Living on the Edge:

Abuse of Microsoft Edge for Persistence

REVERSEC

Who uses a Chromium based browsers?

Who uses their browser almost every time they use their computer?

Who knows what a Java Applet is?

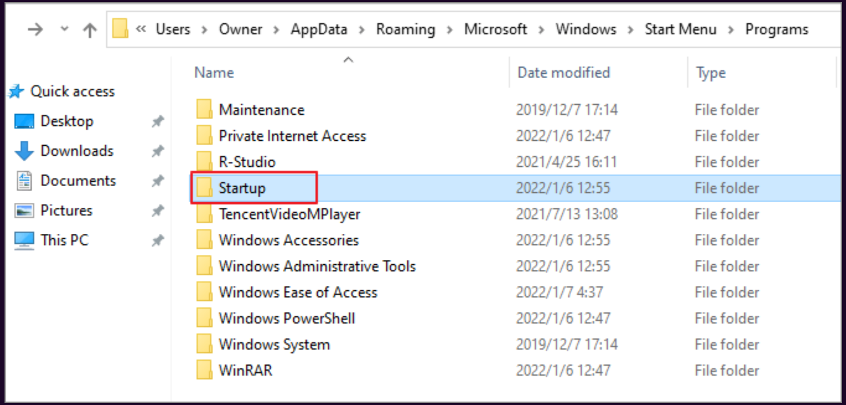
WHOAMI

- Alex Brown
- Experience: Met Office REVERSEC
- Certs: eJPT CREST CRT REGISTERED OFFENSIVE security OSCP
- Interests: GHIDRA

What is persistence?

Persistence

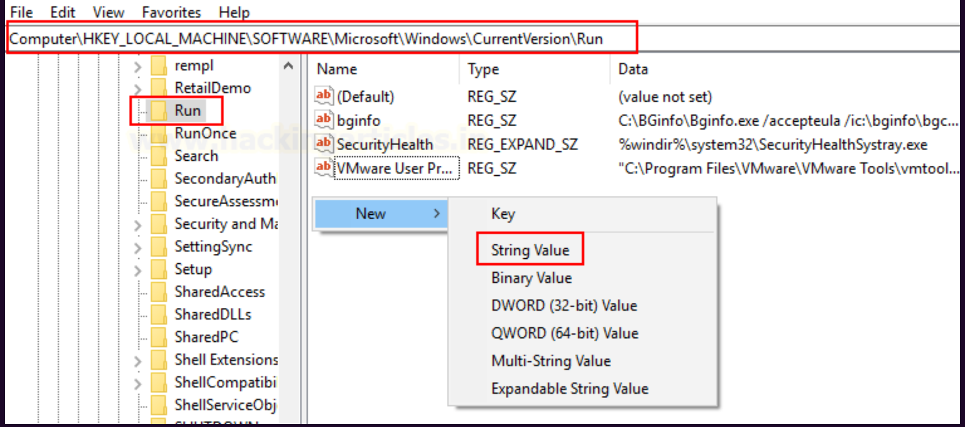
Startup folder



« Users › Owner › AppData › Roaming › Microsoft › Windows › Start Menu › Programs

Name	Date modified	Type
Maintenance	2019/12/7 17:14	File folder
Private Internet Access	2022/1/6 12:47	File folder
R-Studio	2021/4/25 16:11	File folder
Startup	2022/1/6 12:55	File folder
TencentVideoMPlayer	2021/7/13 13:08	File folder
Windows Accessories	2022/1/6 12:55	File folder
Windows Administrative Tools	2022/1/6 12:55	File folder
Windows Ease of Access	2022/1/7 4:37	File folder
Windows PowerShell	2022/1/6 12:47	File folder
Windows System	2019/12/7 17:14	File folder
WinRAR	2022/1/6 12:47	File folder

Run Keys

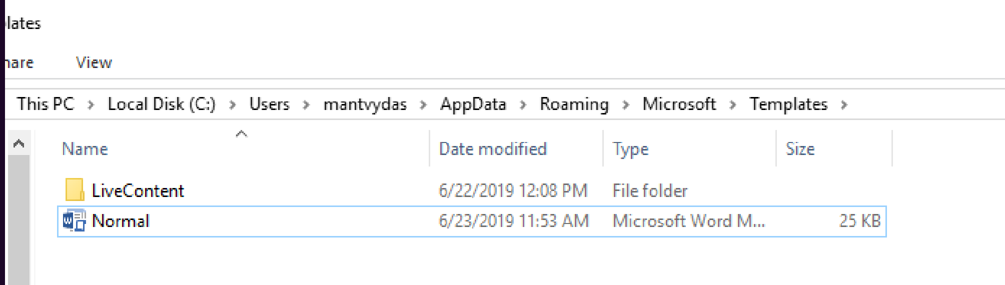


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
bginfo	REG_SZ	C:\BGinfo\Bginfo.exe /accepteula /ic:\bginfo\bgc...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtool...

Persistence

Office templates



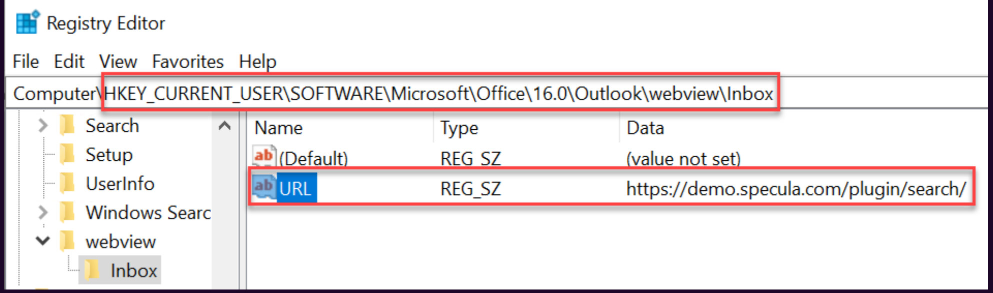
lates

hare View

This PC › Local Disk (C:) › Users › mantvydas › AppData › Roaming › Microsoft › Templates ›

Name	Date modified	Type	Size
LiveContent	6/22/2019 12:08 PM	File folder	
Normal	6/23/2019 11:53 AM	Microsoft Word M...	25 KB

Outlook homepage



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Outlook\webview\Inbox

Name	Type	Data
(Default)	REG_SZ	(value not set)
URL	REG_SZ	https://demo.specula.com/plugin/search/

Persistence

?

- It's almost a guarantee that when you start your computer you will open a we browser
- Auto installed on all windows machines
- Web browser making web call isn’t suspicious

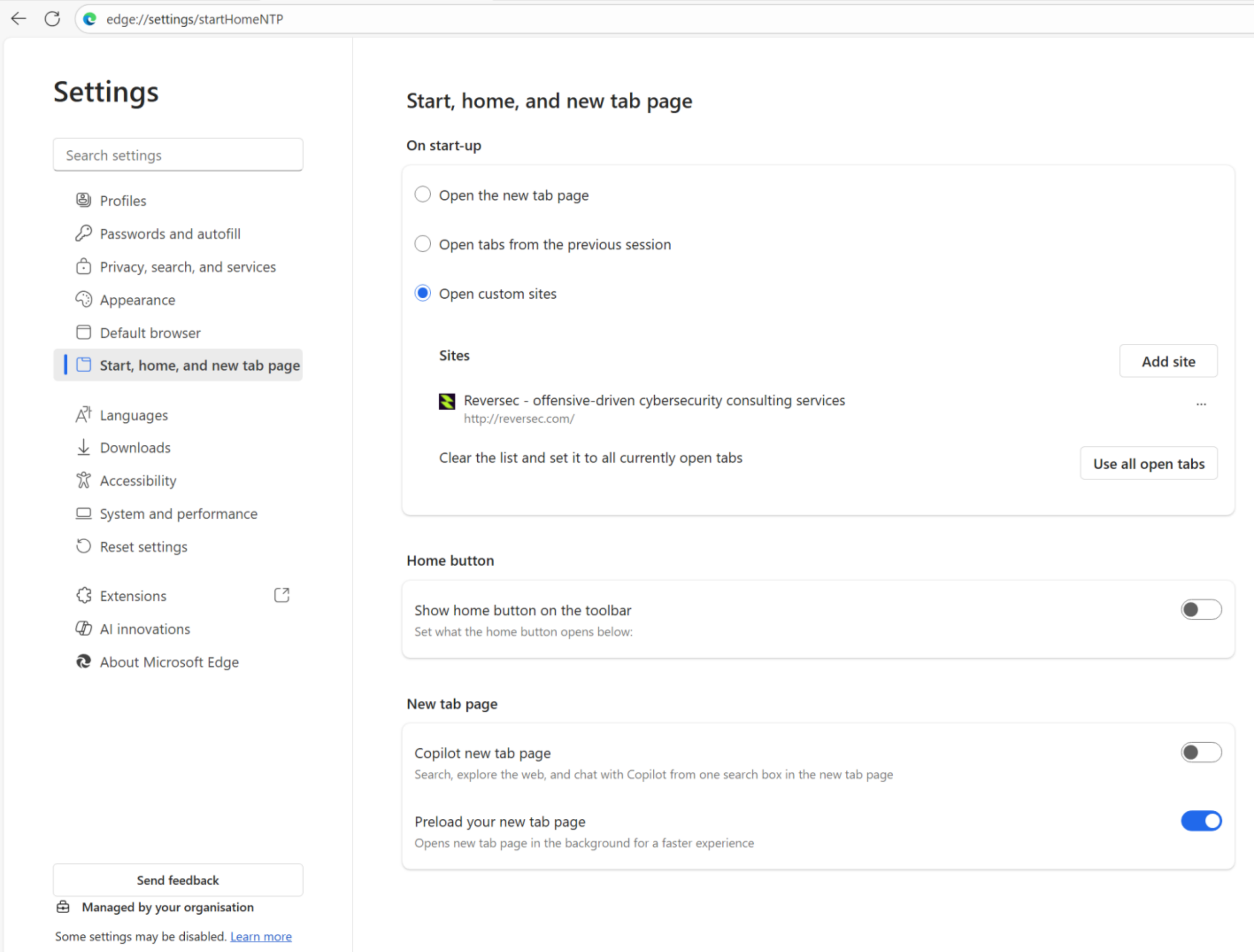
Um...whatcha got there?
A smoothie.
imgflip.com

Methods

1. Startup_urls
2. Java Applets
3. Extensions

Chromium internals

Browser Settings



edge://settings/startHomeNTP

Managed by your organisation

Some settings may be disabled. Learn more

Start, home, and new tab page

On start-up

○ Open the new tab page

○ Open tabs from the previous session

● Open custom sites

Sites — Add site

Reversec - offensive-driven cybersecurity consulting services
http://reversec.com/

Clear the list and set it to all currently open tabs — Use all open tabs

Home button

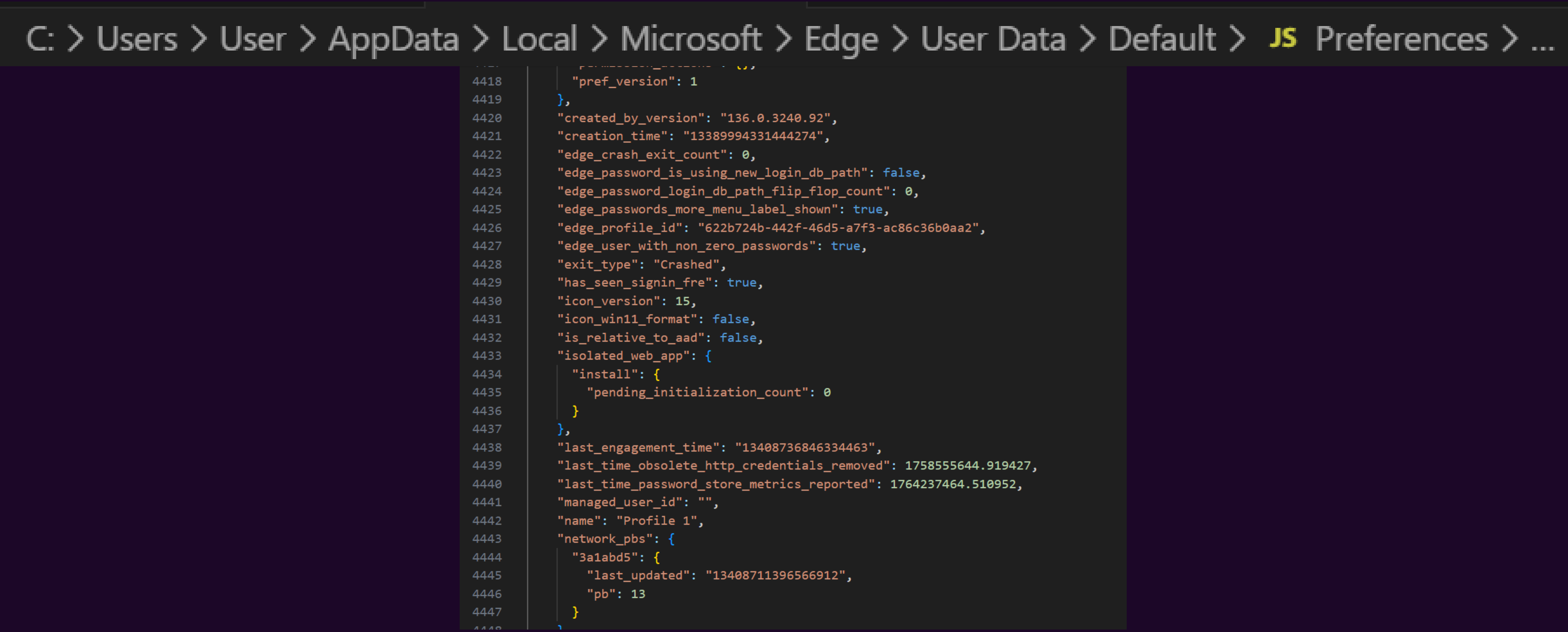
Show home button on the toolbar — Off
Set what the home button opens below:

New tab page

Copilot new tab page — Off
Search, explore the web, and chat with Copilot from one search box in the new tab page

Preload your new tab page — On
Opens new tab page in the background for a faster experience

Preferences File

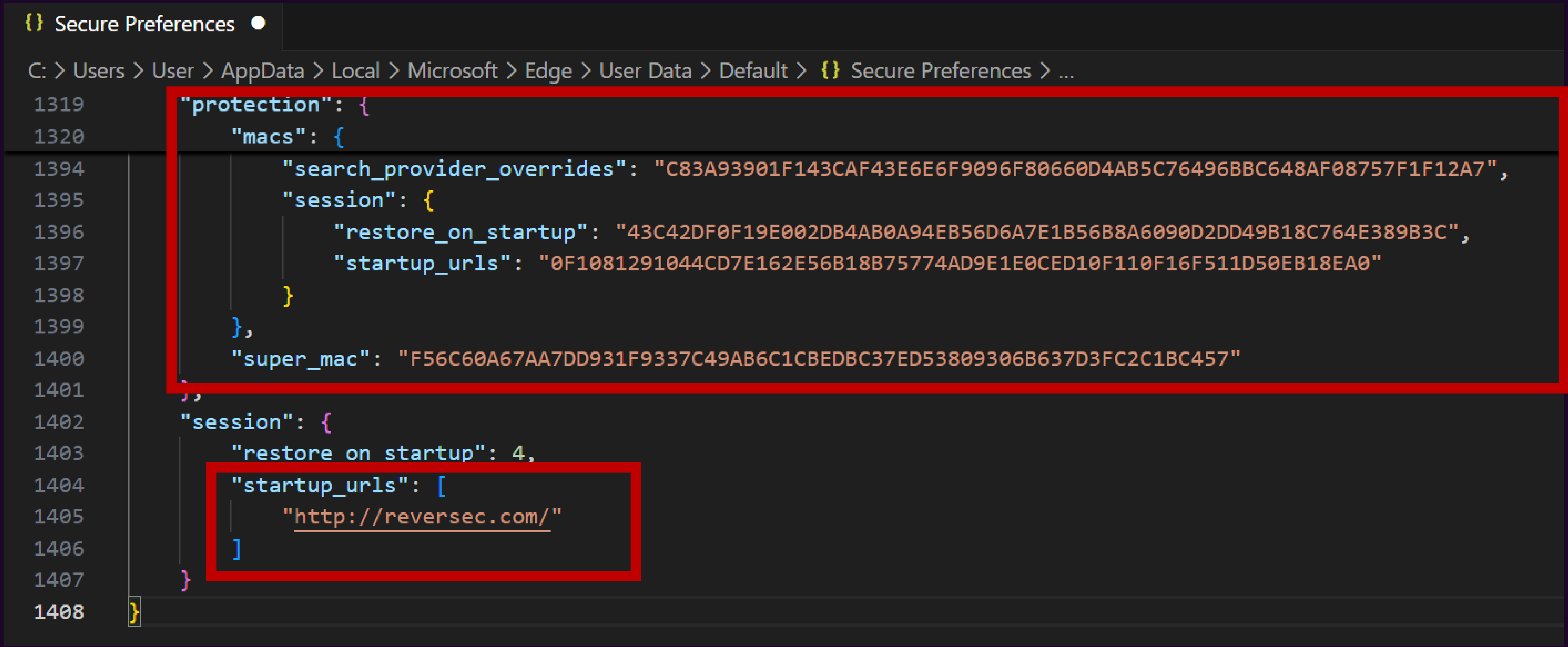


C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > JS Preferences > ...

```
    "pref_version": 1
  },
  "created_by_version": "136.0.3240.92",
  "creation_time": "13389994331444274",
  "edge_crash_exit_count": 0,
  "edge_password_is_using_new_login_db_path": false,
  "edge_password_login_db_path_flip_flop_count": 0,
  "edge_passwords_more_menu_label_shown": true,
  "edge_profile_id": "622b724b-442f-46d5-a7f3-ac86c36b0aa2",
  "edge_user_with_non_zero_passwords": true,
  "exit_type": "Crashed",
  "has_seen_signin_fre": true,
  "icon_version": 15,
  "icon_win11_format": false,
  "is_relative_to_aad": false,
  "isolated_web_app": {
    "install": {
      "pending_initialization_count": 0
    }
  },
  "last_engagement_time": "13408736846334463",
  "last_time_obsolete_http_credentials_removed": 1758555644.919427,
  "last_time_password_store_metrics_reported": 1764237464.510952,
  "managed_user_id": "",
  "name": "Profile 1",
  "network_pbs": {
    "3a1abd5": {
      "last_updated": "13408711396566912",
      "pb": 13
    }
```

