ApolloHRXE

一. 基本訊息

- 名稱：Apollo HR XE
- icon：

- 包名：com.huanuage.skytube

- 版本：V3.0.1

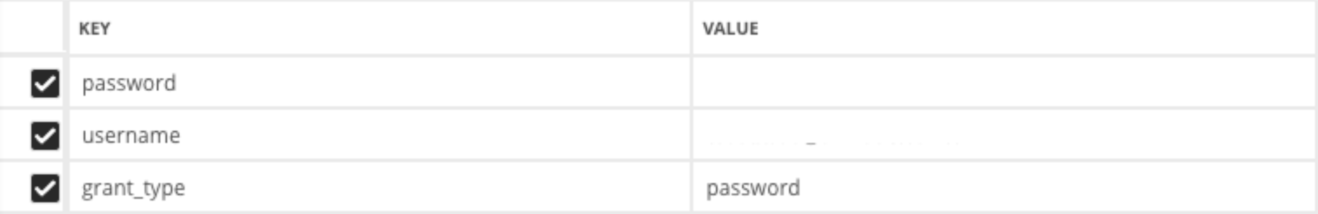
- 採取保護方案：無

二. 解析

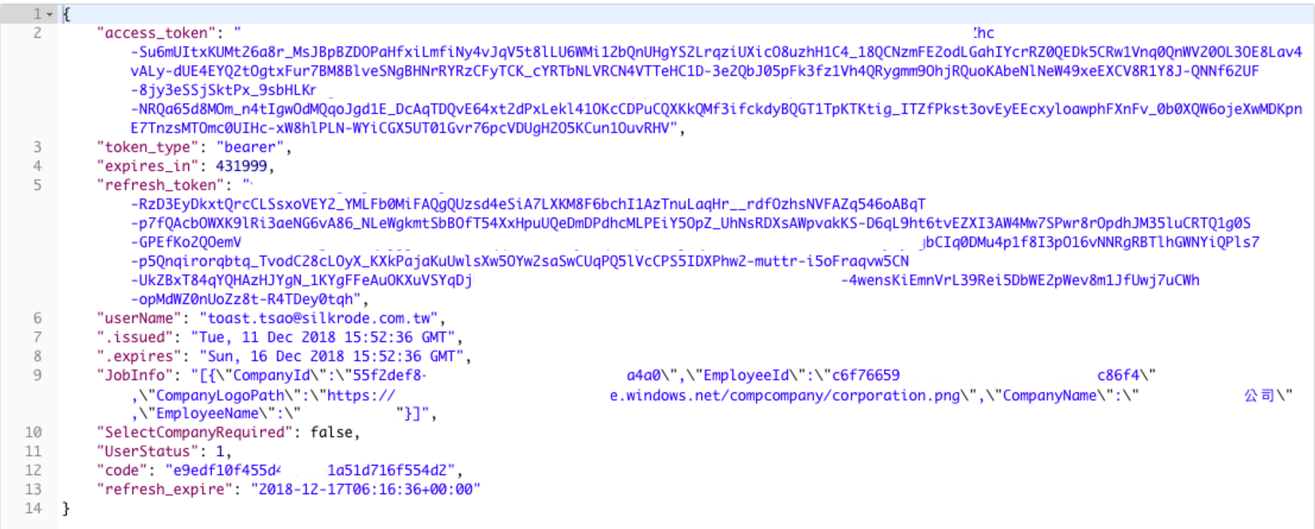
- 採用中間人攻擊方式, 攔截伺服器請求, 提取相對應打卡流程api

1. 登入
   post url: https://auth.mayohr.com/token?time=1543843239&hash=497f9dfaac4a9233e5727ee71f2f7a202344ab013f9a721611b75b0943fe7261&_sd=HRM

參數名	參數
time	543843239
hash	497f9dfaac4a9233e5727ee71f2f7a202344ab013f9a721611b75b0943fe7261
_sd	HRM



