black hat®
EUROPE 2023

DECEMBER 4–7

EXCEL LONDON / UK

#BHEU @BlackHatEvents

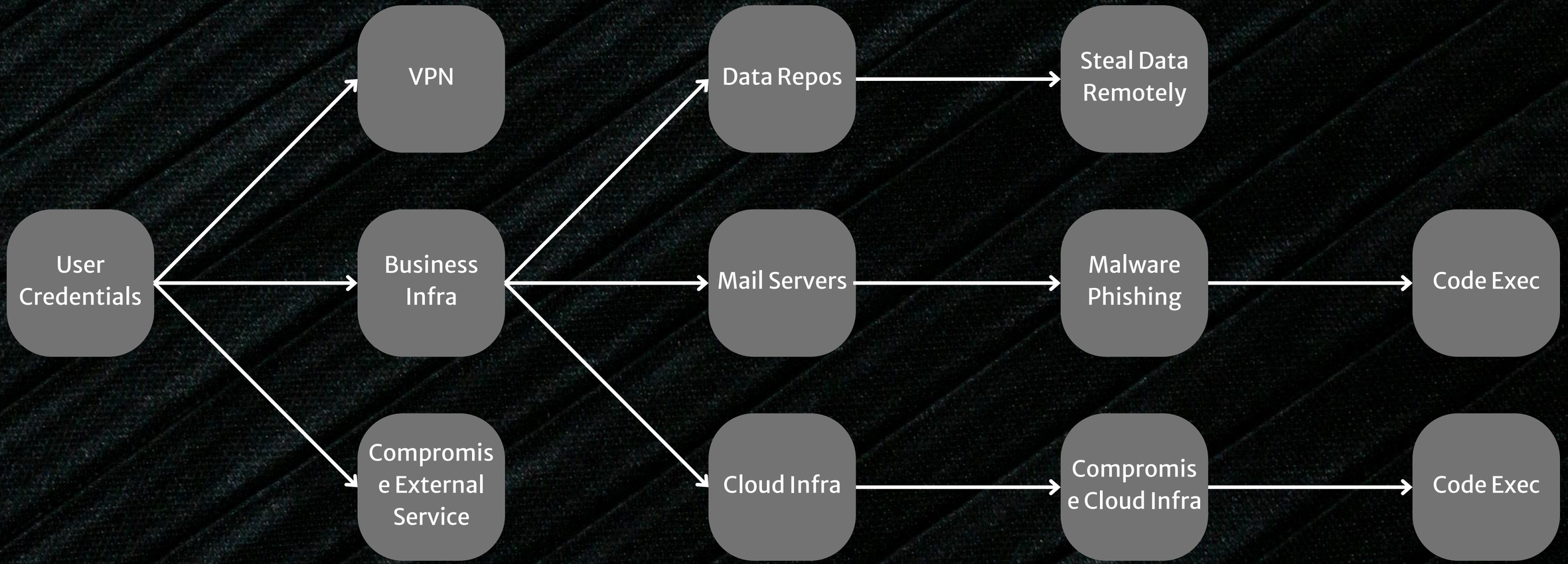
Breaching the Perimeter via Cloud Synchronized Browser Settings

Edward Prior

Cracking the perimeter

User Credentials

Cracking the perimeter



Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross-Site Request Forgery

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross-Site Request Forgery Context

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross-Site Request Forgery Context
- Browser Exploits

Malicious Links

What is the worst thing that can happen when a malicious link is clicked?

- Credential phishing User interaction
- Malware download User interaction
- Cross-Site Request Forgery Context
- Browser Exploits Context

Todays Goal

Demonstrate how cloud sync gives immense context to an attacker, and the tools to trigger remote payloads unavailable without sync.

Whoami

- Edward Prior
- @JankhJankh
- Robotics –> Machine Learning –> Pentester/Red Teamer
- OSCP, OSCE, CRTE, ETC.
- 12 CVEs
- CTF Challenge Designer for AIV@DEF CON

Outline

- Sync Introduction
- Case Studies
- Vuln Demos
- Prevention and Detection
- Automated Emulation

Intro to Cloudsync

Cloudsync is a feature in every browser to allow for a consistent state between devices.

Intro to Cloudsync

Cloudsync is a feature in every browser to allow for a consistent state between devices.

Features:

- Synced Settings, Extensions, Passwords, history, and user data
- Periodically pulls updates from a server

Likelihood of compromise

- M365
- Google Business Suite
- Personal browser accounts

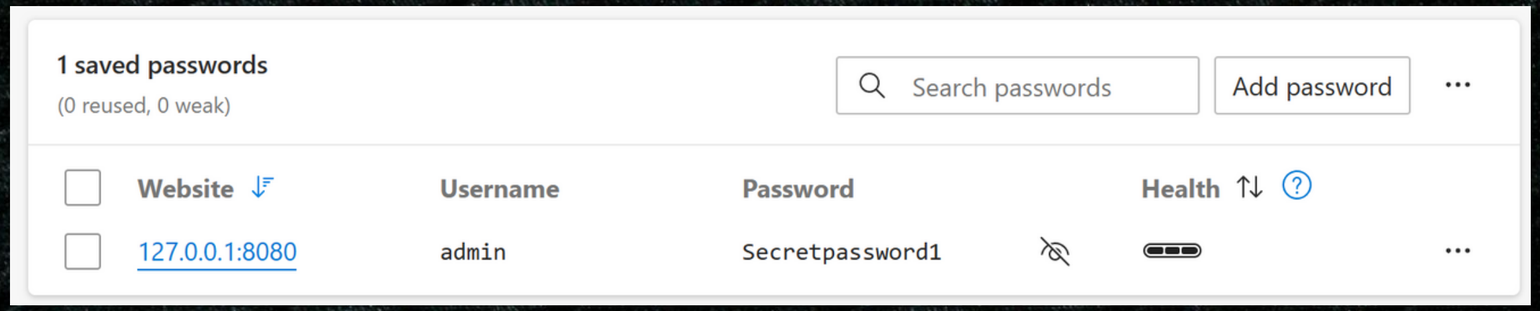
Case Studies

All case studies assume a cloud synchronised account on a corporate device has been compromised, and that the browser is being used regularly.

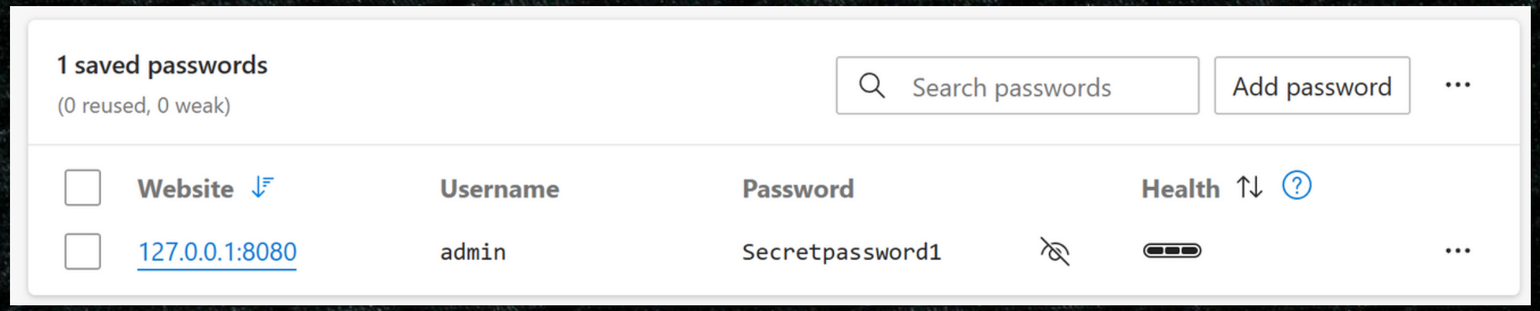
Each case study was conducted against a fully patched Chrome, Edge, and Firefox browser.

Case Study 1: Passive Actions

Case Study 1: Passive Actions

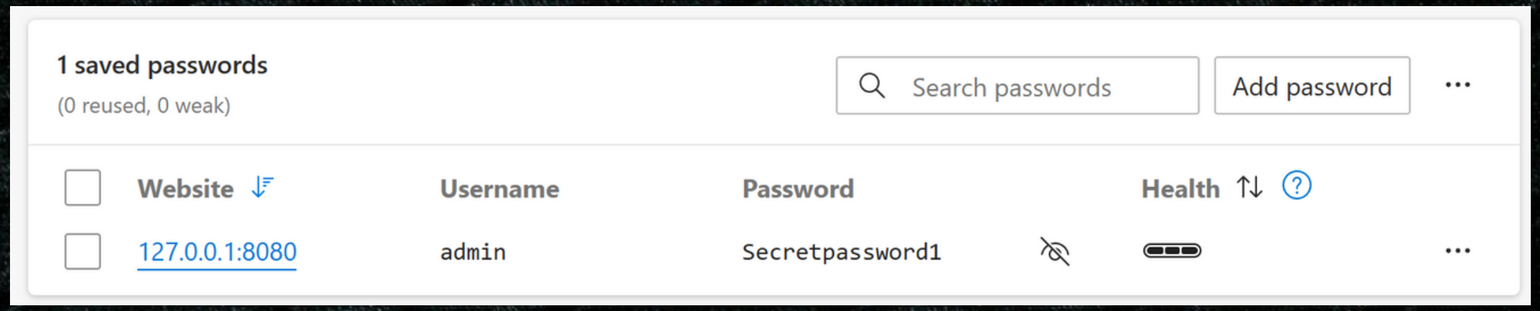


Case Study 1: Passive Actions




```
"NON_UNIQUE_NAME": "cardnumber|42424242424242",
"ORIGINATOR_CACHE_GUID": "",
"ORIGINATOR_CLIENT_ITEM_ID": "",
"PARENT_ID": "",
"SERVER_DEFINED_UNIQUE_TAG": "",
"SPECIFICS": {
  "autofill": {
    "name": "cardnumber",
    "usage_timestamp": [
      "13340874180000000"
    ],
    "value": "42424242424242"
  }
```