Secure Preferences File

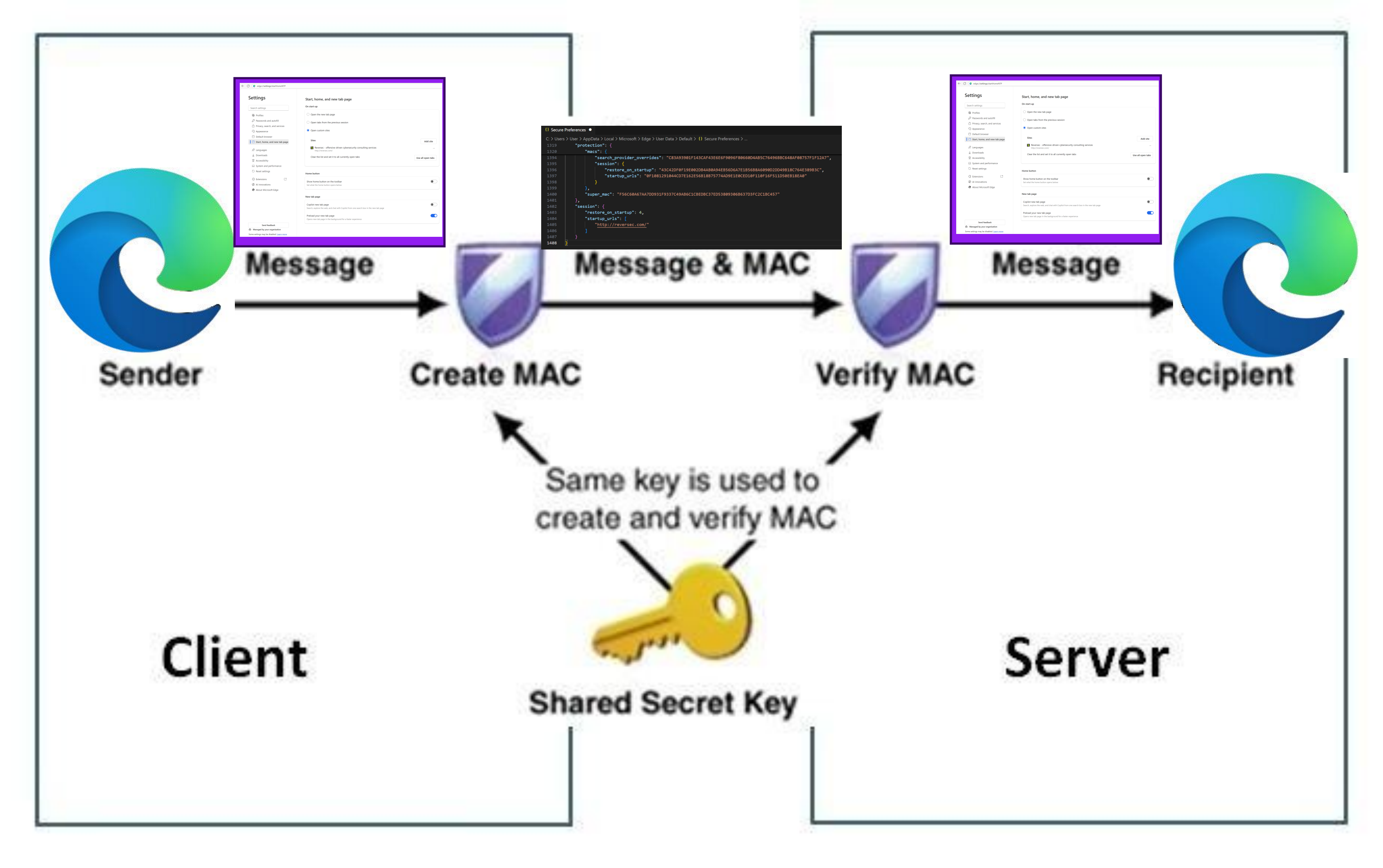
Secure Preferences File



{} Secure Preferences ●
C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > {} Secure Preferences > ...

```
    "protection": {
        "macs": {
            "search_provider_overrides": "C83A93901F143CAF43E6E6F9096F80660D4AB5C76496BBC648AF08757F1F12A7",
            "session": {
                "restore_on_startup": "43C42DF0F19E002DB4AB0A94EB56D6A7E1B56B8A6090D2DD49B18C764E389B3C",
                "startup_urls": "0F1081291044CD7E162E56B18B75774AD9E1E0CED10F110F16F511D50EB18EA0"
            }
        },
        "super_mac": "F56C60A67AA7DD931F9337C49AB6C1CBEDBC37ED53809306B637D3FC2C1BC457"
    },
    "session": {
        "restore_on_startup": 4,
        "startup_urls": [
            "http://reversec.com/"
        ]
    }
}
```

HMAC



edge://settings/startHomeNTP

Settings

Search settings

- Profiles
- Passwords and autofill
- Privacy, search, and services
- Appearance
- Default browser
- Start, home, and new tab page
- Languages
- Downloads
- Accessibility
- System and performance
- Reset settings
- Extensions
- AI innovations
- About Microsoft Edge

Send feedback

Managed by your organisation

Some settings may be disabled. Learn more

Start, home, and new tab page

On start-up

○ Open the new tab page

○ Open tabs from the previous session

● Open custom sites

Sites — Add site

Reversec - offensive-driven cybersecurity consulting services
http://reversec.com/

Clear the list and set it to all currently open tabs — Use all open tabs

Home button

Show home button on the toolbar — Off
Set what the home button opens below

New tab page

Copilot new tab page — Off
Search, explore the web, and chat with Copilot from one search box in the new tab page

Preload your new tab page — On
Opens new tab page in the background for a faster experience

Secure Preferences

C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > Secure Preferences > ...

```
    "protection": {
        "macs": {
            "search_provider_overrides": "C83A93901F143CAF43E6E6F9096F80660D4AB5C76496BBC648AF08757F1F12A7",
            "session": {
                "restore_on_startup": "43C42DF0F19E002DB4AB0A94EB56D6A7E1B56B8A6090D2DD49B18C764E389B3C",
                "startup_urls": "0F1081291044CD7E162E56B18B75774AD9E1E0CED10F110F16F511D50EB18EA0"
            }
        },
        "super_mac": "F56C60A67AA7DD931F9337C49AB6C1CBEDBC37ED53809306B637D3FC2C1BC457"
    },
    "session": {
        "restore_on_startup": 4,
        "startup_urls": [
            "http://reversec.com/"
        ]
    }
}
```

edge://settings/startHomeNTP

Settings

Start, home, and new tab page

On start-up

○ Open the new tab page

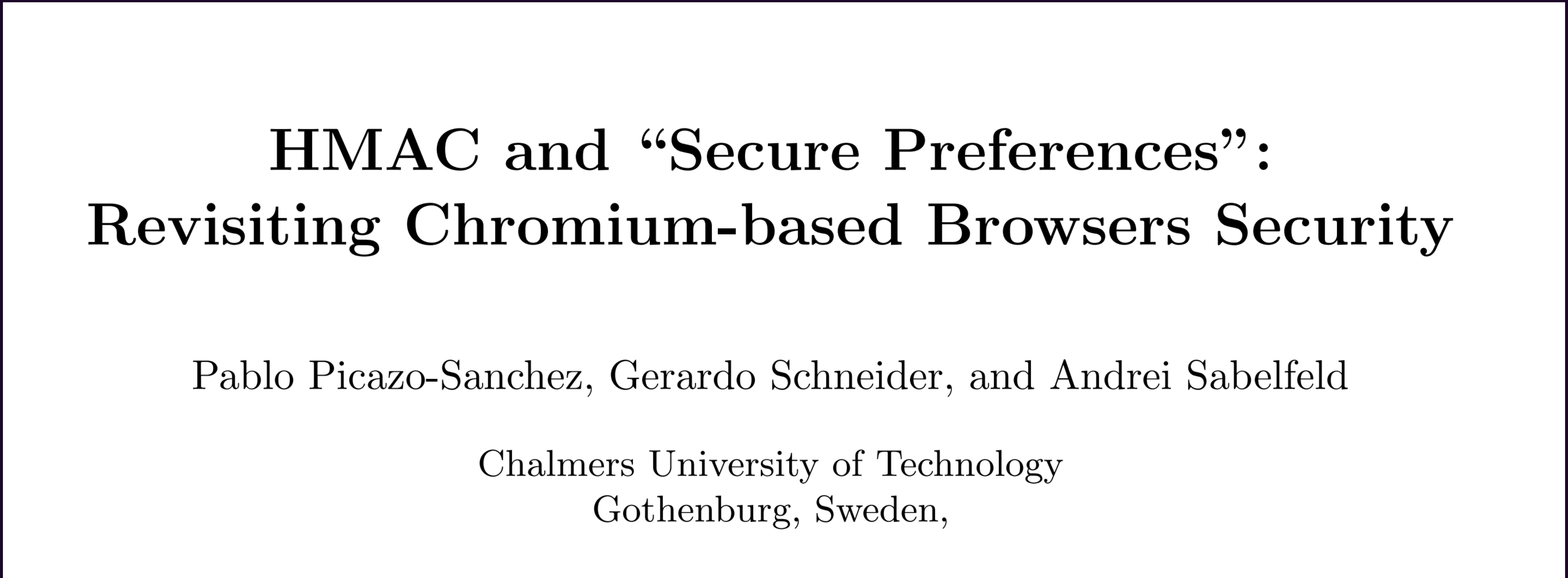
○ Open tabs from the previous session

● Open custom sites

Reversec - offensive-driven cybersecurity consulting services
http://reversec.com/

https://cyberhoot.com/cybrary/hmac-authentication/

That was until I found

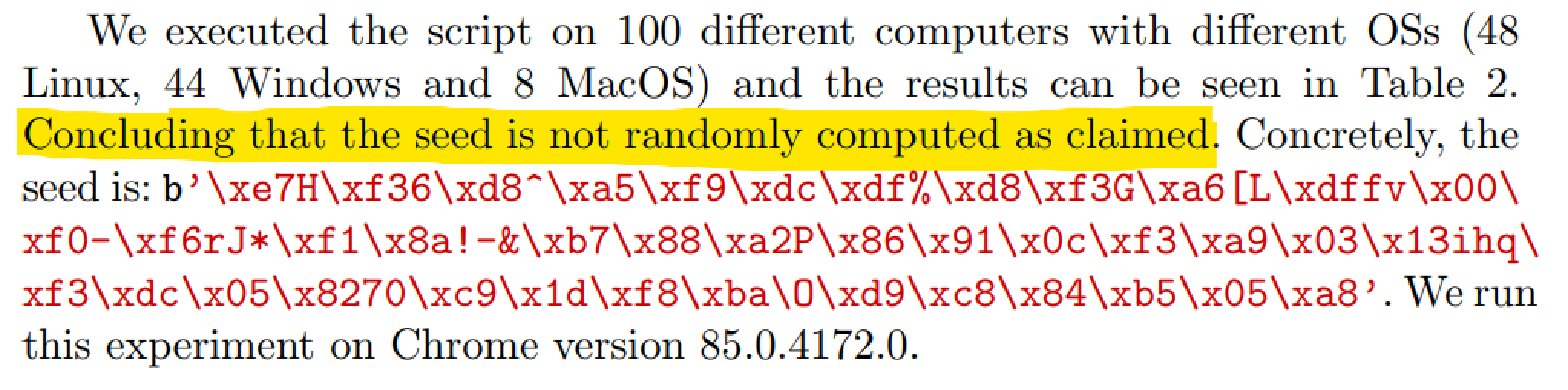


HMAC and "Secure Preferences": Revisiting Chromium-based Browsers Security

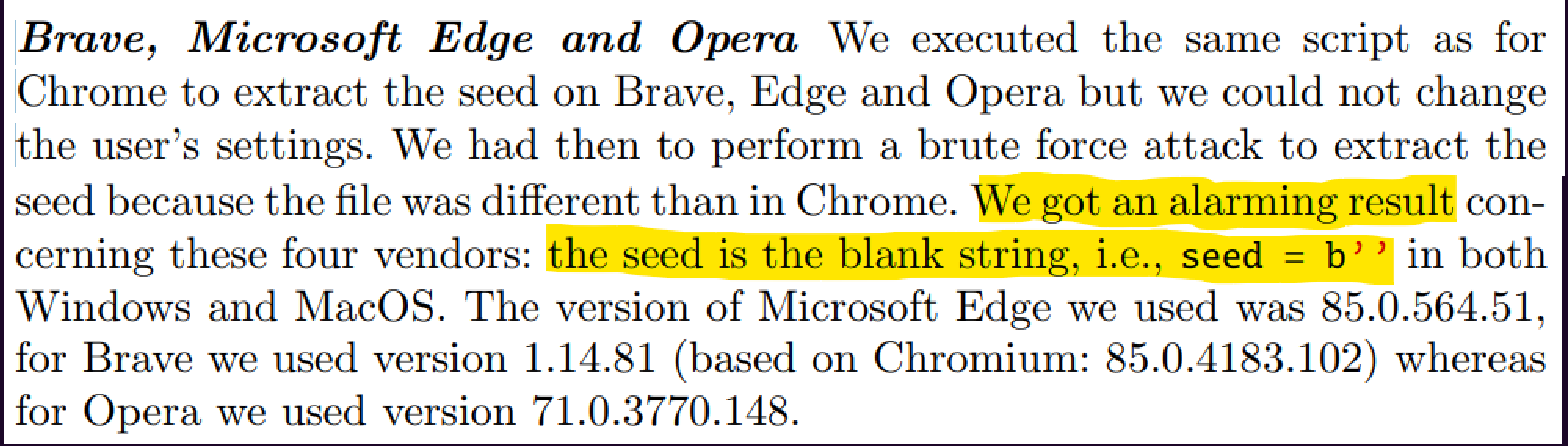
Pablo Picazo-Sanchez, Gerardo Schneider, and Andrei Sabelfeld

Chalmers University of Technology
Gothenburg, Sweden,

https://www.cse.chalmers.se/~andrei/cans20.pdf

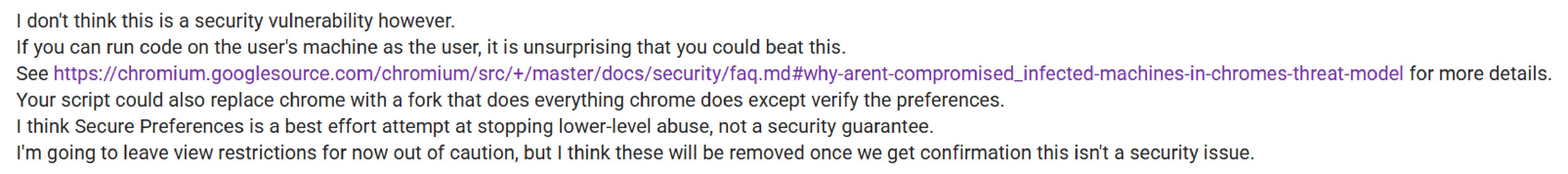


We executed the script on 100 different computers with different OSs (48 Linux, 44 Windows and 8 MacOS) and the results can be seen in Table 2. Concluding that the seed is not randomly computed as claimed. Concretely, the seed is: `b'\xe7H\xf36\xd8^\xa5\xf9\xdc\xdf%\xd8\xf3G\xa6[L\xdffv\x00\xf0-\xf6rJ*\xf1\x8a!-&\xb7\x88\xa2P\x86\x91\x0c\xf3\xa9\x03\x13ihq\xf3\xdc\x05\x8270\xc9\x1d\xf8\xba\0\xd9\xc8\x84\xb5\x05\xa8'`. We run this experiment on Chrome version 85.0.4172.0.

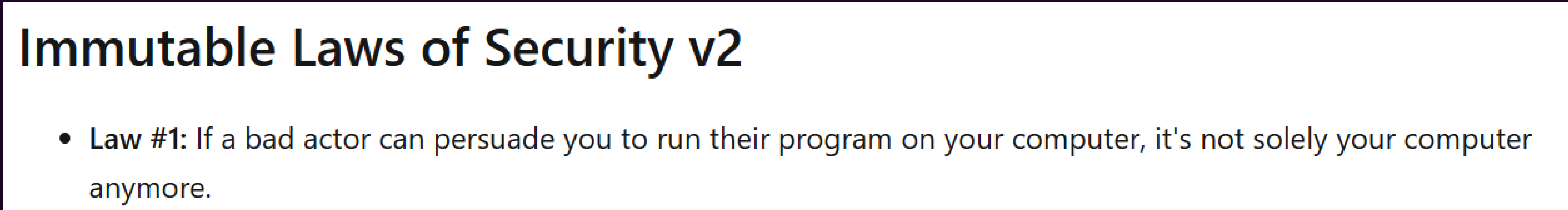


Brave, Microsoft Edge and Opera We executed the same script as for Chrome to extract the seed on Brave, Edge and Opera but we could not change the user's settings. We had then to perform a brute force attack to extract the seed because the file was different than in Chrome. We got an alarming result concerning these four vendors: the seed is the blank string, i.e., `seed = b''` in both Windows and MacOS. The version of Microsoft Edge we used was 85.0.564.51, for Brave we used version 1.14.81 (based on Chromium: 85.0.4183.102) whereas for Opera we used version 71.0.3770.148.

Sorry not in scope



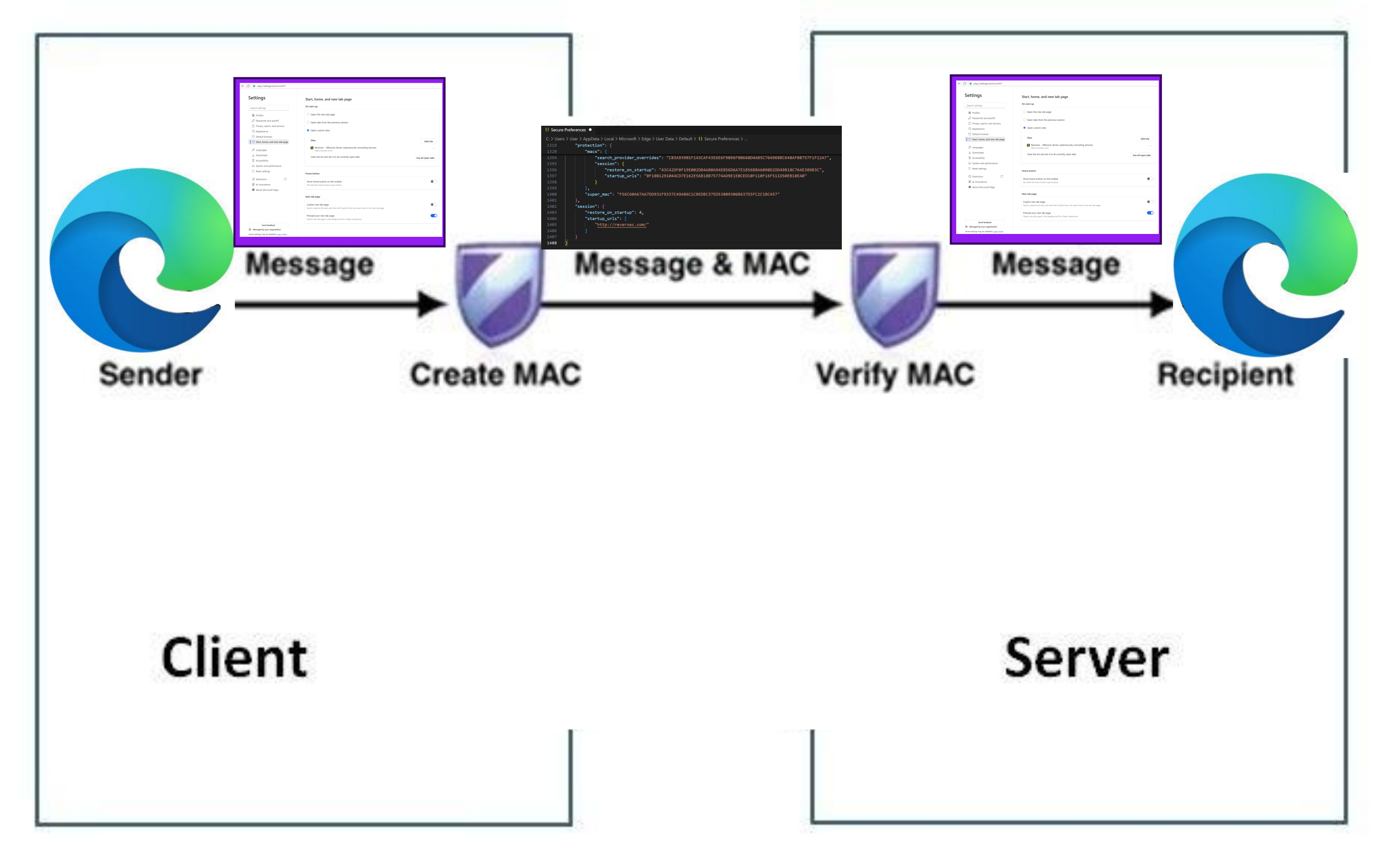
I don't think this is a security vulnerability however.
If you can run code on the user's machine as the user, it is unsurprising that you could beat this.
See https://chromium.googlesource.com/chromium/src/+/master/docs/security/faq.md#why-arent-compromised_infected-machines-in-chromes-threat-model for more details.
Your script could also replace chrome with a fork that does everything chrome does except verify the preferences.
I think Secure Preferences is a best effort attempt at stopping lower-level abuse, not a security guarantee.
I'm going to leave view restrictions for now out of caution, but I think these will be removed once we get confirmation this isn't a security issue.



Immutable Laws of Security v2

- **Law #1:** If a bad actor can persuade you to run their program on your computer, it's not solely your computer anymore.

