GROUP2

挖掘漏洞的奇幻之旅

- ECB漏洞工具之開發
- ZERO DAY挖掘

動機

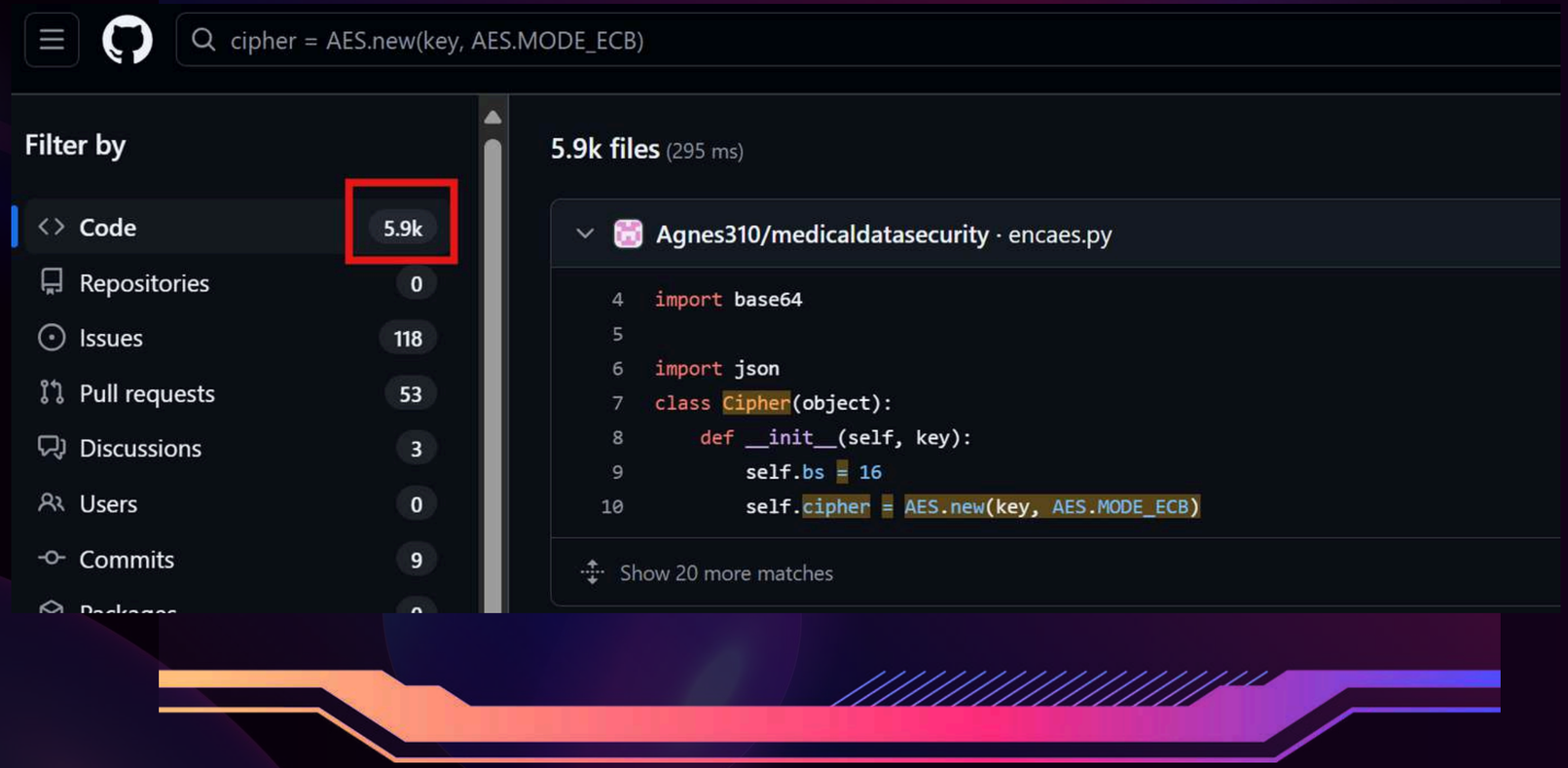
一切的一切從 CRYLOGGER : Detecting Crypto Misuses Dynamically 這篇論文開始 .....

pycrypto

ECB漏洞工具之開發

cipher = AES.new(key, AES.MODE_ECB)

動機



ECB 漏洞工具之開發

RELATED WORK

理想很豐滿現實很骨感

Bandit	Python	靜態	一般安全性掃描（弱點檢查）	透過 AST 分析 Python 原始碼，檢查是否使用了不安全函式或模式（如 eval()、弱加密）
Semgrep	多種語言（含 Python JavaScript、Go 等）	靜態	靈活的安全規則檢查與程式分析（包含加密誤用）	使用自訂語法模式規則（rule-based matching），快速找出程式中的不當使用情境
CryptoGuard	Java	靜態	Java 加密誤用檢查（如弱金鑰、ECB）	使用 bytecode 分析 + 資料流追蹤（data-flow analysis），找出密碼 API 誤用
CryLogger	Android Java	動態	加密 API 誤用檢查（實際執行中分析）	利用 instrumentation（如 Monkey 模擬操作）執行 App 並攔截/記錄密碼 API 使用情形後，離線檢查參數是否合法
AFL++	C/C++ 等	動態（模糊測試）	找出程式中可能出現的漏洞或崩潰路徑（fuzzing）	基於 AFL 的模糊測試技術，透過突變輸入與 coverage-guided feedback 來發現潛在錯誤點

ECB 漏洞工具之開發

BANDIT

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: .\bandit/opsany.py
Line number: 38
More info: https://bandit.readthedocs.io/en/1.8.3/plugins/b324_hashlib.html

```
37              """
38              key = hashlib.md5(key.encode('utf-8')).digest()
39              cipher = AES.new(key, AES.MODE_ECB)
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: .\bandit/opsany.py
Line number: 56
More info: https://bandit.readthedocs.io/en/1.8.3/plugins/b324_hashlib.html

```
55
56              key = hashlib.md5(key.encode('utf-8')).digest()
```

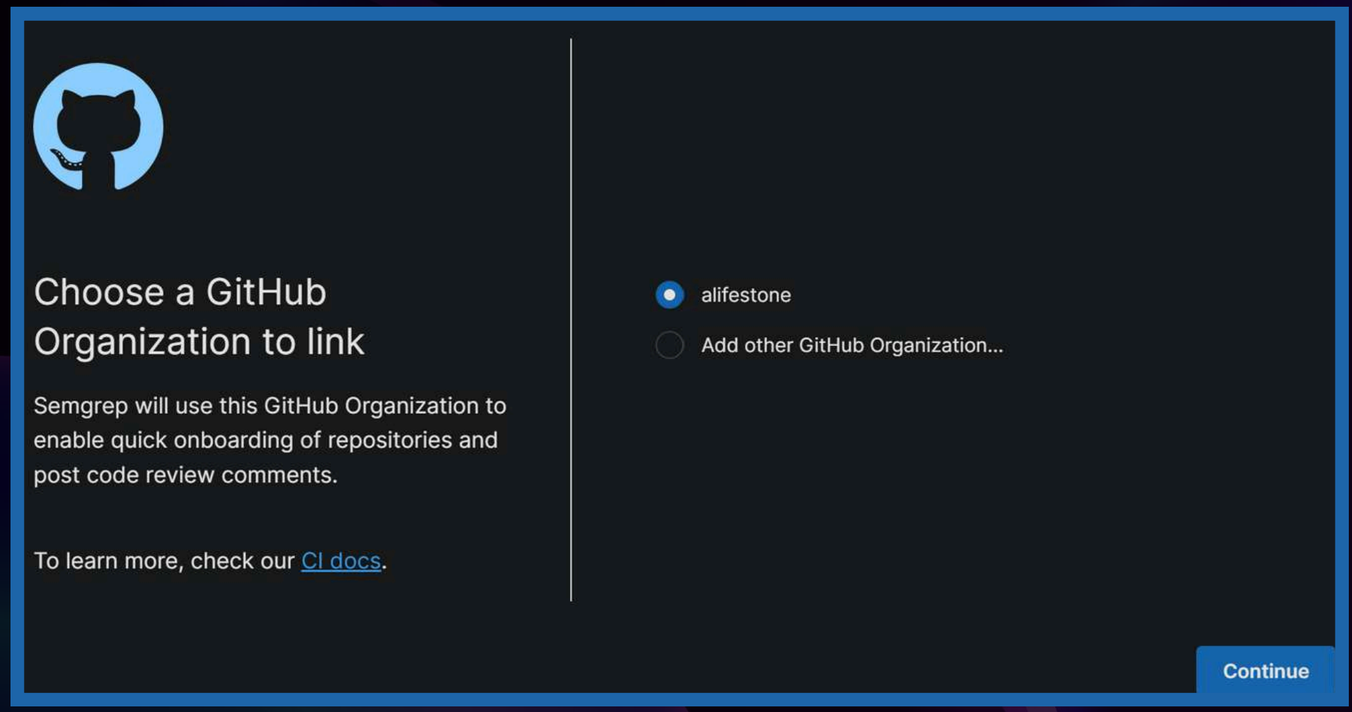
ECB 漏洞工具之開發

SEMGREP

