



### OAuth sicher mit Single-Page-Applications nutzen

Architektur-Pattern und Best Practices Benjamin Häublein OWASP Stammtisch Heilbronn, 8.5.2025



### Agenda

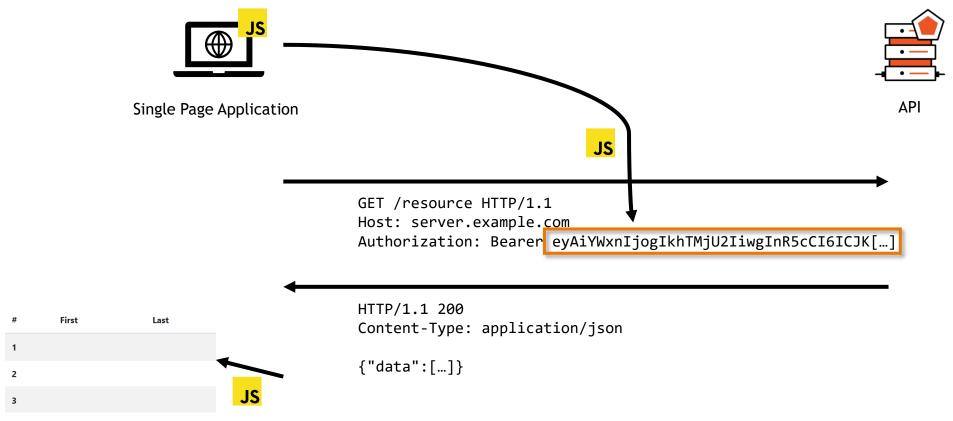
cirosec

- Single Page Applications
- OAuth2 Grundlagen
- Pattern beim Einsatz von OAuth2 mit SPAs

POLICIES AVERAGEMENT ZE LA PROJECTION CHECK TO STREET LA PROJECTION SEICHERHEIT LA PROJECTION CHECK TO STREET LA PROJECTION SEICHERHEIT CLOUD SECURITY VERWUNDBARKEITSMANAGEMENT ZE SECURITY OPERATION CENTER CHECK TO STREET LA PROJECTION CHECK TO STREET LA PROJECTION SEICHERHEIT CLOUD SECURITY VERWUNDBARKEITSMANAGEMENT ZE SECURITY OPERATION CENTER CHECK TO STREET LA PROJECTION CHECK TO STREET LA

### Single Page Application (SPA)





POLICIES NO SECURITY OF EATION CENTER

POLICIES NO SECURITY OF EATIONS

POLICIES NO SECURITY OF EAT

# OAuth Problemstellung



Facebook/LinkedIn/...

möchte auf deine Gmail/... Kontakte zugreifen, um dein Netzwerk um Menschen die du kennst zu erweitern.

Wie macht man das?



### OAuth Lösung (2008)



Are your friends already on Yelp?		
Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.		
Your Email Service		OO! MAIL ⊚ AOL >> Mail ⊚ GMail
Your Email Address	ima.testguy@gmail.com	(e.g. bob@gmail.com)
Your Gmail Password	•••••	(The password you use to log into your Gmail email)
	Skip this step Check Contacts	

https://blog.codinghorror.com/please-give-us-your-email-password/



#### **OAuth**



- "Delegierte Zugriffsberechtigung"
- Vergabe von Zugriffsberechtigungen durch den Benutzer des Dienstes an eine dritte Partei auf Ressourcen eines Dienstes
- OpenID
  - Delegation der Berechtigung zum Zugriff auf die Identität des Benutzers



