【XCTF 攻防世界】WEB 高手进阶区PHP2

原创

Kal1 于 2020-08-25 11:38:28 发布 174 收藏

分类专栏： CTF刷题 WEB 文章标签： web 安全 url编码

本文链接：https://blog.csdn.net/weixin_45844670/article/details/108218036

题目链接：https://adworld.xctf.org.cn/task/answer?type=web&number=3&grade=1&id=4820&page=1

预备知识：

1,什么是phps文件？

phps文件就是php的源代码文件，通常用于提供给用户（访问者）查看php代码，因为用户无法直接通过Web浏览器看到php文件的内容，所以需要用phps文件代替。其实，只要不用php等已经在服务器中注册过的MIME类型为文件即可，但为了国际通用，所以才用了phps文件类型。

它的MIME类型为：text/html, application/x-httpd-php-source, application/x-httpd-php3-source。

2，phps文件就是php的源代码文件，是给用户查看源代码的，无法接受变量传参，因为不能当做php进行解析，所以index.phps?id=是不行的，将s去掉即可

传递参数

3，浏览器在上传数据时，会对参数值进行一次解码（与php代码无关，是浏览器自身会解码一次）

4,

ASCII Value	URL-encode	ASCII Value	URL-encode	ASCII Value	URL-encode
æ	0%	0	30%	`	60%
	1%	1	31%	a	61%
	2%	2	32%	b	62%
	3%	3	33%	c	63%
	4%	4	34%	d	64%
	5%	5	35%	e	65%
	6%	6	36%	f	66%
	7%	7	37%	g	67%
backspace	8%	8	38%	h	68%
tab	9%	9	39%	i	69%
linefeed	%0a	:	%3a	j	%6a
	%0b	;	%3b	k	%6b
	%0c	<	%3c	l	%6c
c return	%0d	=	%3d	m	%6d
	%0e	>	%3e	n	%6e
	%0f	?	%3f	o	%6f
	10%	@	40%	p	70%
	11%	A	41%	q	71%
	12%	B	42%	r	72%
	13%	C	43%	s	73%
	14%	D	44%	t	74%
	15%	E	45%	u	75%
	16%	F	46%	v	76%
	17%	G	47%	w	77%
	18%	H	48%	x	78%
	19%	I	49%	y	79%
	%1a	J	%4a	z	%7a
	%1b	K	%4b	{	%7b
	%1c	L	%4c	|	%7c
	%1d	M	%4d	}	%7d
	%1e	N	%4e	~	%7e
	%1f	O	%4f		%7f
space	20%	P	50%	€	80%
!	21%	Q	51%		81%
"	22%	R	52%	‚	82%
#	23%	S	53%	ƒ	83%
$	24%	T	54%	„	84%
%	25%	U	55%	…	85%
&	26%	V	56%	†	86%
'	27%	W	57%	‡	87%
(	28%	X	58%	ˆ	88%
)	29%	Y	59%	‰	89%
*	%2a	Z	%5a	Š	%8a
+	%2b	[	%5b	‹	%8b
,	%2c	\	%5c	Œ	%8c
-	%2d	]	%5d		%8d
.	%2e	^	%5e	Ž	%8e
/	%2f	_	%5f		%8f

打开链接，页面只有一句话
用御剑扫描后台
得到index.php
这时候就可以考虑index.phps了
果然发现一段代码

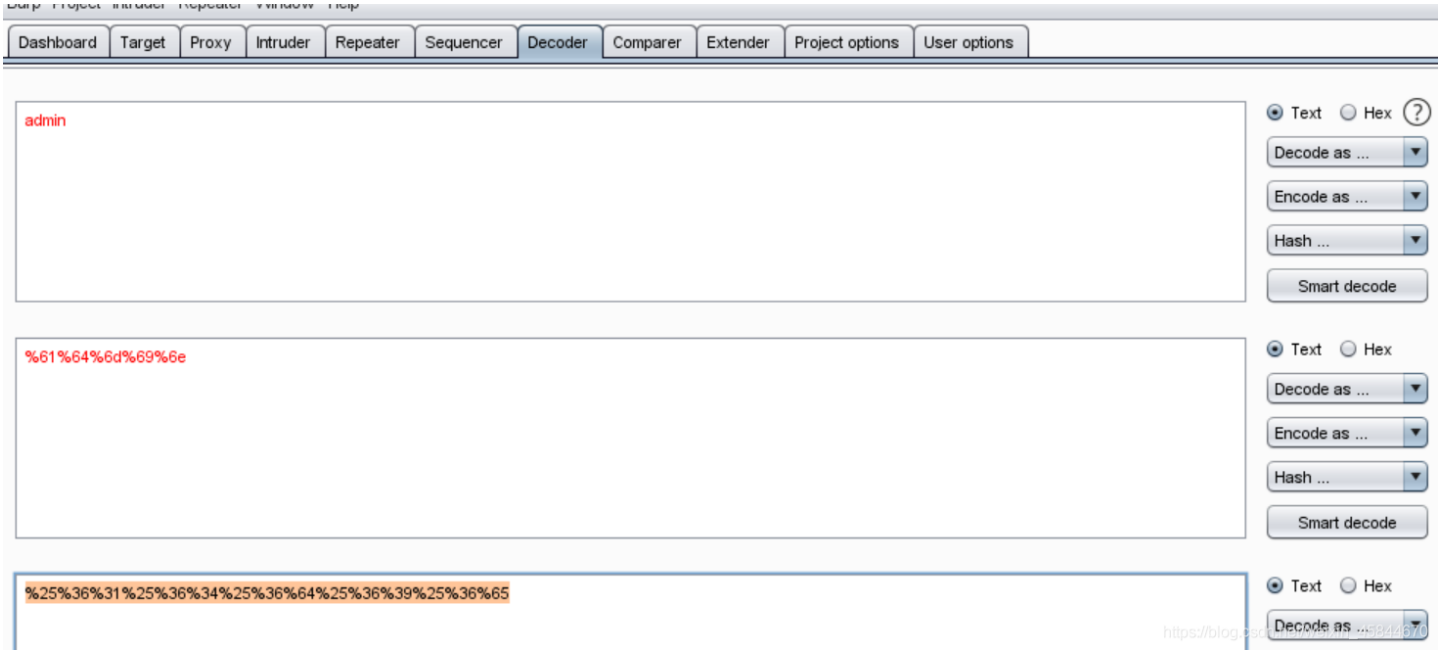
```php
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>

Can you anthenticate to this website?
```


这里考虑二次绕过（参考预备知识3）

使用burp编码，很方便




```
%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65
```

payload：`/?id=%2561%2564%256d%2569%256e`
得到flag