Case Study 1: Passive Actions

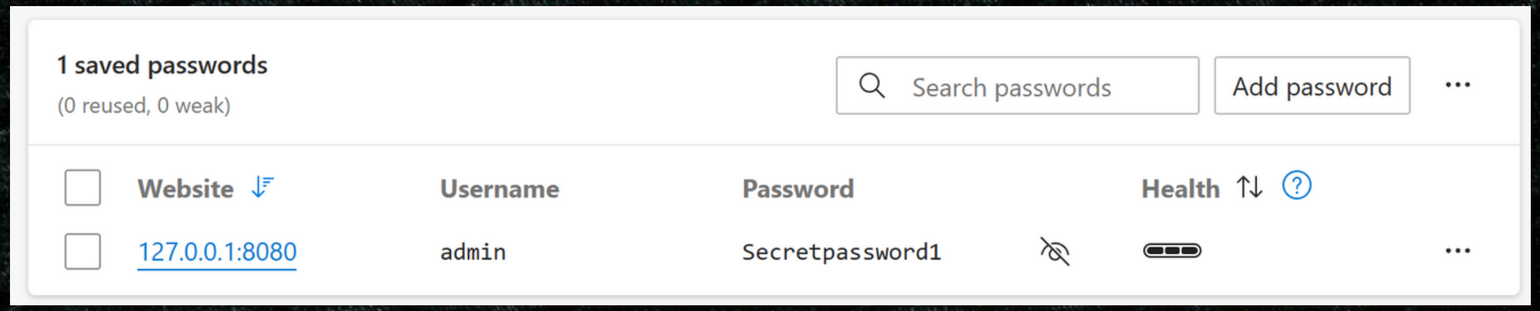


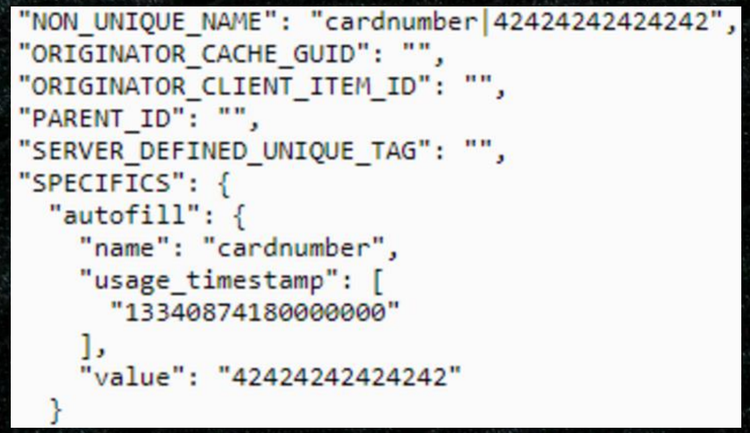

```
"NON_UNIQUE_NAME": "cardnumber|42424242424242",
"ORIGINATOR_CACHE_GUID": "",
"ORIGINATOR_CLIENT_ITEM_ID": "",
"PARENT_ID": "",
"SERVER_DEFINED_UNIQUE_TAG": "",
"SPECIFICS": {
  "autofill": {
    "name": "cardnumber",
    "usage_timestamp": [
      "13340874180000000"
    ],
    "value": "42424242424242"
  }
```

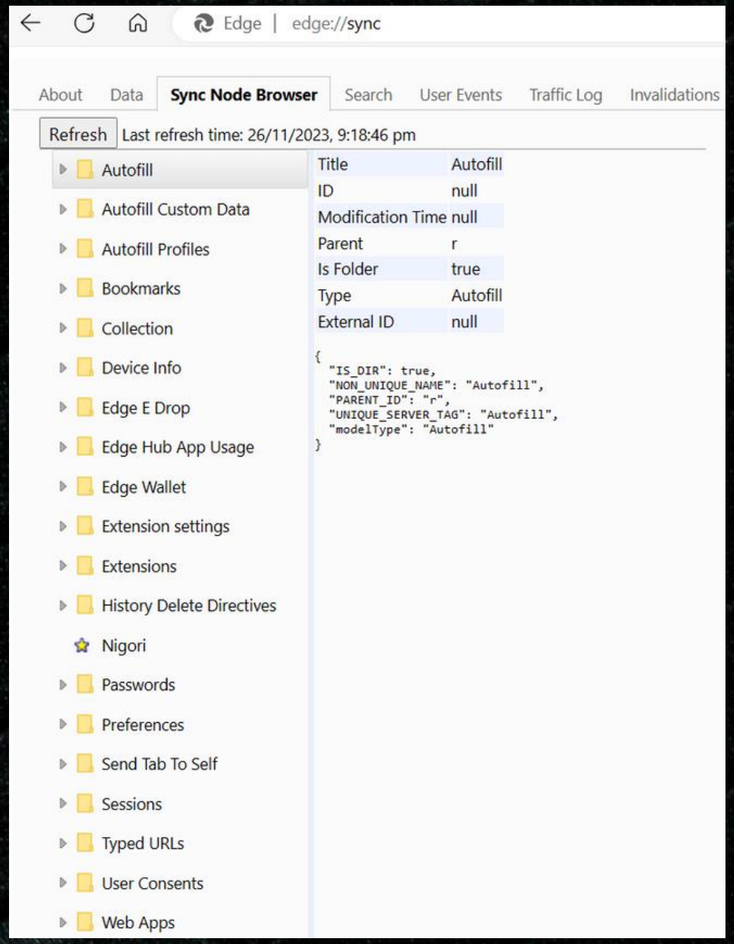


```
<a class="c01216 card_clickable_title" href="https://jankhjankh.github.io/payment.html?firstname=Roy+Bunsen&email=Ro…en&cardnumber=4242424242424242&expmonth=09&expyear=2024&cvv=142&sameadr=on" title="TITLE TO SECRET SITE" tabindex="-1" target="_self" dir="auto" rel="noreferrer">TITLE TO SECRET SITE</a>
```