### OAuth Grober Ablauf











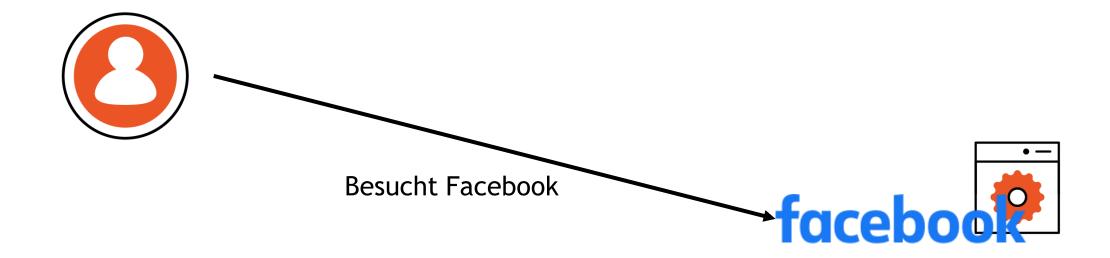


### OAuth Grober Ablauf











### **Oauth Grober Ablauf**

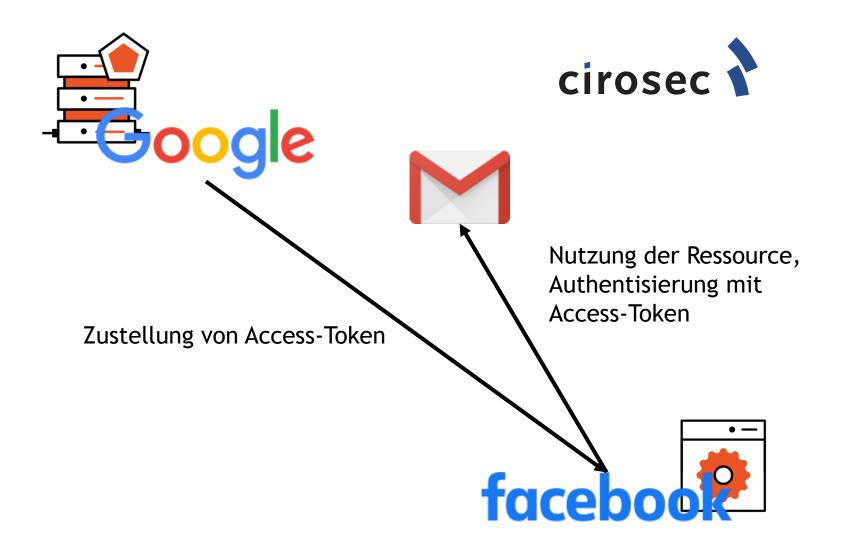






### Oauth Grober Ablauf

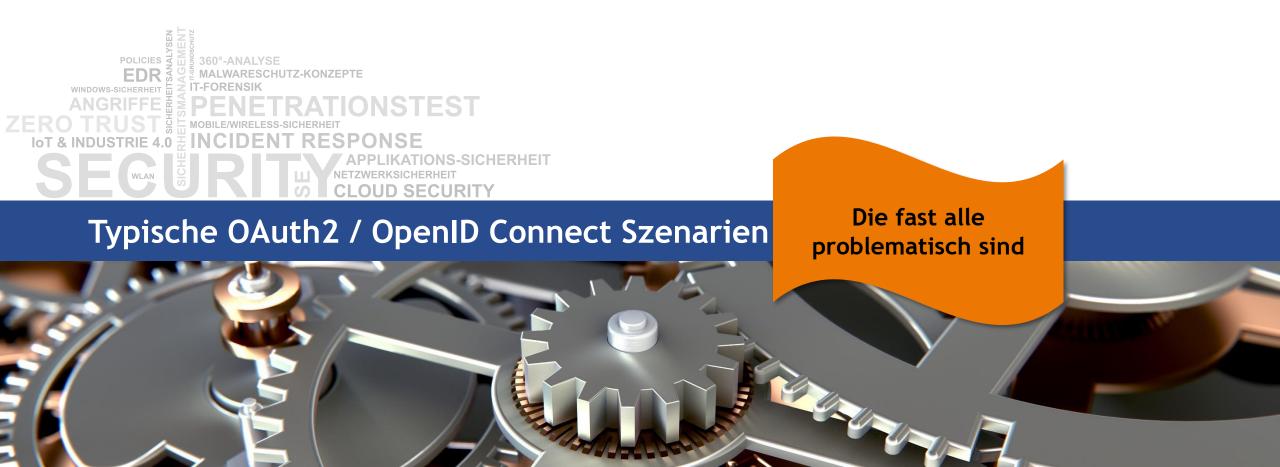






## **OAuth** cirosec **Authorization Code Grant User Agent Relying Party OpenID Provider Authorization Request** Client Identifier, Redirection URI Stellt Identität fest **Authorization Response Authorization Code Token Request Authorization Code Token Response** Access-Token, (ID-Token)





# cirosec ID Token über SPA an das Backend Access Token **ID Token** Problem: Jeder kann ID Token und Access Token SPA erlangen Problem: ID Token ist keine Session!