H ~~MAC~~



edge://settings/startHomeNTP

Settings

Search settings

- Profiles
- Passwords and autofill
- Privacy, search, and services
- Appearance
- Default browser
- Start, home, and new tab page
- Languages
- Downloads
- Accessibility
- System and performance
- Reset settings
- Extensions
- AI innovations
- About Microsoft Edge

Send feedback

Managed by your organisation

Some settings may be disabled. Learn more

Start, home, and new tab page

On start-up

○ Open the new tab page

○ Open tabs from the previous session

● Open custom sites

Sites — Add site

Reversec - offensive-driven cybersecurity consulting services
http://reversec.com/

Clear the list and set it to all currently open tabs — Use all open tabs

Home button

Show home button on the toolbar — Off
Set what the home button opens below

New tab page

Copilot new tab page — Off
Search, explore the web, and chat with Copilot from one search box in the new tab page

Preload your new tab page — On
Opens new tab page in the background for a faster experience

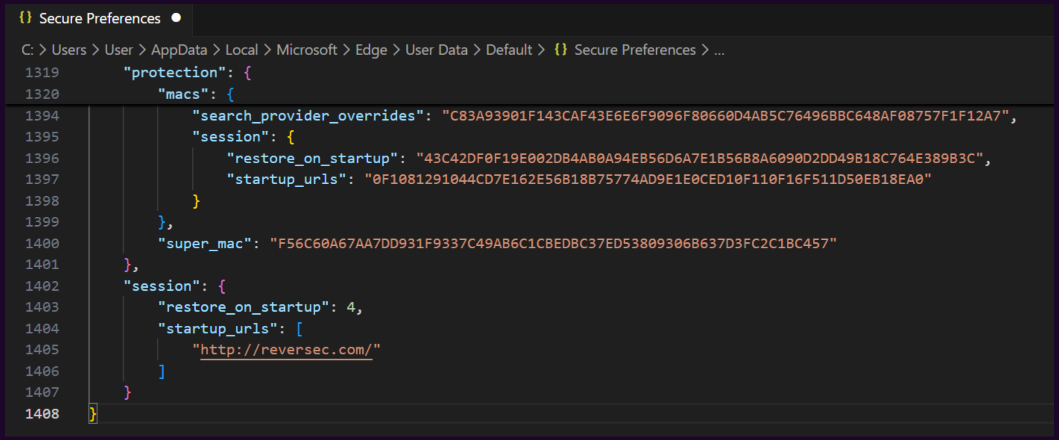
Secure Preferences

C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > Secure Preferences > ...

```
    "protection": {
        "macs": {
            "search_provider_overrides": "C83A93901F143CAF43E6E6F9096F80660D4AB5C76496BBC648AF08757F1F12A7",
            "session": {
                "restore_on_startup": "43C42DF0F19E002DB4AB0A94EB56D6A7E1B56B8A6090D2DD49B18C764E389B3C",
                "startup_urls": "0F1081291044CD7E162E56B18B75774AD9E1E0CED10F110F16F511D50EB18EA0"
            }
        },
        "super_mac": "F56C60A67AA7DD931F9337C49AB6C1CBEDBC37ED53809306B637D3FC2C1BC457"
    },
    "session": {
        "restore_on_startup": 4,
        "startup_urls": [
            "http://reversec.com/"
        ]
    }
}
```

Attack Path

Local Access



{} Secure Preferences ●
C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > {} Secure Preferences > ...

```
    "protection": {
        "macs": {
            "search_provider_overrides": "C83A93901F143CAF43E6E6F9096F80660D4AB5C76496BBC648AF08757F1F12A7",
            "session": {
                "restore_on_startup": "43C42DF0F19E002DB4AB0A94EB56D6A7E1B56B8A6090D2DD49B18C764E389B3C",
                "startup_urls": "0F1081291044CD7E162E56B18B75774AD9E1E0CED10F110F16F511D50EB18EA0"
            }
        },
        "super_mac": "F56C60A67AA7DD931F9337C49AB6C1CBEDBC37ED53809306B637D3FC2C1BC457"
    },
    "session": {
        "restore_on_startup": 4,
        "startup_urls": [
            "http://reversec.com/"
        ]
    }
}
```

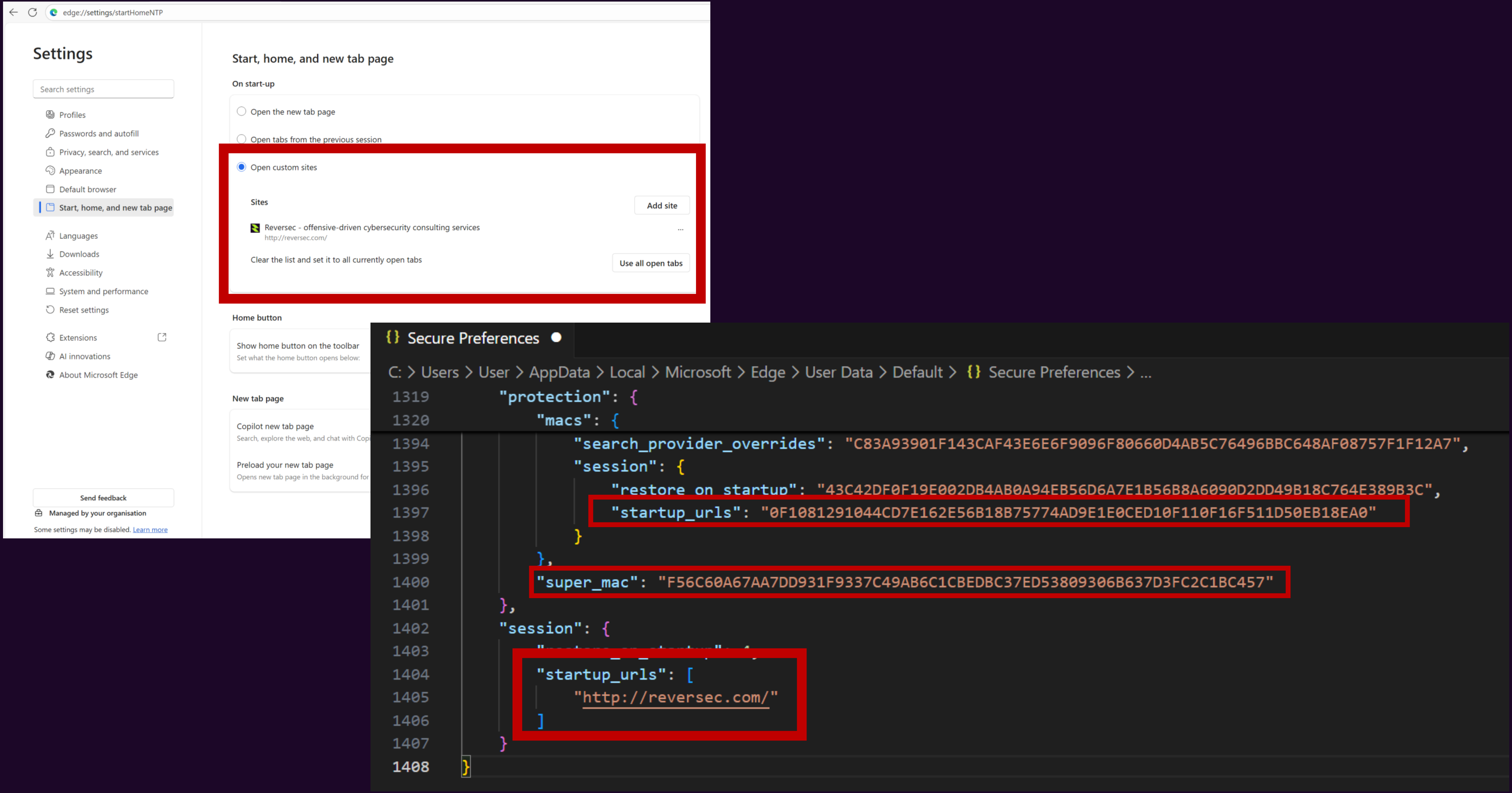
Edit the Secure Preferences file

Edge Loads settings

Methods

1. Startup_urls
2. Java Applets
3. Extensions

1. Startup_url



Settings

Managed by your organisation

Some settings may be disabled. Learn more

Start, home, and new tab page

On start-up

○ Open the new tab page

○ Open tabs from the previous session

● Open custom sites

Sites

Reversec - offensive-driven cybersecurity consulting services
http://reversec.com/

Clear the list and set it to all currently open tabs

Home button

Show home button on the toolbar
Set what the home button opens below:

New tab page

Copilot new tab page
Search, explore the web, and chat with Copi

Preload your new tab page
Opens new tab page in the background for

{} Secure Preferences

C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > {} Secure Preferences > ...

```
    "protection": {
      "macs": {
        "search_provider_overrides": "C83A93901F143CAF43E6E6F9096F80660D4AB5C76496BBC648AF08757F1F12A7",
        "session": {
          "restore_on_startup": "43C42DF0F19E002DB4AB0A94EB56D6A7E1B56B8A6090D2DD49B18C764E389B3C",
          "startup_urls": "0F1081291044CD7E162E56B18B75774AD9E1E0CED10F110F16F511D50EB18EA0"
        }
      },
      "super_mac": "F56C60A67AA7DD931F9337C49AB6C1CBEDBC37ED53809306B637D3FC2C1BC457"
    },
    "session": {
      "restore_on_startup": 4,
      "startup_urls": [
        "http://reversec.com/"
      ]
    }
}
```

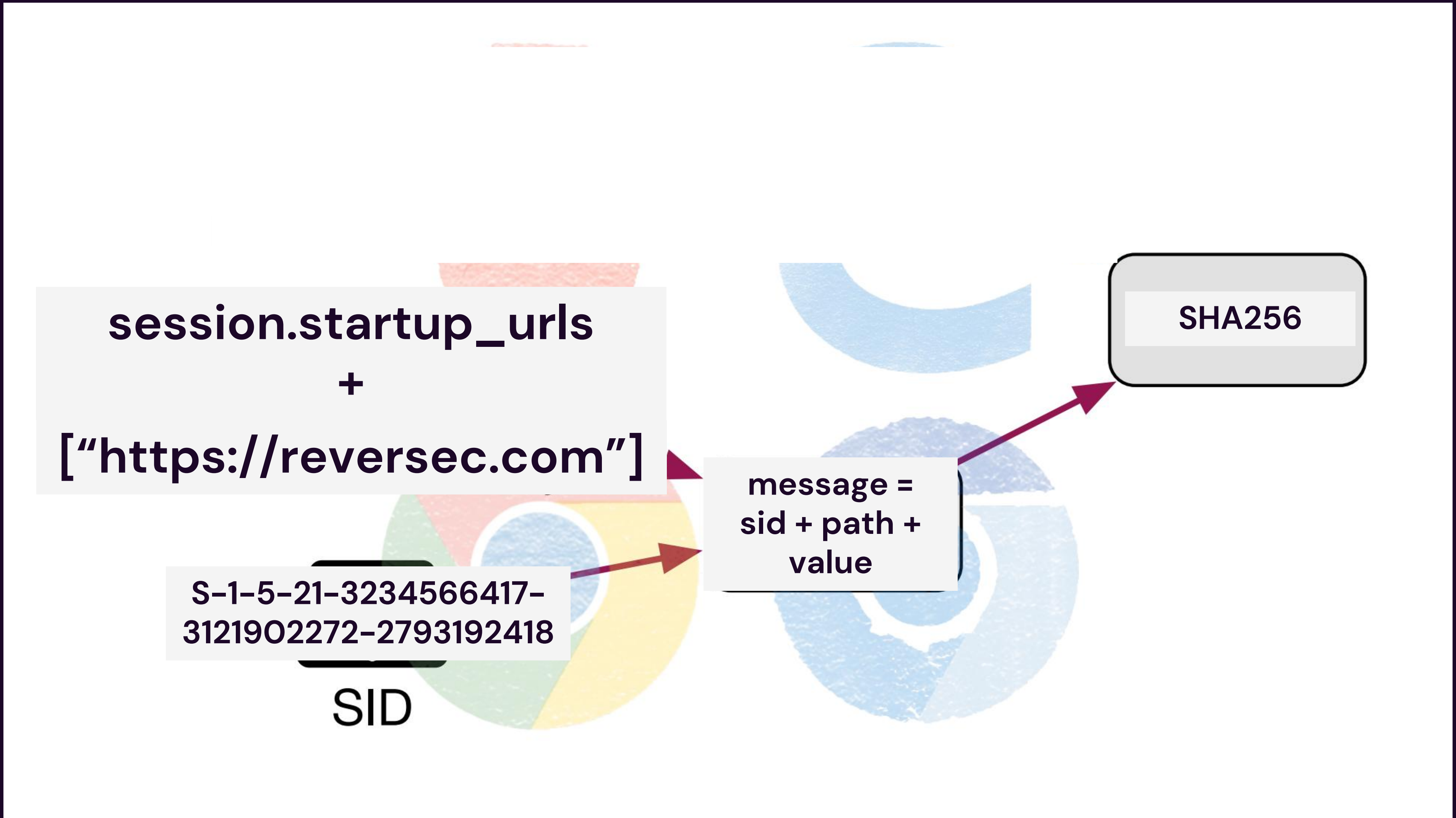
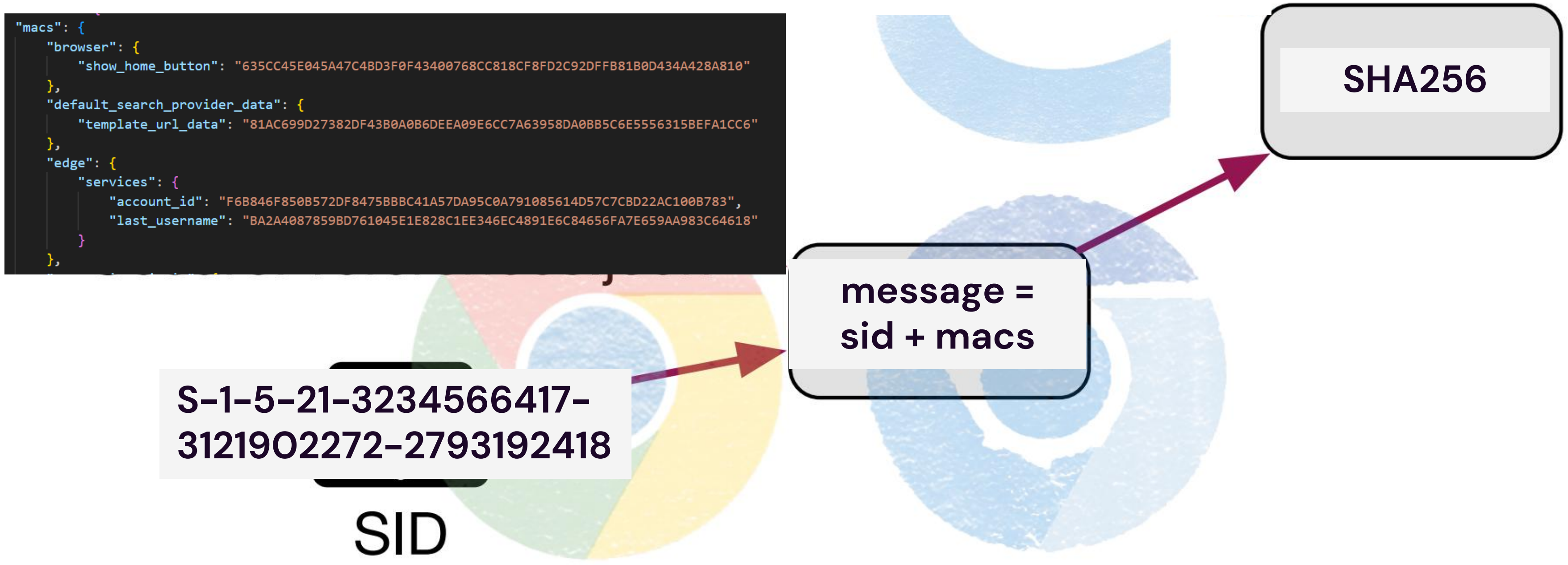


Fig. 2. HMAC protocol in Chromium based browsers

https://www.cse.chalmers.se/~andrei/cans20.pdf



```
"macs": {
    "browser": {
        "show_home_button": "635CC45E045A47C4BD3F0F43400768CC818CF8FD2C92DFFB81B0D434A428A810"
    },
    "default_search_provider_data": {
        "template_url_data": "81AC699D27382DF43B0A0B6DEEA09E6CC7A63958DA0BB5C6E5556315BEFA1CC6"
    },
    "edge": {
        "services": {
            "account_id": "F6B846F850B572DF8475BBBC41A57DA95C0A791085614D57C7CBD22AC100B783",
            "last_username": "BA2A4087859BD761045E1E828C1EE346EC4891E6C84656FA7E659AA983C64618"
        }
    },
```