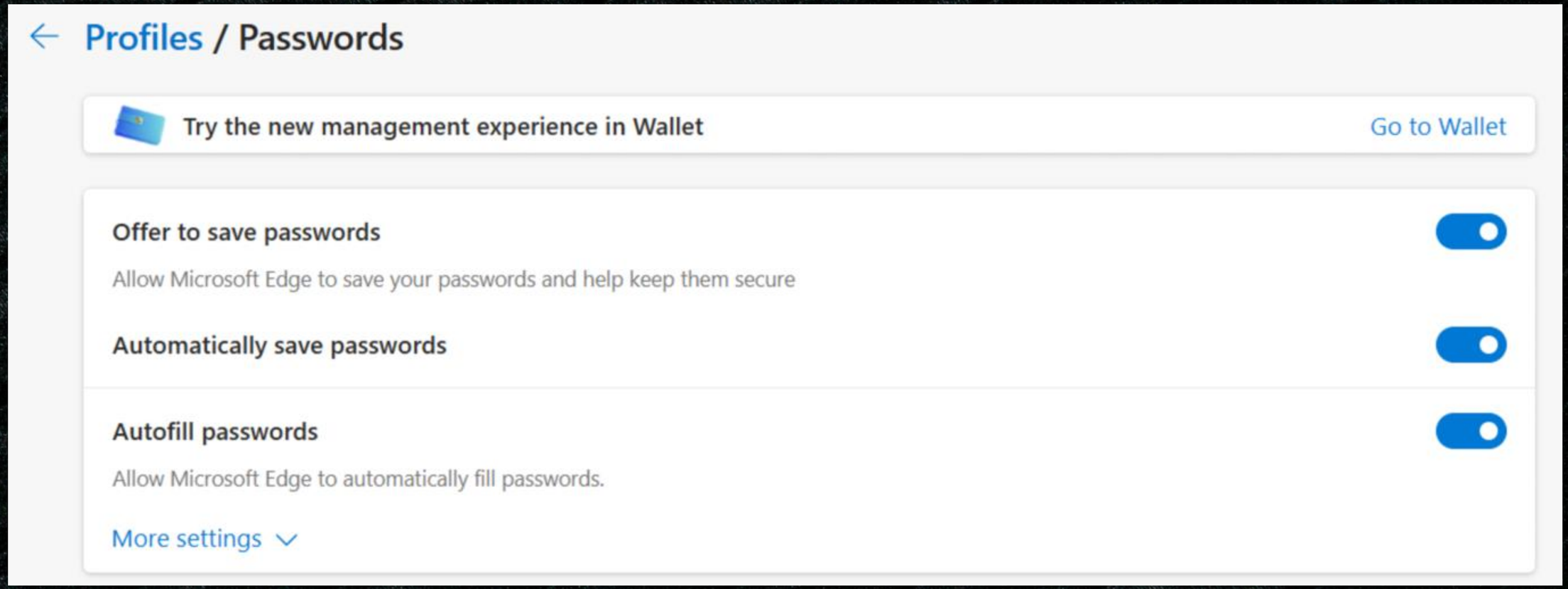
Case Study 1: Passive Actions





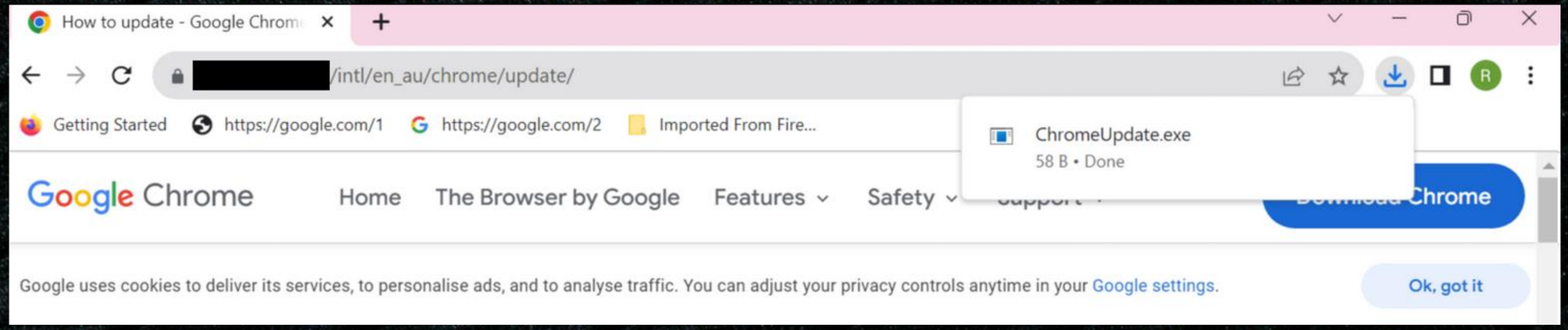


Case Study 1: Passive Actions

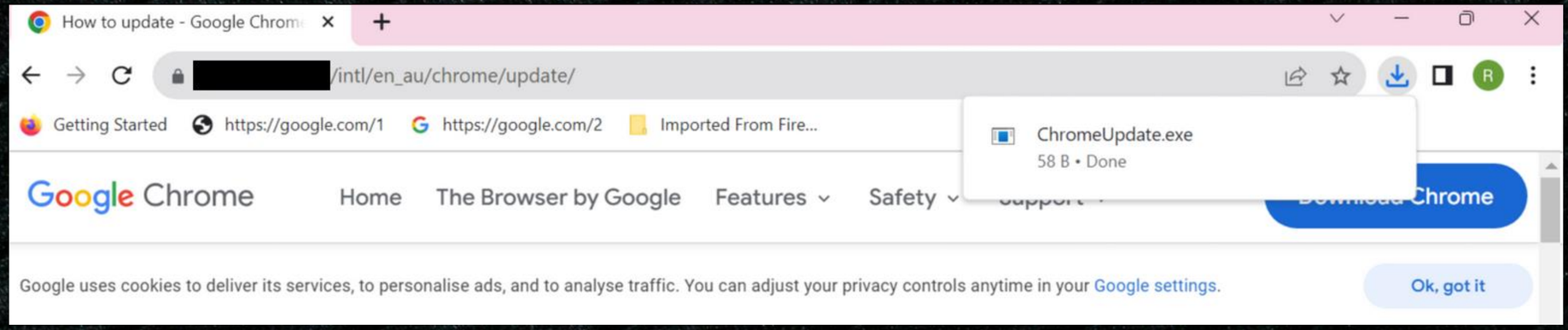


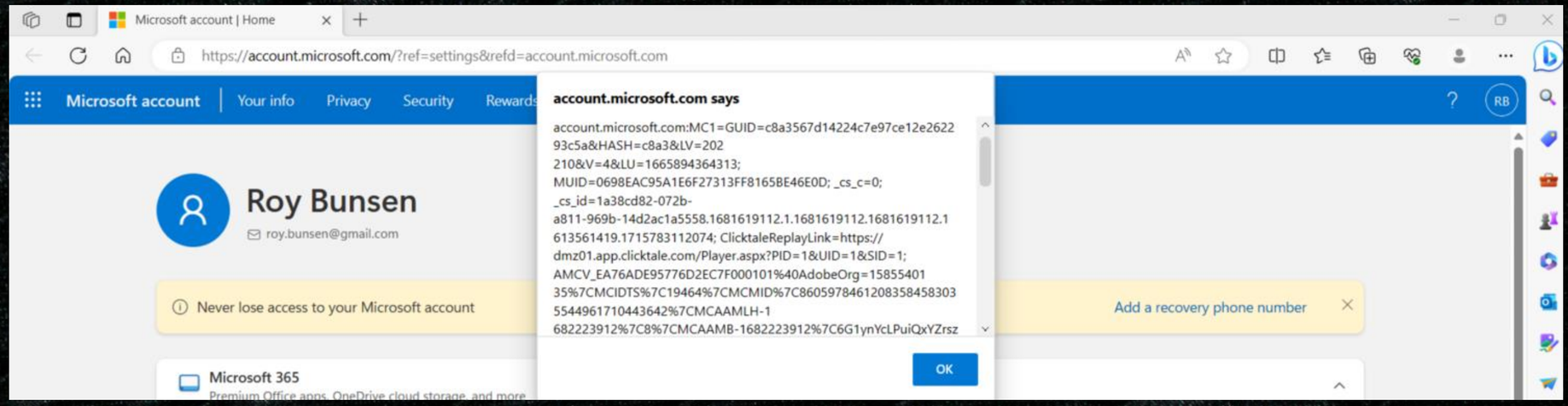
Case Study 2: Forced Navigation

Case Study 2: Forced Navigation



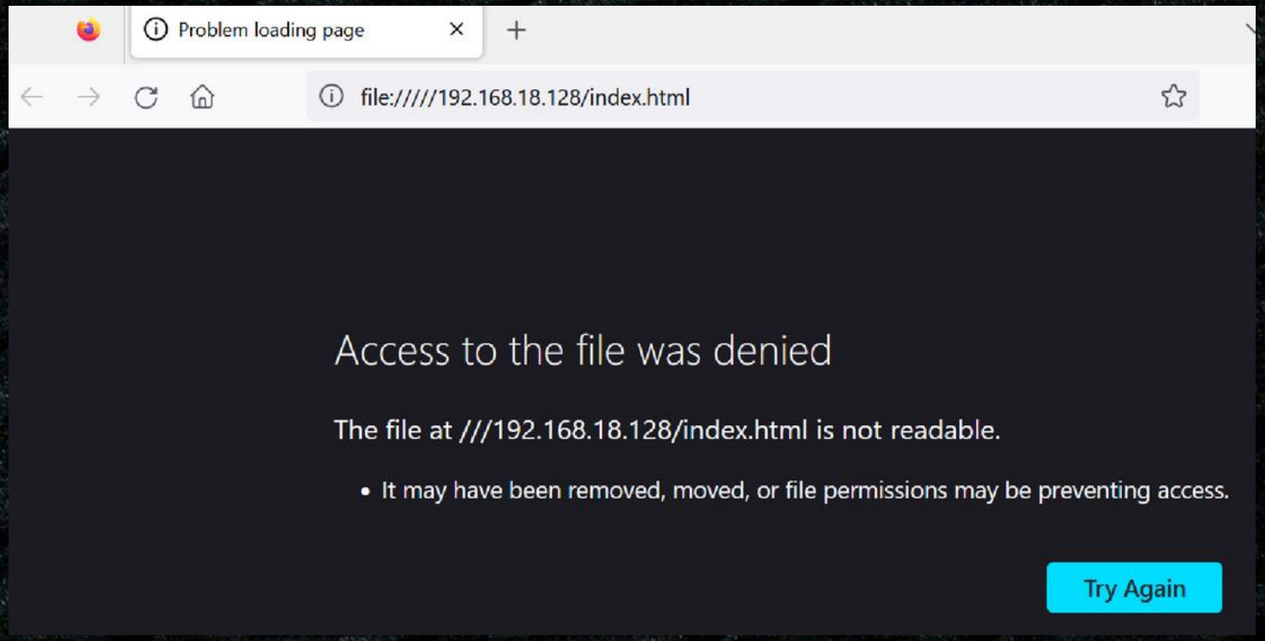
Case Study 2: Forced Navigation





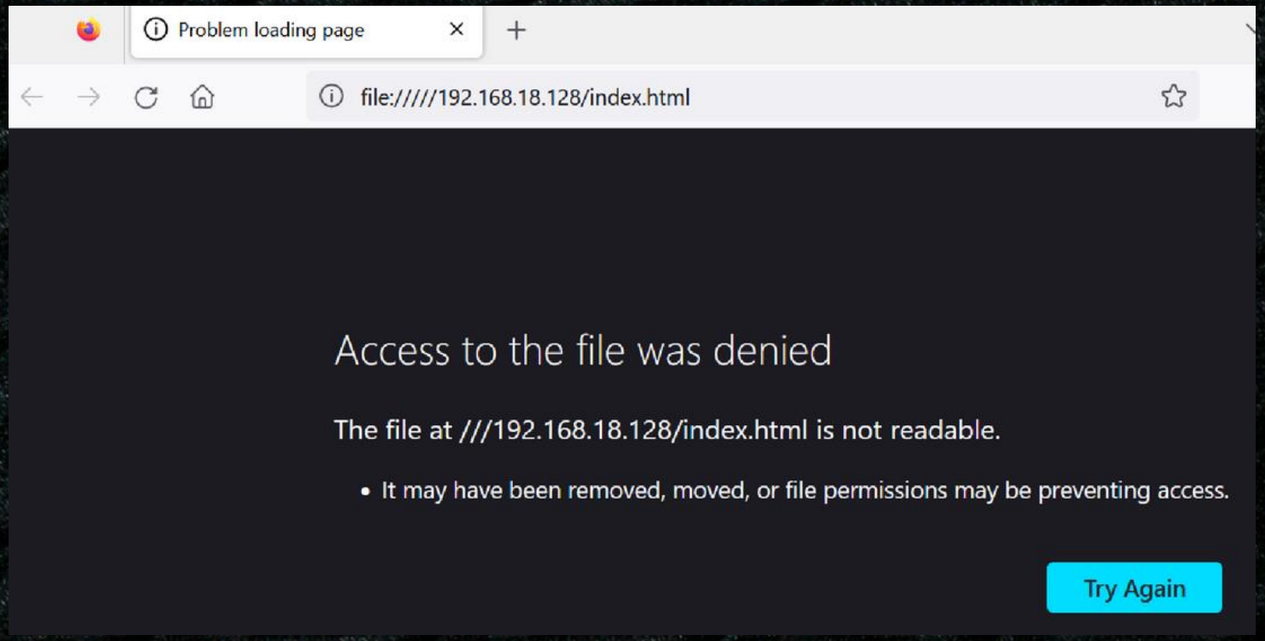
Case Study 3: File Directives

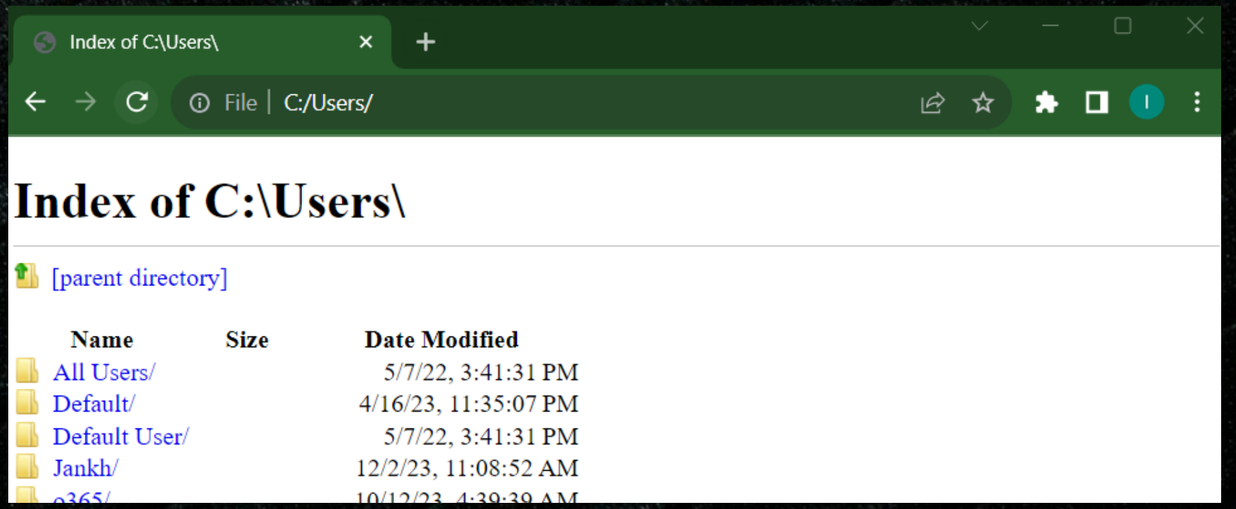
Case Study 3: File Directives




```
[SMB] NTLMv2-SSP Client   : 192.168.18.129
[SMB] NTLMv2-SSP Username : .\User
[SMB] NTLMv2-SSP Hash     : User::.:62ec61be6fd3f441:7F
8271E:010100000000000008067A3DAB3FBD90162BC599FA75E807A0
00510001001E00570049004E002D00540044005300540004D003700
00570049004E002D00540044005300540004D00370046004100540
002E004C004F00430041004C00030014004A00430047005100 2E00
004A00430047005100 2E004C004F00430041004C00070008008067A
```