```
ifestone@DESKTOP-0D33E7R:~$ semgrep scan opsany-paas-main/

  ooo
 Semgrep CLI

METRICS: Using configs from the Registry (like --config=p/ci) reports pseudonymous rule metrics to semgrep.dev.
To disable Registry rule metrics, use "--metrics=off".
Using configs only from local files (like --config=xyz.yml) does not enable metrics.

More information: https://semgrep.dev/docs/metrics

Scanning 6863 files (only git-tracked) with:

✔ Semgrep OSS
  ✔ Basic security coverage for first-party code vulnerabilities.

✔ Semgrep Code (SAST)
  ✔ Find and fix vulnerabilities in the code you write with advanced scanning and expert security rules.

✗ Semgrep Supply Chain (SCA)
  ✗ Find and fix the reachable vulnerabilities in your OSS dependencies.

-                                                    2% 0:03:06
```

ECB 漏洞工具之開發

SEMGREP



ECB漏洞工具之開發

自動爬取github

bandit掃描

後綴攻擊

ECB漏洞工具之開發

DEMO !!!

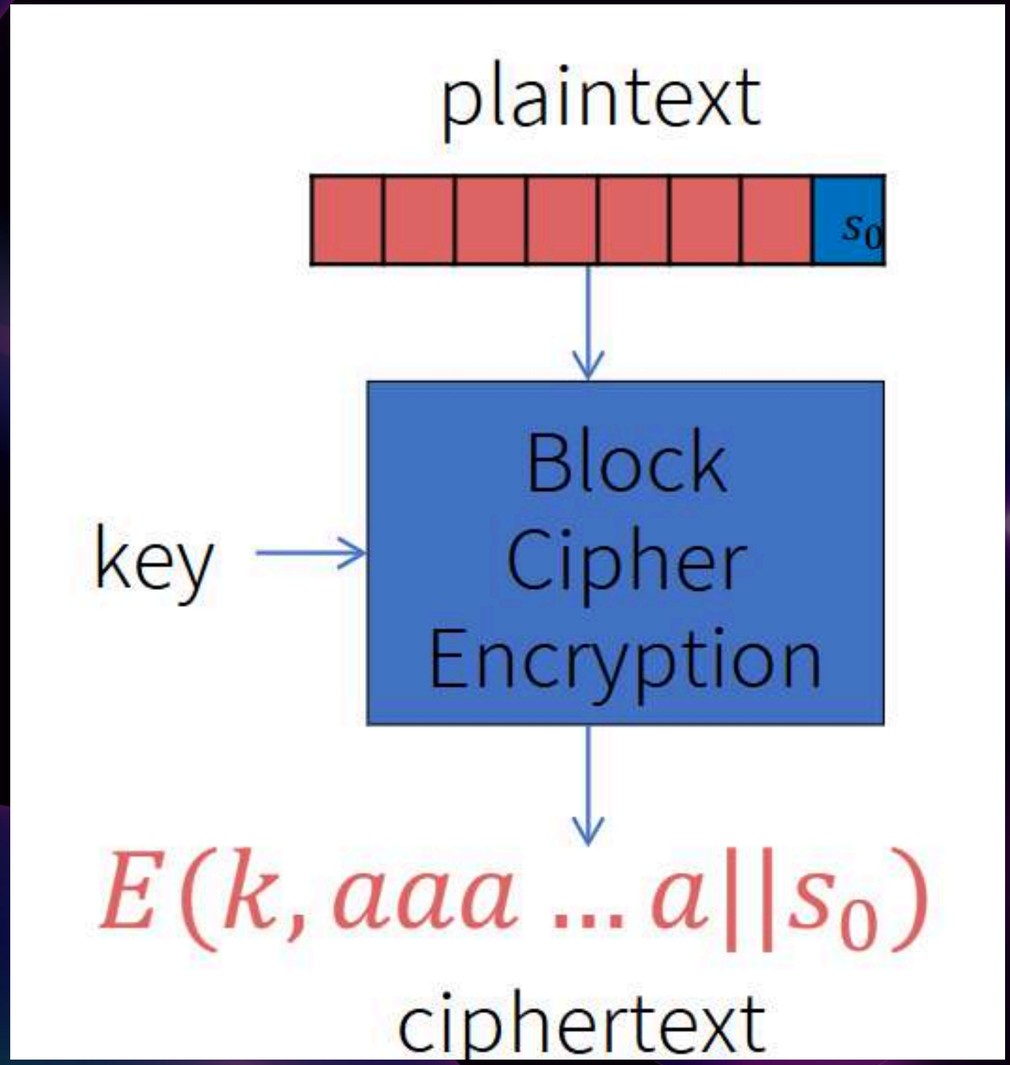
ECB 漏洞工具之開發

Encryption Oracle Attack

Let $E(k,\cdot)$ be a block cipher encryption in the ECB mode

Assumption: attacker can control A, and the oracle will return $E(k, P||A||S)$

ECB 漏洞工具之開發


plaintext
s_0
Block Cipher Encryption
key
$E(k, aaa \ldots a||s_0)$
ciphertext

REFEREN

用 Bandit 靜態掃描工具，掃描 Python 專案中的安全性問題

這陣子看了 10 common security gotchas in Python and how to avoid the
該文章主要介紹幾種撰寫 Python 程式時需注意的安全問題，例如處理來自外部的 XM
YAML 檔案等可能會面臨的安全性問題，相當□得一讀，保證精彩。 該文的最後也

MyApollo / Mar 24, 2019

Semgrep

Quickstart

Learn how to set up Semgrep and scan your first repository.

semgrep.dev

tabneib/**ecbacp**

Simple tool for ECB adaptive chosen plaintext attack

1 Contributor · 0 Issues · 3 Stars · 1 Fork

tabneib/ecbacp: Simple tool for ECB adaptive chosen plaintext attack

Simple tool for ECB adaptive chosen plaintext attack - tabneib/ecbacp

GitHub

https://github.com/keybase/kbpgp
https://github.com/belldandyxtq/MA_cheater
https://github.com/programa-stic/snapchat-decrypt