S-1-5-21-3234566417-3121902272-2793192418

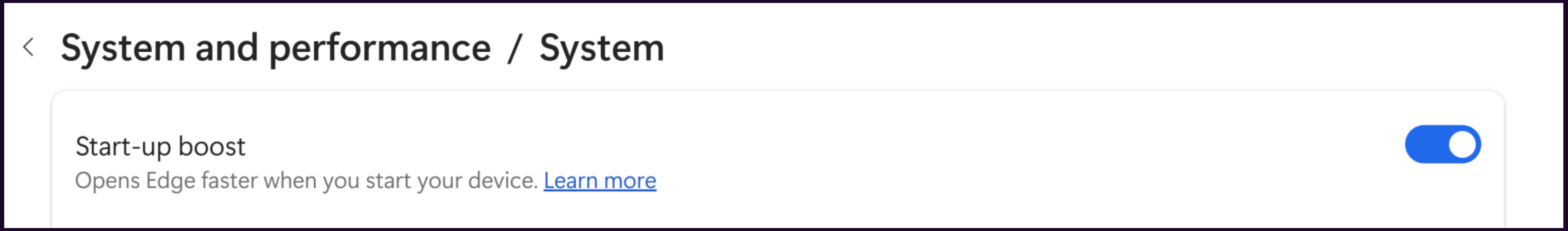
message = sid + macs

SHA256

Fig. 2. HMAC protocol in Chromium based browsers

https://www.cse.chalmers.se/~andrei/cans20.pdf

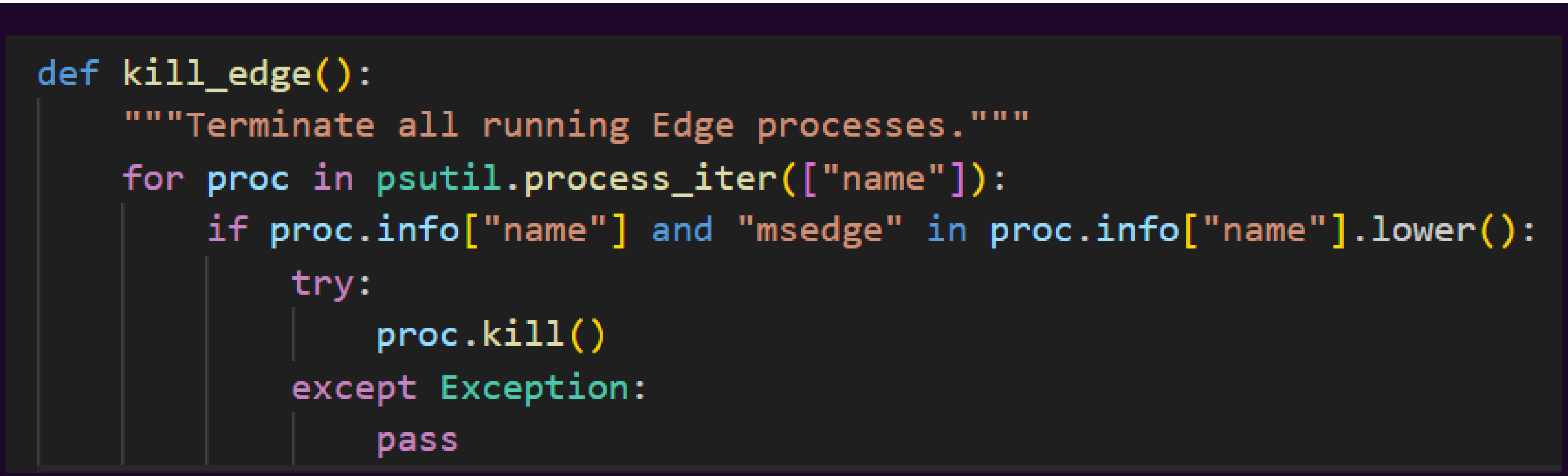
Edge runs in background



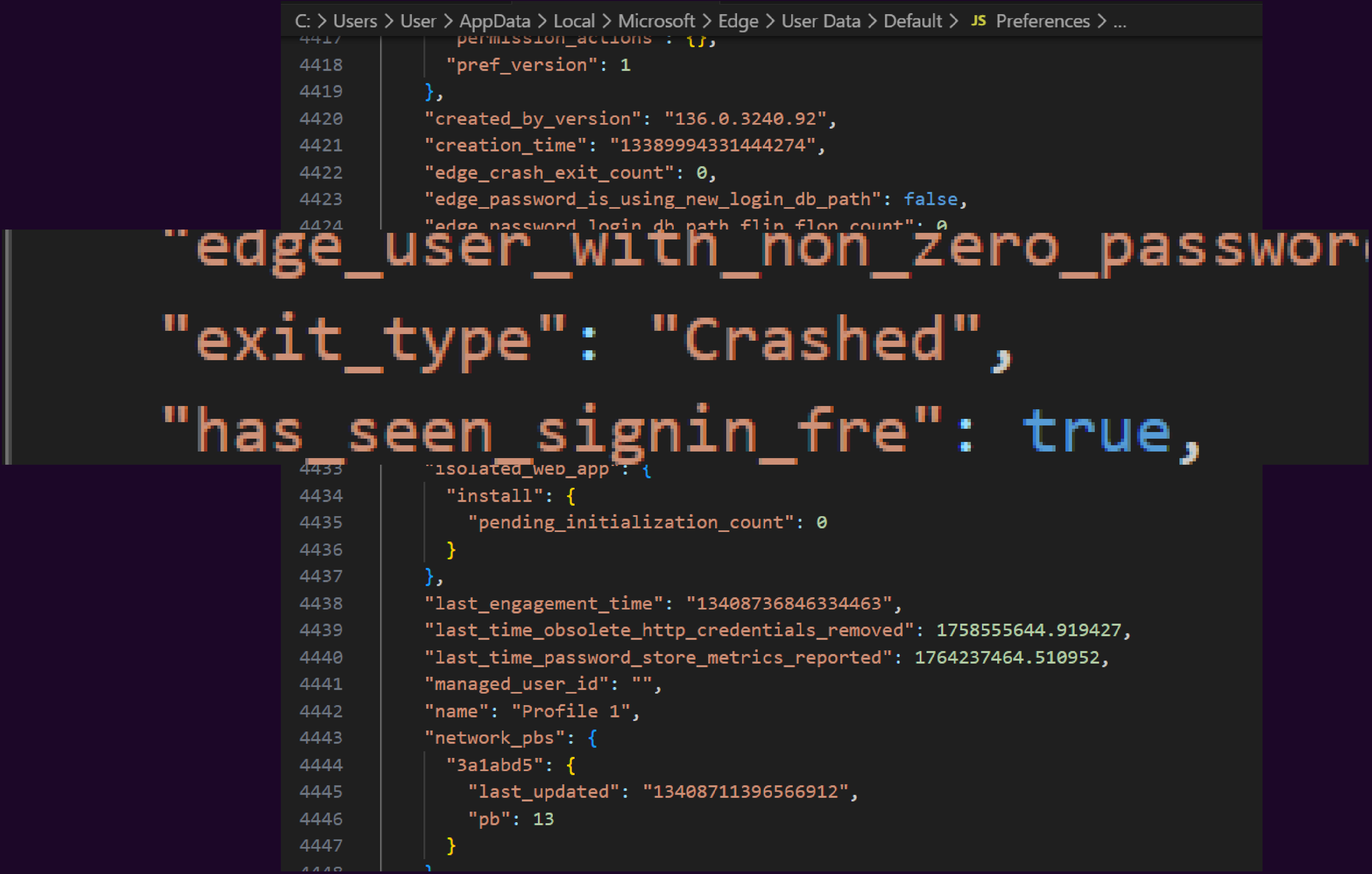
System and performance / System

Start-up boost ●

Opens Edge faster when you start your device. Learn more

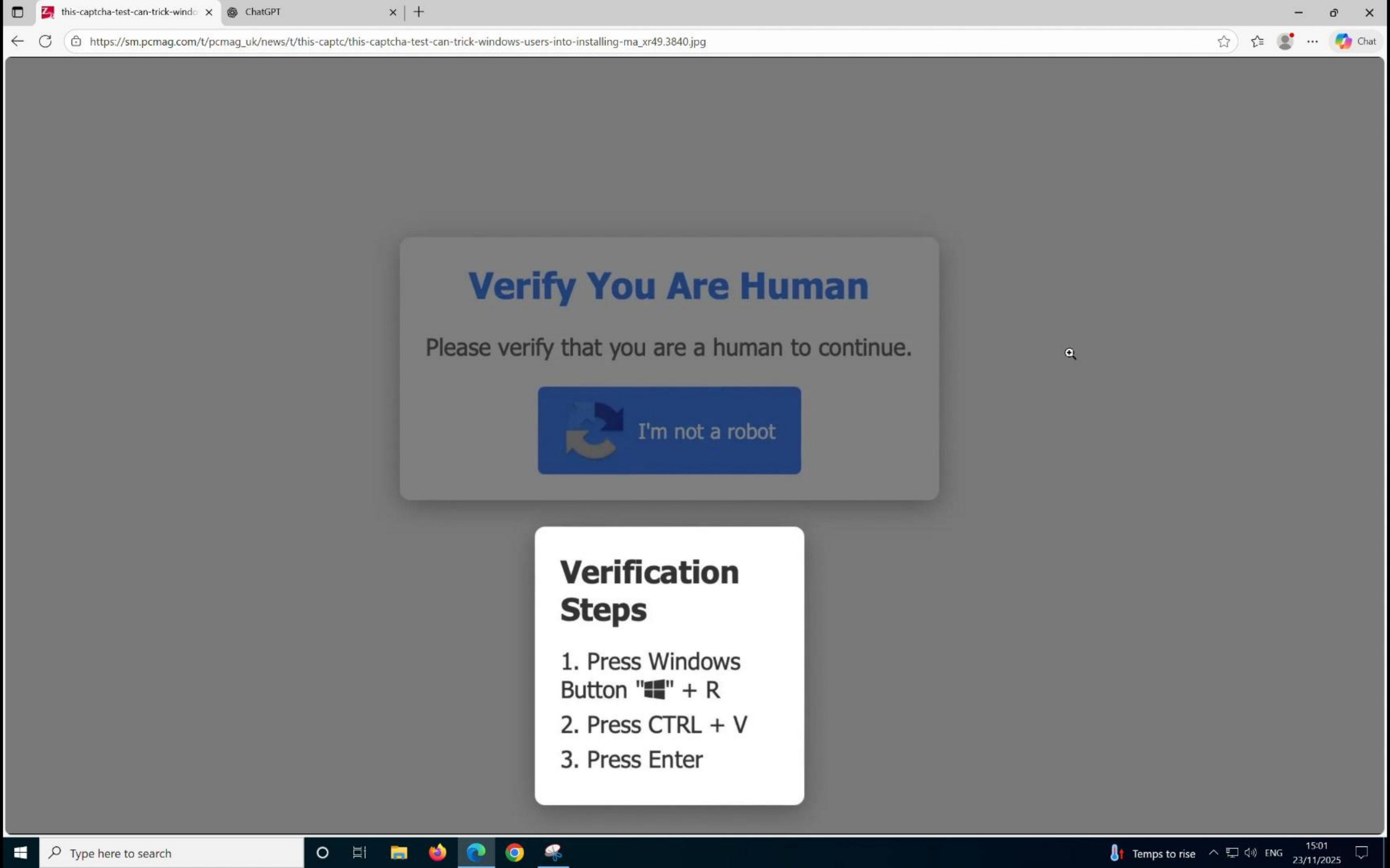


```python
def kill_edge():
    """Terminate all running Edge processes."""
    for proc in psutil.process_iter(["name"]):
        if proc.info["name"] and "msedge" in proc.info["name"].lower():
            try:
                proc.kill()
            except Exception:
                pass
```



C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > JS Preferences > ...

```
      "permission_actions": {},
      "pref_version": 1
    },
    "created_by_version": "136.0.3240.92",
    "creation_time": "13389994331444274",
    "edge_crash_exit_count": 0,
    "edge_password_is_using_new_login_db_path": false,
    "edge_password_login_db_path_flip_flop_count": 0
    "edge_user_with_non_zero_passwor
    "exit_type": "Crashed",
    "has_seen_signin_fre": true,
    "isolated_web_app": {
      "install": {
        "pending_initialization_count": 0
      }
    },
    "last_engagement_time": "13408736846334463",
    "last_time_obsolete_http_credentials_removed": 1758555644.919427,
    "last_time_password_store_metrics_reported": 1764237464.510952,
    "managed_user_id": "",
    "name": "Profile 1",
    "network_pbs": {
      "3a1abd5": {
        "last_updated": "13408711396566912",
        "pb": 13
      }
    }
```



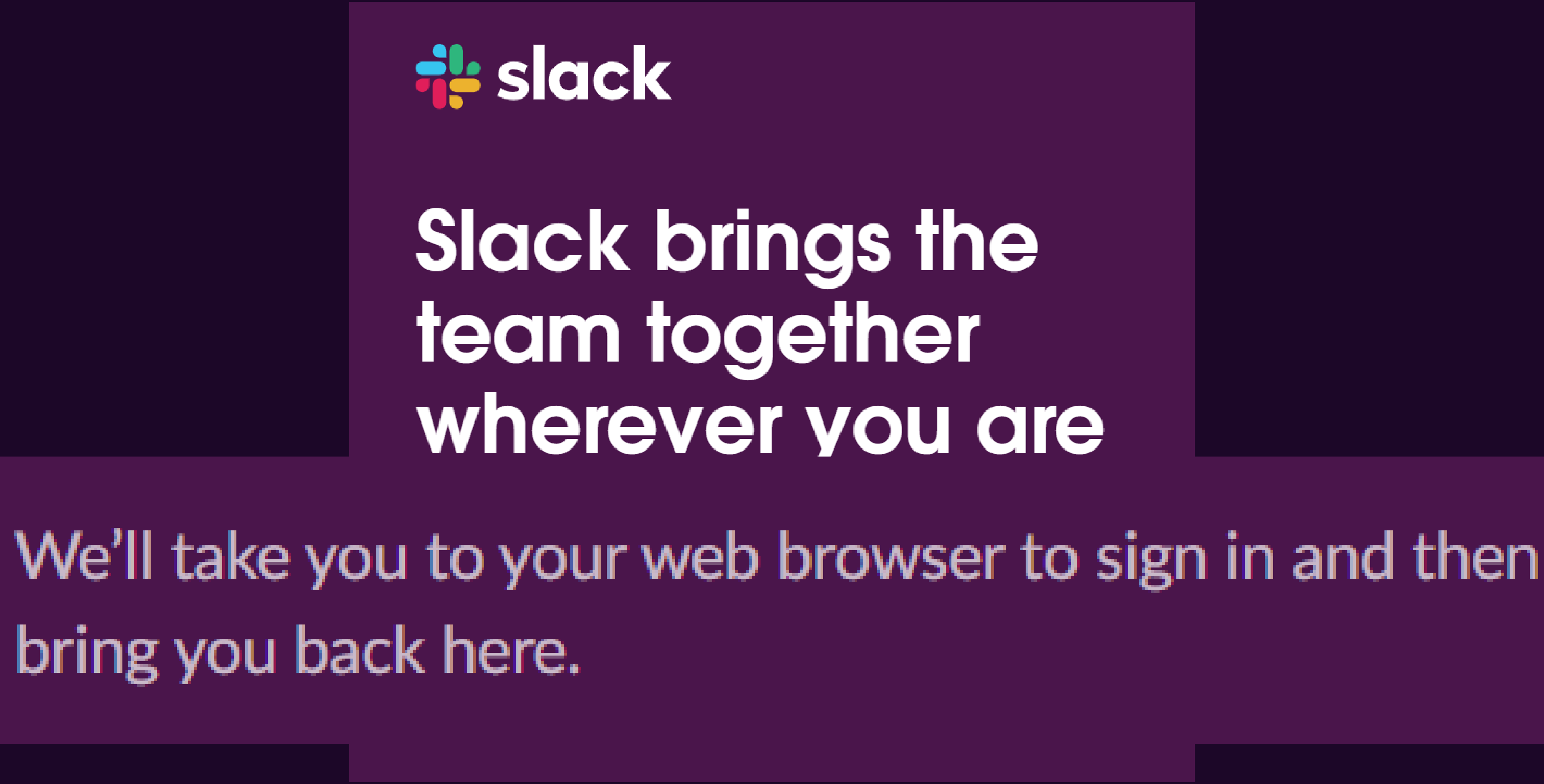
https://sm.pcmag.com/t/pcmag_uk/news/t/this-captc/this-captcha-test-can-trick-windows-users-into-installing-ma_xr49.3840.jpg

Verify You Are Human

Please verify that you are a human to continue.

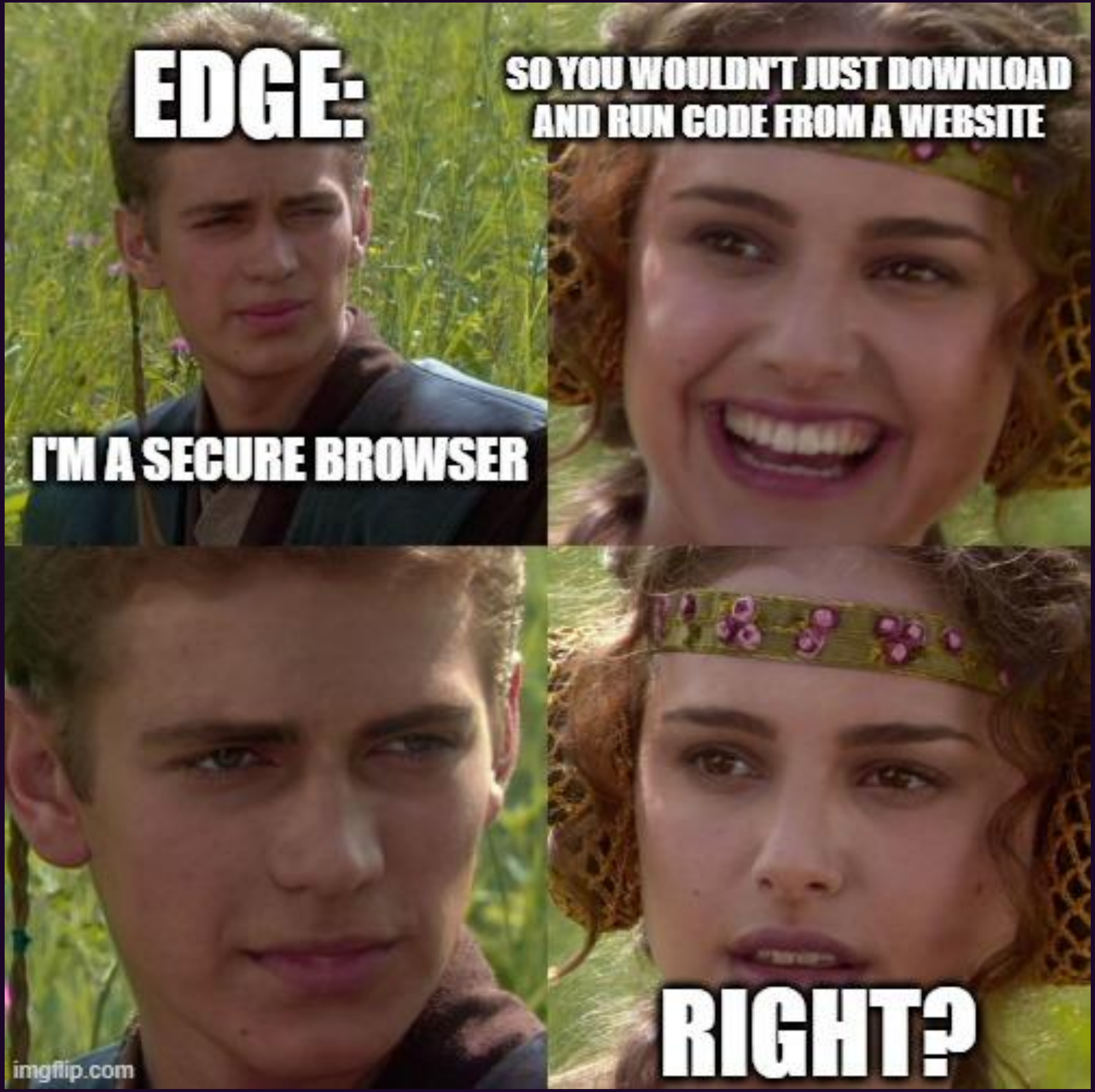
Verification Steps

1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter



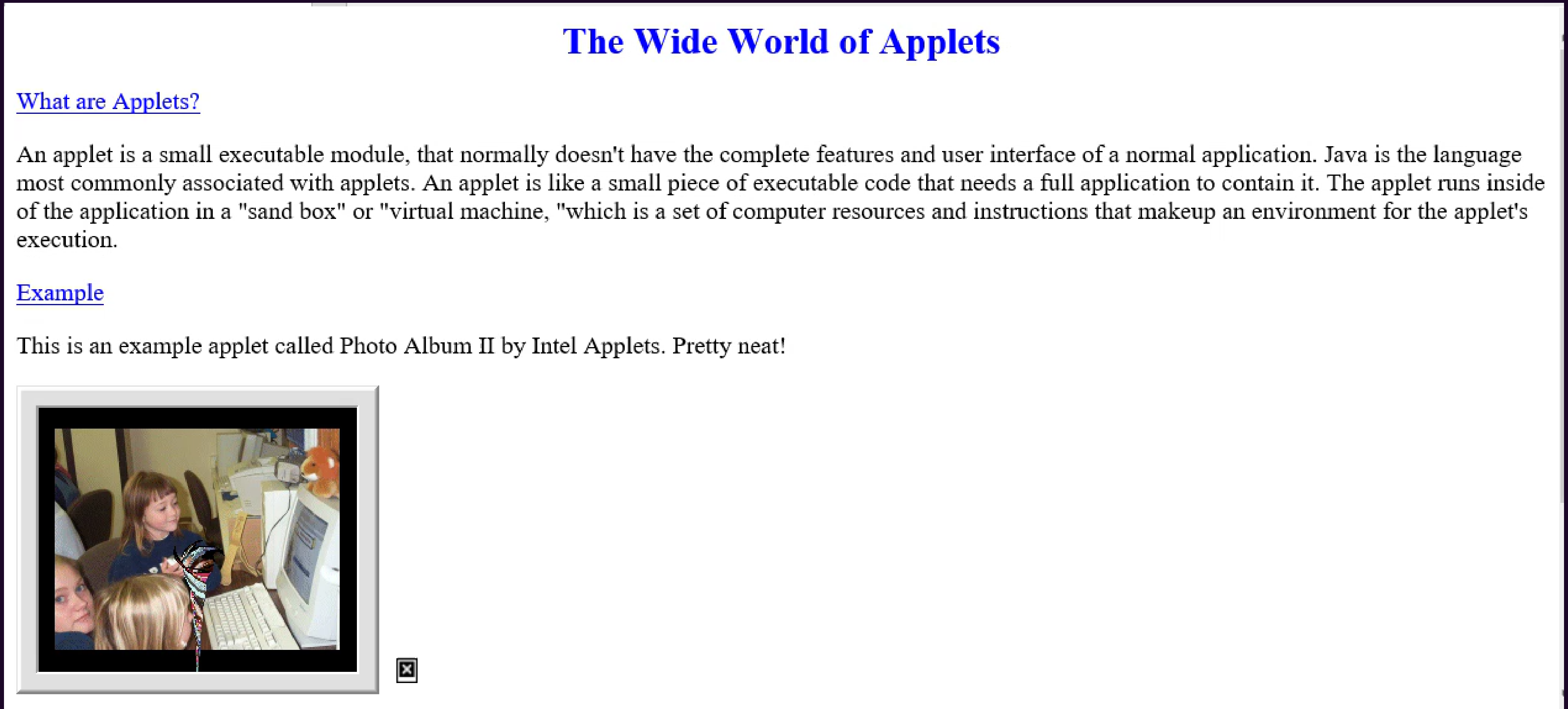
Slack brings the team together wherever you are

We’ll take you to your web browser to sign in and then bring you back here.