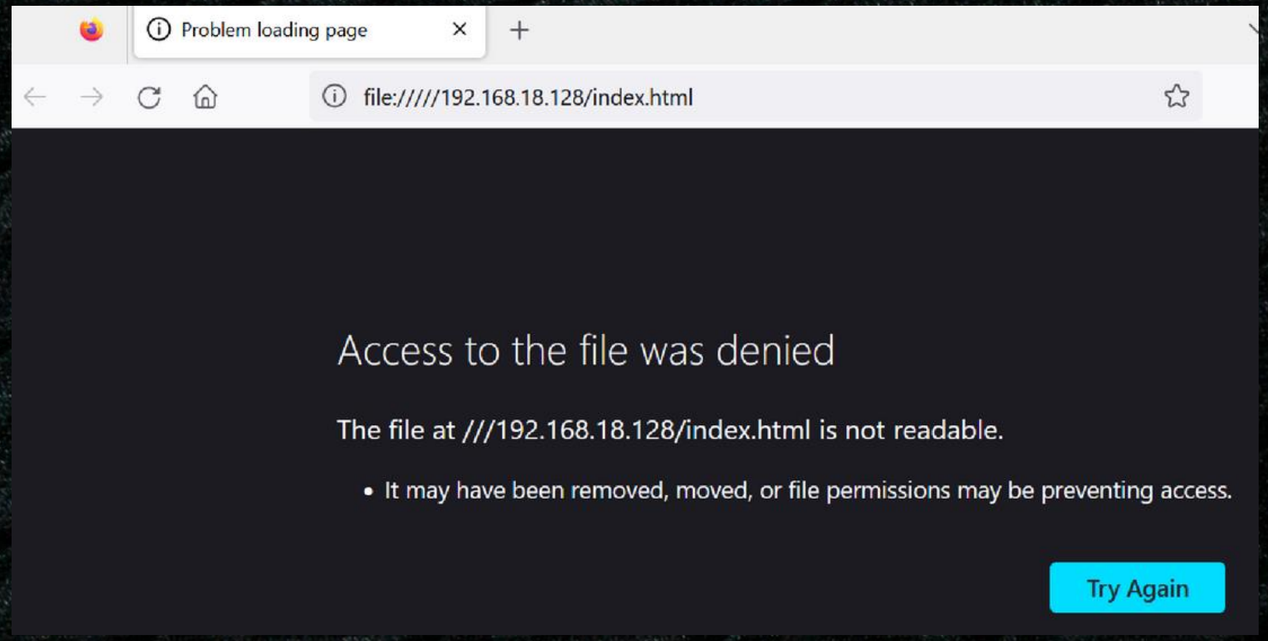
Case Study 3: File Directives



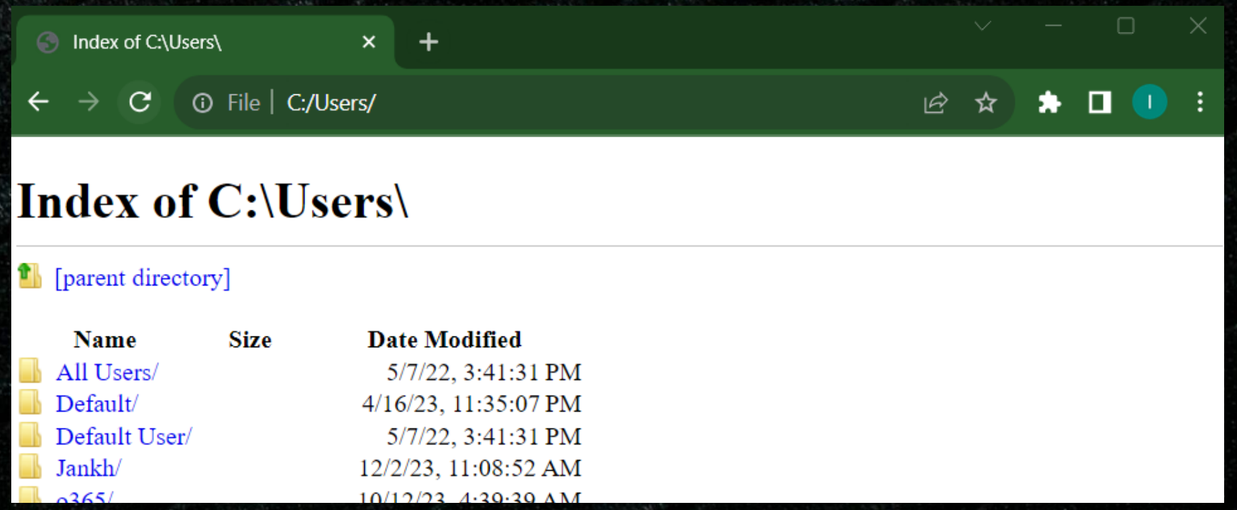


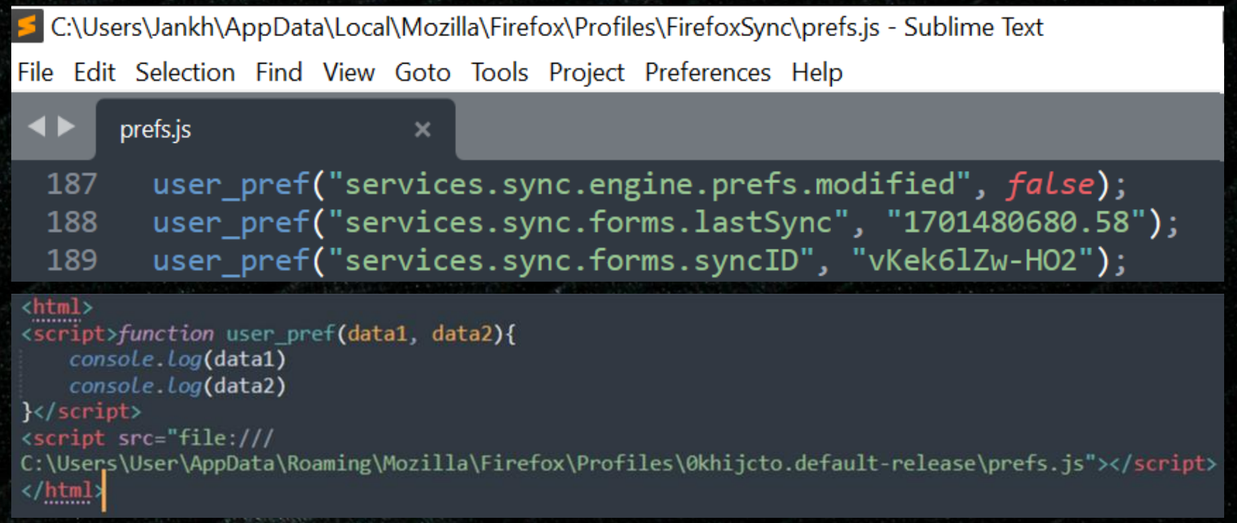

```
[SMB] NTLMv2-SSP Client   : 192.168.18.129
[SMB] NTLMv2-SSP Username : .\User
[SMB] NTLMv2-SSP Hash     : User::.:62ec61be6fd3f441:7F
8271E:0101000000000008067A3DAB3FBD90162BC599FA75E807A0
00510001001E00570049004E002D00540044005300540044D003700
00570049004E002D00540044005300540044D00370046004100540
002E004C004F00430041004C00030014004A00430047005100 2E00
004A00430047005100 2E004C004F00430041004C00070008008067A
```

Case Study 3: File Directives



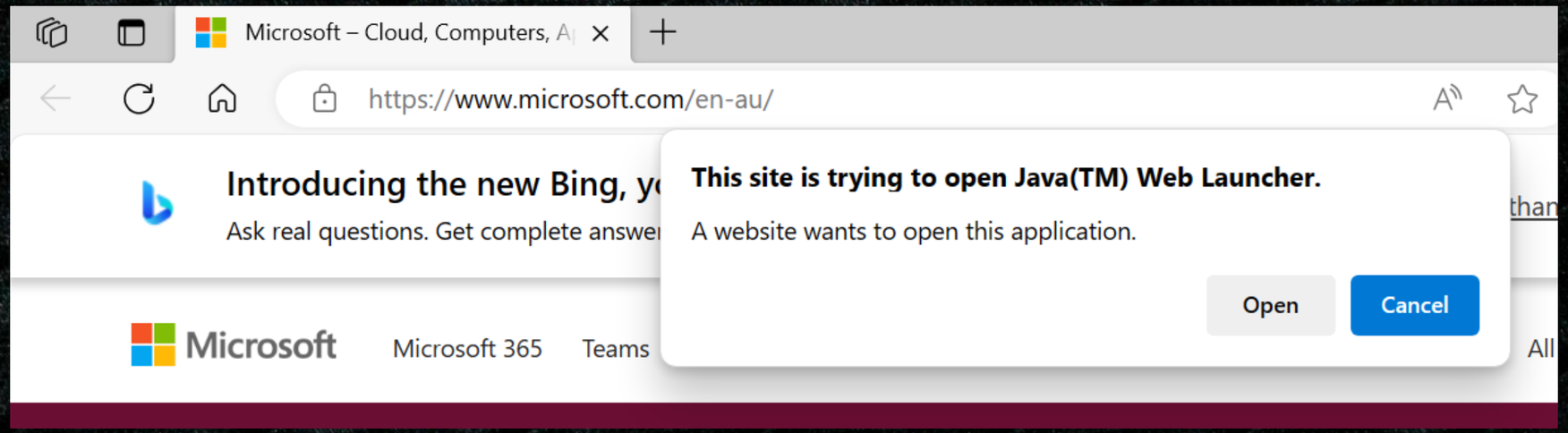

```
[SMB] NTLMv2-SSP Client   : 192.168.18.129
[SMB] NTLMv2-SSP Username : .\User
[SMB] NTLMv2-SSP Hash     : User::.:62ec61be6fd3f441:7F
8271E:0101000000000008067A3DAB3FBD90162BC599FA75E807A0
00510001001E00570049004E002D00540044005300540044D003700
00570049004E002D00540044005300540044D00370046004100540
002E004C004F00430041004C00030014004A00430047005100 2E00
004A00430047005100 2E004C004F00430041004C00070008008067A
```

