BugkuCTF web1~10 writeup

原创

Mitch311 于 2020-12-21 12:22:04 发布 273 收藏 2
分类专栏： CTF 文章标签： html5 javascript unctf

目录

---

web1.签到

原题链接

key：查看网页源代码

类似XCTF的第一题，虽然打开题目地址发现一堆滑稽笑脸，有点懵

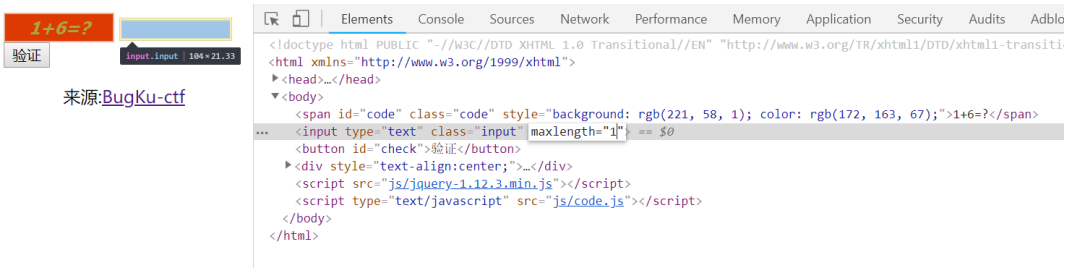
但是签到题应该不会太难，查看源代码后会找到flag

web2.计算器

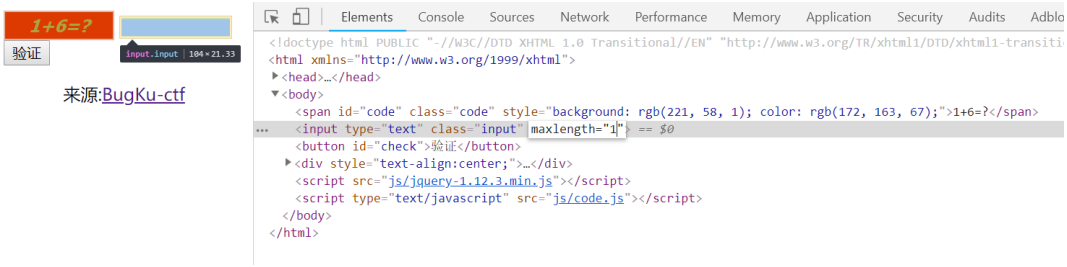
原题链接

key:js代码审计和修改

验证码小学计算题，但是输入框却输入不了完整的答案，猜测是通过js代码把长度锁定了



查看源代码果然发现了maxlength=1，删去，重新输入答案即可

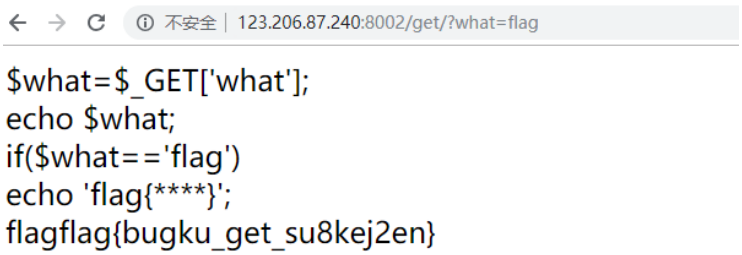


web3.$_GET

原题链接

key:get传参

没啥好说的，按照要求直接get传参what=flag即可



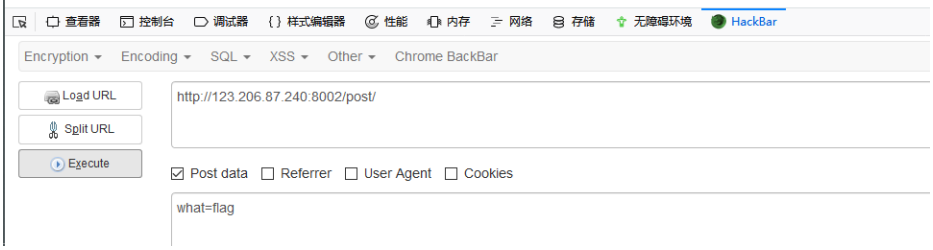
web4.$_POST

原题链接

key:post传参

一样没啥好说的，按照要求post传个参就完事了

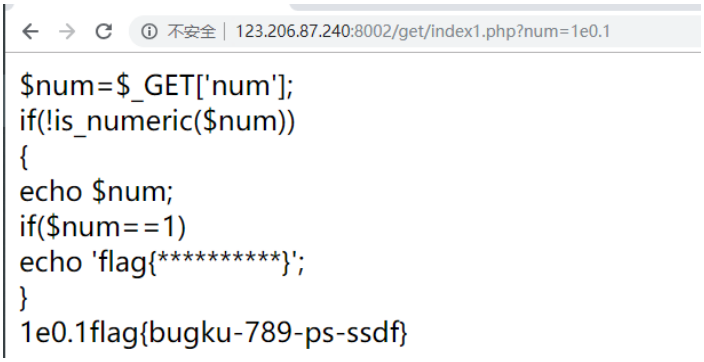
```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_ssseint67se}
```