	KEY	VALUE
☑	password	
☑	username	
☑	grant_type	password



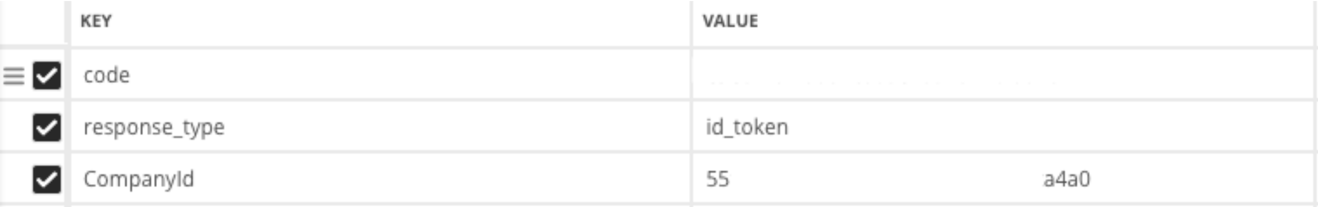
```
{
    "access_token": "                                                                                    !hc
        -Su6mUItxKUMt26a8r_MsJBpBZDOPaHfxiLmfiNy4vJqV5t8lLU6WMi12bQnUHgYS2LrqziUXicO8uzhH1C4_18QCNzmFE2odLGahIYcrRZ0QEDk5CRw1Vnq0QnWV20OL3OE8Lav4
        vALy-dUE4EYQ2tOgtxFur7BM8BlveSNgBHNrRYRzCFyTCK_cYRTbNLVRCN4VTTeHC1D-3e2QbJ05pFk3fz1Vh4QRygmm9OhjRQuoKAbeNlNeW49xeEXCV8R1Y8J-QNNf62UF
        -8jy3eSSjSktPx_9sbHLKr
        -NRQa65d8MOm_n4tIgwOdMQqoJgd1E_DcAqTDQvE64xt2dPxLekl41OKcCDPuCQXKkQMf3ifckdyBQGT1TpKTKtig_ITZfPkst3ovEyEEcxyloawphFXnFv_0b0XQW6ojeXwMDKpn
        E7TnzsMTOmc0UIHc-xW8hlPLN-WYiCGX5UT01Gvr76pcVDUgH2O5KCun1OuvRHV",
    "token_type": "bearer",
    "expires_in": 431999,
    "refresh_token": "
        -RzD3EyDkxtQrcCLSsxoVEY2_YMLFb0MiFAQgQUzsd4eSiA7LXKM8F6bchI1AzTnuLaqHr__rdfOzhsNVFAZq546oABqT
        -p7fQAcbOWXK9lRi3aeNG6vA86_NLeWgkmtSbBOfT54XxHpuUQeDmDPdhcMLPEiY5OpZ_UhNsRDXsAWpvakKS-D6qL9ht6tvEZXI3AW4Mw7SPwr8rOpdhJM35luCRTQ1g0S
        -GPEfKo2QOemV                                                                          jbCIq0DMu4p1f8I3pO16vNNRgRBTlhGWNYiQPls7
        -p5Qnqirorqbtq_TvodC28cLOyX_KXkPajaKuUwlsXw5OYw2saSwCUqPQ5lVcCPS5IDXPhw2-muttr-i5oFraqvw5CN
        -UkZBxT84qYQHAzHJYgN_1KYgFFeAuOKXuVSYqDj                                          -4wensKiEmnVrL39Rei5DbWE2pWev8m1JfUwj7uCWh
        -opMdWZ0nUoZz8t-R4TDey0tqh",
    "userName": "toast.tsao@silkrode.com.tw",
    ".issued": "Tue, 11 Dec 2018 15:52:36 GMT",
    ".expires": "Sun, 16 Dec 2018 15:52:36 GMT",
    "JobInfo": "[{\"CompanyId\":\"55f2def8-                    a4a0\",\"EmployeeId\":\"c6f76659                    c86f4\"
        ,\"CompanyLogoPath\":\"https://                    e.windows.net/compcompany/corporation.png\",\"CompanyName\":\"          公司\"
        ,\"EmployeeName\":\"          "}]",
    "SelectCompanyRequired": false,
    "UserStatus": 1,
    "code": "e9edf10f455d4      1a51d716f554d2",
    "refresh_expire": "2018-12-17T06:16:36+00:00"
}
```

