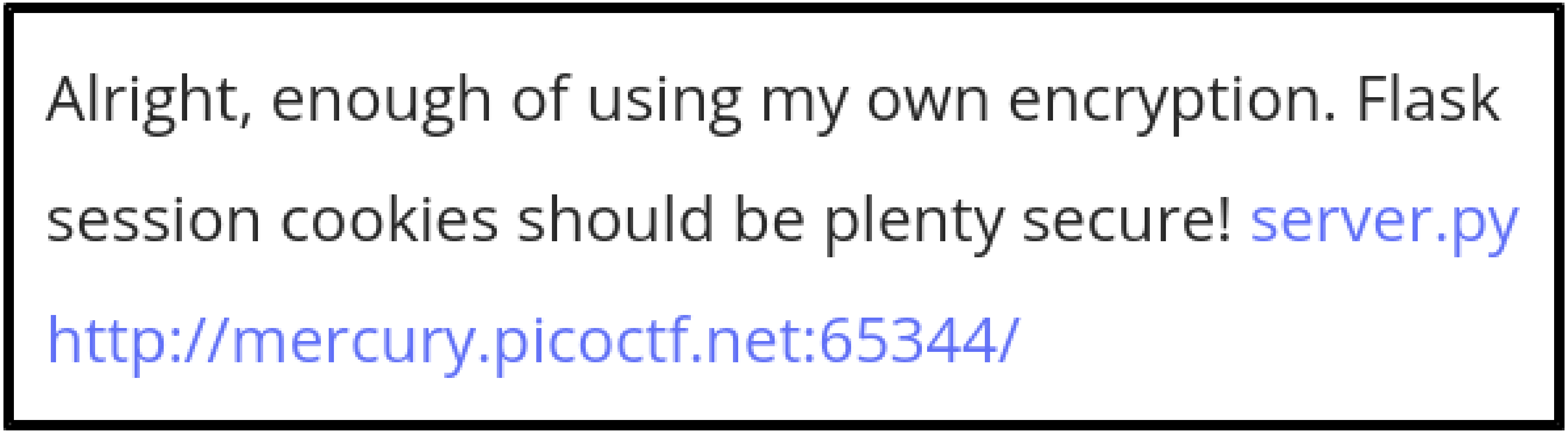
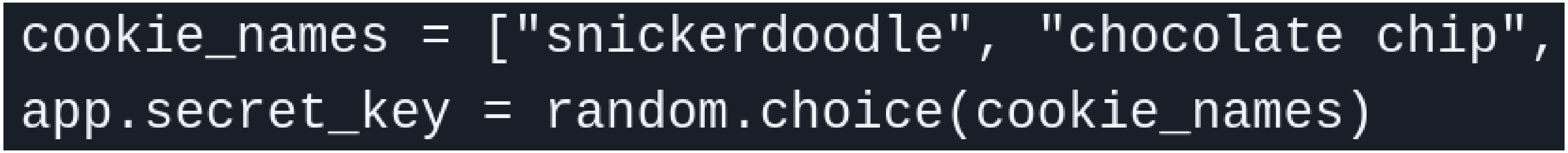
PicoCTF 2021 – Most Cookies



Alright, enough of using my own encryption. Flask session cookies should be plenty secure! server.py http://mercury.picoctf.net:65344/

The web application is is using a Python Flask server, and Flask web apps create user session tokens using a standard method

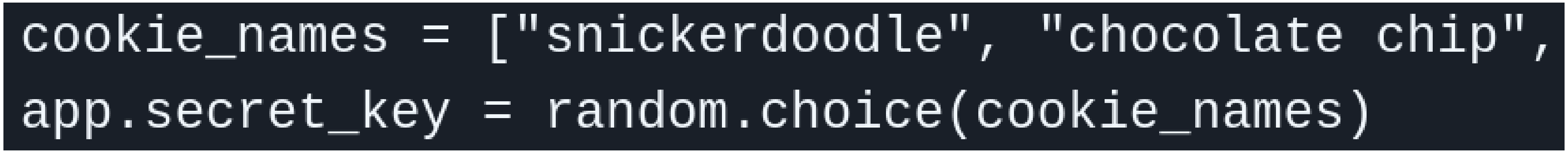
Python Flask Session Tokens



```
cookie_names = ["snickerdoodle", "chocolate chip",
app.secret_key = random.choice(cookie_names)
```

Flask session tokens are encrypted using a secret string; and if we were able to capture or brute force this secret, we could create our own valid Flask session tokens

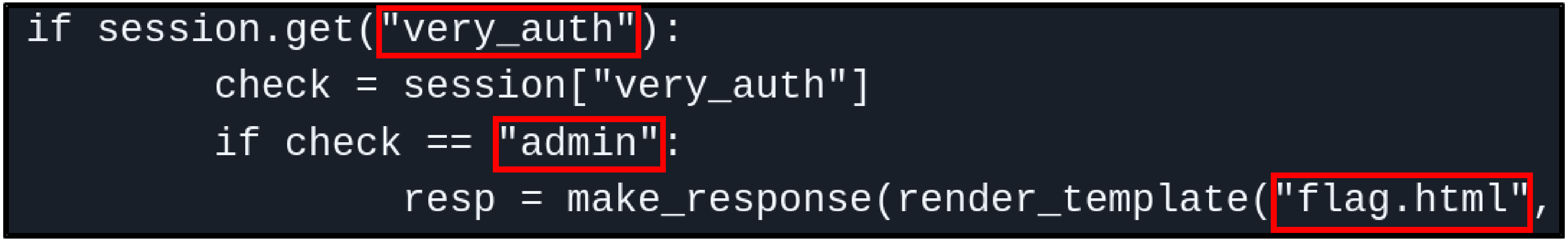
Python Flask Session Tokens



```
cookie_names = ["snickerdoodle", "chocolate chip",
app.secret_key = random.choice(cookie_names)
```

Since we have the code, we know that this app uses a random item from the `cookie_names` list as the value of the secret key

Python Flask Session Tokens



```
if session.get("very_auth"):
        check = session["very_auth"]
        if check == "admin":
                resp = make_response(render_template("flag.html",
```

The code also lets us know that if the data embedded in the cookie has `very_auth=admin` then the flag will be revealed