https://github.com/TinyNiko/mac_wxapkg_decrypt
https://github.com/HG-ha/ICP_Query
https://github.com/huuck/Katalina
https://github.com/superchromia/telepy_old
https://github.com/pxdl/nxshot
https://github.com/ricpacca/cryptopals
https://github.com/CHERWING/CHERWIN_SCRIPTS
https://github.com/hasherezade/crypto_utils
https://github.com/OpenIPC/burn
https://github.com/jasonacox/tuyapower
https://github.com/microsoft/grover-blocks
https://github.com/daiyanan1992/qinglongtest
https://github.com/Ralim/TC66C
https://github.com/sonya75/pooky-bypass
https://github.com/CymatiCorp/CyKit
https://github.com/jbirkholz/webusbAuth
https://github.com/tweksteen/jenkins-decrypt
https://github.com/jbuehl/solaredge/blob/98ce3bdf2cdb483ced8f6f0eb77921f842c3b4cd/se/msg.py
https://github.com/jbuehl/solaredge
https://github.com/yadox666/WiFi_CCC/blob/d405d65ae7eba468025a1694a6e97db60cb6a108/wifichat.py
https://github.com/yadox666/WiFi_CCC
https://github.com/leverimmy/THU-Annual-Eat/blob/613ff23e8874f99da2509167f8812e849c4ad428/main.py
https://github.com/leverimmy/THU-Annual-Eat
https://github.com/4w4k3/Insanity-Framework/blob/cf51ff35b01a4de6f3c3c07299f0899143150227/enc.py
https://github.com/4w4k3/Insanity-Framework

ECB 漏洞工具之開發

漏洞專案

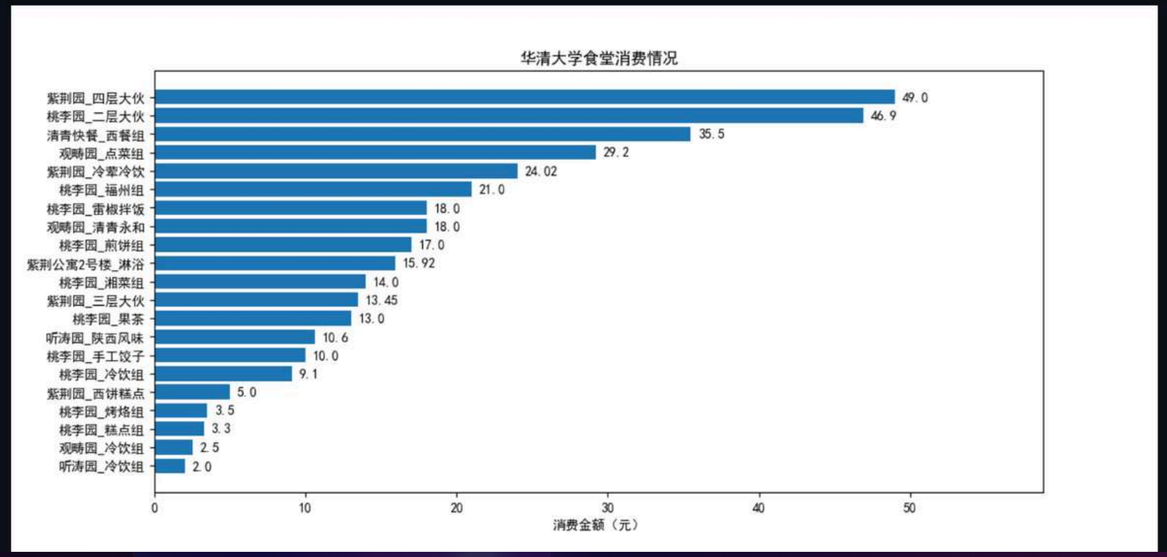
THU-Annual-Eat

一年过去了，你在华子食堂里花的钱都花在哪儿了？

项目简介

> 项目的 idea 来源于 Rose-max111。

本项目是一个用于统计华清大学学生在食堂（和宿舍）的消费情况的脚本。通过模拟登录华清大学校园卡网站，获取学生在华子食堂的消费记录，并通过数据可视化的方式展示。



清華大學 校园卡综合服务
Tsinghua University Campus Card Service

ENGLISH

首頁 通知公告 服務大廳 資訊查詢 登入 商家入口

請輸入關鍵字 搜尋

重要訊息 | 通知公告

看更多

22
2025-01
服務管道
新版校園卡提供綜合服務網站、微信小程式(「清華校園卡」)、自助服務機三種自助服務形式，支援儲值、掛失、解掛、密碼修改、流水查詢、自助補卡（自助服務機）等服務內容。

19
2024-12
教職員家屬副卡校園碼申辦與使用指南
教職員家屬副卡校園碼申辦與使用指南

19
2024-12
因公短期訪客校園碼申辦及使用指南
因公短期訪客校園碼申辦及使用指南

16
2024-12
清華大學校園碼應用管理規範（試行）
清華大學校園碼應用管理規範（試行）

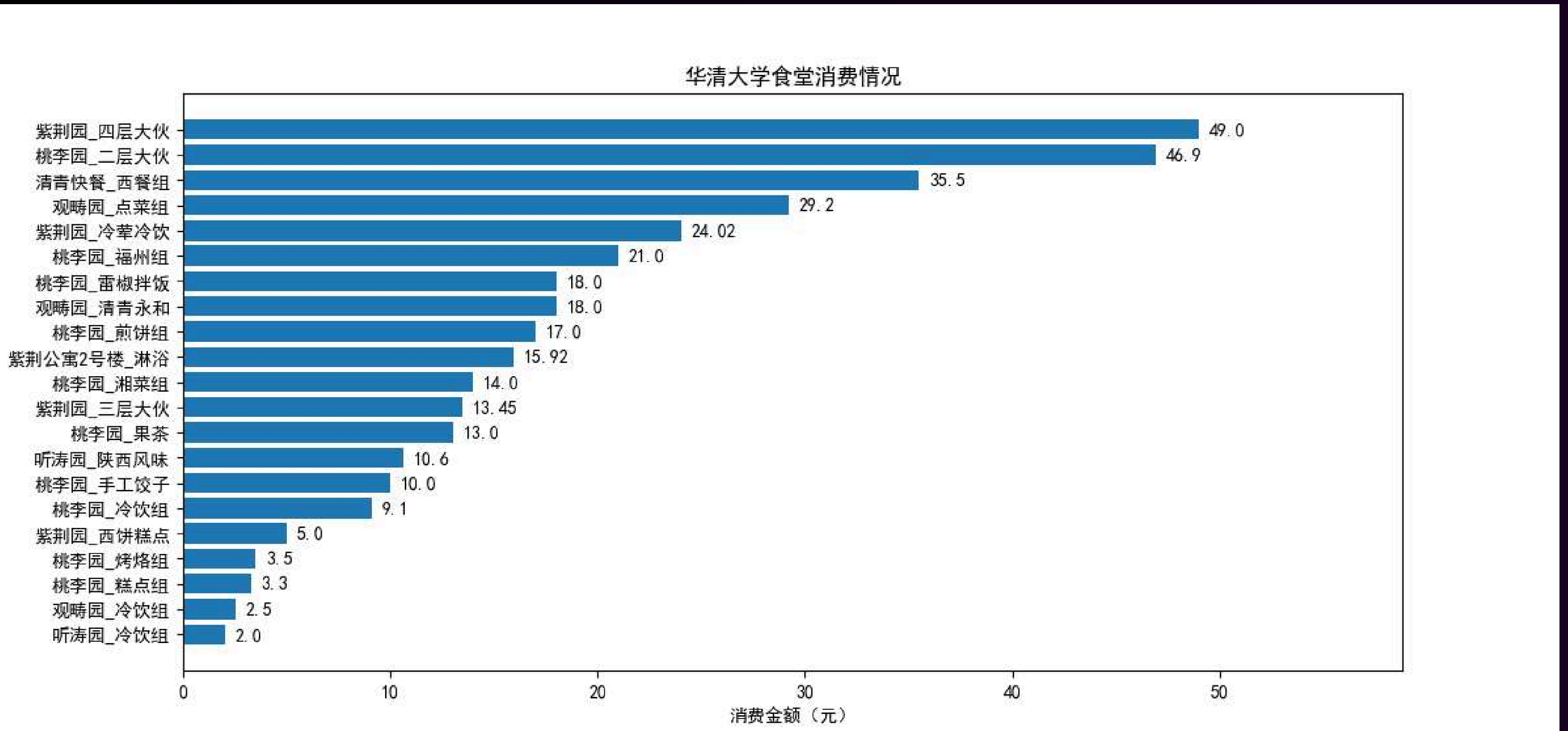
POPULAR APPS
熱門應用

交易记录查询

开始时间 2024/12/14 结束时间 2024/12/21 查询类型 所有

重置 查询 EXCEL导出

交易地点	交易金额（元）	交易时间	交易事件	余额（元）
紫荆公寓2号楼	0.08	2024-12-20 11:31:39	持卡人消费	81.63
