flag.bugku.com就可以拿到flag值。



```
root@kali: ~/Desktop
Edit View Search Terminal Help
bytes copied, 5.41617 s, 0.0 kB/s
root@kali:~/Desktop# man dd
root@kali:~/Desktop# dd if=2.png of=1.png skip=0 bs1
dd: unrecognized operand 'bs1'
'dd --help' for more information.
root@kali:~/Desktop# dd if=2.png of=1.png skip=0
1 records in
1 records out
75 bytes (18 kB, 17 KiB) copied, 0.000290505 s, 60.8 MB/s
root@kali:~/Desktop# ls
DOS.py arping.py full_arp_s
f.py singleportscan.py
ip PythonApplication1.py arspooft.py icmp_flood
WxyVM1 ftp_brute_force.py mac_flood.
root@kali:~/Desktop# vim 1.png
root@kali:~/Desktop# vim /etc/host
host.conf hostname hosts hosts.allow hosts.de
ny
root@kali:~/Desktop# vim /etc/host
host.conf hostname hosts hosts.allow hosts.de
ny
root@kali:~/Desktop# vim /etc/hosts
root@kali:~/Desktop# vim /etc/hosts
root@kali:~/Desktop#
```

KEY{DSAHDSJ82HDS2211}

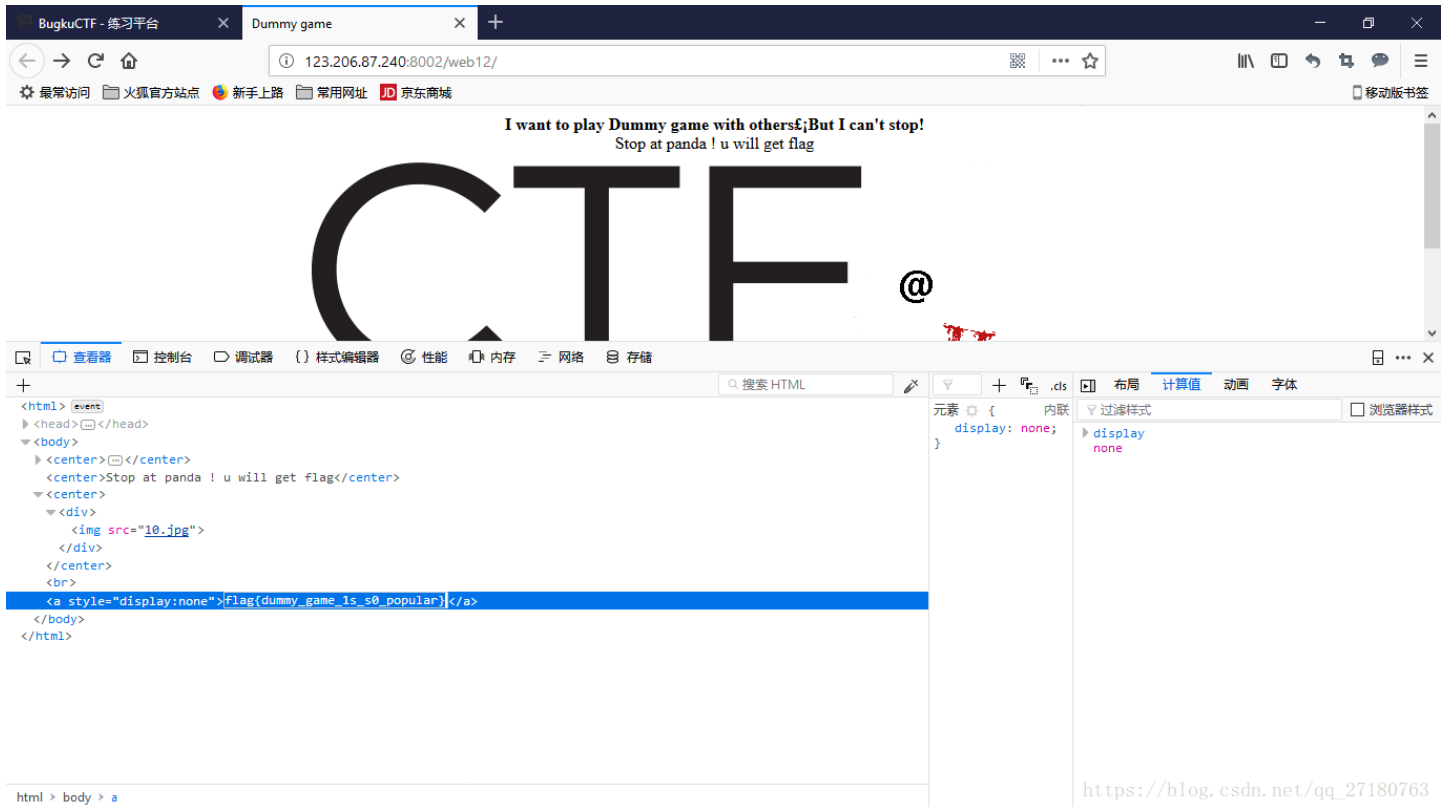
icmp_flood.py arspooft.py

8.22 All

https://blog.csdn.net/qq_27180763

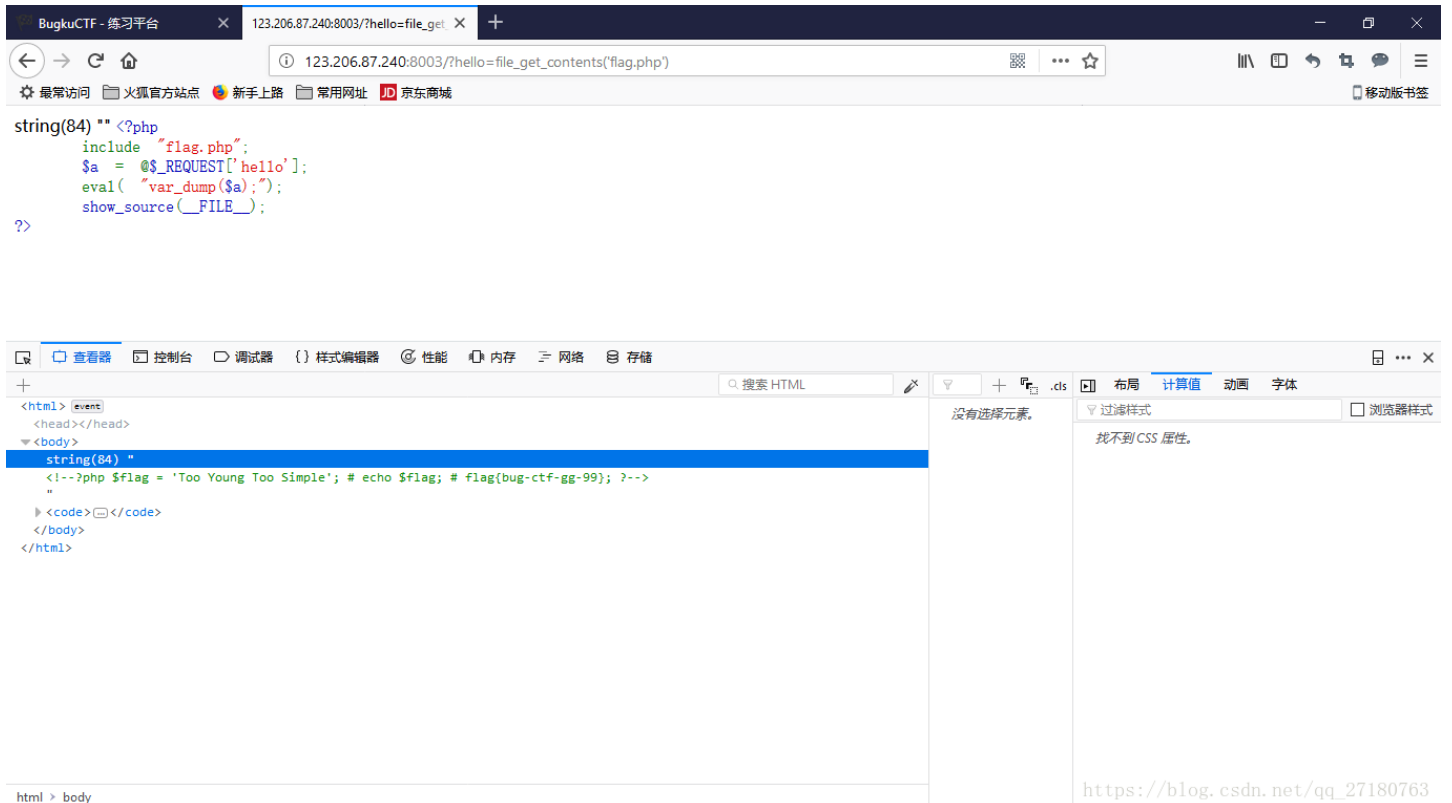
第8题: 你必须让他停下。

首先我们禁用javascript。来避免页面的不断刷新导致无法分析页面。
不断刷新页面，直到图片可以加载，就可以通过审查元素观测页面源码看到flag值。



第9题：本地包含

查看放出的源代码。



可以发现eval函数。直接传入file_get_contents函数读取flag.php,成功包含后查看审查元素拿到flag值。

第10题：变量1

阅读页面源代码，发现eval函数中有两个\$符号，考虑到时php自带的变量。考虑到全局变量global，传入参数。成功拿到flag。



```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
array(7) { ["GLOBALS"]=> *RECURSION* ["_POST"]=> array(0) {} ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_COOKIE"]=> array(0) {} ["_FILES"]=> array(0) {} ["_ZFkwe3"]=> string(38) "flag{92853051ab894a64f7865cf3c2128b34}" ["args"]=> string(7) "GLOBALS" }
```

https://blog.csdn.net/qq_27180763

后续将会陆续放出别的题，欢迎各位关注。