逻辑漏洞

北京联合大学 glzjin

能力要求

- 能梳理系统的业务流程，找出其中不合理的地方，并加以利用

安全的问题，归根到底，其实都是人的问题。

—别管谁说的了

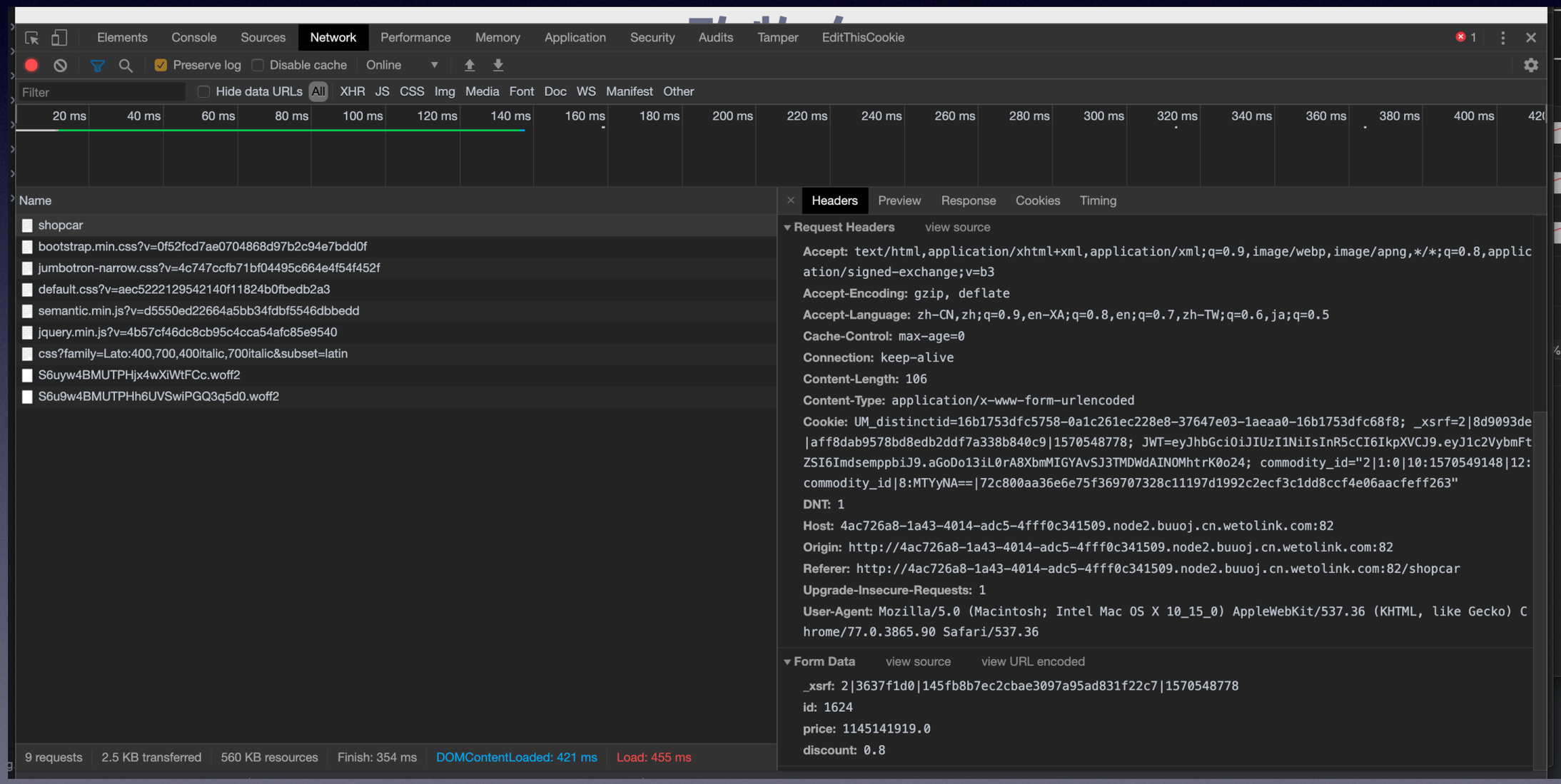
[CISCN2019 华北赛区 Day1 Web2]ikun（薅羊毛）

[CISCN2019 华北赛区 Day1 Web2]ikun

- 正常购买

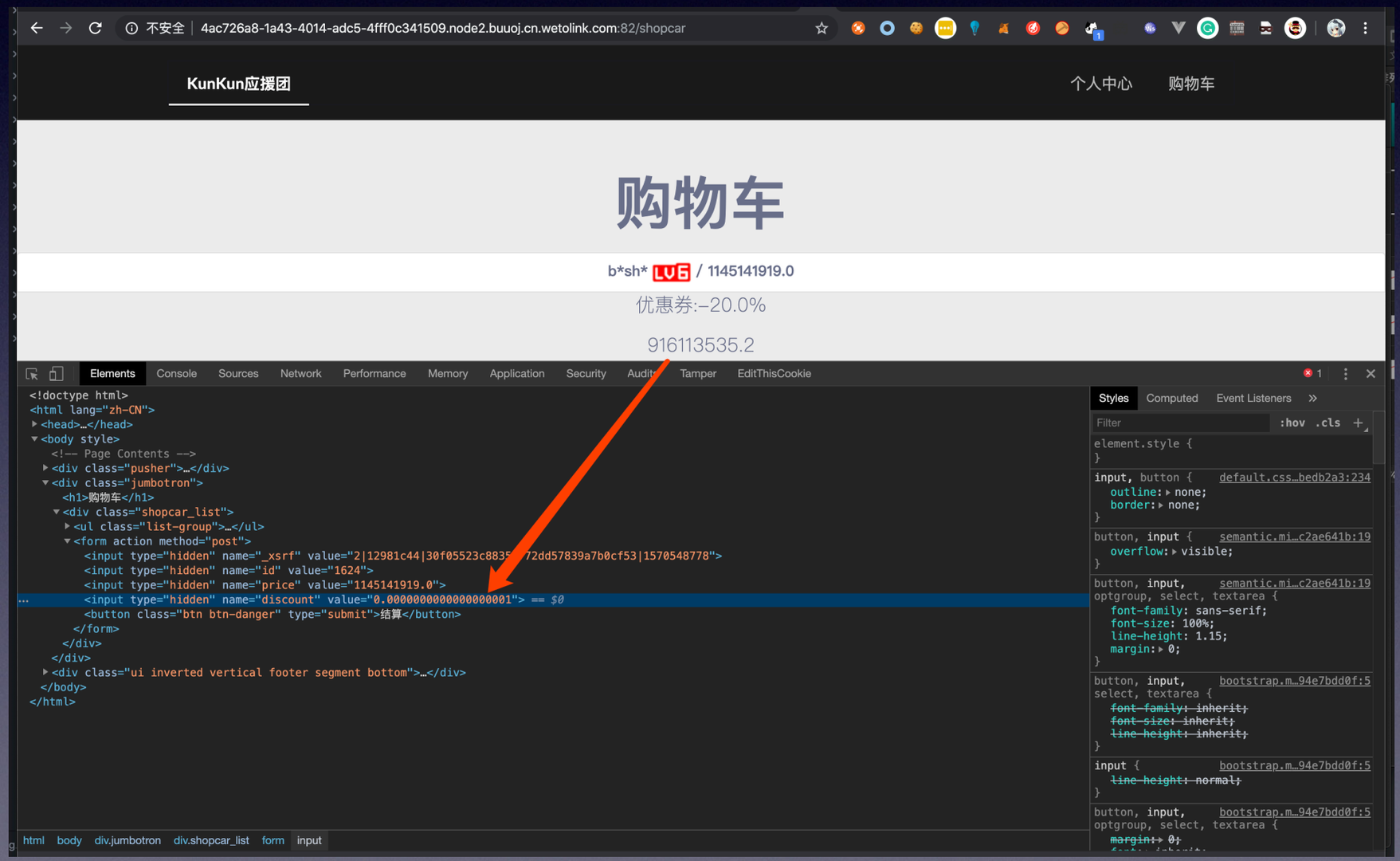
[CISCN2019 华北赛区 Day1 Web2]ikun

- 抓包分析



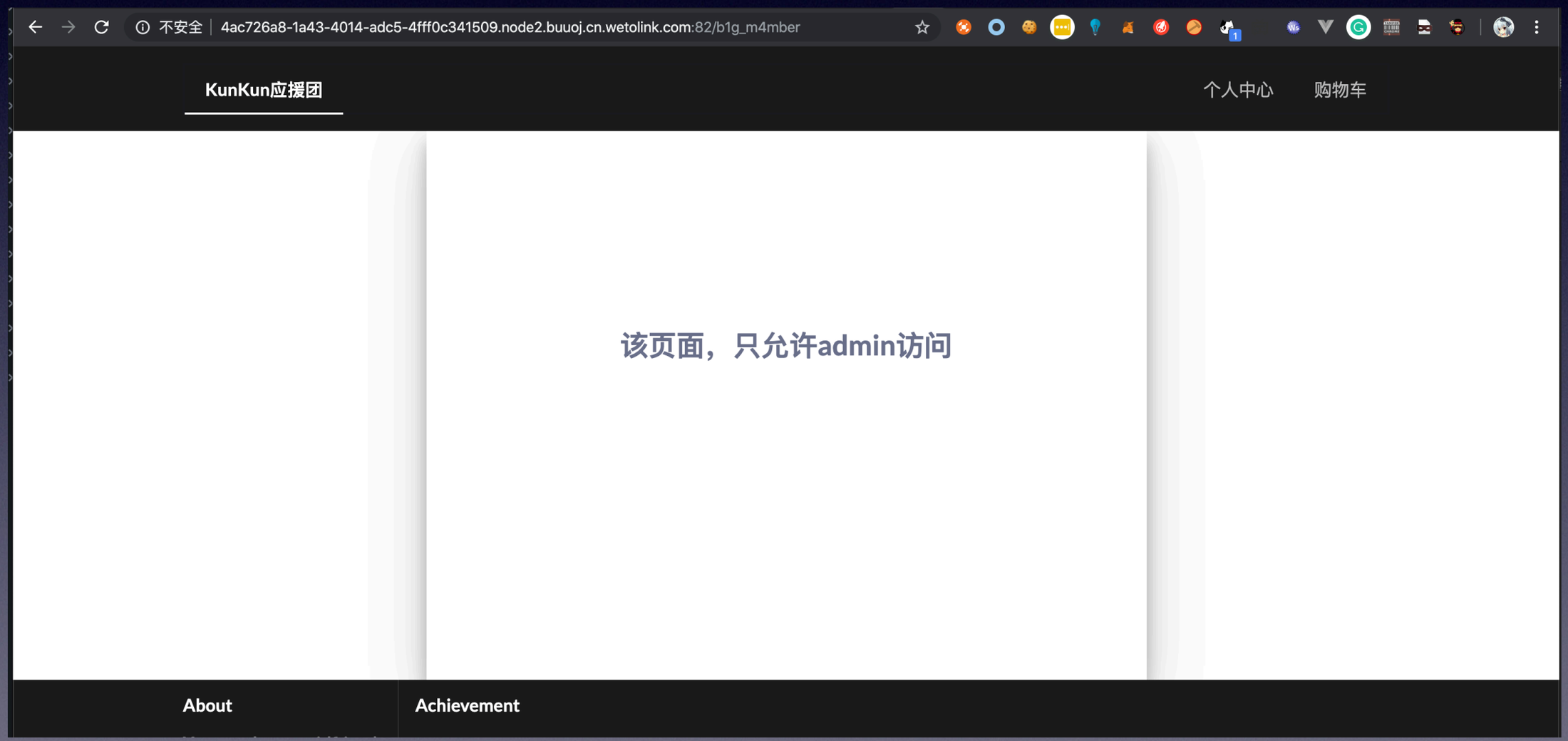
[CISCN2019 华北赛区 Day1 Web2]ikun

- F12 修改元素

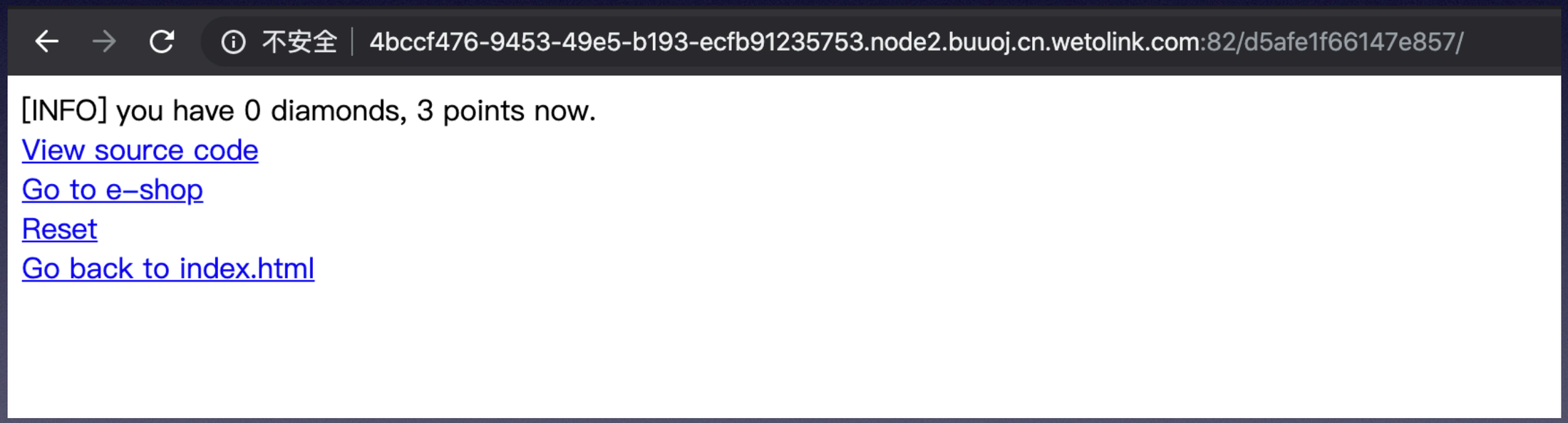


[CISCN2019 华北赛区 Day1 Web2]ikun

- 购买成功之后跳转页面



[DDCTF 2019]homebrew event loop



[DDCTF 2019]homebrew event loop

- 代码审计

不安全 | 4bccf476-9453-49e5-b193-ecfb91235753.node2.buuoj.cn.wetolink.com:82/d5afe1f66147e857/?action:index;True%23False