紫荆公寓2号楼	3.20	2024-12-20 11:31:15	持卡人消费	81.71
紫荆园	5.00	2024-12-19 12:33:10	持卡人消费	84.91
紫荆园	1.60	2024-12-19 12:08:39	持卡人消费	89.91
紫荆园	10.00	2024-12-19 12:02:09	持卡人消费	91.51
在线充值	100.00	2024-12-19 12:01:47	微信充值	101.51
紫荆园	3.50	2024-12-19 12:01:11	持卡人消费	1.51

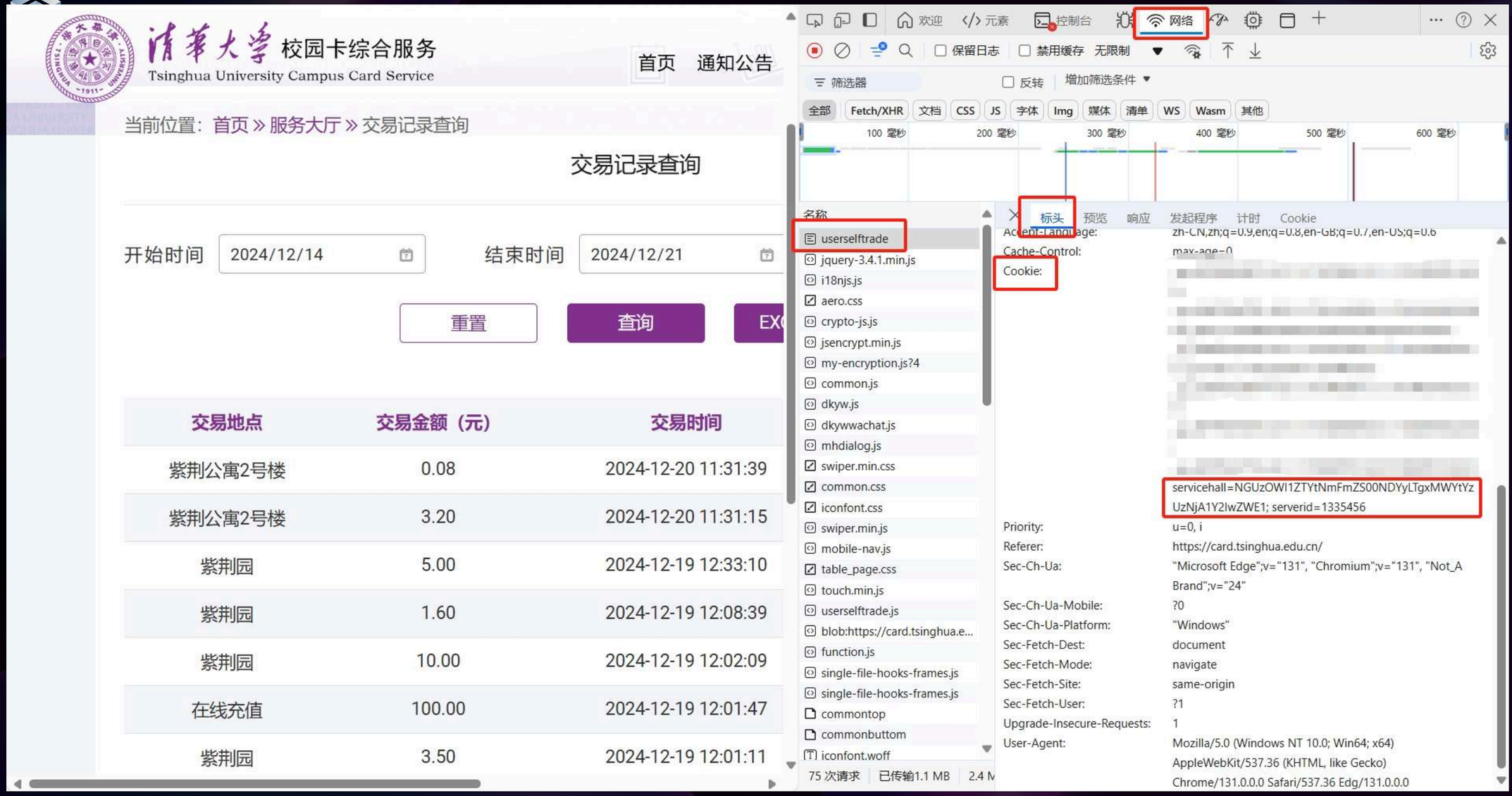

华清大学食堂消费情况
紫荆园_四层大伙
桃李园_二层大伙
清青快餐_西餐组
观畴园_点菜组
紫荆园_冷荤冷饮
桃李园_福州组
桃李园_雷椒拌饭
观畴园_清青永和
桃李园_煎饼组
紫荆公寓2号楼_淋浴
桃李园_湘菜组
紫荆园_三层大伙
桃李园_果茶
听涛园_陕西风味
桃李园_手工饺子
桃李园_冷饮组
紫荆园_西饼糕点
桃李园_烤烙组
桃李园_糕点组
观畴园_冷饮组
听涛园_冷饮组
49.0
46.9
35.5
29.2
24.02
21.0
18.0
18.0
17.0
15.92
14.0
13.45
13.0
10.6
10.0
9.1
5.0
3.5
3.3
2.5
2.0
0
10
20
30
40
50
消费金额（元）

ECB漏洞工具之開發

清大專案架構

登入帳號獲得Cookie → 將學號與Cookie丟給後端獲得密文 → 密文解密獲取Data

ECB漏洞工

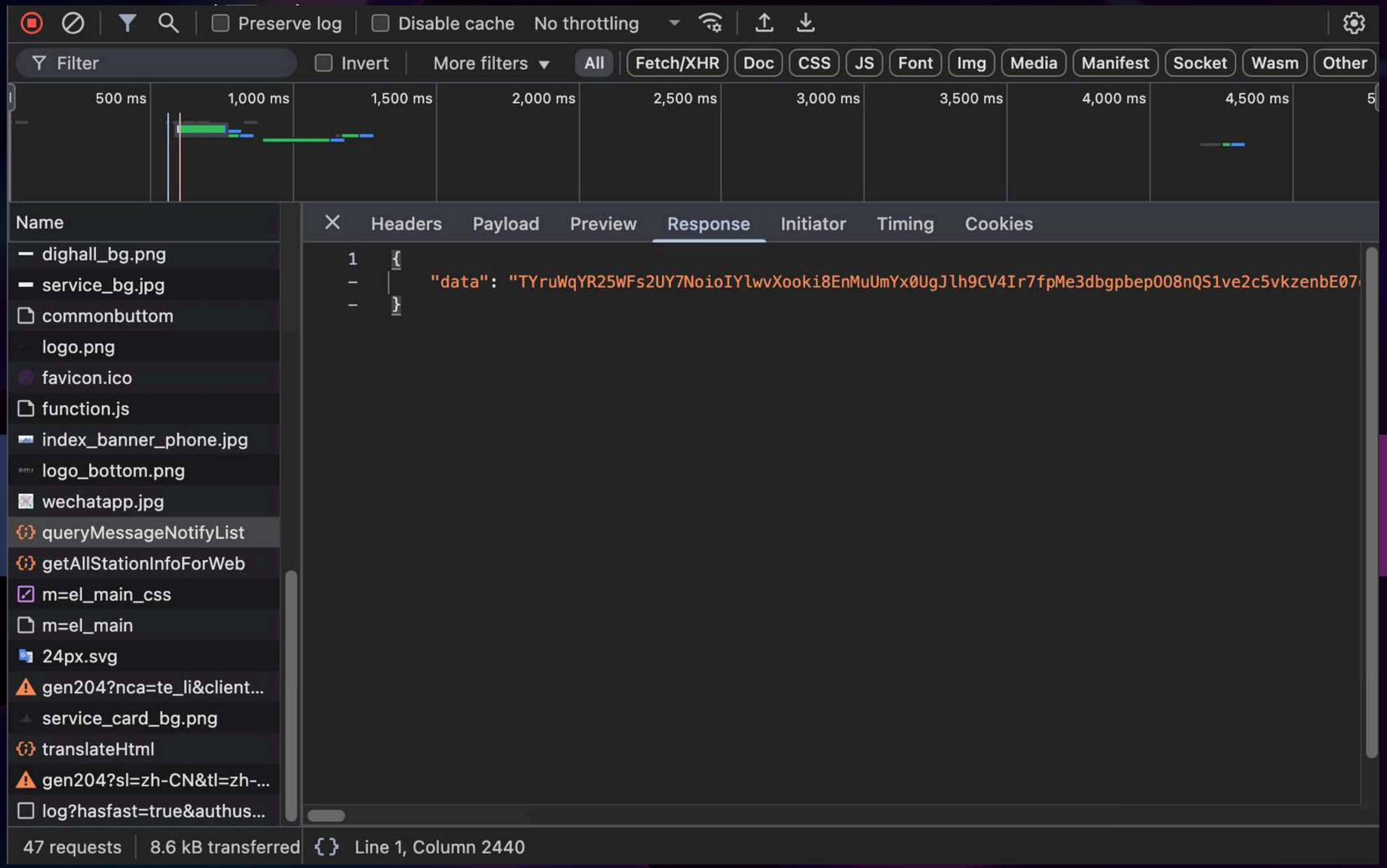

清華大學 校园卡综合服务
Tsinghua University Campus Card Service
首页 通知公告
当前位置：首页 » 服务大厅 » 交易记录查询
交易记录查询
开始时间 2024/12/14
结束时间 2024/12/21
重置
查询
交易地点 交易金额（元） 交易时间
紫荆公寓2号楼 0.08 2024-12-20 11:31:39
紫荆公寓2号楼 3.20 2024-12-20 11:31:15
紫荆园 5.00 2024-12-19 12:33:10
紫荆园 1.60 2024-12-19 12:08:39
紫荆园 10.00 2024-12-19 12:02:09
在线充值 100.00 2024-12-19 12:01:47
紫荆园 3.50 2024-12-19 12:01:11
欢迎 元素 控制台 网络
保留日志 禁用缓存 无限制
筛选器 反转 增加筛选条件
全部 Fetch/XHR 文档 CSS JS 字体 Img 媒体 清单 WS Wasm 其他
100 毫秒 200 毫秒 300 毫秒 400 毫秒 500 毫秒 600 毫秒
名称
userselftrade
jquery-3.4.1.min.js
i18njs.js
aero.css
crypto-js.js
jsencrypt.min.js
my-encryption.js?4
common.js
dkyw.js
dkywwachat.js
mhdialog.js
swiper.min.css
common.css
iconfont.css
swiper.min.js
mobile-nav.js
table_page.css
touch.min.js
userselftrade.js
blob:https://card.tsinghua.e...
function.js
single-file-hooks-frames.js
single-file-hooks-frames.js
commontop
commonbuttom
iconfont.woff
75 次请求 已传输1.1 MB
标头 预览 响应 发起程序 计时 Cookie
Cache-Control: max-age=0
Cookie:
servicehall=NGUzOWI1ZTYtNmFmZS00NDYyLTgxMWYtYzUzNjA1Y2lwZWE1; serverid=1335456
Priority: u=0, i
Referer: https://card.tsinghua.edu.cn/
Sec-Ch-Ua: "Microsoft Edge";v="131", "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0

