Description

seriously, are you a master of webshell?   
rules: you should submit a \*\*python script\*\* that takes a randomly generated lowercase string and outputs a php script. the php script should output the given string, and will be wafed as described in the following code:

**def** **waf**(phpshell):

**if** **not** phpshell.startswith(b'<?php'):

**return** True

phpshell = phpshell[**6**:]

**for** c **in** phpshell:

**if** c **not** **in** b'0-9$\_;+[].=<?>':

**return** True

**else**:

**print**(chr(c), end='')

**return** False

which means that except for the '<?php' in the beginning of the output, no characters other than '0-9$\_;+[].=<?>' shall exist.   
most importantly, the generated shell SHALL NOT be longer than a competing algorithm for the same goal. the initial algorithm is kept in secret.   
**Flag Format: d3ctf{this\_is\_a\_sample\_flag}**   
⚠️：  
\* you are submitting a \*\***python**\*\* script, for example:

target = input()

**print**(f'<?php echo "{target}";')

the code above will end up being wafed, but it does generate the correct results.   
⚠️ 3.6 3:32AM additional hint： waf rules are loosened

echo -n {random\_str()} | python3 /your\_script.py | waf | php

the result of the command above should be exactly the same as the generated random\_str

Challenge Address

<http://e1d11fb086.shellgen2.d3ctf.io>

Base Score

1000

Now Score

424.63

Team solved

[25](javascript:;)