Download this .py file
Go back to index.html

```
from flask import Flask, session, request, Response
import urllib

app = Flask(__name__)
app.secret_key = '**********'  # censored
url_prefix = '/d5afe1f66147e857'


def FLAG():
    return '**********'  # censored


def trigger_event(event):
    session['log'].append(event)
    if len(session['log']) > 5:
        session['log'] = session['log'][-5:]
    if type(event) == type([]):
        request.event_queue += event
    else:
        request.event_queue.append(event)


def get_mid_str(haystack, prefix, postfix=None):
    haystack = haystack[haystack.find(prefix)+len(prefix):]
    if postfix is not None:
        haystack = haystack[:haystack.find(postfix)]
    return haystack


class RollBackException:
    pass


def execute_event_loop():
    valid_event_chars = set(
        'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_0123456789:;#')
    resp = None
    while len(request.event_queue) > 0:
        # `event` is something like "action:ACTION;ARGS0#ARGS1#ARGS2....."
        event = request.event_queue[0]
```

[DDCTF 2019]homebrew event loop

- 需求：有五个钻石，才能得到 FLAG
- 现状：只有三块钱，可以买三个钻石。可以通过 URL 调用带 _function 或者 _handler 的函数。在 session 里有调用函数的历史记录。
- 分析：购买钻石的函数是先加钻石数，再触发扣减钱数，只要能通过某些方法在钻石数增加到五个的时候去调用获取 FLAG 的函数，让其留下历史记录，即可拿到 FLAG。

[DDCTF 2019]homebrew event loop

- 操作：
  - 先正常购买三个钻石。
  - 访问 /d5afe1f66147e857/?action:trigger_event%23;action:buy;1%23action:buy;1%23action:get_flag;1
    - 同时购买两个钻石并获取 FLAG
  - 解码 cookie，得到 flag。
- 成因：
  - 购买操作不具有原子性，先加钻石再扣减钱数，中间可以插入其他操作。

2014 年魅族账号系统任一账户密码重置

2014 年魅族账号系统任一账户密码重置

2014 年魅族账号系统任一账户密码重置

- 成因：
- https://www.zhaoj.in/read-196.html
- 时间太久我忘了- -||
- 不过现在看起来是对验证码请求的输入没有校验，直接使用，导致能任意接收其他人的验证码。

总结与练习

- 此点不常出现，但一旦出现题一般就会非常有意思。
- 平常测试的时候多思考业务流程，从中寻找漏洞，会有意想不到的发现。
- 练习：
  - [CISCN2019 华北赛区 Day1 Web2]ikun
  - [DDCTF 2019]homebrew event loop