```
{
    "idserial": "你的学号",
    "servicehall": "你的服务代码"
}
```

ECB漏洞工具之開發

清華專案架構

登入帳號獲得Cookie → 將學號與Cookie丟給後端獲得密文 → 密文解密獲取Data


Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
Socket
Wasm
Other
500 ms
1,000 ms
1,500 ms
2,000 ms
2,500 ms
3,000 ms
3,500 ms
4,000 ms
4,500 ms
Name
dighall_bg.png
service_bg.jpg
commonbuttom
logo.png
favicon.ico
function.js
index_banner_phone.jpg
logo_bottom.png
wechatapp.jpg
queryMessageNotifyList
getAllStationInfoForWeb
m=el_main_css
m=el_main
24px.svg
gen204?nca=te_li&client...
service_card_bg.png
translateHtml
gen204?sl=zh-CN&tl=zh-...
log?hasfast=true&authus...
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
1 {
"data": "TYruWqYR25WFs2UY7NoioIYlwvXooki8EnMuUmYx0UgJlh9CV4Ir7fpMe3dbgpbepOO8nQS1ve2c5vkzenbE07
}
47 requests
8.6 kB transferred
{ } Line 1, Column 2440

ECB 漏洞工具之開發

解密方式！？

```python
def decrypt_aes_ecb(encrypted_data: str) -> str:

    key = encrypted_data[:16].encode('utf-8')
    encrypted_data = encrypted_data[16:]
    encrypted_data_bytes = base64.b64decode(encrypted_data)

    cipher = AES.new(key, AES.MODE_ECB)

    decrypted_data = unpad(cipher.decrypt(encrypted_data_bytes), AES.block_size)