EDGE:
I'M A SECURE BROWSER
SO YOU WOULDN'T JUST DOWNLOAD AND RUN CODE FROM A WEBSITE
RIGHT?
imgflip.com

2. Java Applet

What is a Java Applet



The Wide World of Applets

What are Applets?

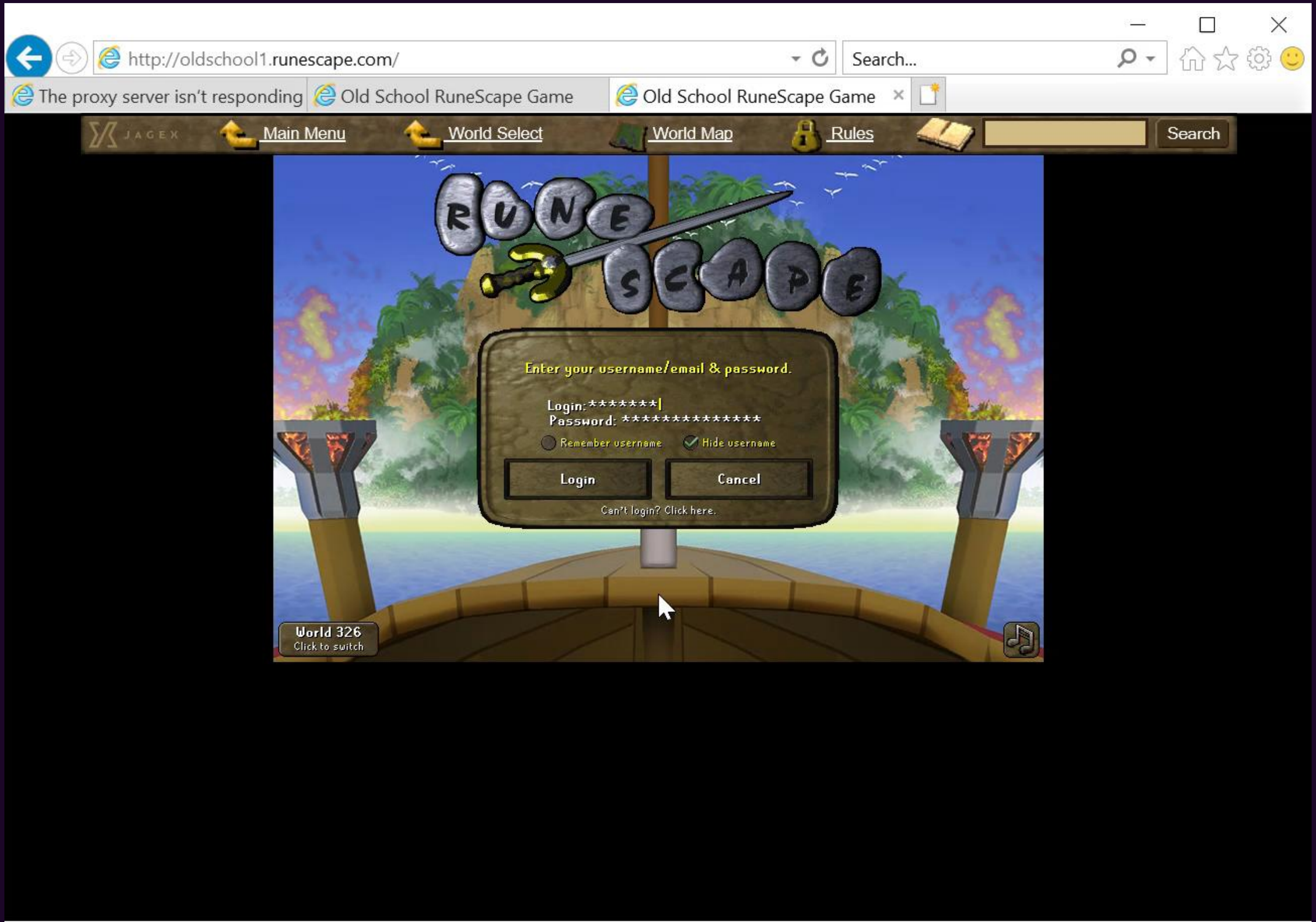
An applet is a small executable module, that normally doesn't have the complete features and user interface of a normal application. Java is the language most commonly associated with applets. An applet is like a small piece of executable code that needs a full application to contain it. The applet runs inside of the application in a "sand box" or "virtual machine, "which is a set of computer resources and instructions that makeup an environment for the applet's execution.

Example

This is an example applet called Photo Album II by Intel Applets. Pretty neat!

https://lessonplans.btskinner.com/applet.html

RuneScape!



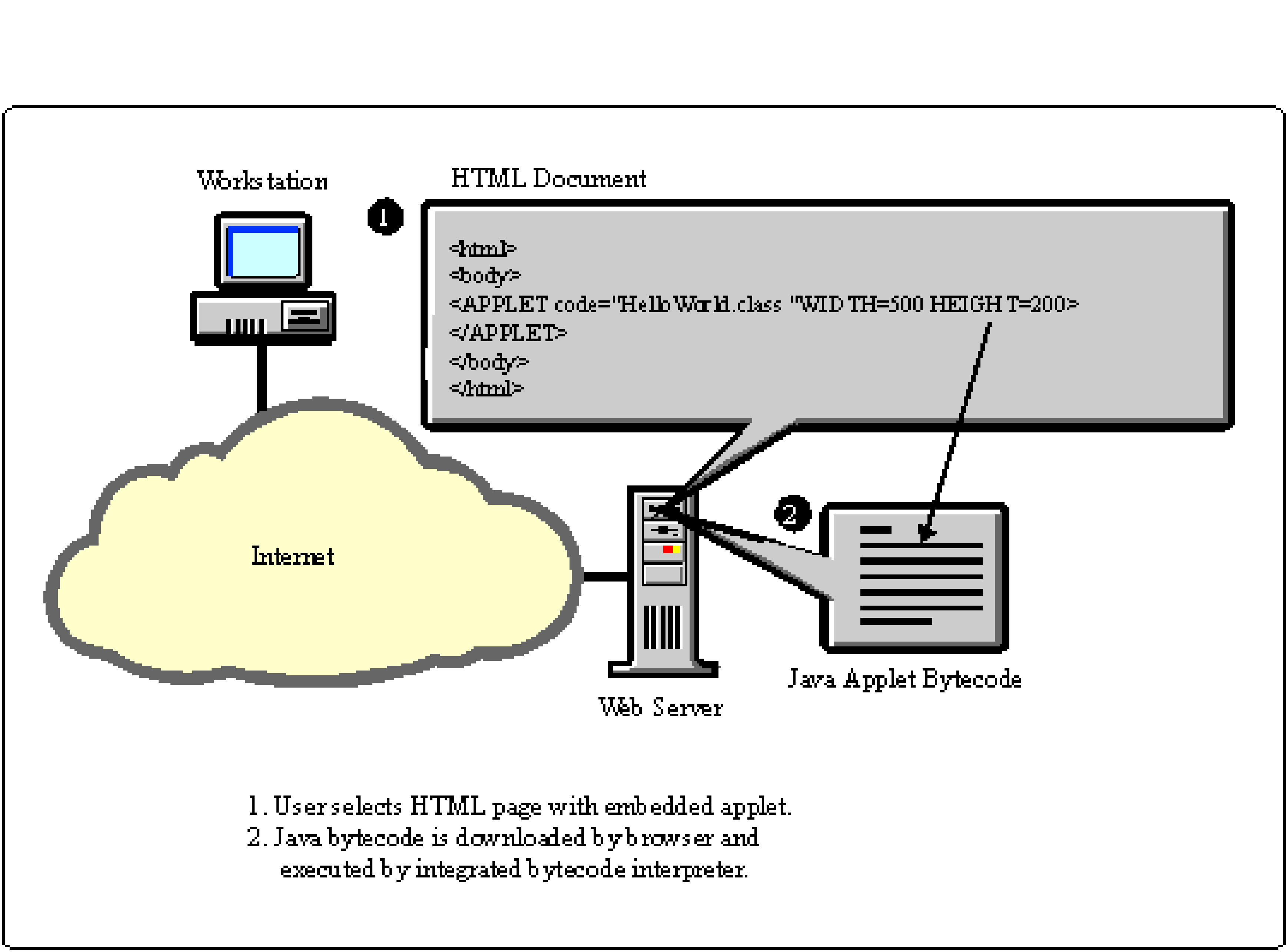
http://oldschool1.runescape.com/
Search...
The proxy server isn't responding
Old School RuneScape Game
Old School RuneScape Game
JAGEX
Main Menu
World Select
World Map
Rules
Search
RUNE SCAPE

Enter your username/email & password.

Login: *******

Password: **************

○ Remember username ☑ Hide username



```
<html>
<body>
<APPLET code="HelloWorld.class "WIDTH=500 HEIGHT=200>
</APPLET>
</body>
</html>
```

1. User selects HTML page with embedded applet.
2. Java bytecode is downloaded by browser and executed by integrated bytecode interpreter.

https://support.novell.com/techcenter/articles/dnd19960801.html

Um...whatcha got there?
A smoothie.
imgflip.com

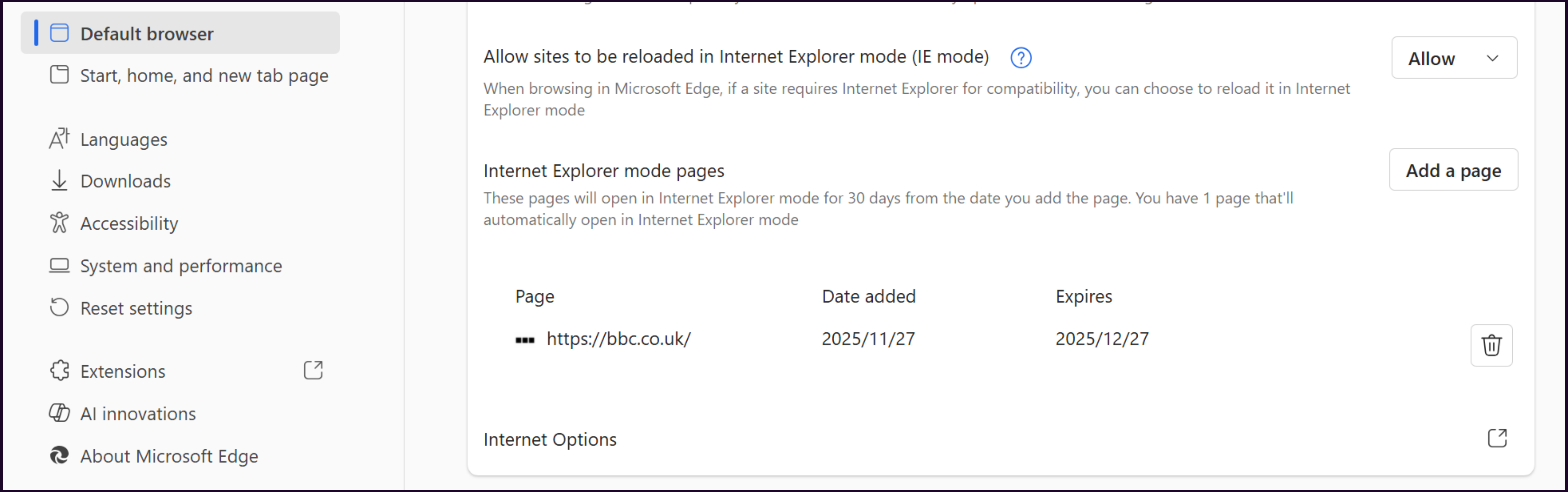
What do we need to make this work?

1. Need to Edge to open the page in IE mode

2. We need the Java Applet to have permissions beyond the Java Sandbox

3. We need the applet to be transparent to the user

IE pages file



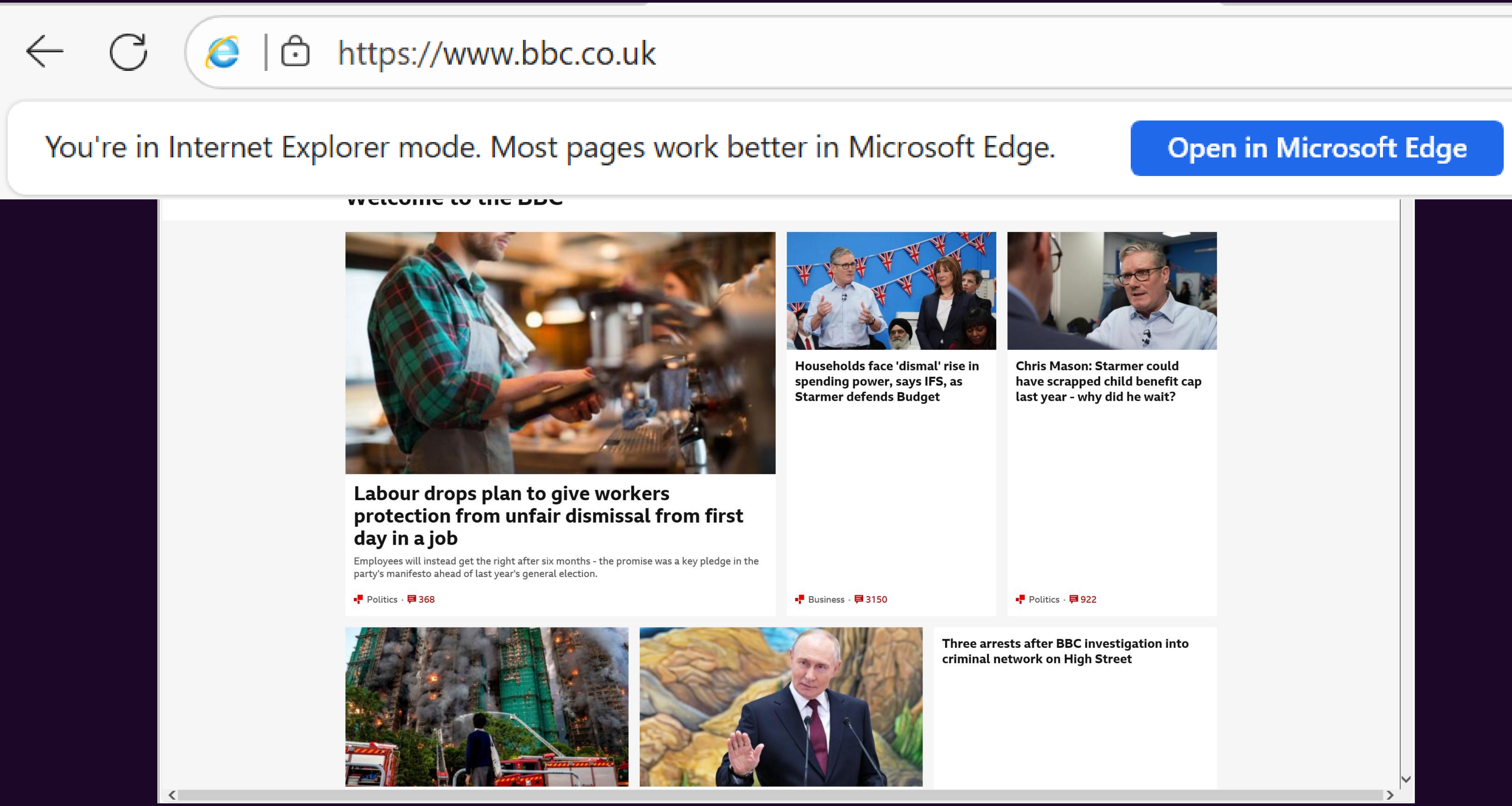
Allow sites to be reloaded in Internet Explorer mode (IE mode): Allow

When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode

Internet Explorer mode pages

These pages will open in Internet Explorer mode for 30 days from the date you add the page. You have 1 page that'll automatically open in Internet Explorer mode

Page	Date added	Expires
https://bbc.co.uk/	2025/11/27	2025/12/27



https://www.bbc.co.uk

You're in Internet Explorer mode. Most pages work better in Microsoft Edge.

Welcome to the BBC

Labour drops plan to give workers protection from unfair dismissal from first day in a job

Employees will instead get the right after six months - the promise was a key pledge in the party's manifesto ahead of last year's general election.

Politics · 368

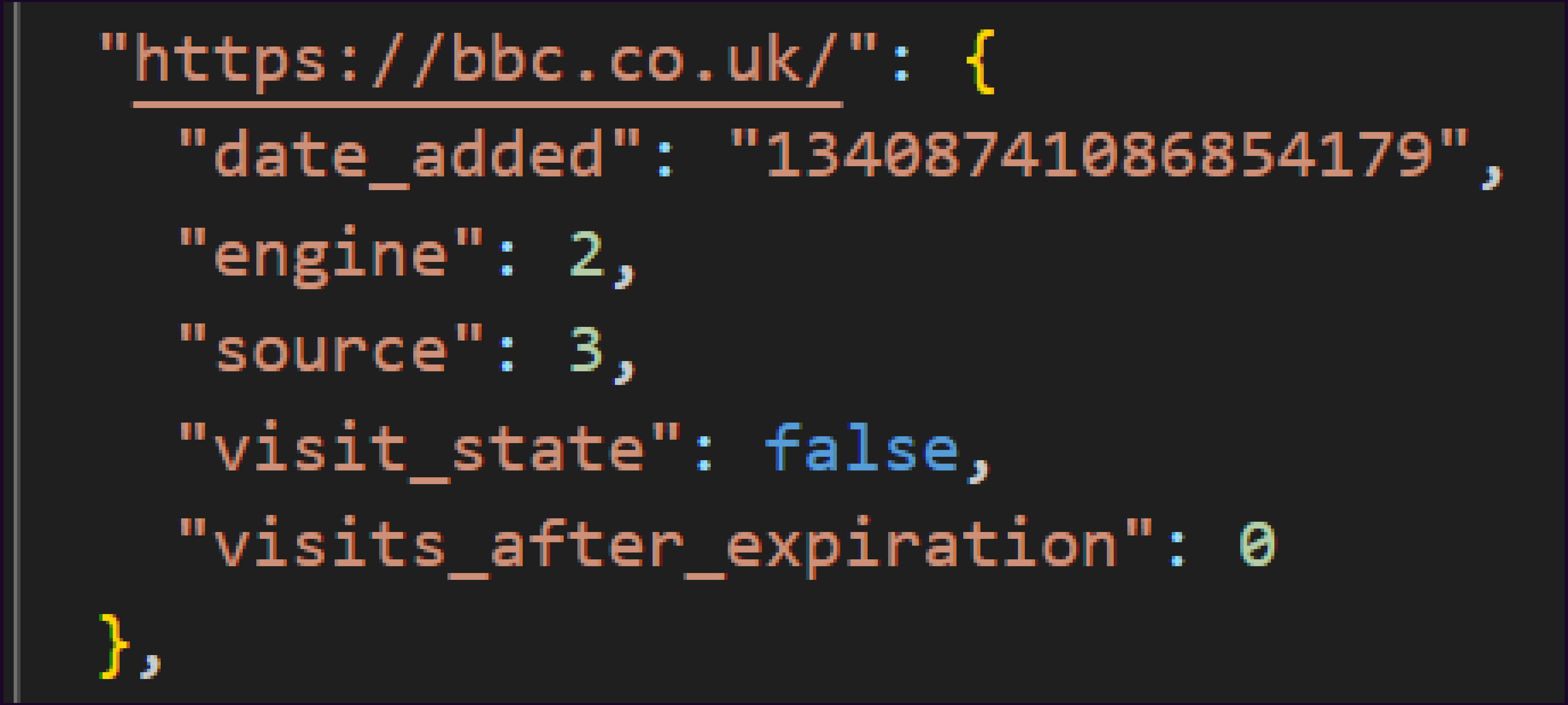
Households face 'dismal' rise in spending power, says IFS, as Starmer defends Budget

Business · 3150

Chris Mason: Starmer could have scrapped child benefit cap last year - why did he wait?