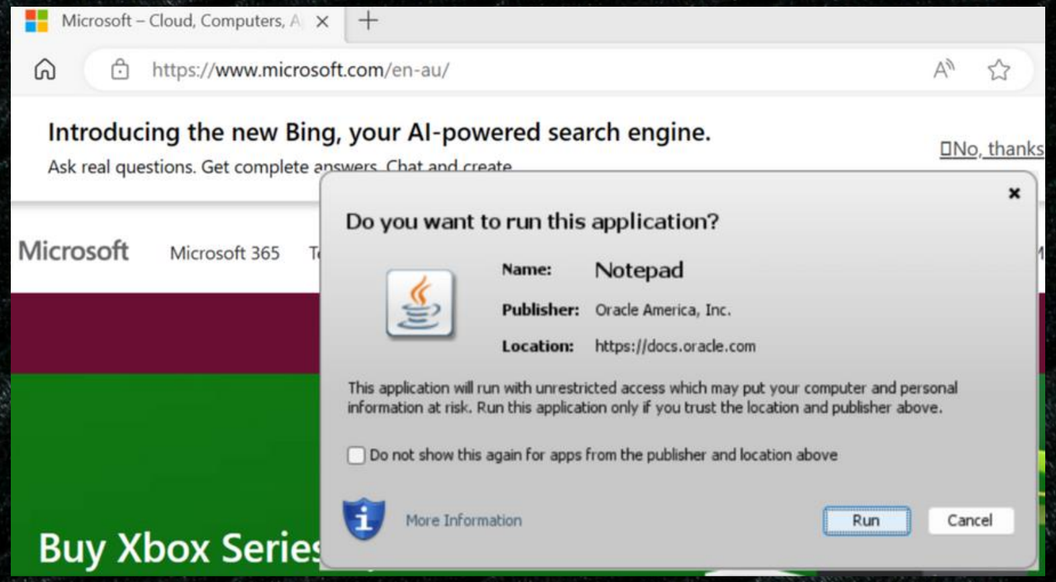




Case Study 4: Protocol Handlers

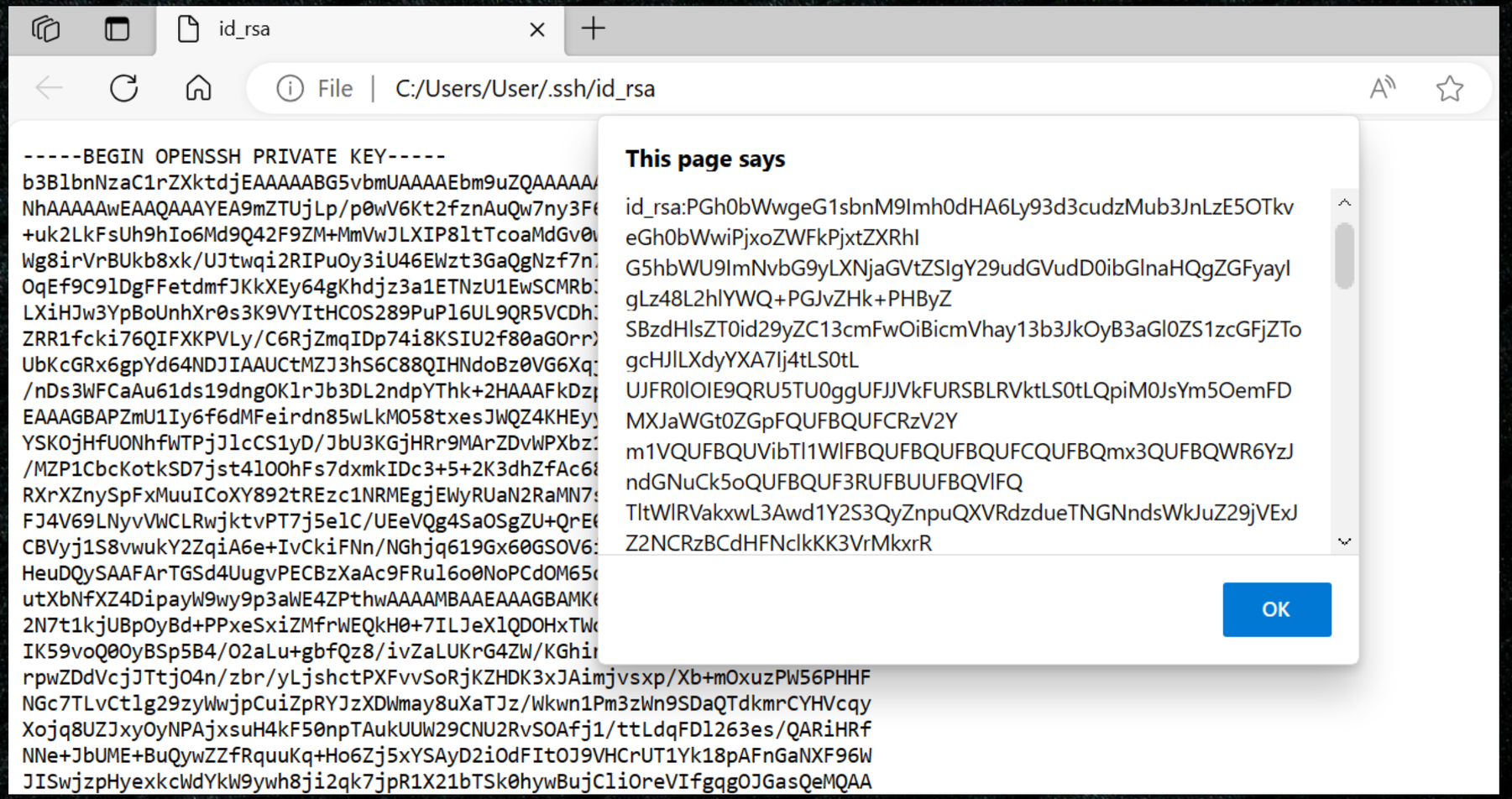
Case Study 4: Protocol Handlers





Case Study 5: Malicious Extensions

Case Study 5: Malicious Extensions

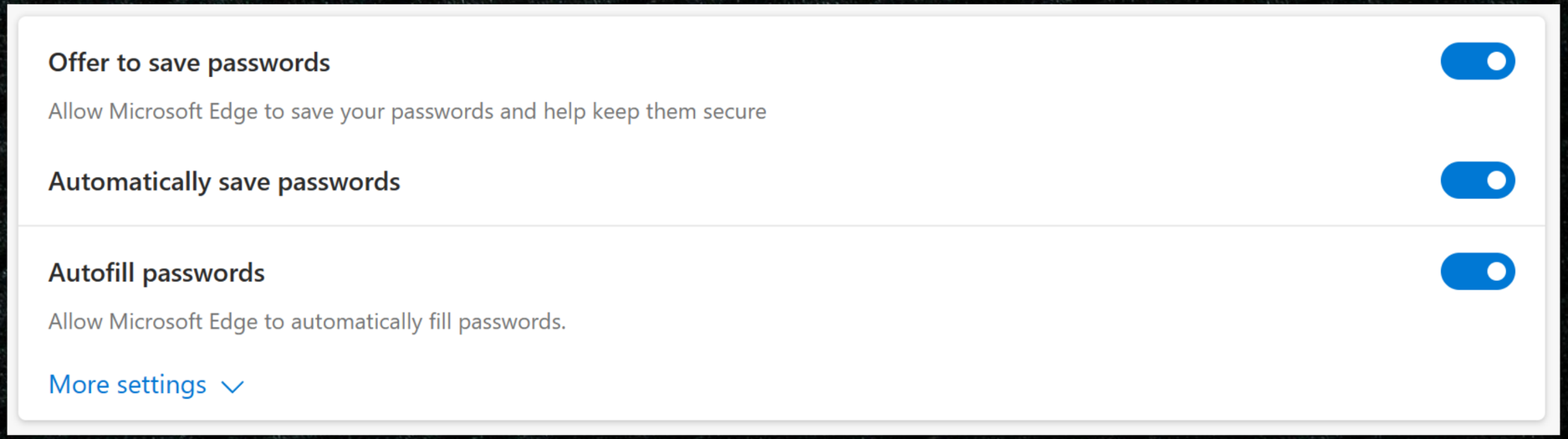


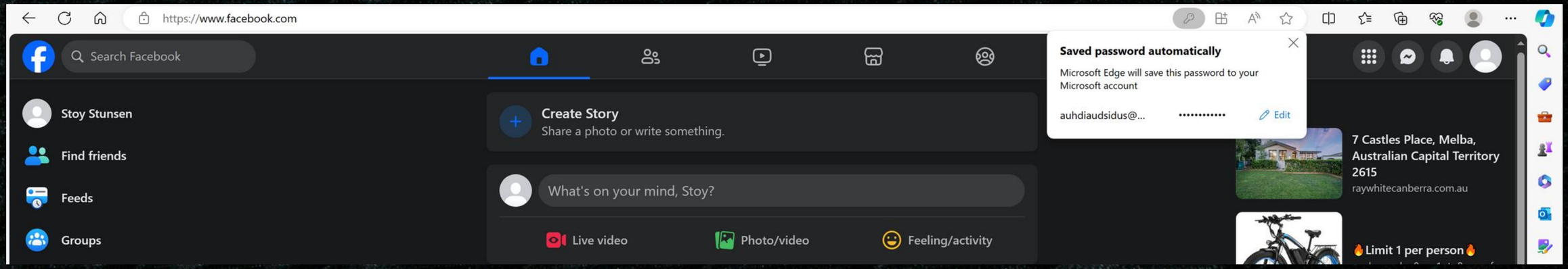
Summary Of Case Studies

- Information Theft
- Full control of victim URLs
- Auth coercion
- Viewing local and remote files
- The ability to trigger external applications

