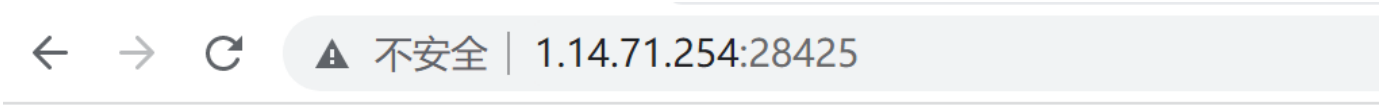
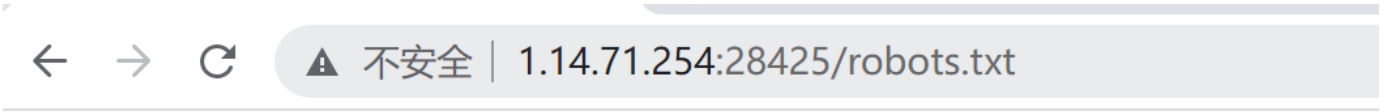
[NISACTF 2022]is secret

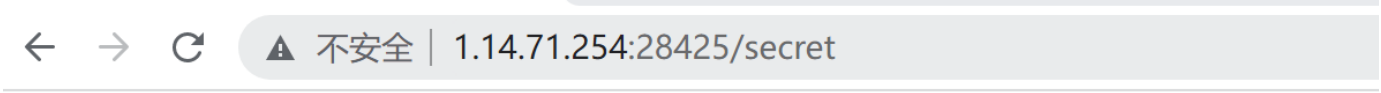


Welcome To Find Secret

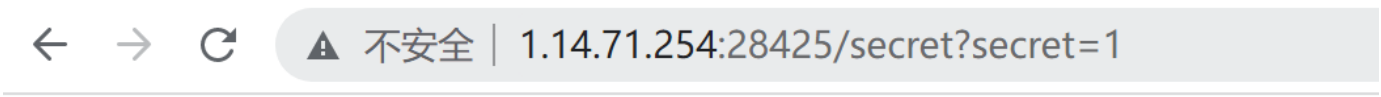


It is Android ctf

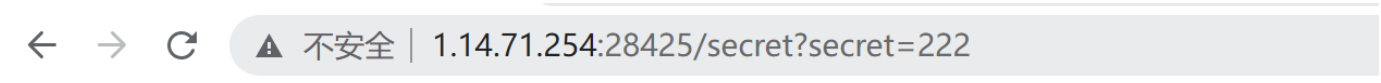
真的吗 我不信



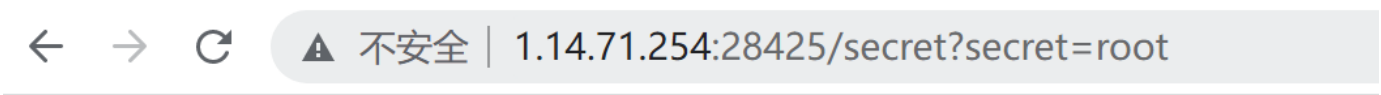
Tell me your secret.I will encrypt it so others can't see



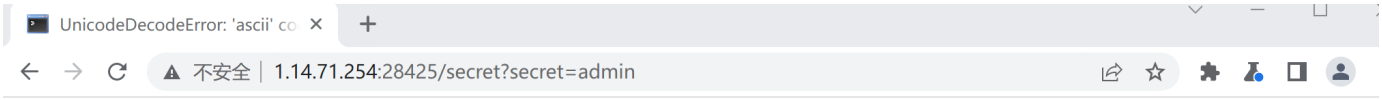
d



g]



'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

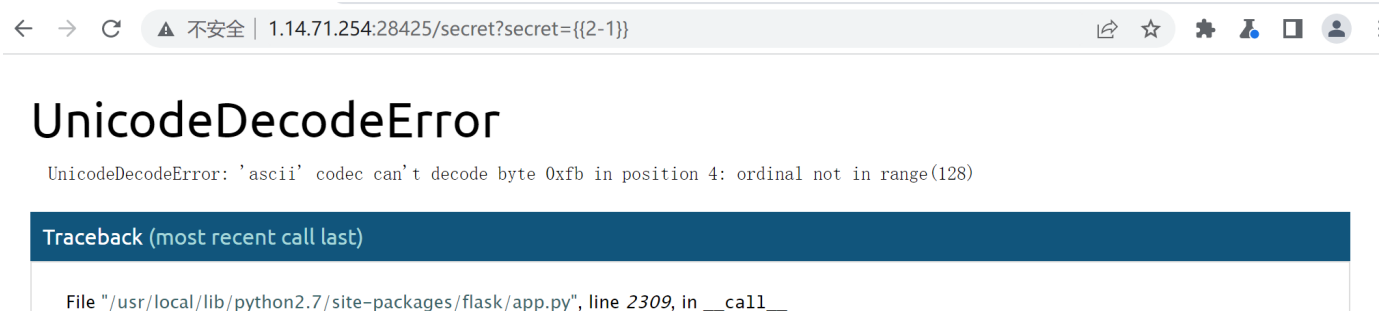
```
    if(secret==None):
        return 'Tell me your secret.I will encrypt it so others can\'t see'
    rc=rc4_Modified.RC4("HereIsTreasure")   #解密
    deS=rc.do_crypt(secret)

    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

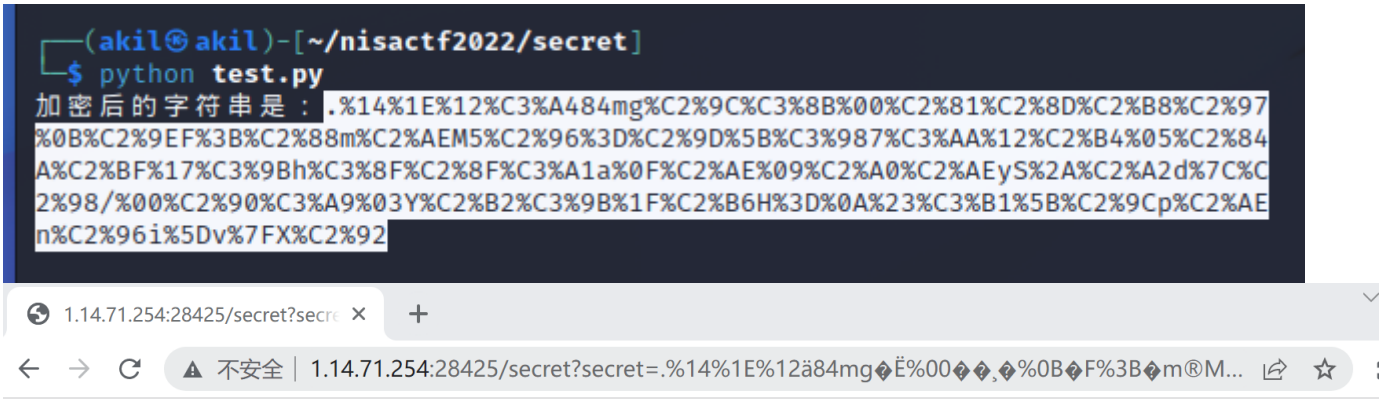
https://www.freebuf.com/articles/web/279670.html



好像不能直接来

RC4加密脚本：

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



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