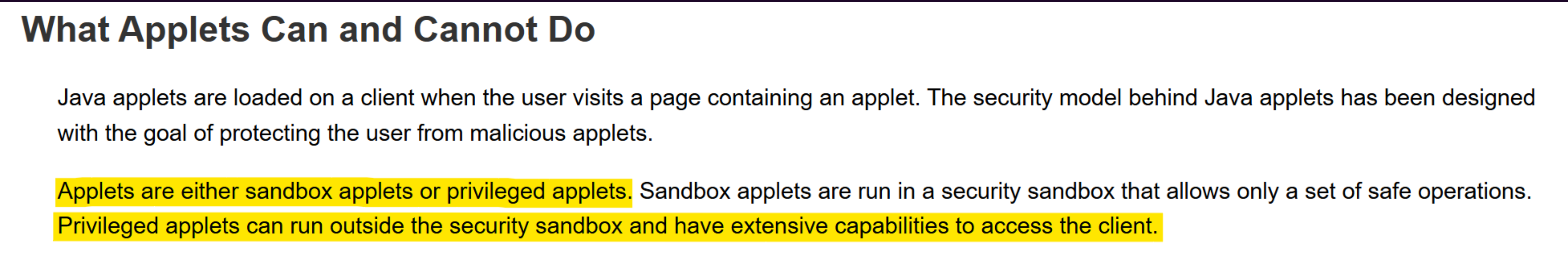
Politics · 922

Three arrests after BBC investigation into criminal network on High Street



```
  "https://bbc.co.uk/": {
    "date_added": "13408741086854179",
    "engine": 2,
    "source": 3,
    "visit_state": false,
    "visits_after_expiration": 0
  },
```

Java Applet Permissions



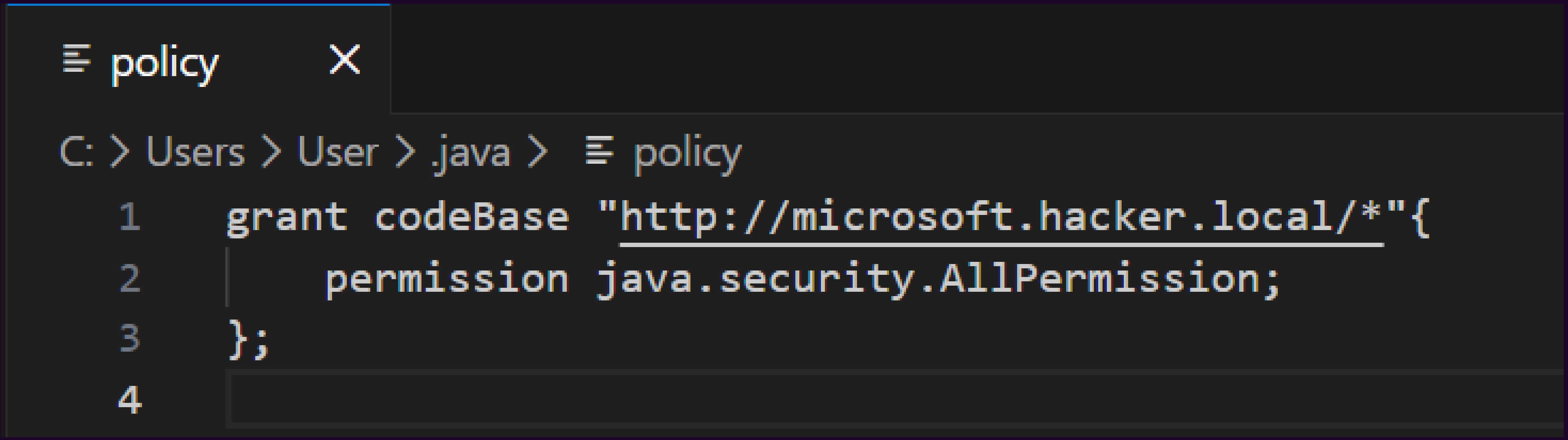
What Applets Can and Cannot Do

Java applets are loaded on a client when the user visits a page containing an applet. The security model behind Java applets has been designed with the goal of protecting the user from malicious applets.

Applets are either sandbox applets or privileged applets. Sandbox applets are run in a security sandbox that allows only a set of safe operations. Privileged applets can run outside the security sandbox and have extensive capabilities to access the client.

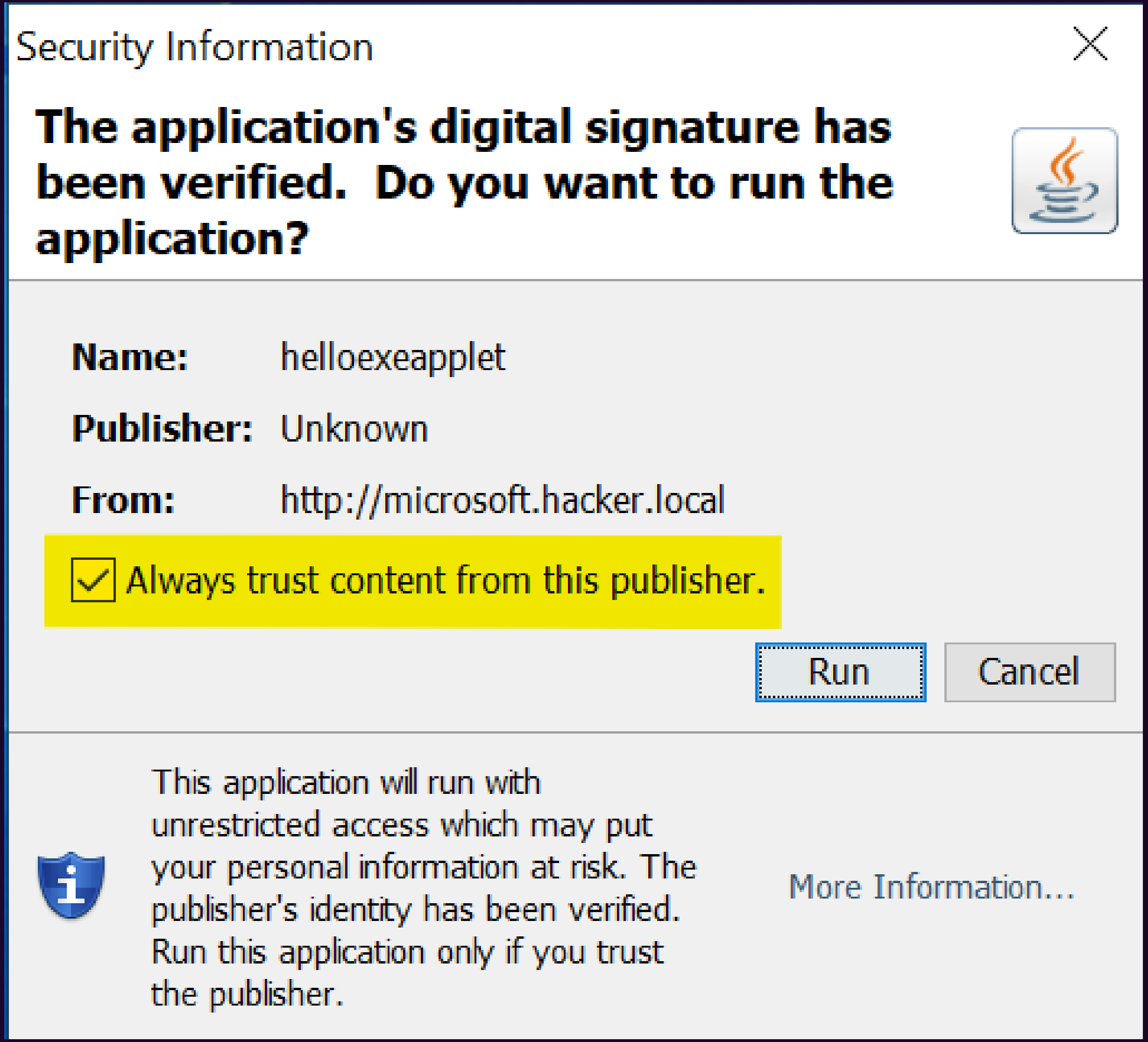
https://docs.oracle.com/javase/tutorial/deployment/applet/security.html

Java Applet Permissions



```
grant codeBase "http://microsoft.hacker.local/*"{
    permission java.security.AllPermission;
};

```

User Warnings



Security Information

The application's digital signature has been verified. Do you want to run the application?

Name: helloexeapplet

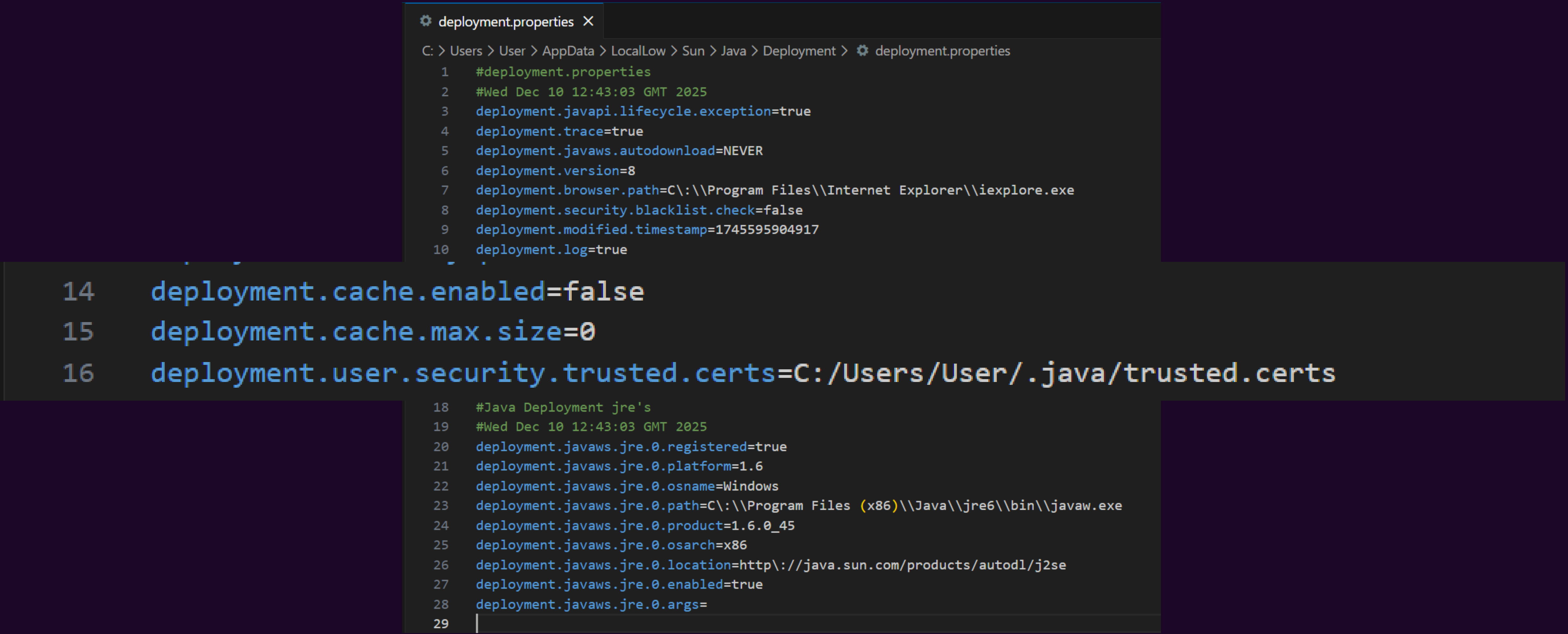
Publisher: Unknown

From: http://microsoft.hacker.local

☑ Always trust content from this publisher.

This application will run with unrestricted access which may put your personal information at risk. The publisher's identity has been verified. Run this application only if you trust the publisher.

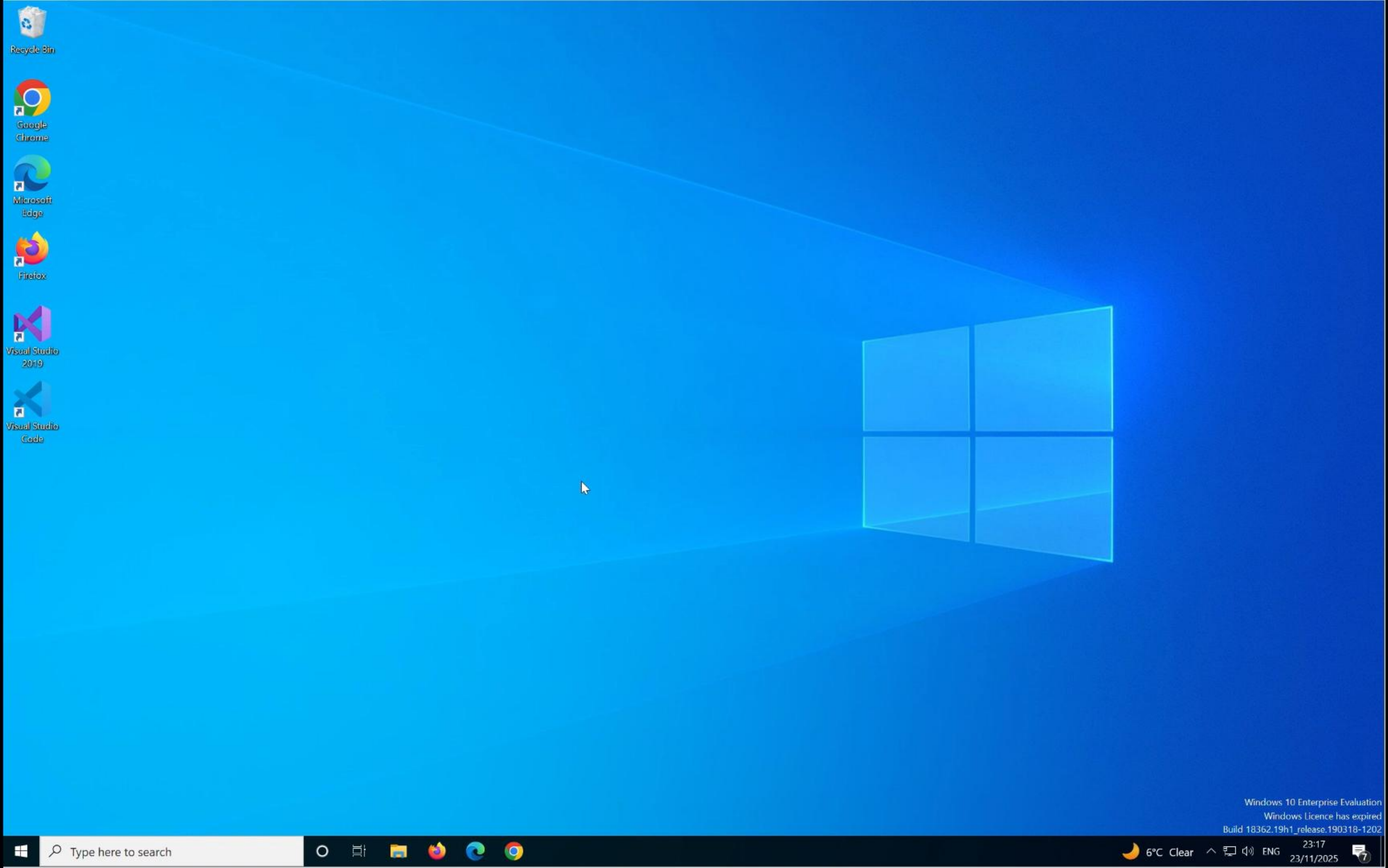
deployment.properties


deployment.properties
C: > Users > User > AppData > LocalLow > Sun > Java > Deployment > deployment.properties

```
#deployment.properties
#Wed Dec 10 12:43:03 GMT 2025
deployment.javapi.lifecycle.exception=true
deployment.trace=true
deployment.javaws.autodownload=NEVER
deployment.version=8
deployment.browser.path=C\:\\Program Files\\Internet Explorer\\iexplore.exe
deployment.security.blacklist.check=false
deployment.modified.timestamp=1745595904917
deployment.log=true
```

```
deployment.cache.enabled=false
deployment.cache.max.size=0
deployment.user.security.trusted.certs=C:/Users/User/.java/trusted.certs
```

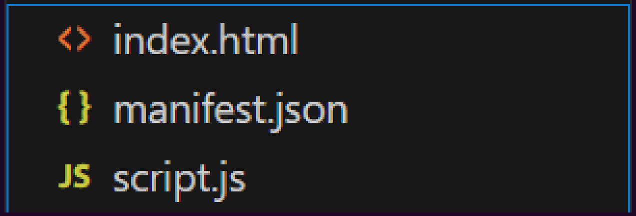
```
#Java Deployment jre's
#Wed Dec 10 12:43:03 GMT 2025
deployment.javaws.jre.0.registered=true
deployment.javaws.jre.0.platform=1.6
deployment.javaws.jre.0.osname=Windows
deployment.javaws.jre.0.path=C\:\\Program Files (x86)\\Java\\jre6\\bin\\javaw.exe
deployment.javaws.jre.0.product=1.6.0_45
deployment.javaws.jre.0.osarch=x86
deployment.javaws.jre.0.location=http\://java.sun.com/products/autodl/j2se
deployment.javaws.jre.0.enabled=true
deployment.javaws.jre.0.args=
```



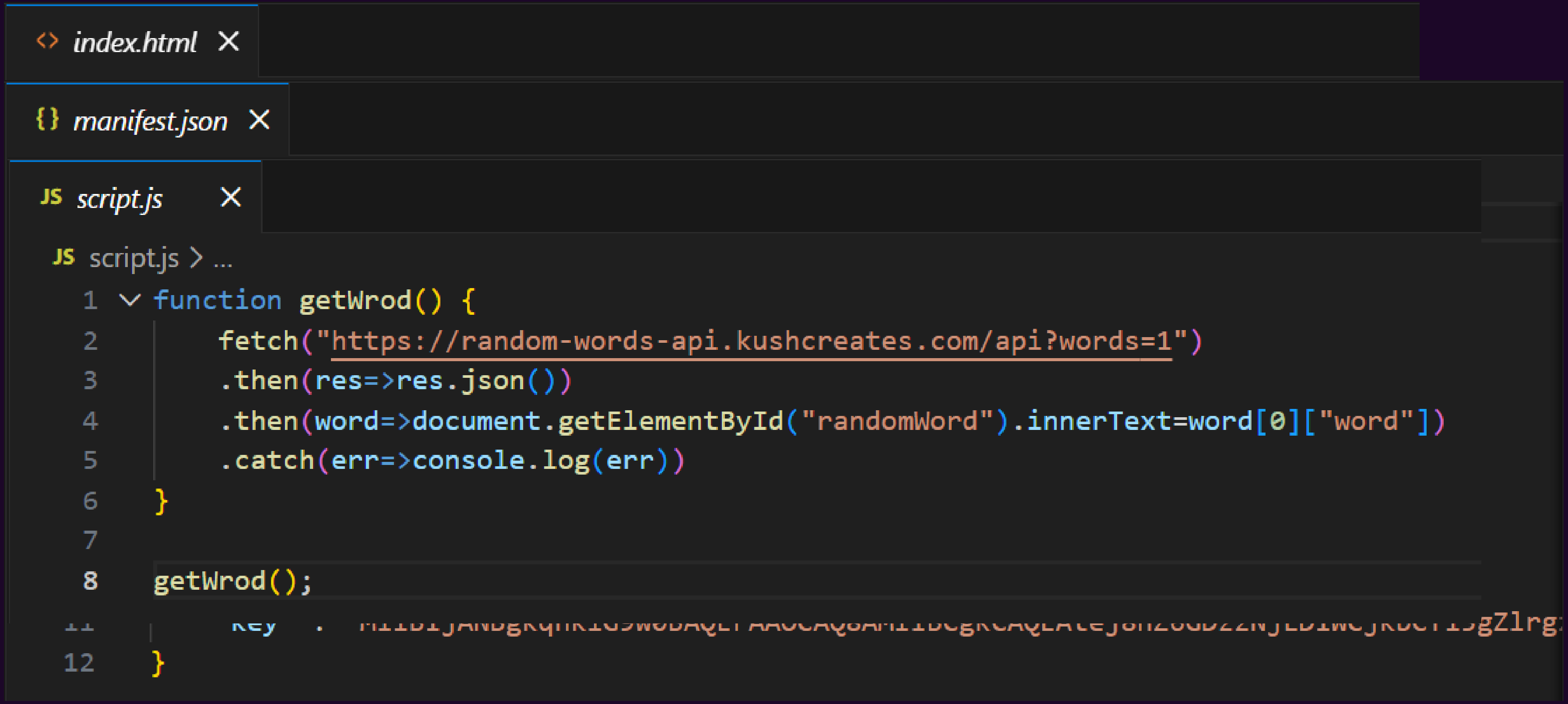
Windows 10 Enterprise Evaluation
Windows Licence has expired
Build 18362.19h1_release.190318-1202