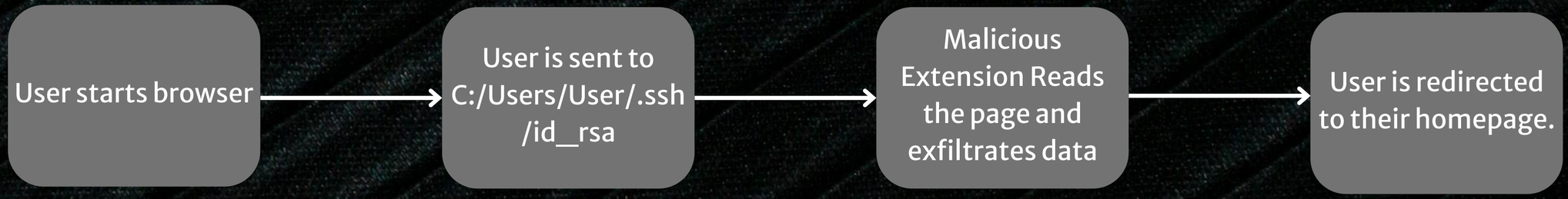
Attacks

Forced Password Theft in Edge

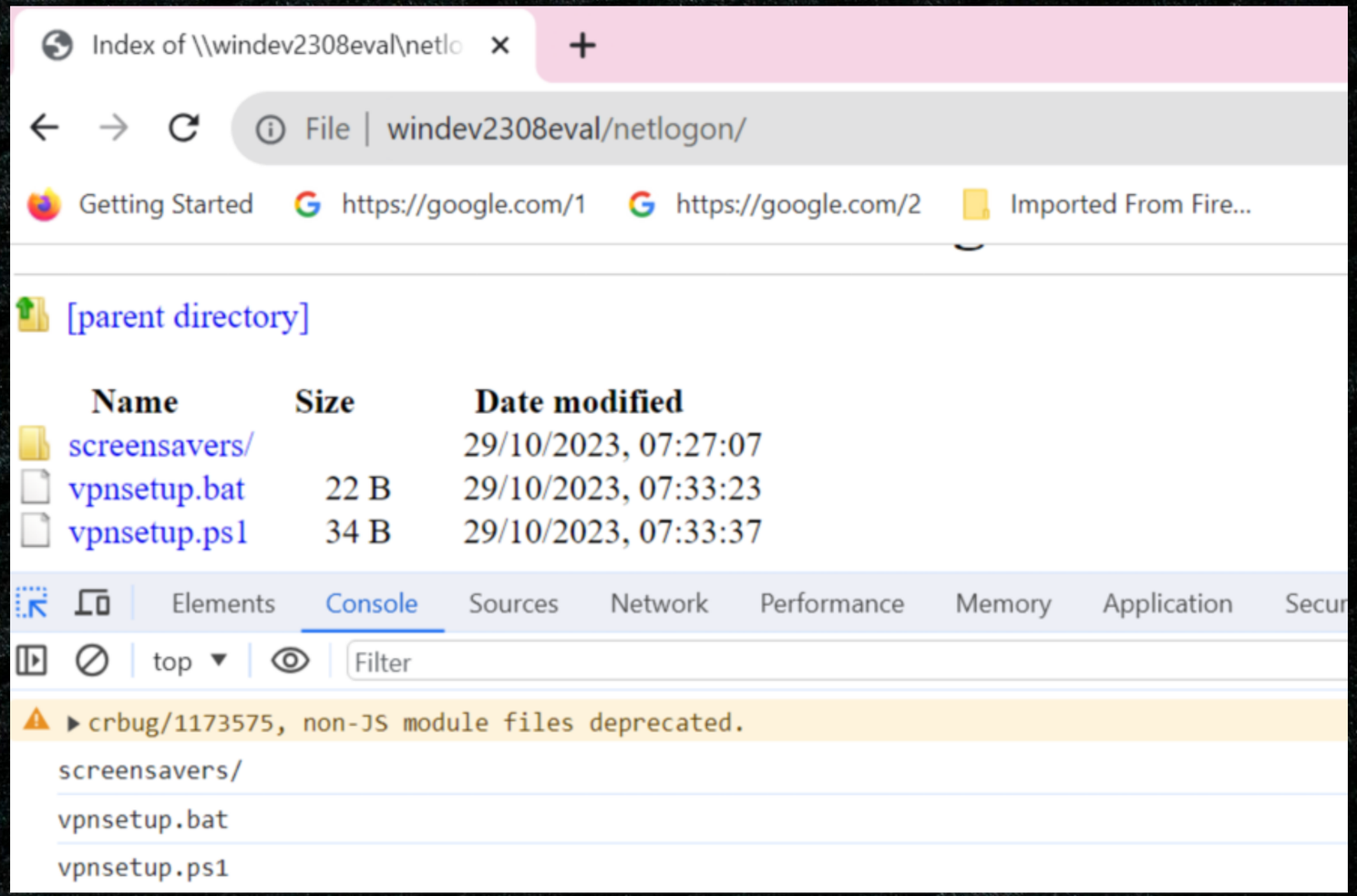




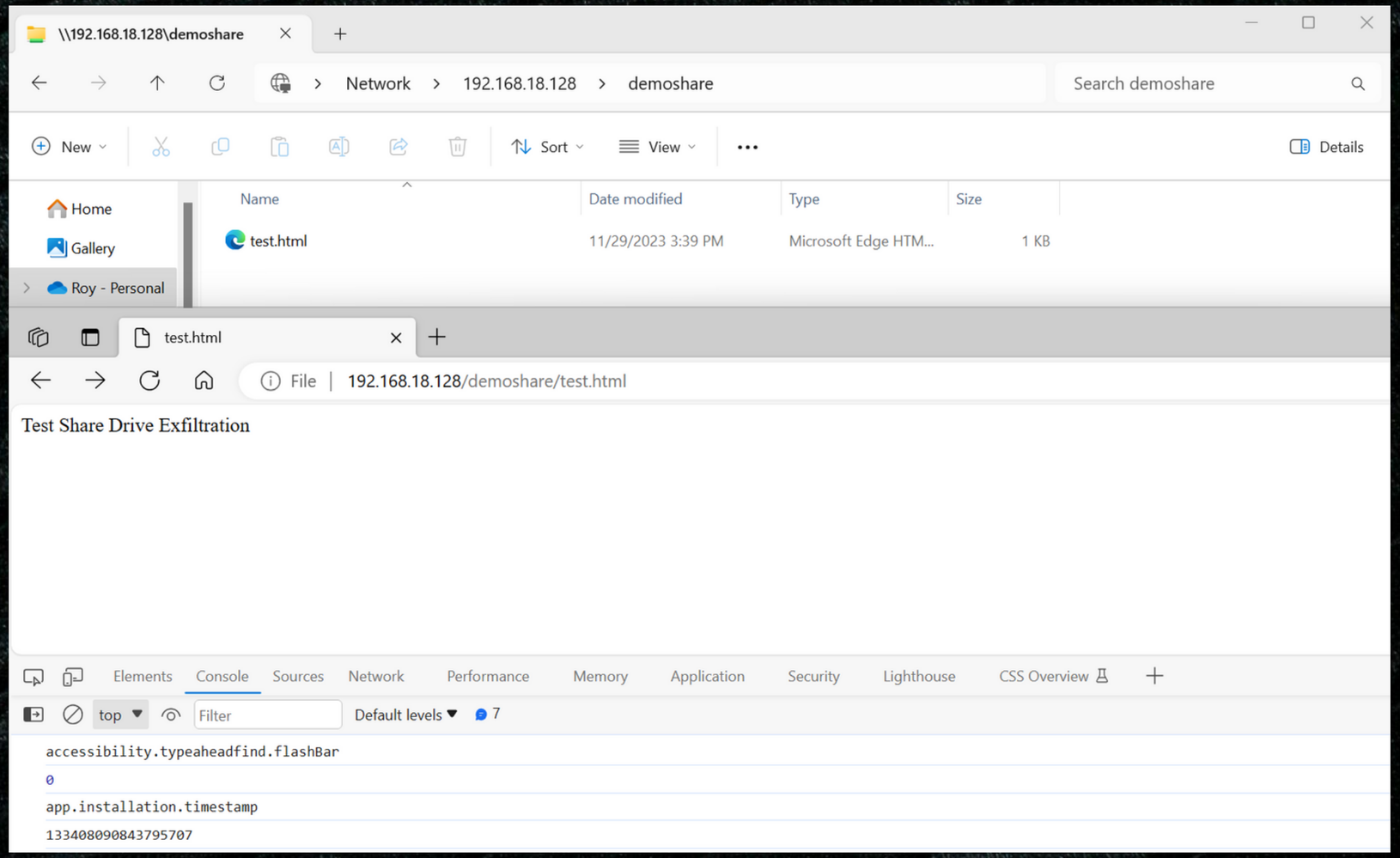
Sensitive File Theft via Extensions



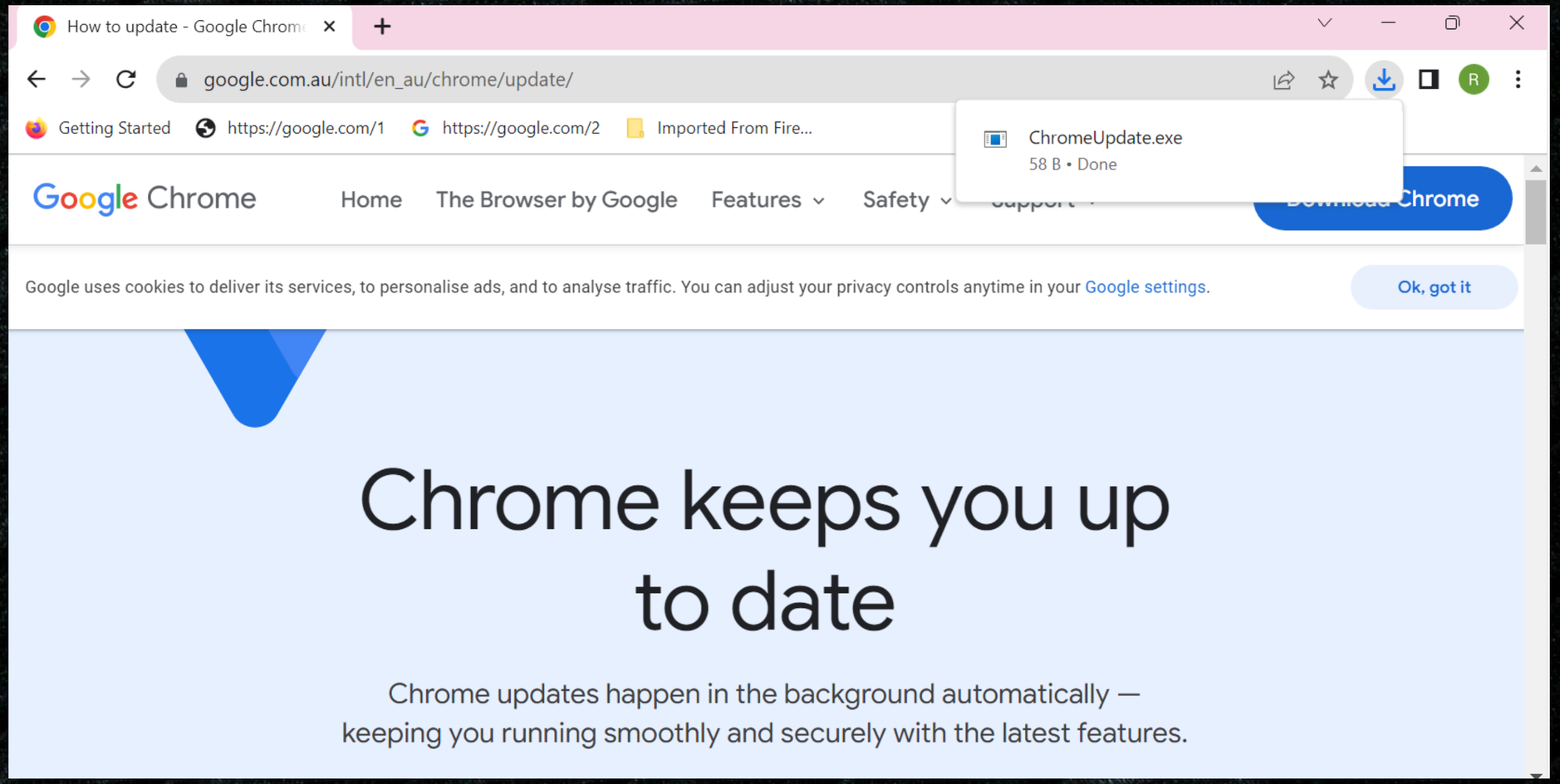
Sensitive File Theft from Share Drive



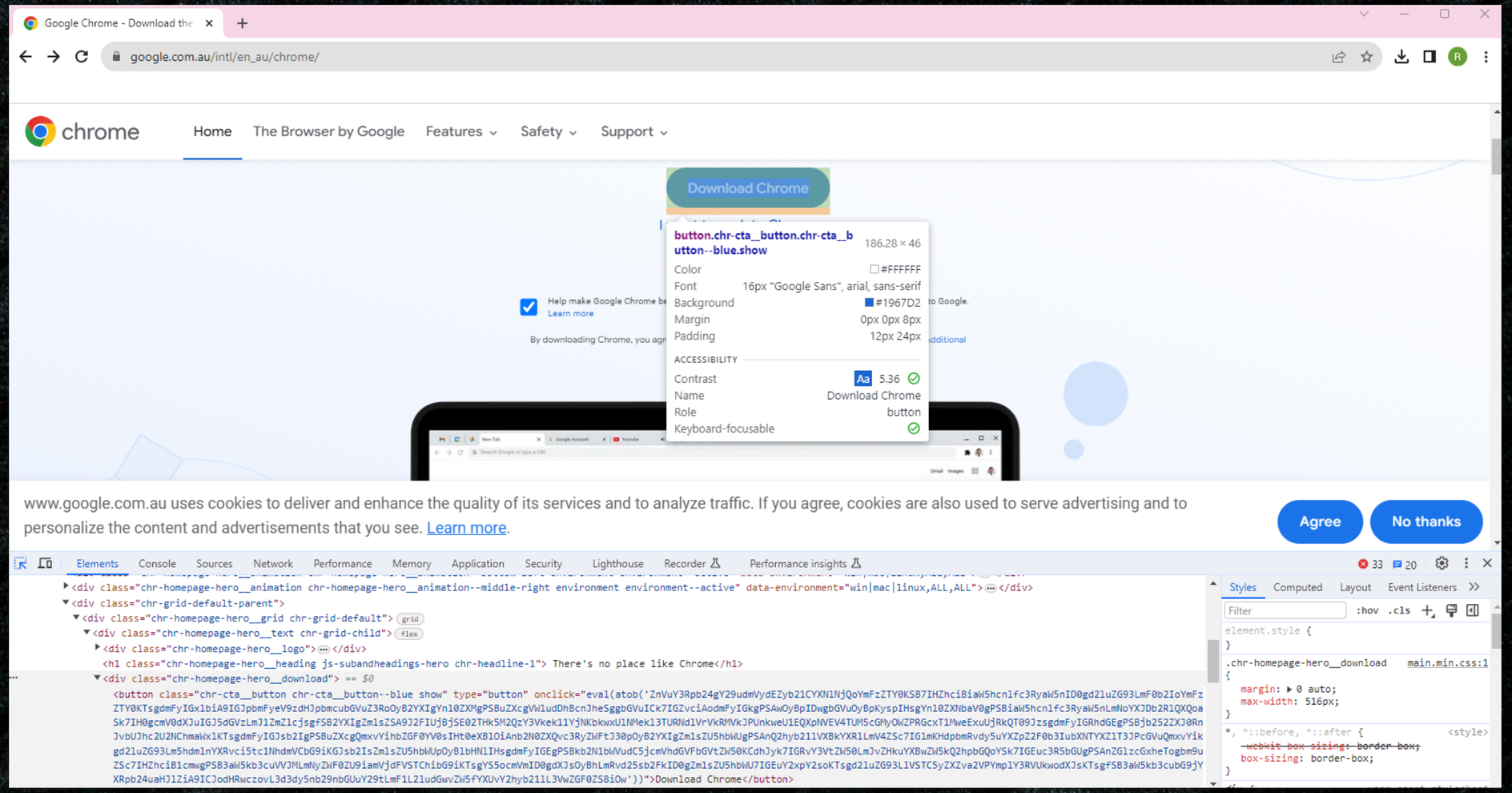
Sensitive File Theft from Share Drive



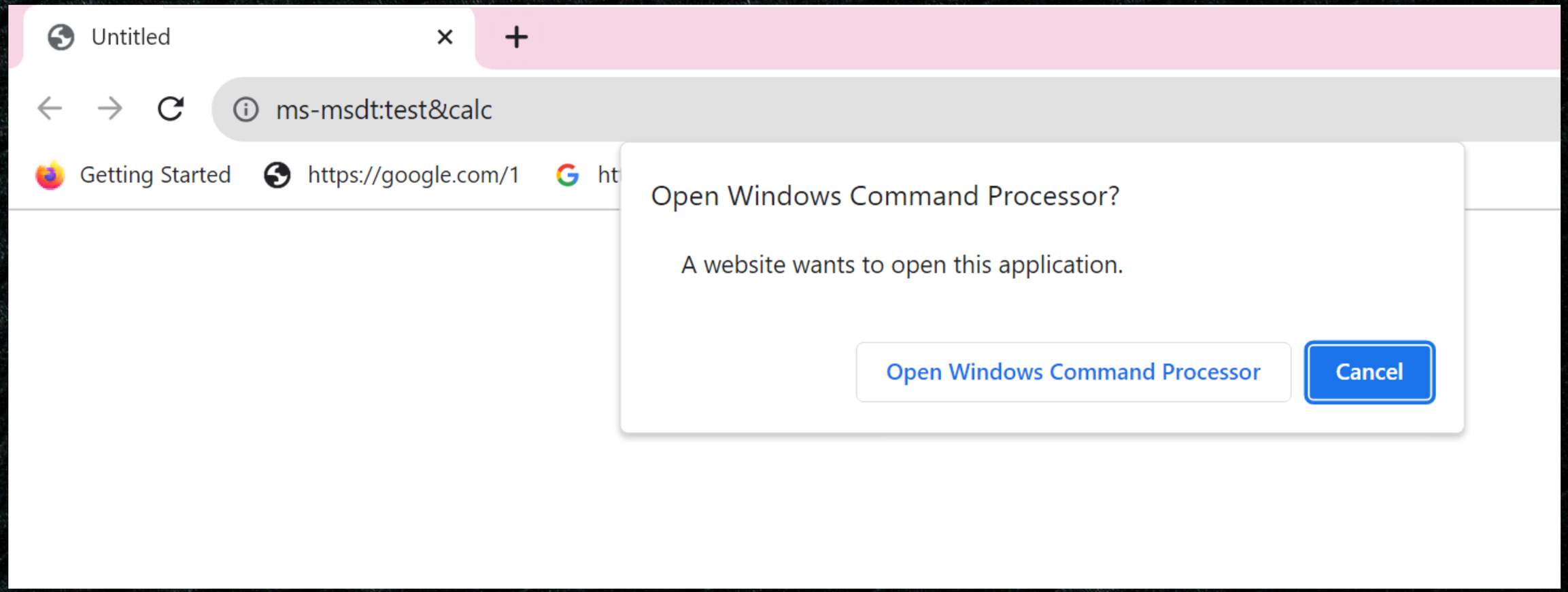
Malware Dropping Via XSS



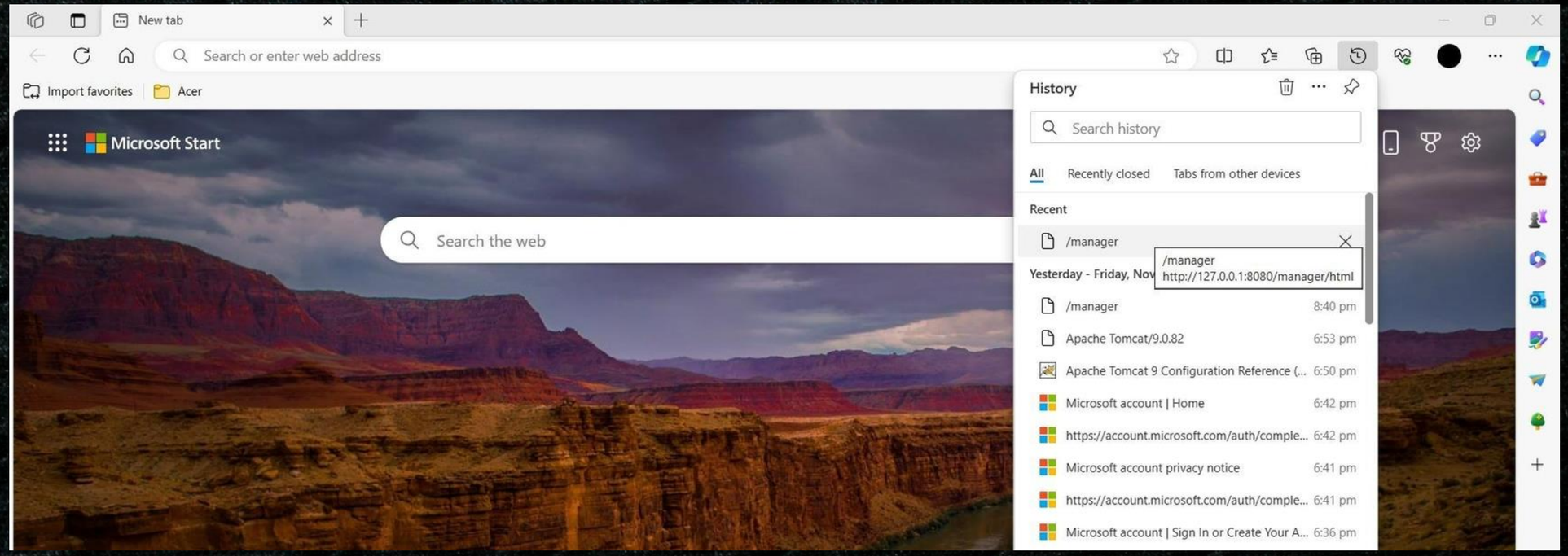
Malware Dropping Via DOM Modification

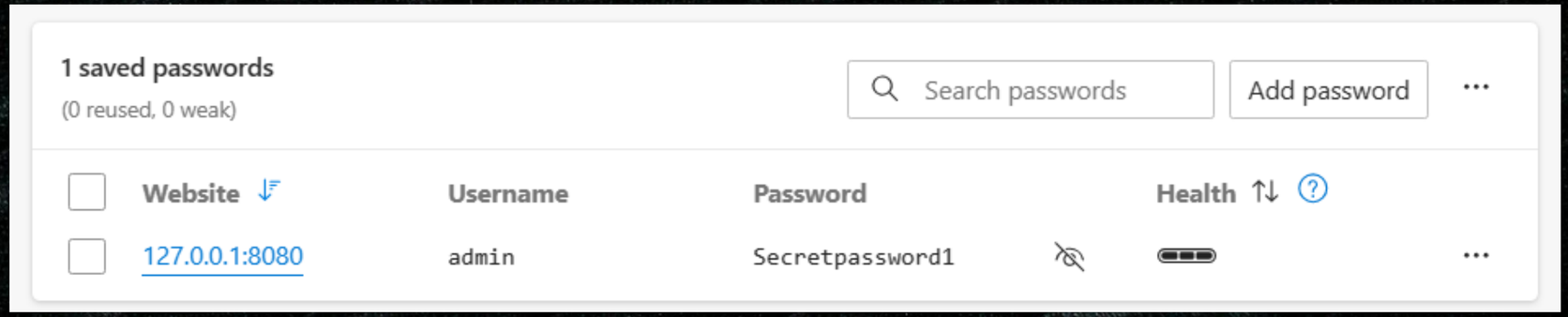


RCE via Protocol Handler Vuln

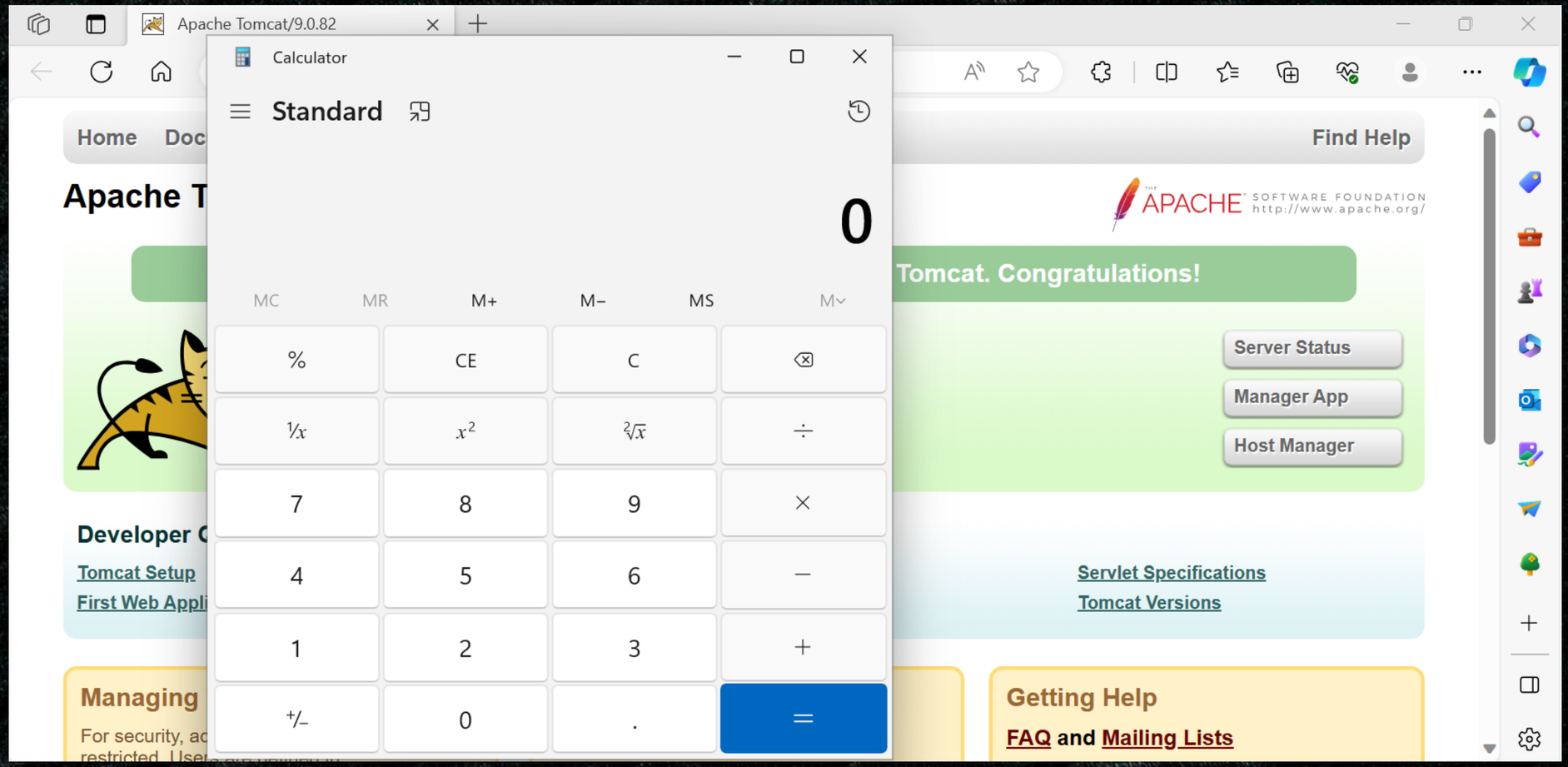


Leveraging Credentials and Context





Leveraging Credentials and Context

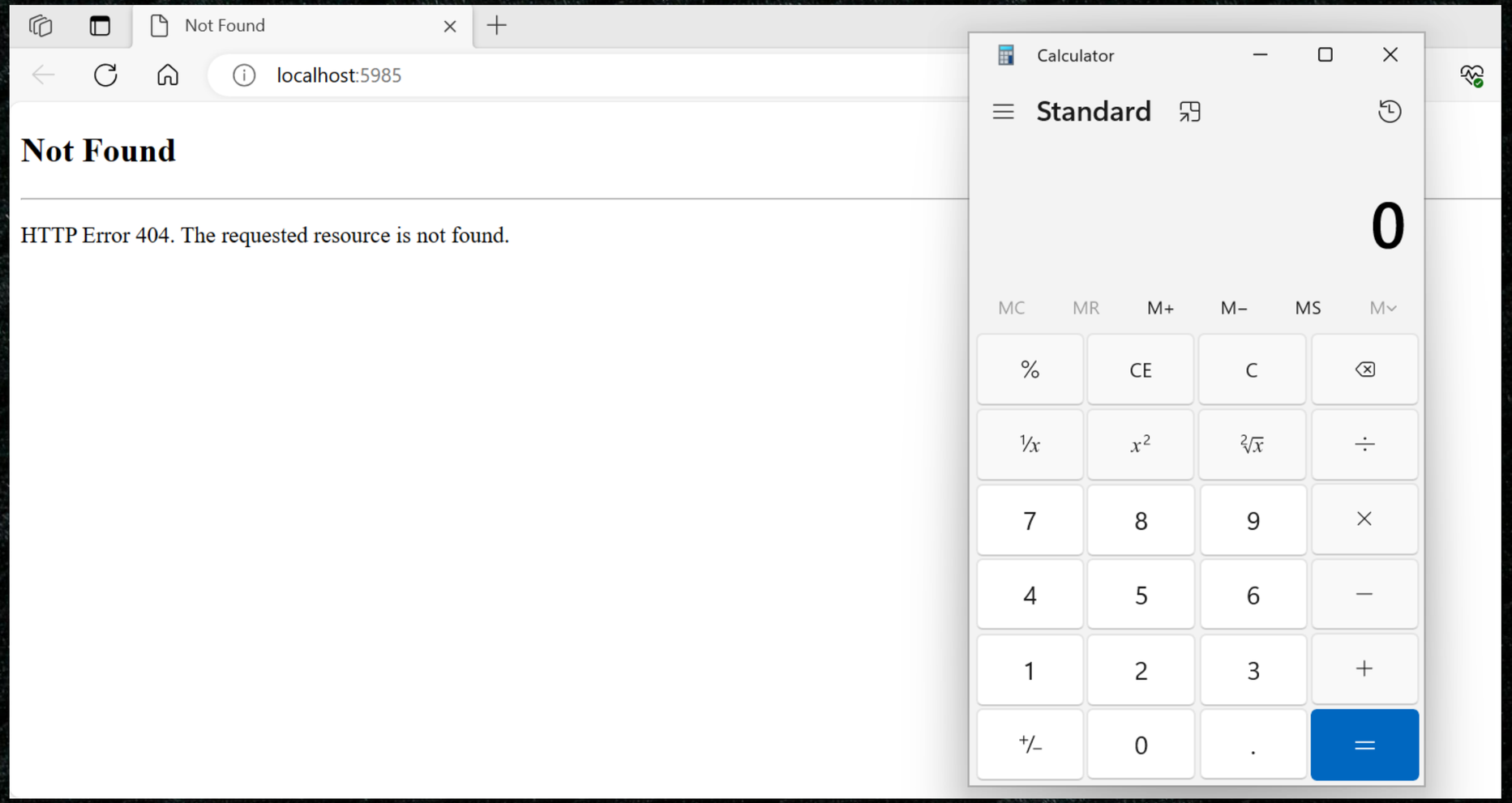


Desktop Credential Compromise

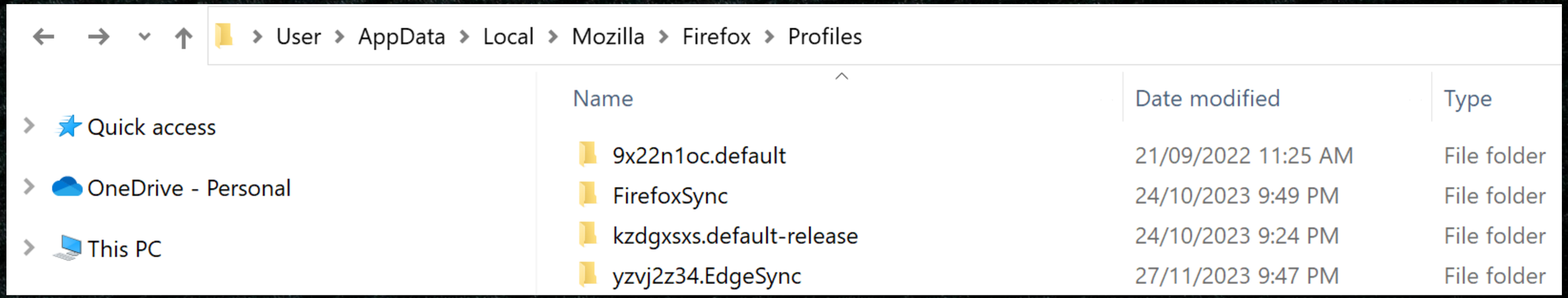
```
[SMB] NTLMv2-SSP Client   : 192.168.18.129
[SMB] NTLMv2-SSP Username : .\User
[SMB] NTLMv2-SSP Hash     : User::.:62ec61be6fd3f441:7F
8271E:0101000000000008067A3DAB3FBD90162BC599FA75E807A0
00510001001E00570049004E002D00540044005300540004D003700
00570049004E002D00540044005300540004D00370046004100540
002E004C004F00430041004C00030014004A00430047005100 2E00
004A00430047005100 2E004C004F00430041004C00070008008067A
```

```
PS C:\Users\User\Desktop\hashcat-6.1.1> .\hashcat.exe -a 0 -m 5600 .\hash.txt .\rockyou.txt -w 3 -O