2. checkTicket 檢驗

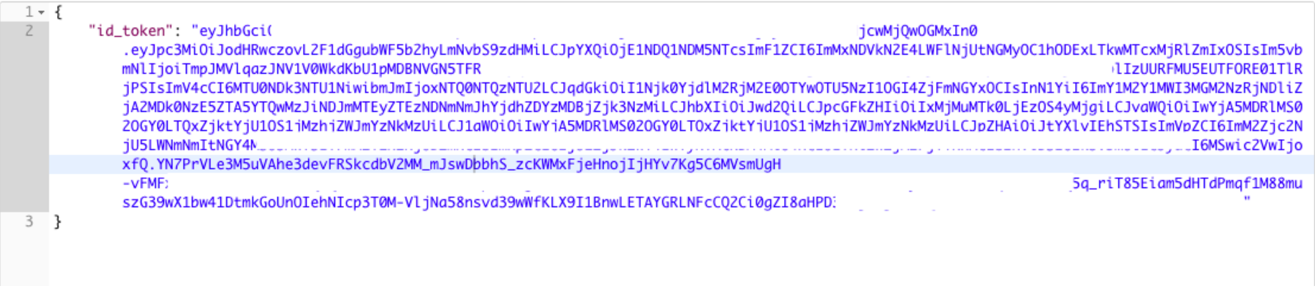
   get url: https://foundation.mayohr.com/api/auth/checkticket?code=(由登入api取得 tag:code)&response*type=id*token&CompanyId=(由登入api取得 tag:JobInfo)

參數名	參數
code	(由登入api取得 tag:code)
response_type	id_token
CompanyId	(由登入api取得 tag:JobInfo)

其中 code 與 CompanyId 由登入api response 取得



	KEY	VALUE
☑	code	
☑	response_type	id_token
☑	CompanyId	55 a4a0

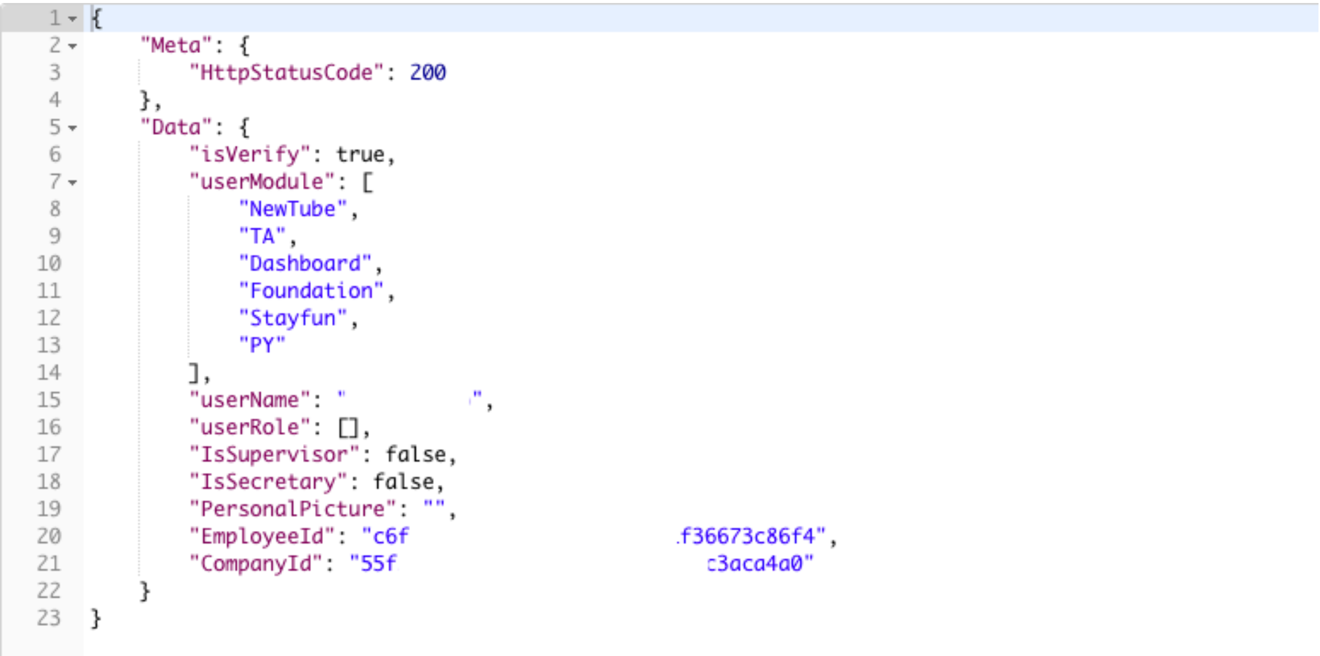


```
{
    "id_token": "eyJhbGci(                                                            jcwMjQwOGMxIn0
        .eyJpc3MiOiJodHRwczovL2F1dGgubWF5b2hyLmNvbS9zdHMiLCJpYXQiOjE1NDQ1NDM5NTcsImF1ZCI6ImMxNDVkN2E4LWFlNjUtNGMyOC1hODExLTkwMTcxMjRlZmIxOSIsIm5vb
        mNlIjoiTmpJMVlqazJNV1V0WkdKbU1pMDBNVGN5TFR                                                                  lIzUURFMU5EUTFORE01TlR
        jPSIsImV4cCI6MTU0NDk3NTU1NiwibmJmIjoxNTQ0NTQzNTU2LCJqdGkiOiI1Njk0YjdlM2RjM2E0OTYwOTU5NzI1OGI4ZjFmNGYxOCIsInN1YiI6ImY1M2Y1MWI3MGM2NzRjNDliZ
        jA2MDk0NzE5ZTA5YTQwMzJiNDJmMTEyZTEzNDNmNmJhYjdhZDYzMDBjZjk3NzMiLCJhbXIiOiJwd2QiLCJpcGFkZHIiOiIxMjMuMTk0LjEzOS4yMjgiLCJvaWQiOiIwYjA5MDRlMS0
        2OGY0LTQxZjktYjU1OS1jMzhiZWJmYzNkMzUiLCJ1aWQiOiIwYjA5MDRlMS02OGY0LTQxZjktYjU1OS1jMzhiZWJmYzNkMzUiLCJpZHAiOiJtYXlvIEhSTSIsImVpZCI6ImM2Zjc2N
        jU5LWNmNmItNGY4M                                                                                          I6MSwic2VwIjo
        xfQ.YN7PrVLe3M5uVAhe3devFRSkcdbV2MM_mJswDbbhS_zcKWMxFjeHnojIjHYv7Kg5C6MVsmUgH
        -vFMF                                                                            5q_riT85Eiam5dHTdPmqf1M88mu
        szG39wX1bw41DtmkGoUnOIehNIcp3T0M-VljNa58nsvd39wWfKLX9I1BnwLETAYGRLNFcCQ2Ci0gZI8aHPD                    "
}
```