Extensions

Anatomy of an Extension



- index.html
- manifest.json
- script.js



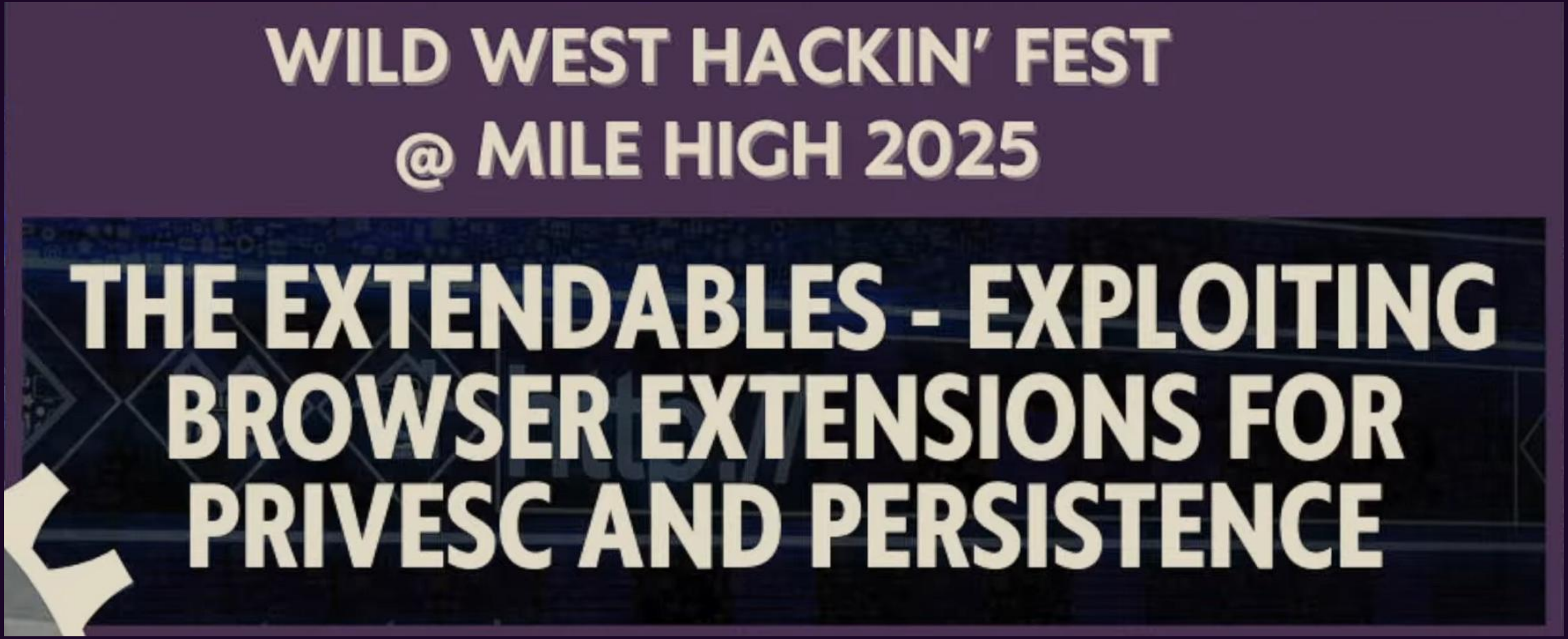
```javascript
function getWrod() {
    fetch("https://random-words-api.kushcreates.com/api?words=1")
    .then(res=>res.json())
    .then(word=>document.getElementById("randomWord").innerText=word[0]["word"])
    .catch(err=>console.log(err))
}

getWrod();
```

```
}
```

Very powerful permissions

- Cookies
- History
- Bookmarks
- Clipboard Read & Write
- Debugger
  - *Read and change all your data on all websites.*
- Proxy

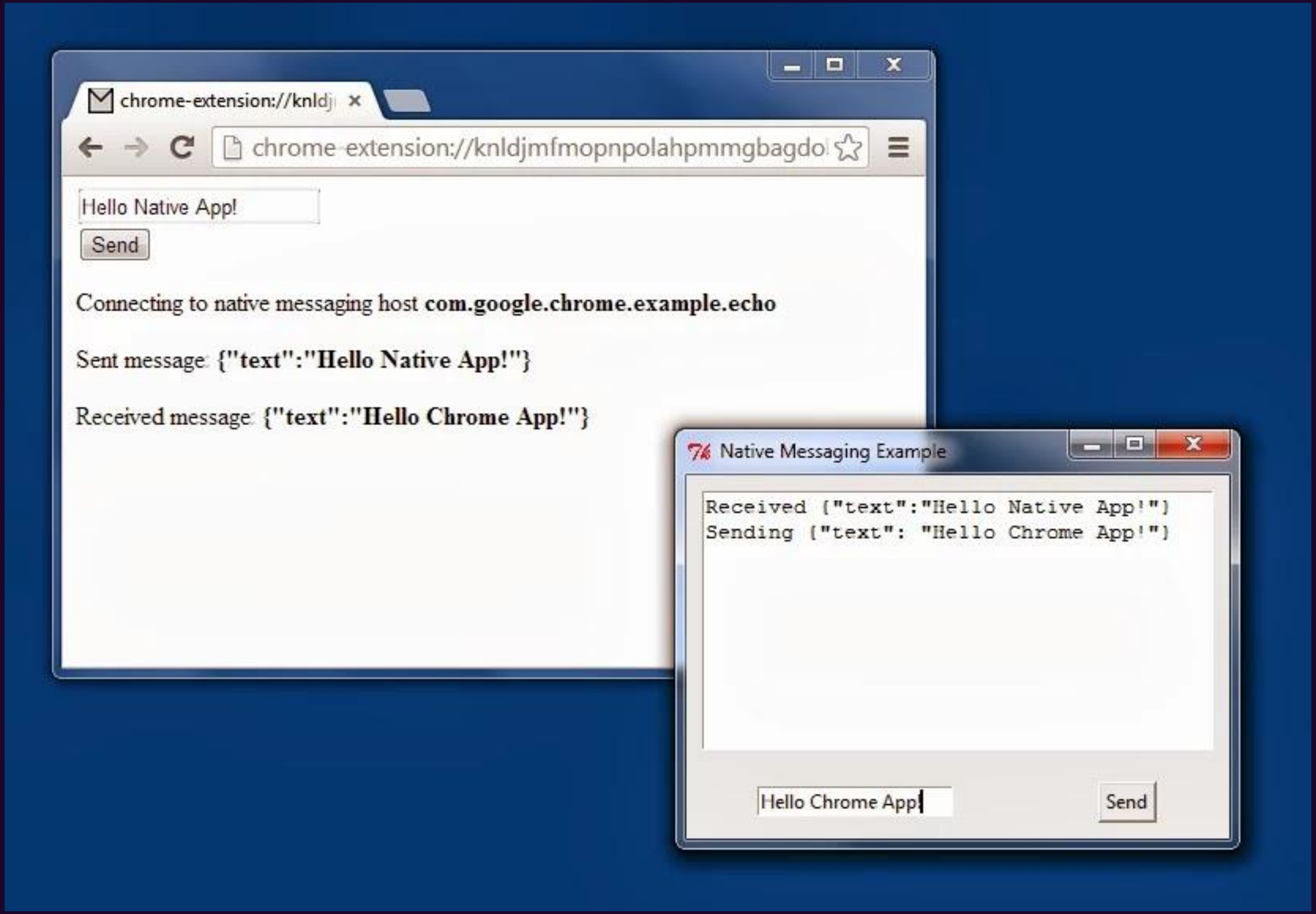
Can also run local binaries



WILD WEST HACKIN' FEST
@ MILE HIGH 2025

THE EXTENDABLES - EXPLOITING BROWSER EXTENSIONS FOR PRIVESC AND PERSISTENCE

Native messaging



Connecting to native messaging host **com.google.chrome.example.echo**

Sent message: **{"text":"Hello Native App!"}**

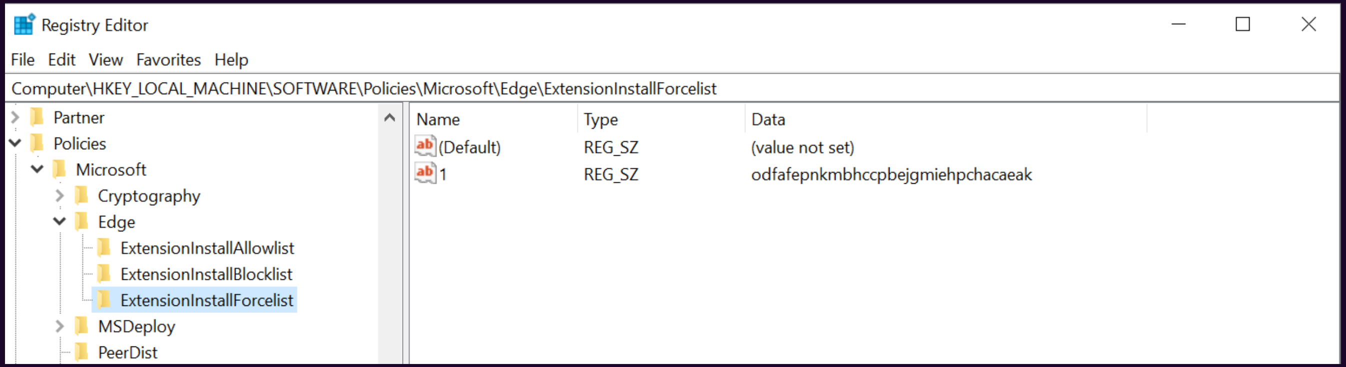
Received message: **{"text":"Hello Chrome App!"}**

```
Received {"text":"Hello Native App!"}
Sending {"text": "Hello Chrome App!"}
```

https://blog.chromium.org/2013/10/connecting-chrome-apps-and-extensions.html

Silently Installing extensions

- Force Install

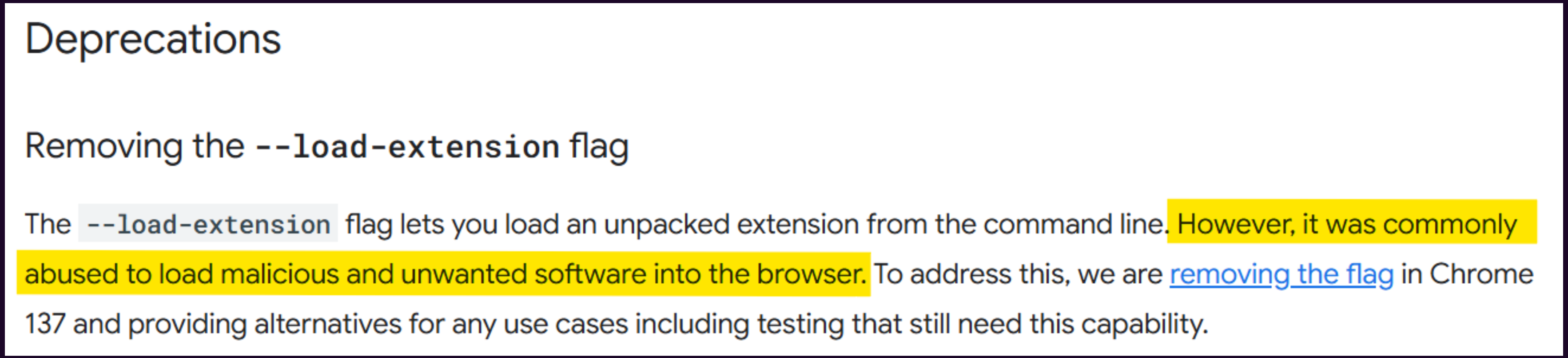


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist

- Partner
- Policies
  - Microsoft
    - Cryptography
    - Edge
      - ExtensionInstallAllowlist
      - ExtensionInstallBlocklist
      - ExtensionInstallForcelist
    - MSDeploy
    - PeerDist

Name	Type	Data
(Default)	REG_SZ	(value not set)
1	REG_SZ	odfafepnkmbhccpbejgmiehpchacaeak

- --load-extension

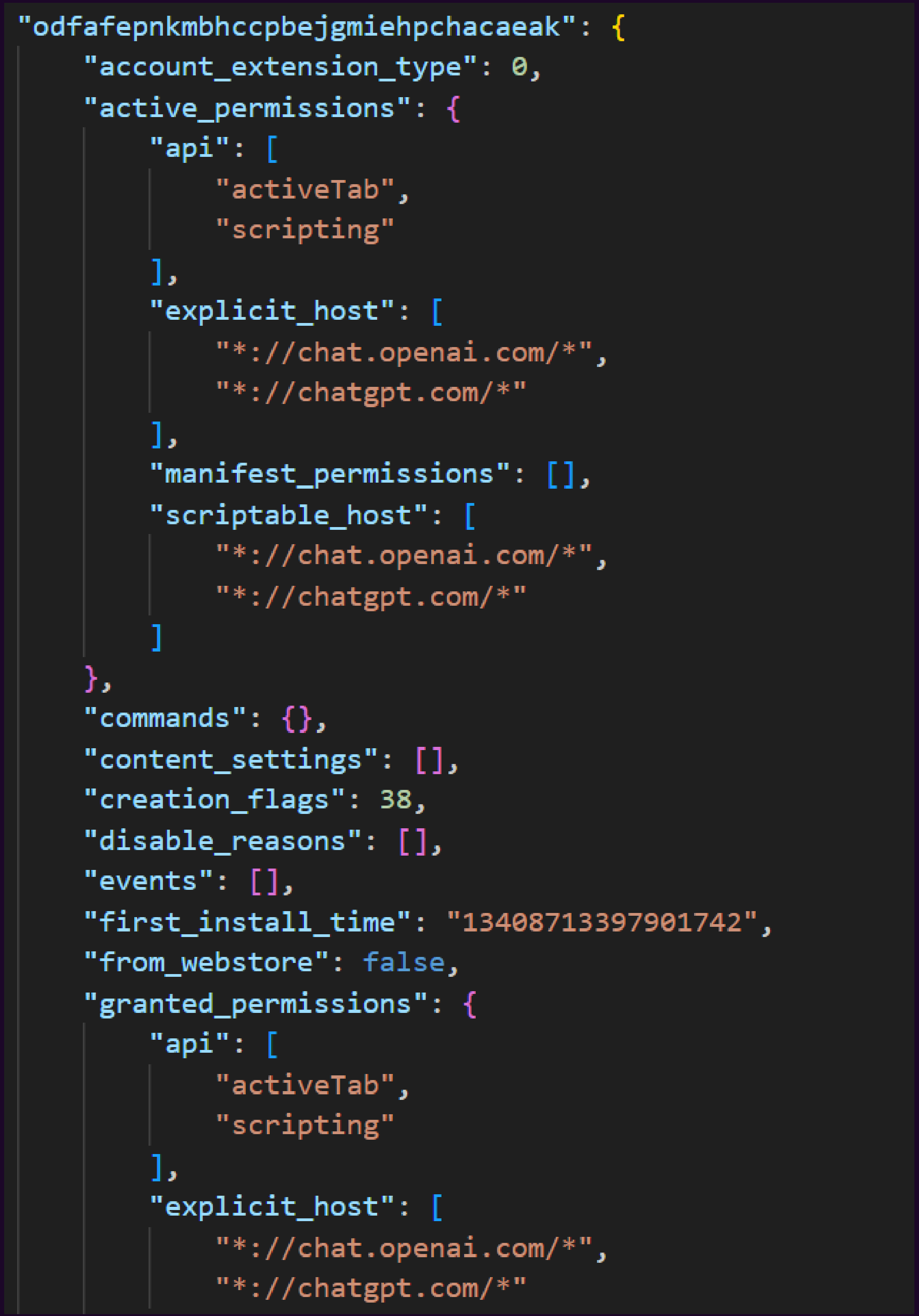


Deprecations

Removing the `--load-extension` flag

The `--load-extension` flag lets you load an unpacked extension from the command line. However, it was commonly abused to load malicious and unwanted software into the browser. To address this, we are removing the flag in Chrome 137 and providing alternatives for any use cases including testing that still need this capability.

https://developer.chrome.com/blog/extension-news-june-2025#deprecations



```
"odfafepnkmbhccpbejgmiehpchacaeak": {
    "account_extension_type": 0,
    "active_permissions": {
        "api": [
            "activeTab",
            "scripting"
        ],
        "explicit_host": [
            "*://chat.openai.com/*",
            "*://chatgpt.com/*"
        ],
        "manifest_permissions": [],
        "scriptable_host": [
            "*://chat.openai.com/*",
            "*://chatgpt.com/*"
        ]
    },
    "commands": {},
    "content_settings": [],
    "creation_flags": 38,
    "disable_reasons": [],
    "events": [],
    "first_install_time": "13408713397901742",
    "from_webstore": false,
    "granted_permissions": {
        "api": [
            "activeTab",
            "scripting"
        ],
        "explicit_host": [
            "*://chat.openai.com/*",
            "*://chatgpt.com/*"
```

Bypassing allowlisting

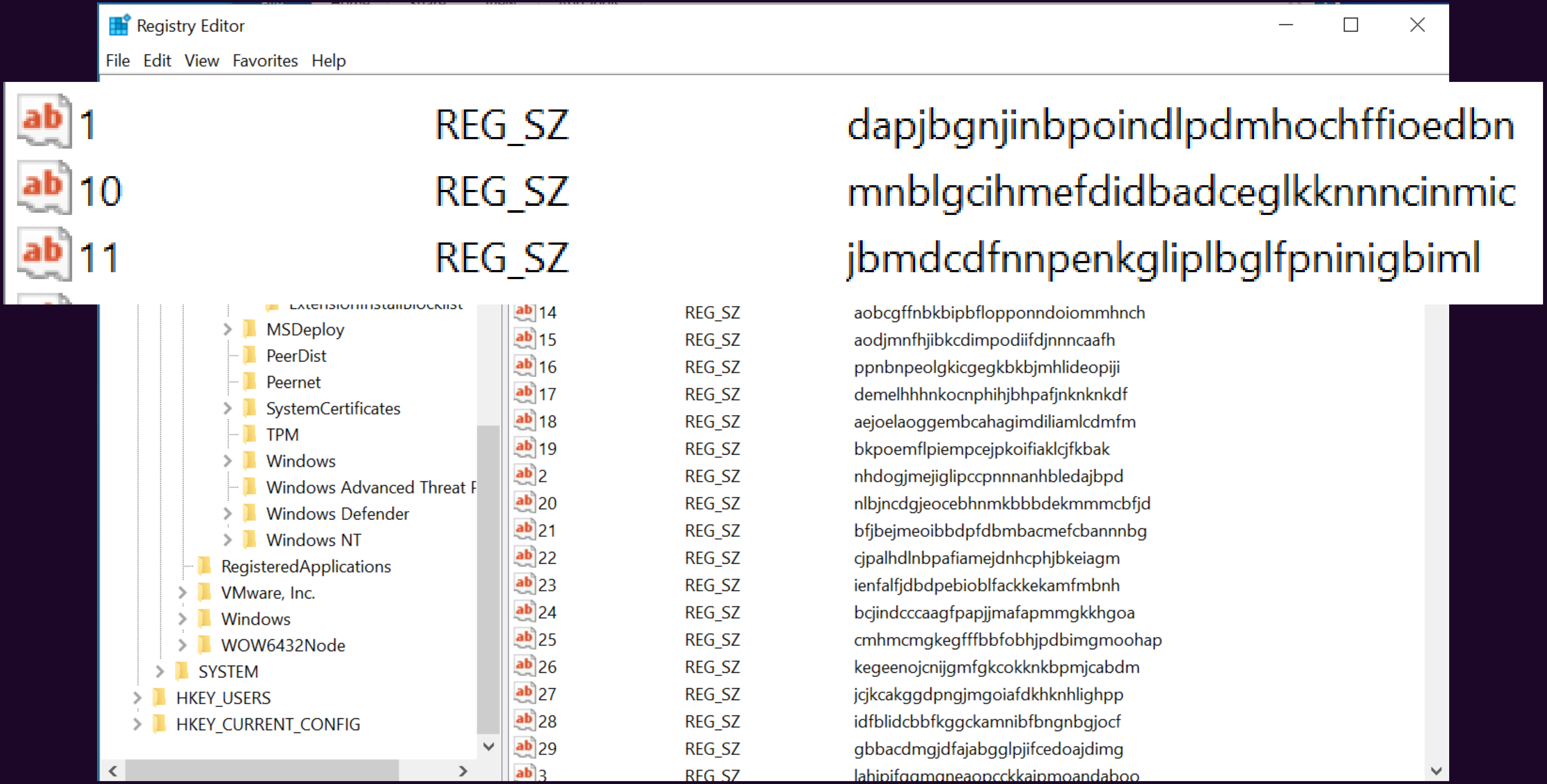
Credit to:

THE PHANTOM EXTENSION: BACKDOORING CHROME THROUGH UNCHARTED PATHWAYS

Written by Riadh Bouchahoua - 23/09/2025 - in Pentest - Download

https://www.synacktiv.com/en/publications/the-phantom-extension-backdooring-chrome-through-uncharted-pathways

Allowlisting Extensions

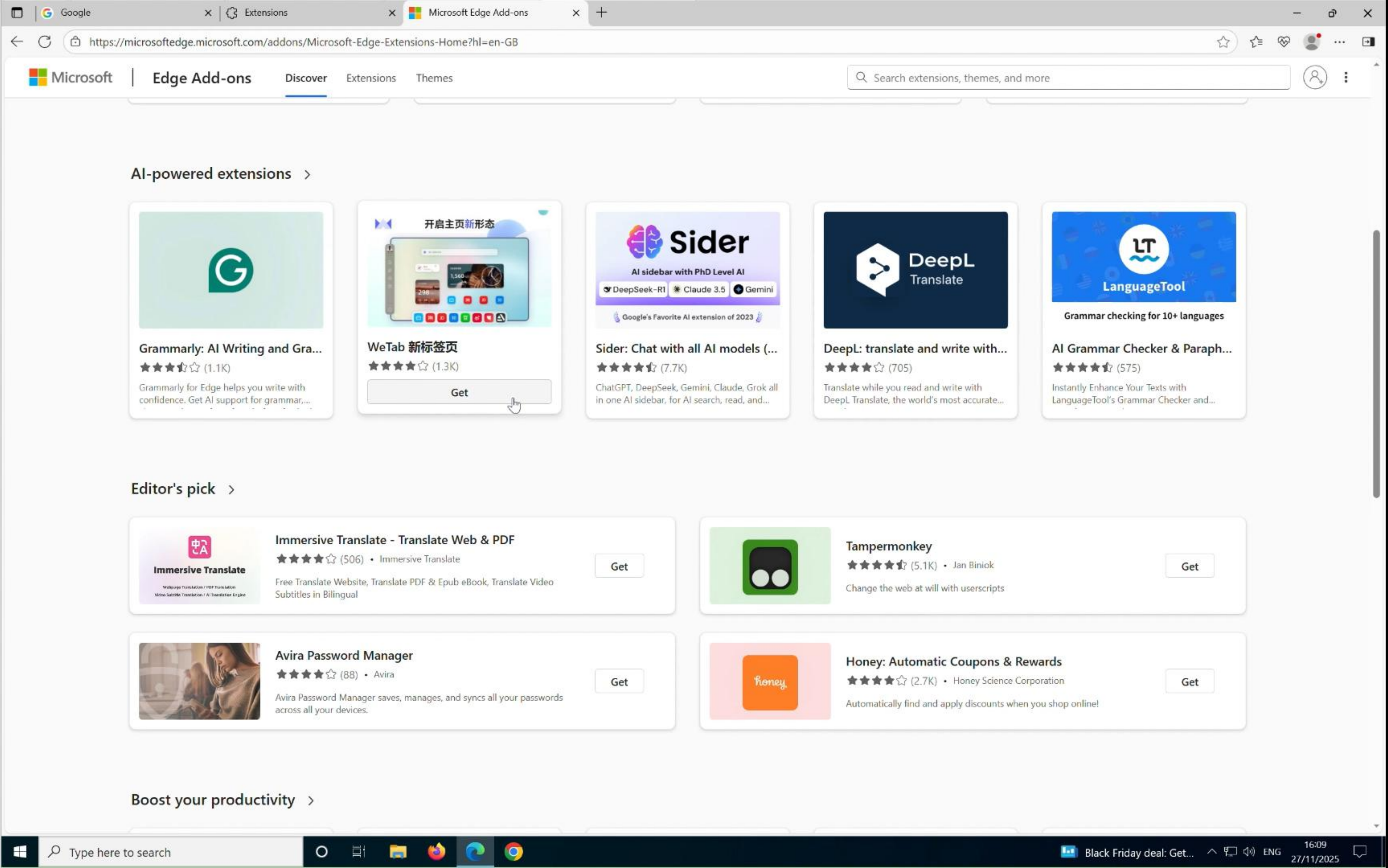


1	REG_SZ	dapjbgnjinbpoindlpdmhochffioedbn
10	REG_SZ	mnblgcihmefdidbadceglkknnncinmic
11	REG_SZ	jbmdcdfnnpenkgliplbglfpninigbiml
14	REG_SZ	aobcgffnbkbipbflopponndoiommhnch
15	REG_SZ	aodjmnfhjibkcdimpodiifdjnnncaafh
16	REG_SZ	ppnbnpeolgkicgegkbkbjmhlideopiji
17	REG_SZ	demelhhhnkocnphihjbhpafjnknknkdf
18	REG_SZ	aejoelaoggembcahagimdiliamlcdmfm
19	REG_SZ	bkpoemflpiempcejpkoifiaklcjfkbak
2	REG_SZ	nhdogjmejiglipccpnnnanhbledajbpd
20	REG_SZ	nlbjncdgjeocebhnmkbbbdekmmmcbfjd
21	REG_SZ	bfjbejmeoibbdpfdbmbacmefcbannnbg
22	REG_SZ	cjpalhdlnbpafiamejdnhcphjbkeiagm
23	REG_SZ	ienfalfjdbdpebioblfackkekamfmbnh
24	REG_SZ	bcjindcccaagfpapjjmafapmmgkkhgoa
25	REG_SZ	cmhmcmgkegfffbbfobhjpdbimgmoohap
26	REG_SZ	kegeenojcnijgmfgkcokknkbpmjcabdm
27	REG_SZ	jcjkcakggdpngjmgoiafdkhknhlighpp
28	REG_SZ	idfblidcbbfkggckamnibfbngnbgjocf
29	REG_SZ	gbbacdmgjdfajabgglpjifcedoajdimg
3	REG_SZ	lahipifggmgneaopcckkaipmoandaboo

How does the browser calculate IDs

- A Chrome Extension ID is the first 32 characters of the SHA256 hash of a public key, where characters 0-9a-f are translated to their respective a-p counterparts.

- The Public key is stored in the manifest.json


Google
Extensions
Microsoft Edge Add-ons
https://microsoftedge.microsoft.com/addons/Microsoft-Edge-Extensions-Home?hl=en-GB
Microsoft
Edge Add-ons
Discover
Extensions
Themes
Search extensions, themes, and more

AI-powered extensions >

开启主页新形态
Sider
AI sidebar with PhD Level AI
DeepSeek-R1
Claude 3.5
Gemini
Google's Favorite AI extension of 2023
DeepL
Translate
LanguageTool
Grammar checking for 10+ languages

Grammarly: AI Writing and Gra...
★★★½☆ (1.1K)
Grammarly for Edge helps you write with confidence. Get AI support for grammar,...

WeTab 新标签页
★★★★☆ (1.3K)
Get

Sider: Chat with all AI models (...
★★★★½ (7.7K)
ChatGPT, DeepSeek, Gemini, Claude, Grok all in one AI sidebar, for AI search, read, and...

DeepL: translate and write with...
★★★★☆ (705)
Translate while you read and write with DeepL Translate, the world's most accurate...

AI Grammar Checker & Paraph...
★★★★½ (575)
Instantly Enhance Your Texts with LanguageTool's Grammar Checker and...

Editor's pick >

Immersive Translate - Translate Web & PDF
★★★★☆ (506) • Immersive Translate
Free Translate Website, Translate PDF & Epub eBook, Translate Video Subtitles in Bilingual
Get

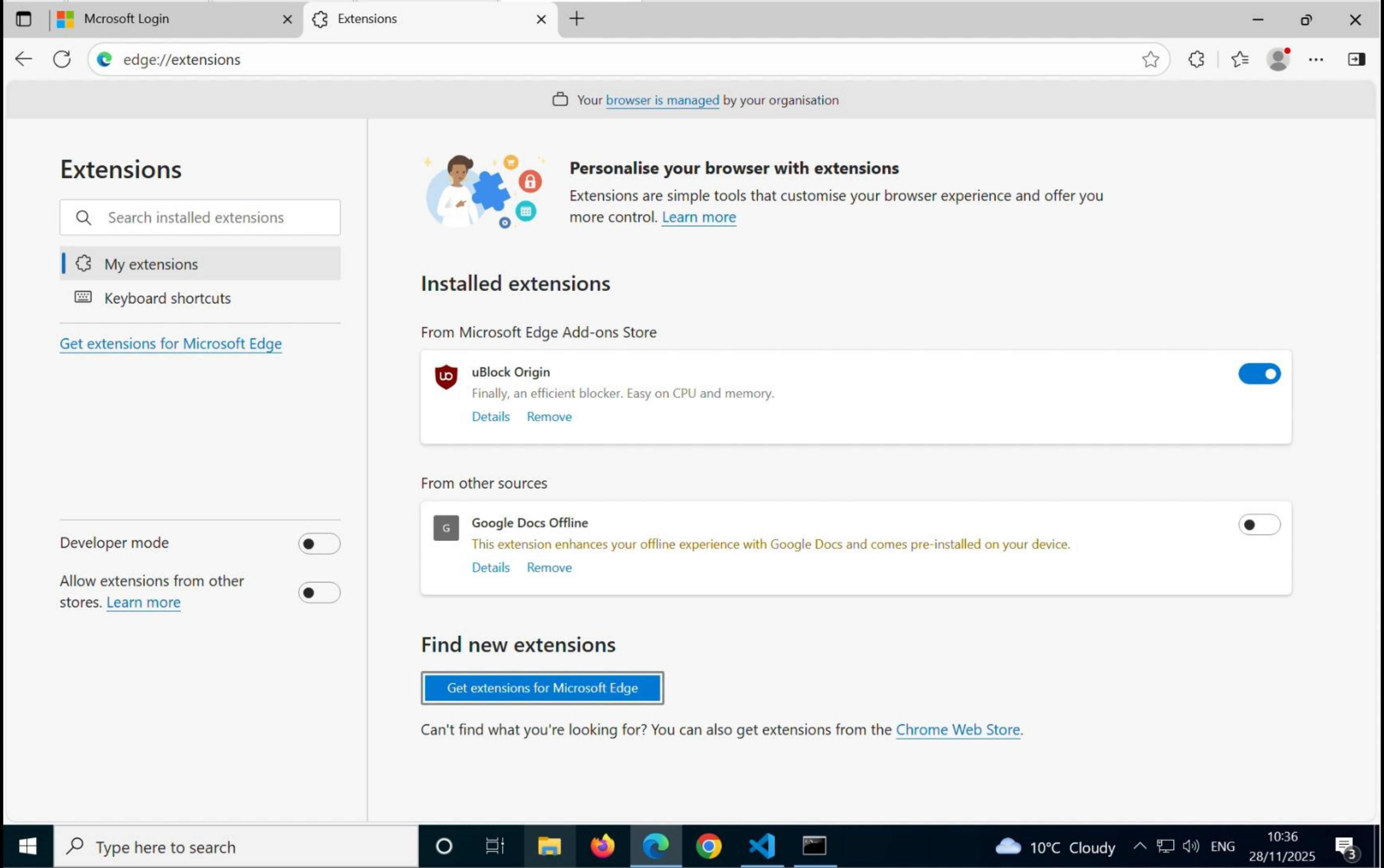
Tampermonkey
★★★★½ (5.1K) • Jan Biniok
Change the web at will with userscripts
Get

Avira Password Manager
★★★★☆ (88) • Avira
Avira Password Manager saves, manages, and syncs all your passwords across all your devices.
Get

Honey: Automatic Coupons & Rewards
★★★★☆ (2.7K) • Honey Science Corporation
Automatically find and apply discounts when you shop online!
Get

Boost your productivity >

But there is more



Your browser is managed by your organisation

Extensions

Get extensions for Microsoft Edge

Developer mode ○

Allow extensions from other stores. Learn more ○

Personalise your browser with extensions

Extensions are simple tools that customise your browser experience and offer you more control. Learn more

Installed extensions

From Microsoft Edge Add-ons Store

uBlock Origin ●
Finally, an efficient blocker. Easy on CPU and memory.
Details Remove

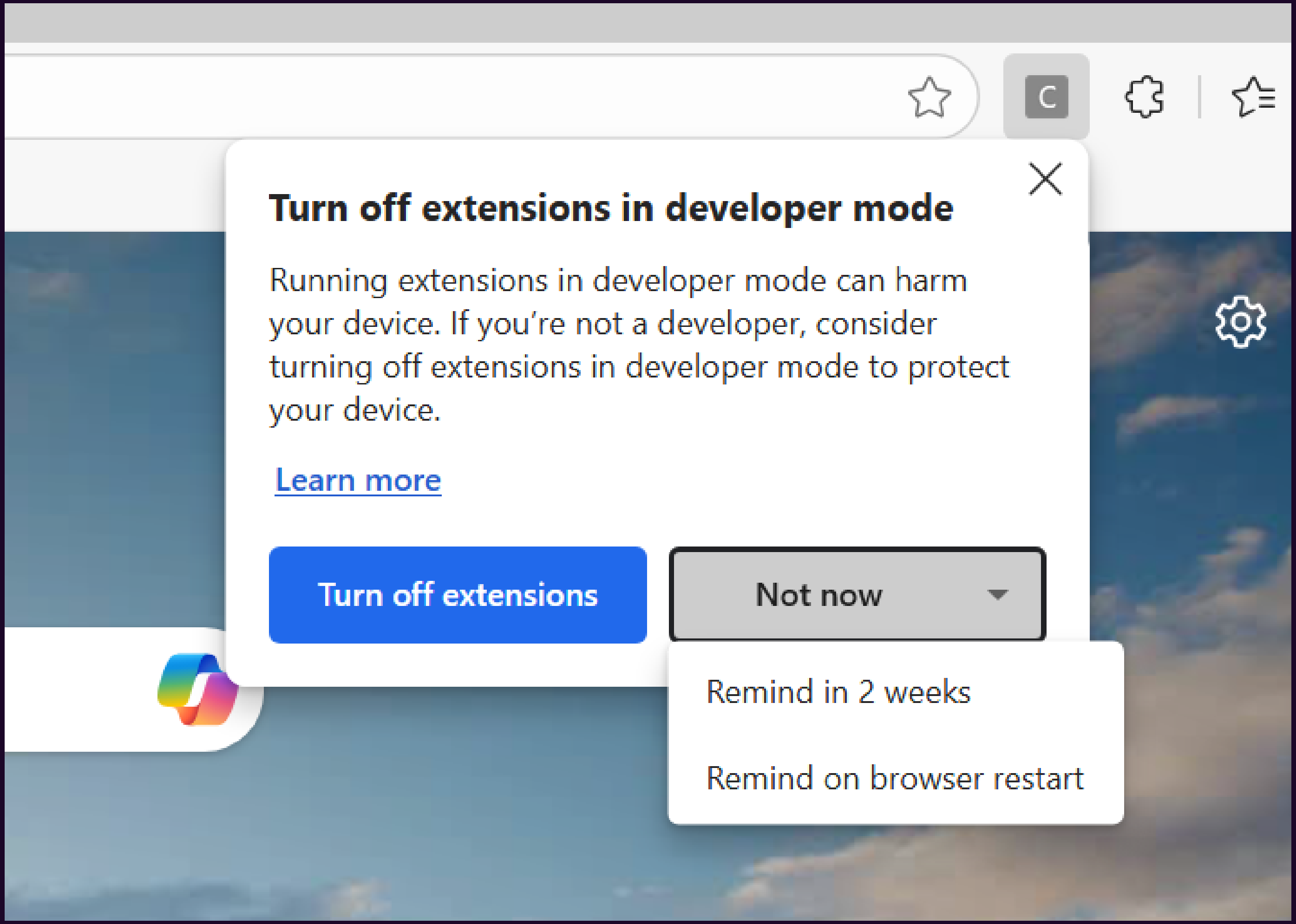
From other sources

Google Docs Offline ○
This extension enhances your offline experience with Google Docs and comes pre-installed on your device.
Details Remove

Find new extensions

Can't find what you're looking for? You can also get extensions from the Chrome Web Store.

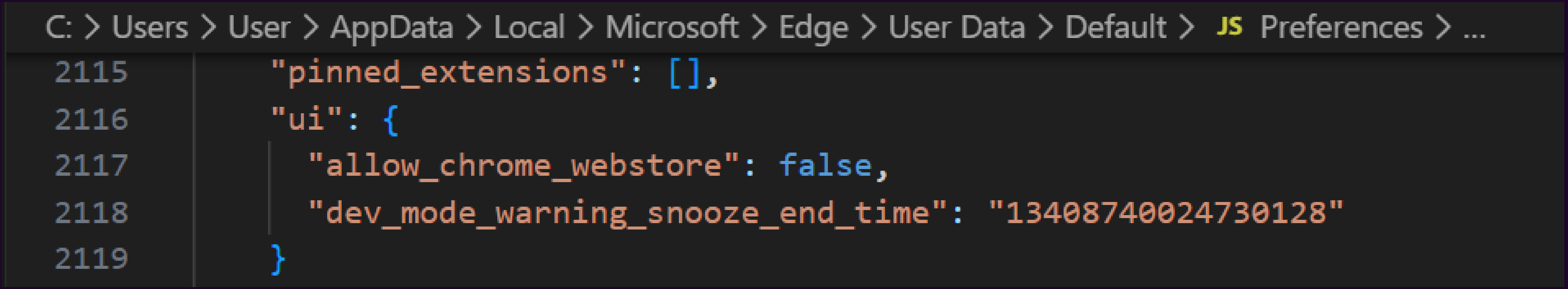
Warnings about developer mode



Turn off extensions in developer mode

Running extensions in developer mode can harm your device. If you’re not a developer, consider turning off extensions in developer mode to protect your device.

Warnings about developer mode



C: > Users > User > AppData > Local > Microsoft > Edge > User Data > Default > JS Preferences > ...

```
    "pinned_extensions": [],
    "ui": {
      "allow_chrome_webstore": false,
      "dev_mode_warning_snooze_end_time": "13408740024730128"
    }
```

How to defend

- Startup_url
  - Create an alert for SPF file for being modified for any other the appropriate browser

- Java applet
  - Disable IE mode
  - Application allowlisting (app locker would be bypassed by local admin)
  - Vulnerability and Patch management – flag old java versions

- Extensions
  - Fully disable extensions – Might be too much for most orgs
  - Force install extensions
  - Manage allowed permissions
  - Prevent access to sites via Runtime block hosts
  - Review installed extensions – We have done assessments like this
  - Identify anomalous chrome extension file locations
  - Detailed guide to the ExtensionSettings policy | Microsoft Learn

Disclosure timeline

- A few day ago, Microsoft Security Response Centre (MSRC) reached out to me about this talk to verify that it wouldn’t contain any unreported vulnerabilities
  - I replied confirming that it didn’t
- MSRC then ask for a preview of my talk
  - I supplied them with a PDF of my slides

REVERSEC

Thank you

References

- (2020) *HMAC and "Secure preferences": Revisiting chromium-based browsers security*. Available at: https://www.cse.chalmers.se/~andrei/cans20.pdf (Accessed: 11 December 2025).

- ReversecLabs (2025) *ReversecLabs/theextendables, GitHub*. Available at: https://github.com/ReversecLabs/TheExtendables (Accessed: 11 December 2025).

- Bouchahoua, R. (2025) *The phantom extension: Backdooring chrome through uncharted pathways, Synacktiv*. Available at: https://www.synacktiv.com/en/publications/the-phantom-extension-backdooring-chrome-through-uncharted-pathways (Accessed: 11 December 2025).

- *Silent chrome extension installation revisited* (no date) *Syntax*. Available at: https://syntax-err0r.github.io/Return_Of_The_Extension.html (Accessed: 11 December 2025).