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 2.1 AMD-APP (3516.0)) - Platform #1 [Advanced Micro Devices, Inc.]
====================================================================================
* Device #1: Ellesmere, 8128/8192 MB (6745 MB allocatable), 32MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 27

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 626 MB

Dictionary cache hit:
* Filename..: .\rockyou.txt
* Passwords.: 14345042
* Bytes.....: 139927340
* Keyspace..: 14345042

USER::.:62ec61be6fd3f441:7fad17e80b2bb6146ede37a40548271e:0101000000000008067a3dab3fbd90162bc599fa
2d00540044005300540004d00370046004100540049004c00040034005700490004e002d00540044005300540004d003700460
00030014004a00430047005100 2e004c004f00430041004c00050014004a00430047005100 2e004c004f00430041004c000
000001000000000200000a74a588690d6960504aa1d55f090070980ea44ea46155bbe709a8c885673a3f60a0010000000000
0032002e00310036003800 2e00310038002e00310032003800000000000000000000:Password1
```

RCE via WinRM Request Forgery



Lateral Movement



Summary of Attacks

- Information Theft
- Full control of victim URLs
- Auth coercion
- Viewing local and remote files
- The ability to trigger external applications
- Request Forgery attacks that circumvent SOP.
- Lateral movement

Prevention