web5.矛盾

原题链接

key:php弱比较



不能是数字，还要求满足==1，那么在数字1之后加上一个字母即可，例如num=1a

PHP在判断数字相等时，会将字符串转换为数字来比较

web6.flag就在这里

原题链接

key:禁用网页js+unicode解码+burpsuite的综合使用

方法一：

①打开网址发现无限弹窗，使用BurpSuite对网页进行截包，并发送到Repeater，通过观察服务端反馈的消息发现最下方有密文

②打开BurpSuite自带的编码解码及散列转换工具Decoder，选择HTML格式解码，找到flag(或者用ASCII码转换也可以）

方法二：

①直接“阻止此页面创建更多的对话框”or禁止JS后再打开

各种浏览器禁用js的方法

②查看源代码，发现最底下有一串&#xxxx格式的“编码”（实际上这是一些转义序列而不是编码）

&#后接十进制数字 &#x后面接十六进制数字 unicode编码的标志就是&#开头

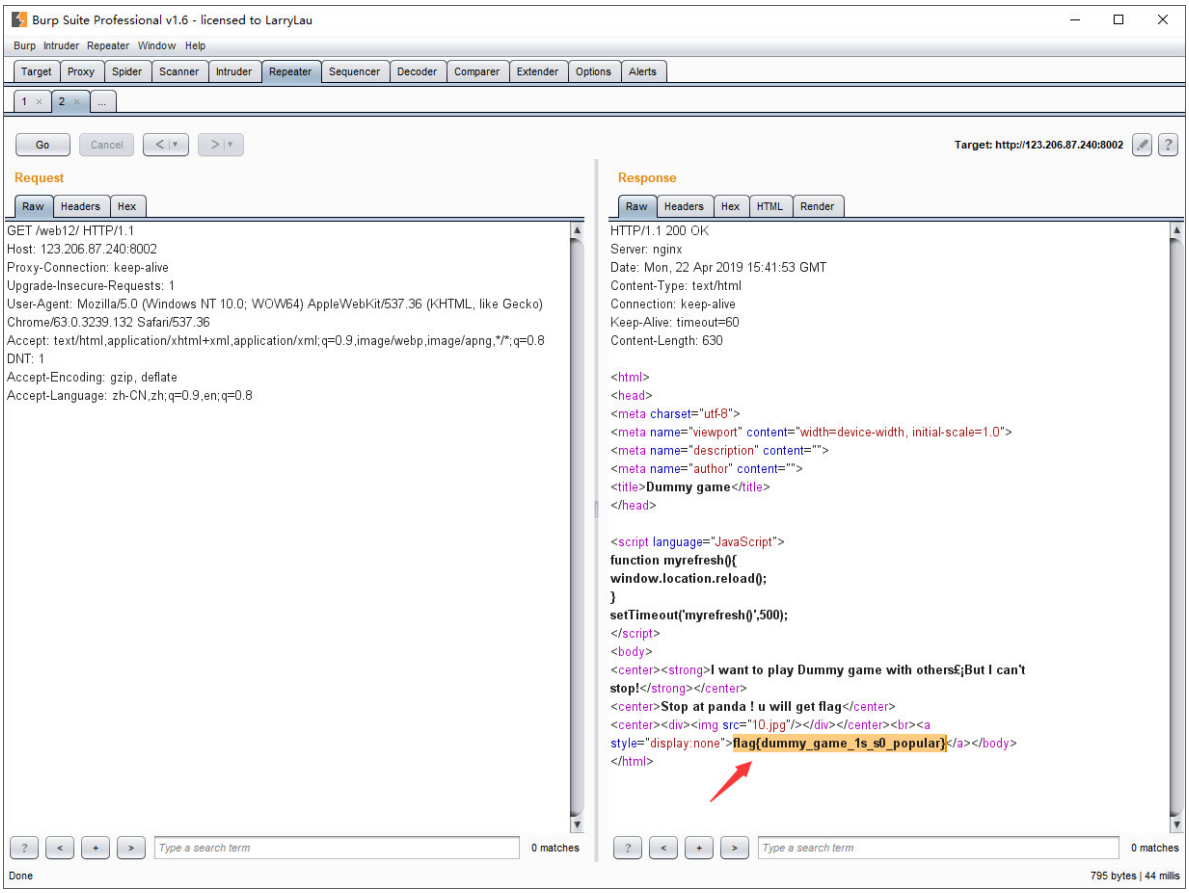
③直接把这一串序列找个在线转码（比如unicode解码器）扔进去就好

web7.你必须让他停下来

原题链接

key:burpsuite的综合使用

一进去就不断刷新，查看源码，有一个javascript函数一直刷新，使用Burpsuite抓包不断提交



web8.本地包含

原题链接

key:php攻击指令构造

```
<?php
    include "flag.php";
    $a = @$_REQUEST['hello'];
    eval("var_dump($a);");
    show_source(__FILE__);
?
```

> 知识补充：
>
> ①**$_request**这个变量和**$_GET**、**$_POST**一样，都属于超级全局变量，但是呢，运行时修改后者不会影响前者，反之亦然
>
> ②**eval**函数把字符串当作命令直接执行
>
> ③**show_source(__FILE__);**把本页代码以高亮语法显示出来,是 **highlight_file()** 的别名

方法一：

eval存在命令执行漏洞，使用hello构造payload

```
构造?hello=);print_r(file("flag.php")