3. userInfo

   get url: https://foundation.mayohr.com/api/userInfo

headers	參數
Authorization	由 checkTicket-api-response 取得



```
{
    "Meta": {
        "HttpStatusCode": 200
    },
    "Data": {
        "isVerify": true,
        "userModule": [
            "NewTube",
            "TA",
            "Dashboard",
            "Foundation",
            "Stayfun",
            "PY"
        ],
        "userName": "            ",
        "userRole": [],
        "IsSupervisor": false,
        "IsSecretary": false,
        "PersonalPicture": "",
        "EmployeeId": "c6f                        .f36673c86f4",
        "CompanyId": "55f                          c3aca4a0"
    }
}
```

4. 第二次 userInfo
   get https://foundation.mayohr.com/api/userInfo/app?language=zh-tw

headers	參數
Authorization	由 checkTicket-api-response 取得

取得用戶資訊

5. Post Users Registration
   post url: https://foundation.mayohr.com/api/UsersRegistration/PostUsersRegistration

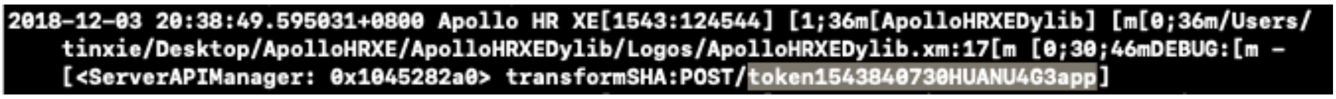
參數名	參數
EmployeeId	由 checkTicket-api-response 取得
DeviceToken	1f0260df3e9a1f56dfd3da75475352aefedb144a423bdfcce0d32252906124fc (隨意捏造)
DeviceLanguage	zh-tw
Type	apple
DeviceSerialId	C346EF16-5326-4368-995D-47658D0AAEC1 (隨意捏造)
CompanyId	由 checkTicket-api-response 取得

6. 打卡
   post url: https://pt.mayohr.com/api/checkin/punch/locate

參數名	參數
AttendanceType	2
Latitude	25.033711
Longitude	121.56482
LocationDetails	大門口
IdentifyCode	PostUsersRegistration的參數DeviceSerialId
PunchesLocationId	3dc56752-8f13-45d9-9e7e-519ef9e3e525