    return decrypted_data.decode('utf-8')
```

ECB 漏洞工具之開發

問題

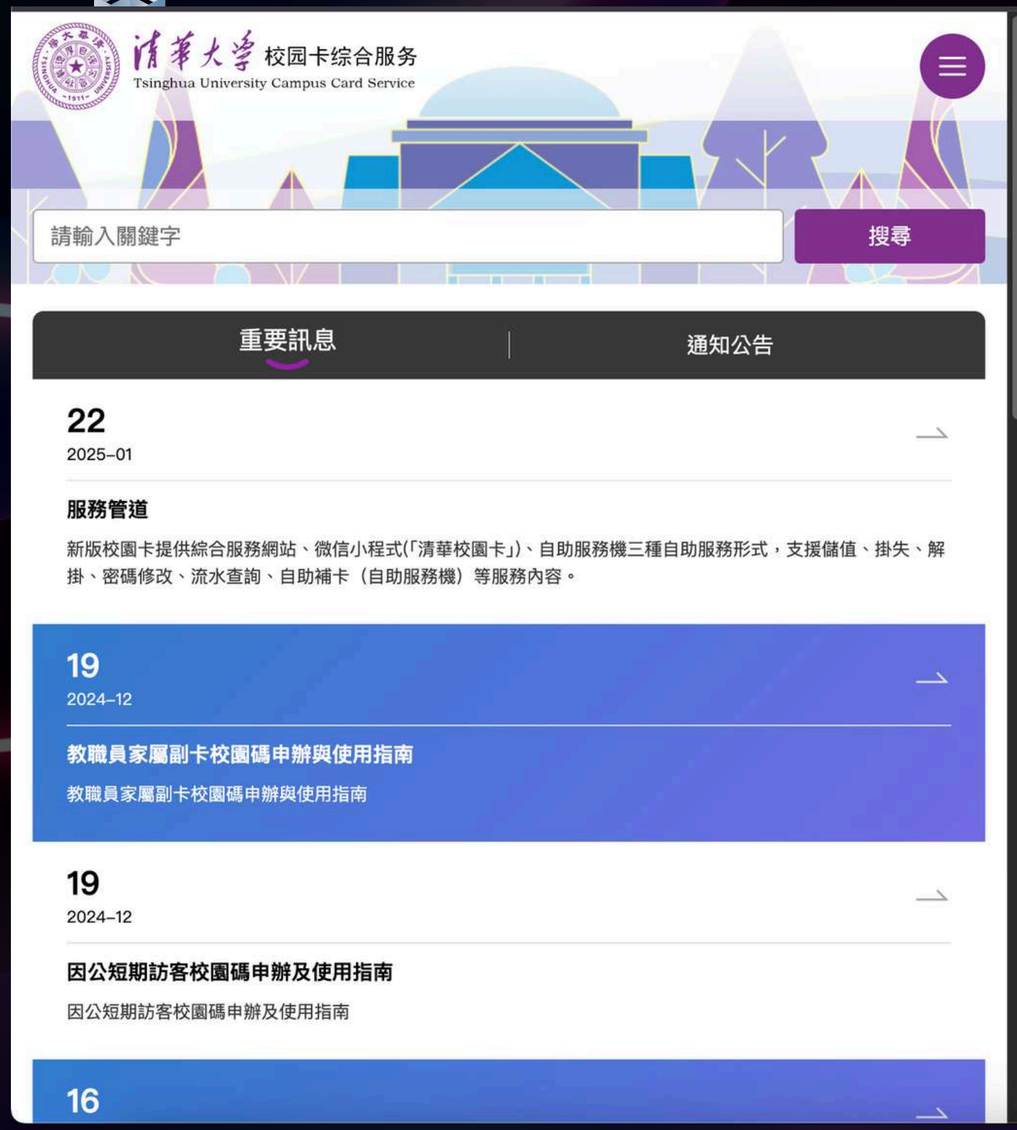
- 使用不安全的 AES-ECB 模式
  → 相同明文區塊會產生相同密文
- 密鑰直接包含在密文中
  → 前 16 字元為 key，任何人都能解密
- 缺乏完整性驗證（無 MAC）
  → 密文可被偽造，前端仍照常解密顯示
- 加密無明確目的，無法提供真正保護
  → 既非防止竊聽，也無法防篡改
- 前端完全信任解密結果
  → 一旦密文被替換，用戶即被誤導

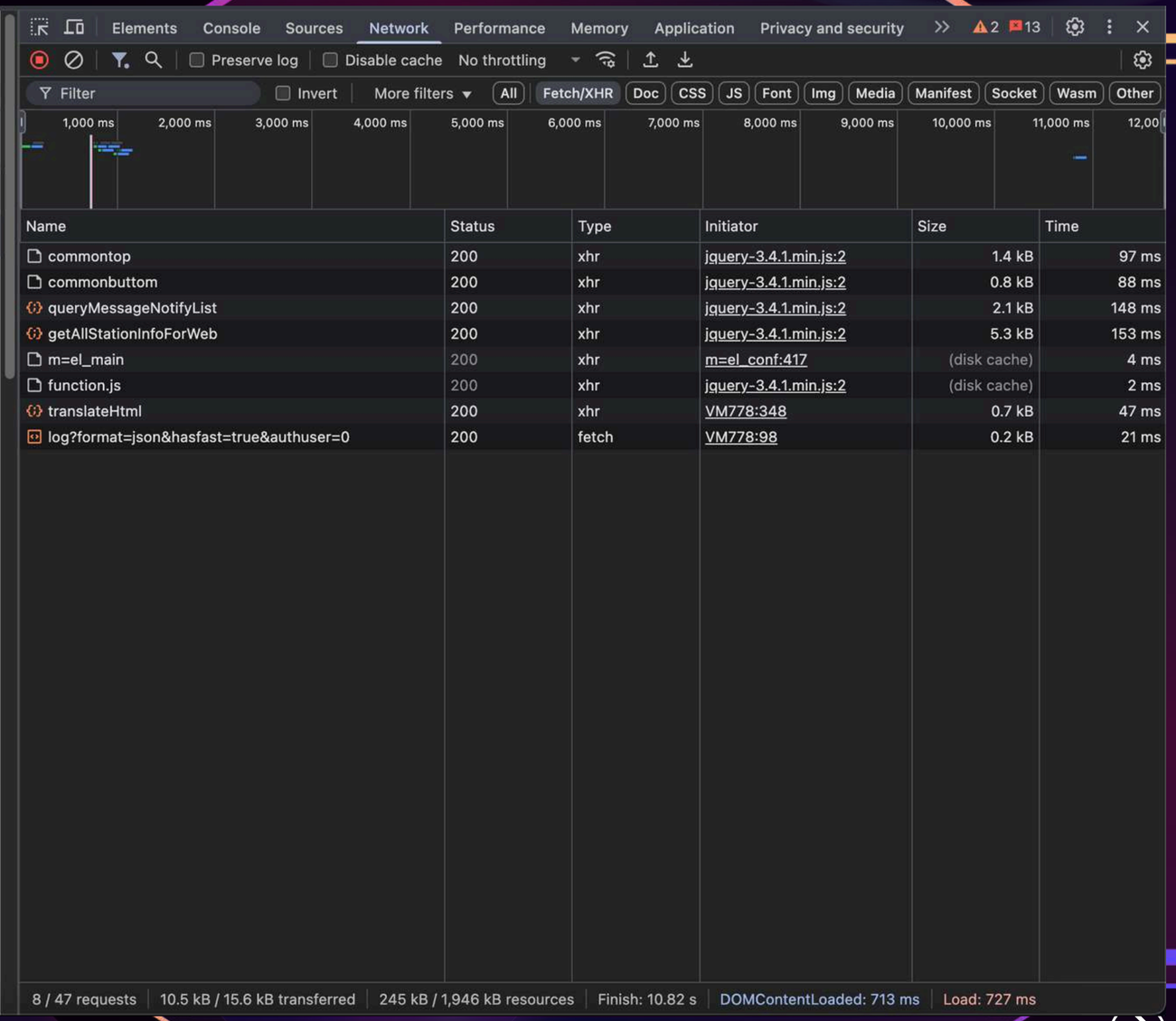
ECB漏洞工具之開發

其他發現

- 網站上其他api均用此方法加密

ECB漏洞工


清華大學 校園卡综合服务
Tsinghua University Campus Card Service
請輸入關鍵字
搜尋
重要訊息
通知公告
22
2025–01
服務管道
新版校園卡提供綜合服務網站、微信小程式(「清華校園卡」)、自助服務機三種自助服務形式，支援儲值、掛失、解掛、密碼修改、流水查詢、自助補卡（自助服務機）等服務內容。
19
2024–12
教職員家屬副卡校園碼申辦與使用指南
教職員家屬副卡校園碼申辦與使用指南
19
2024–12
因公短期訪客校園碼申辦及使用指南
因公短期訪客校園碼申辦及使用指南
16

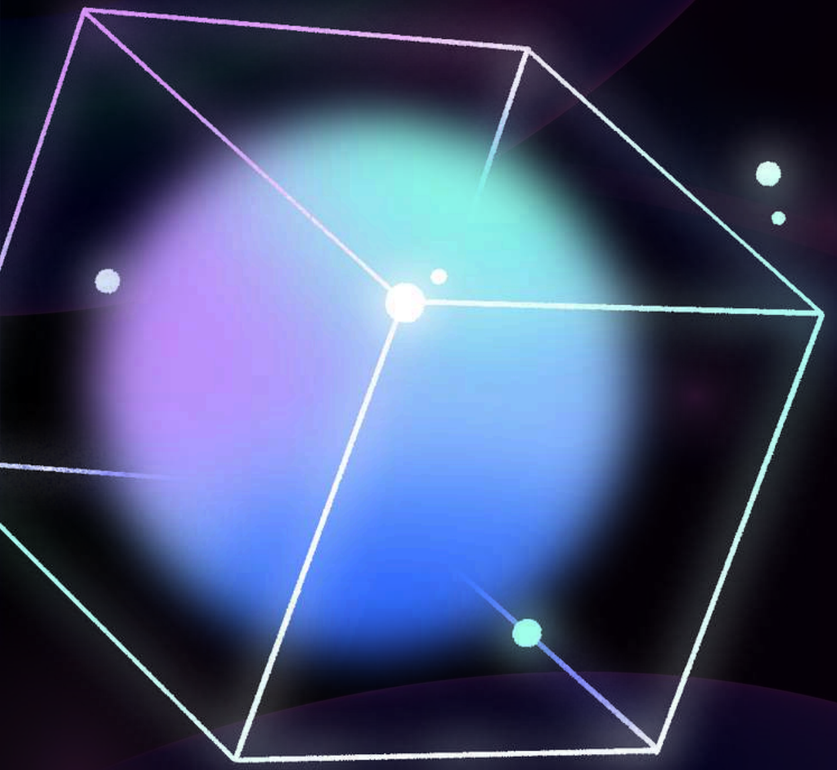

Elements Console Sources Network Performance Memory Application Privacy and security
Preserve log Disable cache No throttling
Filter Invert More filters All Fetch/XHR Doc CSS JS Font Img Media Manifest Socket Wasm Other
1,000 ms 2,000 ms 3,000 ms 4,000 ms 5,000 ms 6,000 ms 7,000 ms 8,000 ms 9,000 ms 10,000 ms 11,000 ms 12,00
Name Status Type Initiator Size Time
commontop 200 xhr jquery-3.4.1.min.js:2 1.4 kB 97 ms
commonbuttom 200 xhr jquery-3.4.1.min.js:2 0.8 kB 88 ms
queryMessageNotifyList 200 xhr jquery-3.4.1.min.js:2 2.1 kB 148 ms
getAllStationInfoForWeb 200 xhr jquery-3.4.1.min.js:2 5.3 kB 153 ms
m=el_main 200 xhr m=el_conf:417 (disk cache) 4 ms
function.js 200 xhr jquery-3.4.1.min.js:2 (disk cache) 2 ms
translateHtml 200 xhr VM778:348 0.7 kB 47 ms
log?format=json&hasfast=true&authuser=0 200 fetch VM778:98 0.2 kB 21 ms
8 / 47 requests 10.5 kB / 15.6 kB transferred 245 kB / 1,946 kB resources Finish: 10.82 s DOMContentLoaded: 713 ms Load: 727 ms

ECB漏洞工具

~/Projects/CNS_Final/THU-Annual-Eat-main python decode.py 09:04:04

