[CTF]Bugku Web Writeup (1)



m3gaf0rce

于 2020-12-19 14:36:48 发布 057 🛠 收藏 分类专栏: <u>CTF</u>

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/jaykiller/article/details/111404558



CTF 专栏收录该内容

7篇文章0订阅 订阅专栏 题目: https://ctf.bugku.com/challenges/index.html

1. web1

直接F12。



<!--flag{b1516b2e64ee0929bac5

<script type="text/javascript" src="js/ThreeCanvas.js"></script> <script type="text/javascript" src="js/Snow.js"></script> > <script type="text/javascript"> ... </script</pre> > <div> ··· </div> </body>

</html>

<

Q, 搜索 HTML

html > body#body

2. web2

验证 1

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}

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。

Go Cancel < v > v	Target: http://114.67.246.176:13788
Request	Response
Raw Params Headers Hex	Raw Headers Hex
POST / HTTP/1.1	HTTP/1.1 200 OK
Host: 114.67.246.176:13788	Date: Sat, 19 Dec 2020 06:52:16 GMT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;	Server: Apache/2.4.7 (Ubuntu)
rv:84.0) Gecko/20100101 Firefox/84.0	X-Powered-By: PHP/5.5.9-1ubuntu4.6
Accept:	Vary: Accept-Encoding
<pre>text/html,application/xhtml+xml,application/xml;q=0.9,im</pre>	Content-Length: 138
age/webp,*/*;q=0.8	Connection: close
Accept-Language:	Content-Type: text/html
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	<pre>\$what=\$_POST['what']; </pre>
Accept-Encoding: gzip, deflate	echo \$what;
Connection: keep-alive	if(\$what=='flag')
Upgrade-Insecure-Requests: 1	echo 'flag{****}';
Cache-Control: max-age=0	
Content-Type: application/x-www-form-urlencoded	
Content-Length: 9	flagflag{652d924510f3dde53f96cf894e262c79}
what=flag	
	https://blog.csdn.net/jaykiller

5. web5

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

构造num=1a即可。

6. web6

直接上burpsuite,拉到response的最后,ascii解码。



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	Response
Raw Headers Hex	Raw Headers Hex HTML Render
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,sh;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	<pre>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 D<html> <head> <meta charset="utf-8"/> <meta charset="utf-8"/> <meta charset="utf-8"/> <meta charset="utf-8"/> <meta charset="utf-8"/> <meta content="width=device-width, initial=scale=1.0" name="viewport"/> <meta content="" name="uewcription"/> <meta content="" name="uewcription"/> <meta content="" name="author"/> <meta content="" name="author"/> <meta content="" name="description"/> </head></html></pre>

8. web8 文件包含

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

源码中即可看到flag。

```
1 <?php

2 $flag = 'Too Young Too Simple';

3 # echo $flag;

4 # flag{70fl686869d463da9d20ld050dc8b9db};

5 >><code><span style="color: #000000">

6 <span style="color: #0000BB">&lt; ?php

7 <br />&nbsp;&nbsp;&nbsp;</span><span style="color:

8 <br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:

9 <br />&nbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:

10 <br /><fnbsp;&nbsp;&nbsp;&nbsp;</span><span style="color:

11 <br /></span><span style="color: #0000BB">?&gt;</span>

2 </span>

3 </code> https://blog.csdn.net/jaykiller
```

* 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";
include "flag1.php";
include "flag1.php";
if(isret(file_file_);
if(isret(file_

https://blog.csdn.net/iavkiller

10. web10 头等舱

看Response。

🛃 Burp Suite Professional	v1.6 - licensed to Ları	ryLau									_		Х
Burp Intruder Repeater W	indow Help												
Target Proxy Spider	Scanner Intruder	Repeater	Sequencer	Decoder	Comp	parer	Extender	Options	Alerts				
Intercept HTTP history	WebSockets history	/ Options											
Filter: Hiding CSS, image a	nd general binary con	itent											?
# 🔺 Host	Method U	RL		P	arams	Edited	Status	Length	MIME t	. Extension	n Title		
1 http://114.67.246.176	6:13403 GET /						200	394	HTML				
•													7.
Request Response					s								7►
Request Response	1TML Render				5) •
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Werd 20 Jan 202	1TML Render				5								
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7	HTML Render 1 14:30:27 GMT (Wountu)				•								7.
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34	HTML Render 11 14:30:27 GMT (Wountu) 9-1ubuntu4.6 6ac7332bf89cebb	915da6e}			· · · · · · · · · · · · · · · · · · ·								
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137	HTML Render 1 14:30:27 GMT (Ubuntu) 9-1ubuntu4.6 6ac7332bf89cebb	915da6e}			·								7.
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht	HTML Render 11 14:30:27 GMT (Ubuntu) 5.9-1ubuntu4.6 6ac7332bf89cebb 1 ml	915da6e}			•				_				7.
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht	HTML Render 1 14:30:27 GMT (Ubuntu) 5.9-1ubuntu4.6 5ac7332bf89cebb f ml	915da6e)											
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(807fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht <html> <meta cont<="" http-equiv="Con</td><td>HTML Render
1 14:30:27 GMT
(Ubuntu)
.9-1ubuntu4.6
6ac7332bf89cebb
f
ml
utent-Type" td=""/><td>915da6e) ent="text</td><td>-/html; cha</td><td>arset=UT</td><td>F-8" /</td><td>/></td><td></td><td></td><td></td><td></td><td></td><td></td><td>*</td></html>	915da6e) ent="text	-/html; cha	arset=UT	F-8" /	/>							*	
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht <html> <meta http-equiv="Con
<pre>
<br</td><td>HTML Render 11 14:30:27 GMT (Ubuntu) </td><td>915da6e}
ent=" td="" text<=""/><td>:/html; cha</td><td>arset=UT</td><td>F-8″ /</td><td>· ></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></html>	:/html; cha	arset=UT	F-8″ /	· >									
Request Response Raw Headers Hex HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht <html> <meta< td=""> <pre>< </pre>< </meta<></html>	HTML Render 1 14:30:27 GMT (Ubuntu) ,9-1ubuntu4.6 6ac7332bf89cebb f ml utent-Type" cont 000000 >	915da6e) ent="text	:/html; cha	arset=UT	F-8″ /	/>							
Request Response Raw Headers Hex HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht <html> <pre><dbr><dbr><dbr><dbr> </dbr></dbr></dbr></dbr></pre> </html>	HTML Render 1 14:30:27 GMT (Ubuntu) 1.9-1ubuntu4.6 6ac7332bf89cebb f m1 itent-Type" cont 000000 >	915daće) ent="text	:/html; Cha	arset=UT	F-8" /	· >							
Request Response Raw Headers Hex H HTTP/1.1 200 OK Date: Wed, 20 Jan 202 Server: Apache/2.4.7 X-Powered-By: PHP/5.5 Flag: flag(8d7fc6bc34 Vary: Accept-Encoding Content-Length: 137 Connection: close Content-Type: text/ht <html> <meta http-equiv="Con
<pre> </pre></html>	HTML Render 1 14:30:27 GMT (Ubuntu)	915da6e}	z/html; cha	arset=UT	F-8″ /	/>						0.000	