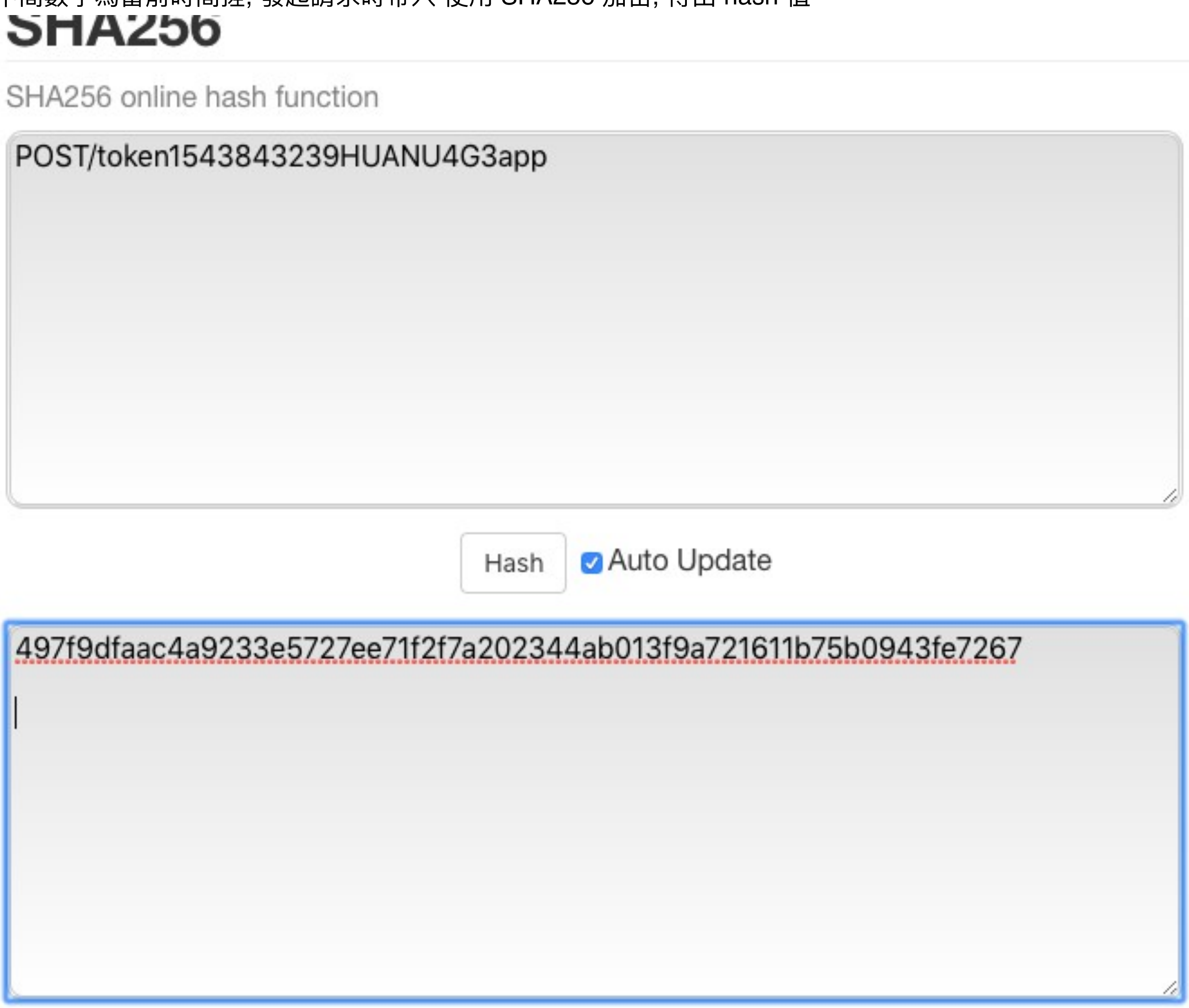
三. 總結

這部分比較困難的是"登入api 參數中的 hash", 經過逆向分析, 得出hash



```
2018-12-03 20:38:49.595031+0800 Apollo HR XE[1543:124544] [1;36m[ApolloHRXEDylib] [m[0;36m/Users/
    tinxie/Desktop/ApolloHRXE/ApolloHRXEDylib/Logos/ApolloHRXEDylib.xm:17[m [0;30;46mDEBUG:[m -
    [<ServerAPIManager: 0x1045282a0> transformSHA:POST/token1543840730HUANU4G3app]
```

中間數字為當前時間搓, 發起請求時帶入 使用 SHA256 加密, 得出 hash 值



SHA256

SHA256 online hash function

POST/token1543843239HUANU4G3app

497f9dfaac4a9233e5727ee71f2f7a202344ab013f9a721611b75b0943fe7267

以上資訊保護，參數數值皆為不正確，本文件僅供學術研究