或者?hello=1);show_source("flag.php");var_dump(2

或者?hello=1);show_source("flag.php");//
```

> **print_r()** 函数只用于输出数组
>
> **var_dump()** 函数可以输出任何内容：输出变量的容，类型或字符串的内容，类型，长度

方法二：

直接将flag.php文件读入变量hello中

```
?hello=get_file_contents('flag.php')

或者?hello=file('flag.php')
```

> **file()**函数的作用是读取文件，然后以数组的形式返回

方法三（有点麻烦）：

```
在URL上构造http://120.24.86.145:8003/index.php?hello=1);include $_POST['f'];//
在POST区域传参f=php://filter/convert.base64-encode/resource=flag.php
```

最后base64解码即可

> **include()**函数和**php://input**，**php://filter**结合很好用，**php://filter**可以用于读取文件源代码，结果是源代码**base64**编码后的结果

web9.变量1

原题链接

key:php正则表达式、可变变量、全局变量

```php
<?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);");
}
?>
```

> 知识补充：
>
> ①**eval**函数：把字符串按照**PHP**代码来计算，该字符串必须是合法的**php**代码，且必须以分号结尾。
>
> ②**var_dump**函数：输出变量的相关信息。
>
> ③**preg_match()**函数：匹配字符，返回**true**或者**false**。
>
> **^**是表示正则表达式的开始，**$**表示正则表达式的结束，**\w**表示任意大小写字母或数字或下划线，**+**号表示**1**到多个**\w.**
>
> 这个正则表达式的意思是匹配任意 **[A-Za-z0-9_]** 的字符，就是任意大小写字母和**0**到**9**以及下划线组成