{"message":"成功","resultData":[[{"createtime":"2024-01-05 14:18:36","inputuserid":"9451565645100810 48","messageflow":"0","language":"1","title":"照澜院建行自助服务机","content":" 服务时间：周一至周日&nbs p; 9:00-18:30
 服务地址：照澜院建行自助设备区 补卡范围：工作证、校园卡（离退休、其他人员 ） 咨询电话：010-62771940、010-62771942 ","orgid":2,"typecode":"02","pageviews":2,"publishdepa rt":"校园卡中心","name":"自助机信息","context":"1","id":"1060440066481979423","username":"杨倩","status ":"3"},{"createtime":"2024-01-05 14:18:31","inputuserid":"945156564510081048","messageflow":"0","langua ge":"1","title":"老环境楼自助服务机","content":" 服务时间：周一至周日 6:00-22:00
 服务 地址：老环境楼大厅 补卡范围：工作证、校园卡（离退休、其他人员） 咨询电话：010-62771940、010 -62771942 ","orgid":2,"typecode":"02","pageviews":4,"publishdepart":"校园卡中心","name":"自助机信息" ,"context":"1","id":"1060439694581432356","username":"杨倩","status":"3"},{"createtime":"2023-12-07 16: 40:54","inputuserid":"945156564510081048","messageflow":"0","language":"1","title":"李兆基大楼自助服务 机1","content":" 服务时间：周一至周日 24小时开放
 服务地址：李兆基大楼B104-2室 左侧 补 卡范围：工作证、校园卡（离退休、其他人员） 咨询电话：010-62771940、010-62771942 ","orgid":2,"t ypecode":"02","pageviews":5,"publishdepart":"校园卡中心","name":"自助机信息","context":"1","id":"955041 890892279826","username":"杨倩","status":"3"}],[{"createtime":"2023-06-16 16:40:17","inputuserid":"9451 56564510081048","messageflow":"0","language":"1","title":"紫荆C楼自助服务机1","content":" 服务时间： 周一至周日<span lang=\"EN-US\" style=\"font-family: Roboto;\"> 24小时开放
 <p style= \"margin: 0cm 0cm 0.0001pt; line-height: 27pt; background-image: initial; background-position: initial; background-size: initial; background-repeat: initial; background-attachment: initial; background-origi n: initial; background-clip: initial; box-sizing: inherit; width: calc(100% - 40px); color: rgba(0, 0, 0, 