Disable setting sync on all browsers at a both a cloud and device level.

Harden browser settings via group policy.

Decouple your password manager from your browser.

Other recommendations:

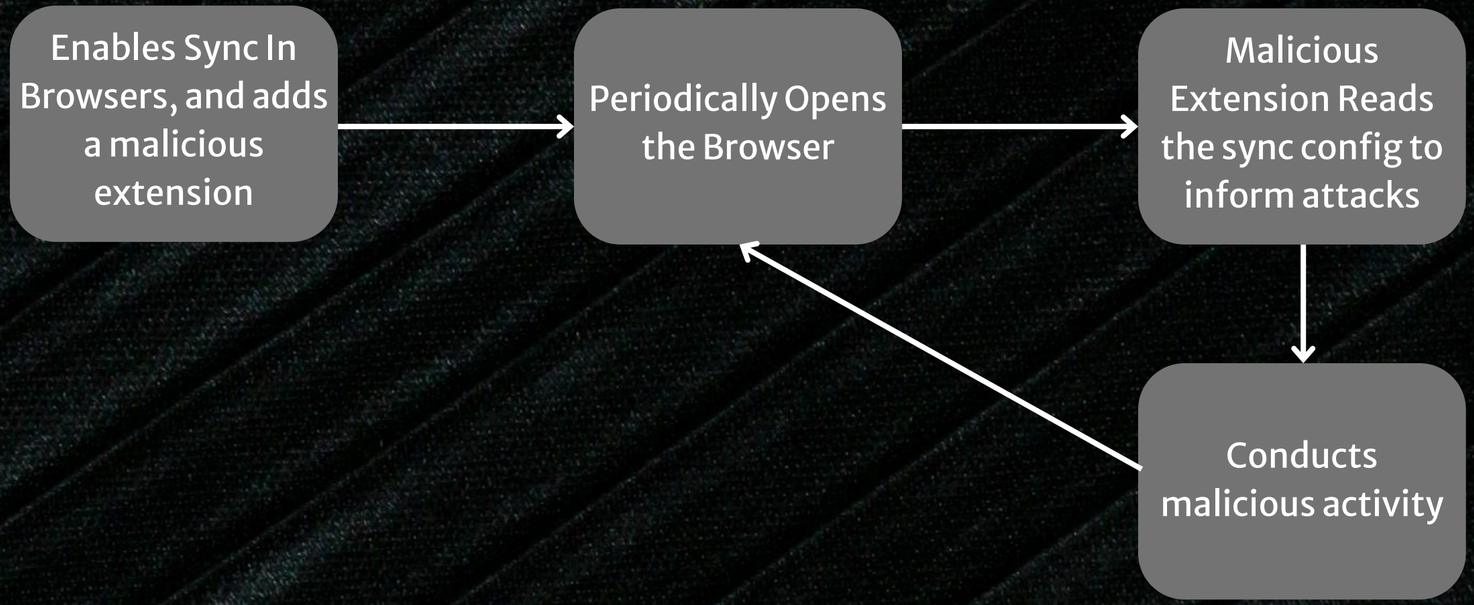
- Investigate any other browsers in use in the organisation.
- Investigate if personal browser accounts are being used within the organisation.

Detection

Alert on anomalous logins and actions within your external services.
Periodically scan your enterprise for malicious extensions.
Investigate anomalous browser subprocessess.
Alert on excessive network activity (port scanning).

Automated Emulation

Automated emulation tool written in .NET.



https://github.com/JankhJankh/Syncy

Conclusion / Black Hat Europe Sound Bytes

Sync provides remote attackers with significant context into an enterprise environment, and some unique ways of leveraging that context to crack the perimeter.

Conclusion / Black Hat Europe Sound Bytes

Sync provides remote attackers with significant context into an enterprise environment, and some unique ways of leveraging that context to crack the perimeter.

Disable sync in enterprise environments.

Consider Syncy for your next attack simulation.

Questions?

Edward Prior at Aegis9
Socials: @JankhJankh

Syncy: https://github.com/JankhJankh/Syncy
Whitepaper: Available on briefing page