此处的var_dump对象是$ $args，如果$args=GLOBALS，那么$ $args=$GLOBALS，是全局变量，那么var_dump打印出的将会是全局变量（包括flag1.php)

因此果断get传参?arg=GLOBALS，得到flag

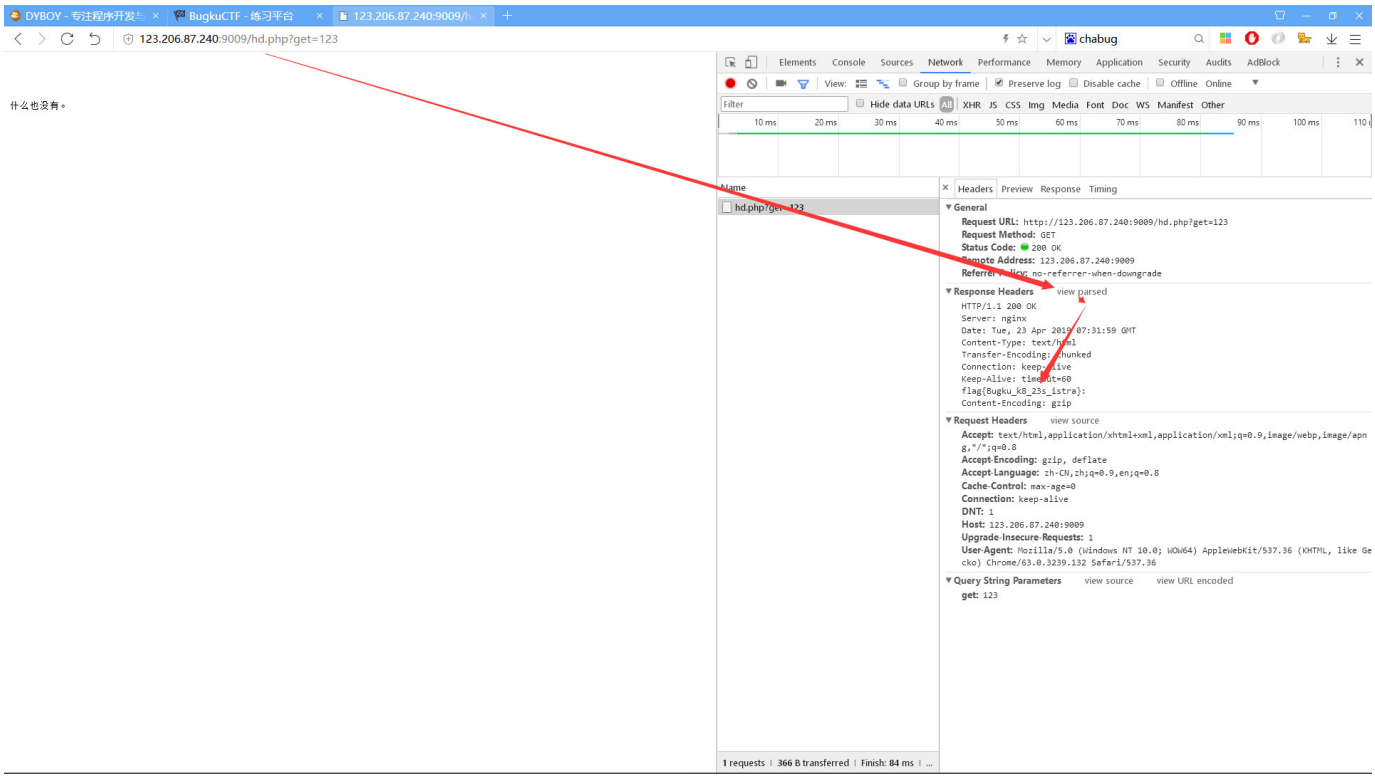
web10.头等舱

原题链接

key:查看网页响应头

思路：根据题目以及查看源码没东西，还有文件名：`hd` => `head`，推测`flag`应该隐藏在数据包头部

方法一：使用Chrome浏览器（或者联想浏览器也行）



方法二：使用burpsuite抓包查看响应头Response