0.87);\" data-v-0a6532bc=\"\">服务地址：紫荆C楼102 自助设备区 <p style=\"margin: 0cm 0cm 0.0001pt ; line-height: 27pt; background-image: initial; background-position: initial; background-size: initial; background-repeat: initial; background-attachment: initial; background-origin: initial; background-cli p: initial; box-sizing: inherit; width: calc(100% - 40px);\" data-v-0a6532bc=\"\"><span style=\"color: rgba(0, 0, 0, 0.87);\"><span style=\"mso-ascii-font-family:Roboto;mso-hansi-font-family:Roboto;color:#3 33333\">补卡范围：学生证<span lang=\"EN-US\" style=\"font-family: Roboto;\"><o:p></o:p></ span> <p style=\"margin: 0cm 0cm 0.0001pt; line-height: 27pt; background-image: initial; background-position: initial; background-size: initial; background-repeat: initial; background-attachment: initial

ECB漏洞工具之開發



假想攻擊方式

偽造密文

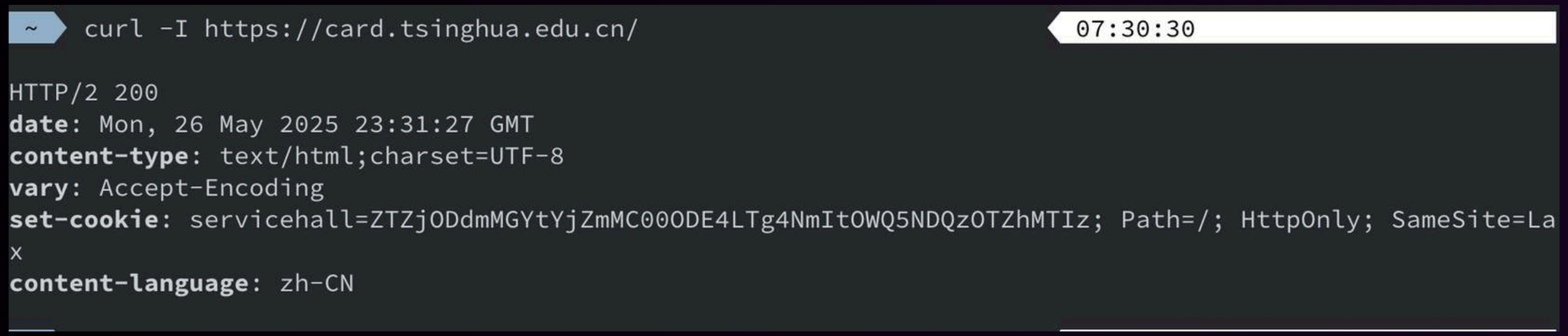
由於加密方法固定（key為前16位元），能隨意偽造

攔截封包與寄偽造密文到前端

沒有驗證機制，得到密文若符合格式就能縣市在前端

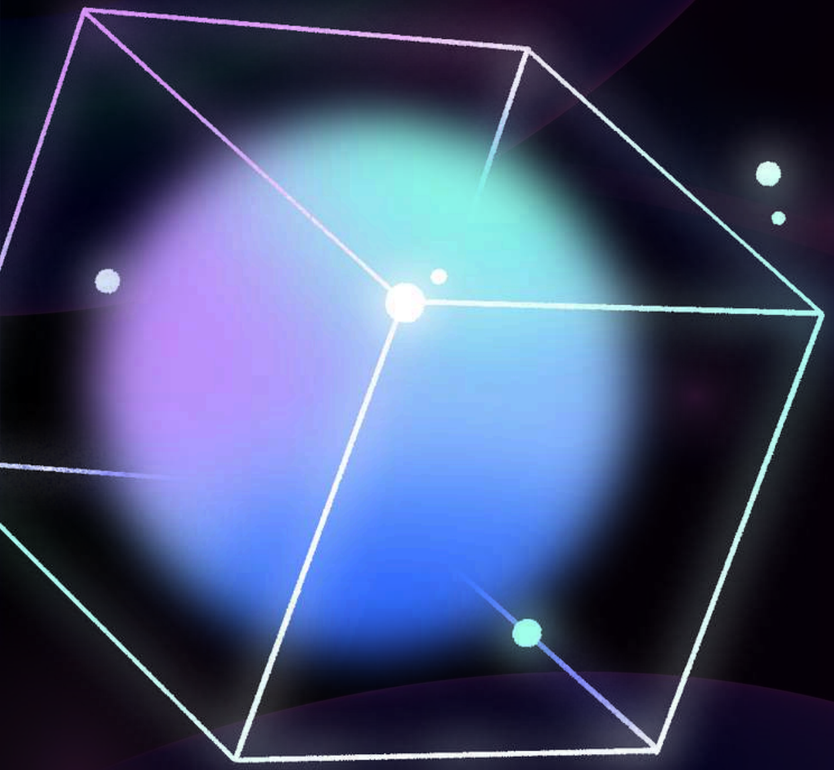
欺騙個資

例如：假消費紀錄、假公告、假登入要求



能進行降級攻擊(sslstrip)
沒HSTS

結論



結論

Bandit工具

目前搜集偵測功能完善，但exploit部分還能增加及改善

清華專案

實際找到網站漏洞（沒HSTS, MAC, 金鑰跟著密文傳輸），但模擬攻擊還未實作完全

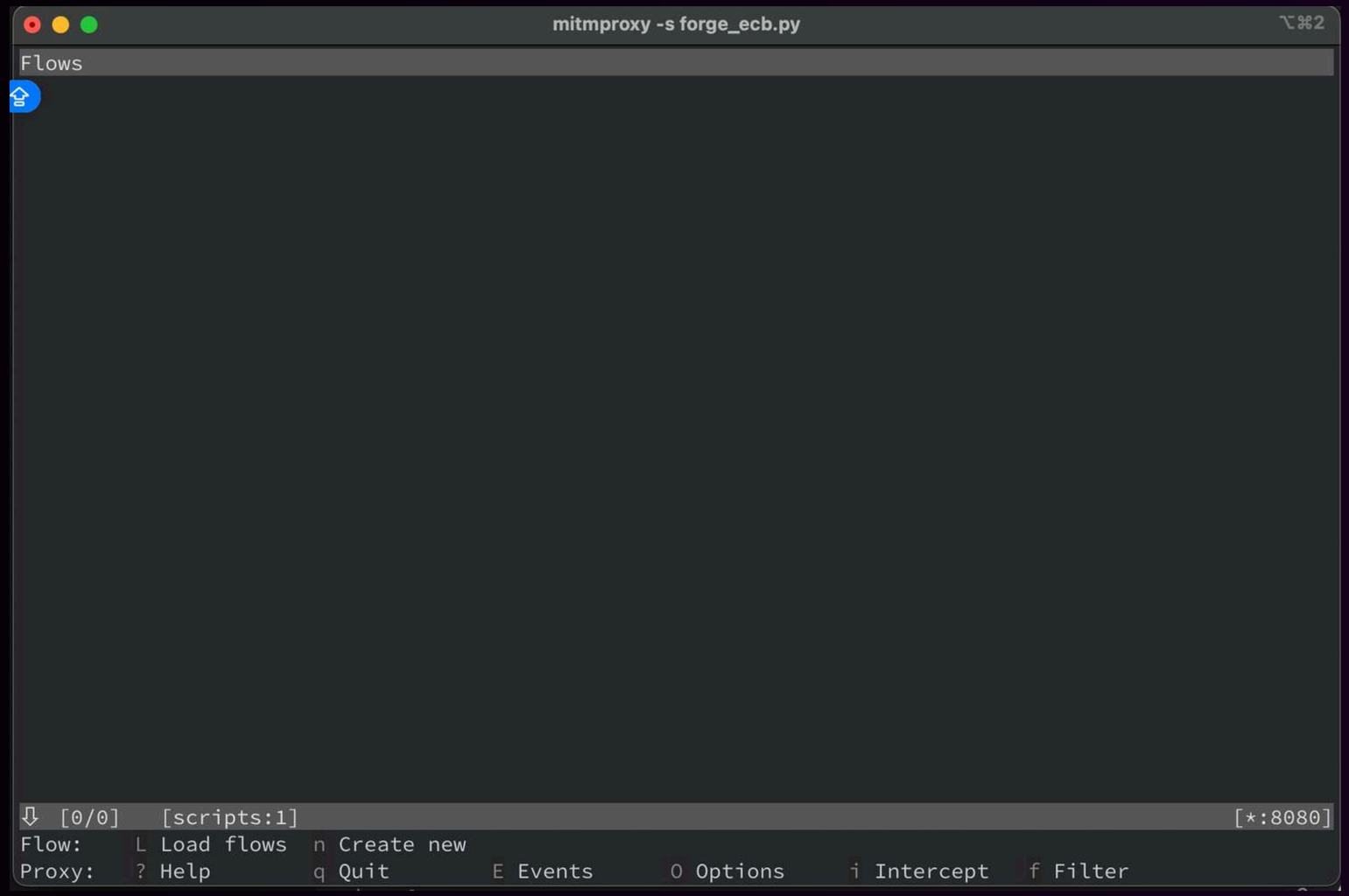
未來展望

特定專案
搜尋

中間人
攻擊

回報

中間人攻撃


mitmproxy -s forge_ecb.py
⌥⌘2
Flows
[0/0]
[scripts:1]
[*:8080]
Flow: L Load flows n Create new
Proxy: ? Help q Quit E Events O Options i Intercept f Filter

交易记录查询

开始时间 2024/12/14 结束时间 2024/12/21 查询类型 所有

重置 查询 EXCEL导出

交易地点	交易金额（元）	交易时间	交易事件	余额（元）
紫荆公寓2号楼	0.08	2024-12-20 11:31:39	持卡人消费	81.63
紫荆公寓2号楼	3.20	2024-12-20 11:31:15	持卡人消费	81.71
紫荆园	5.00	2024-12-19 12:33:10	持卡人消费	84.91
紫荆园	1.60	2024-12-19 12:08:39	持卡人消费	89.91
紫荆园	10.00	2024-12-19 12:02:09	持卡人消费	91.51
在线充值	100.00	2024-12-19 12:01:47	微信充值	101.51
紫荆园	3.50	2024-12-19 12:01:11	持卡人消费	1.51