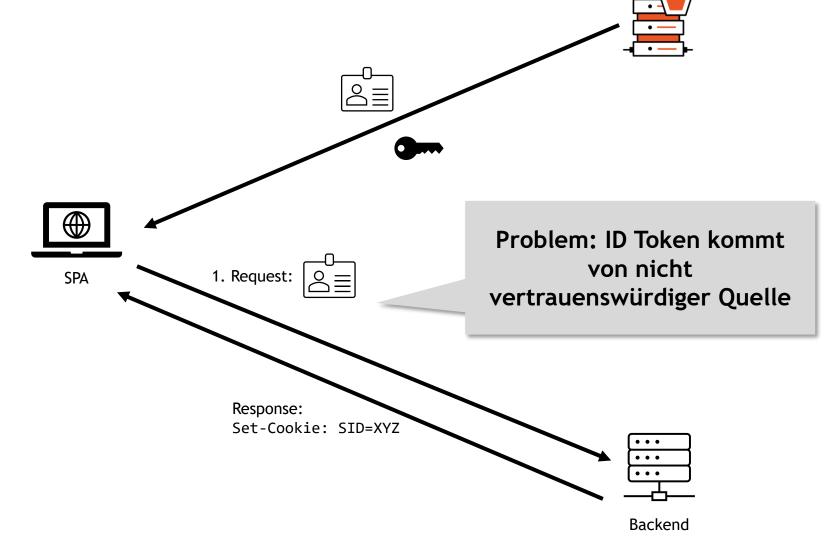
**Backend** 











POLICIES Y WINDOWS-ECREMENT AND STEED TO ANALYSE EVEN WINDOWS-ECREMENT SEED THE WINDOWS-ECREMENT WINDOWS-ECREMENT

## cirosec ? Access Token über SPA an API Access Token **ID** Token Probleme: Access Token ist keine Session SPA Access Token muss vermutlich unsicher im Browser gespeichert werden Zur Anzeige von Benutzeridentität in SPA

API

POLICIES AND ANALYSE
EDR SUPPLIES AND ANALYSE
WIXDOWS SICHERHES SICHERHEST
IOT & INDUSTRIE 4.0 HINCIDENT RESPONSE

LITTURE SICHERHES SICHERHEST
IOT & INDUSTRIE 4.0 HINCIDENT RESPONSE

LITTURE SICHERHEST

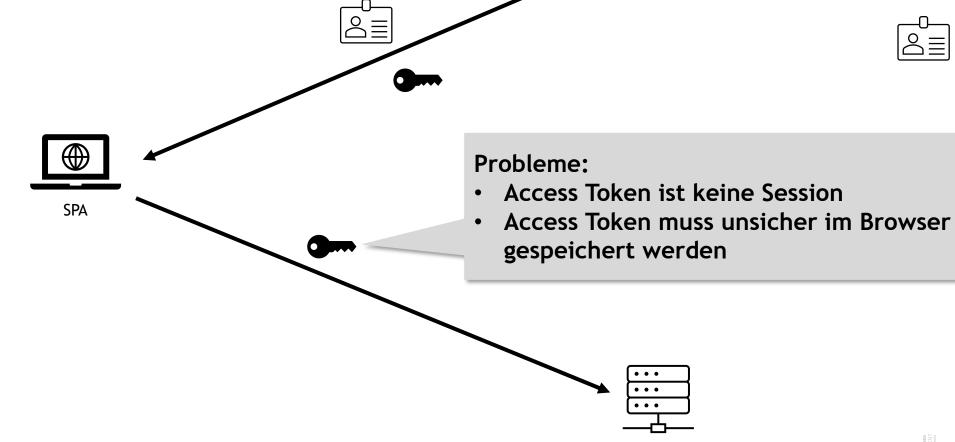
LOUD SECURITY
VERWUNDBARKEITSMANAGEMENT OF CLOUD SECURITY
VERWUNDBARKEITSMANAGEMENT OF CONTROL OF CONTRO

### Access Token von SPA an eine API

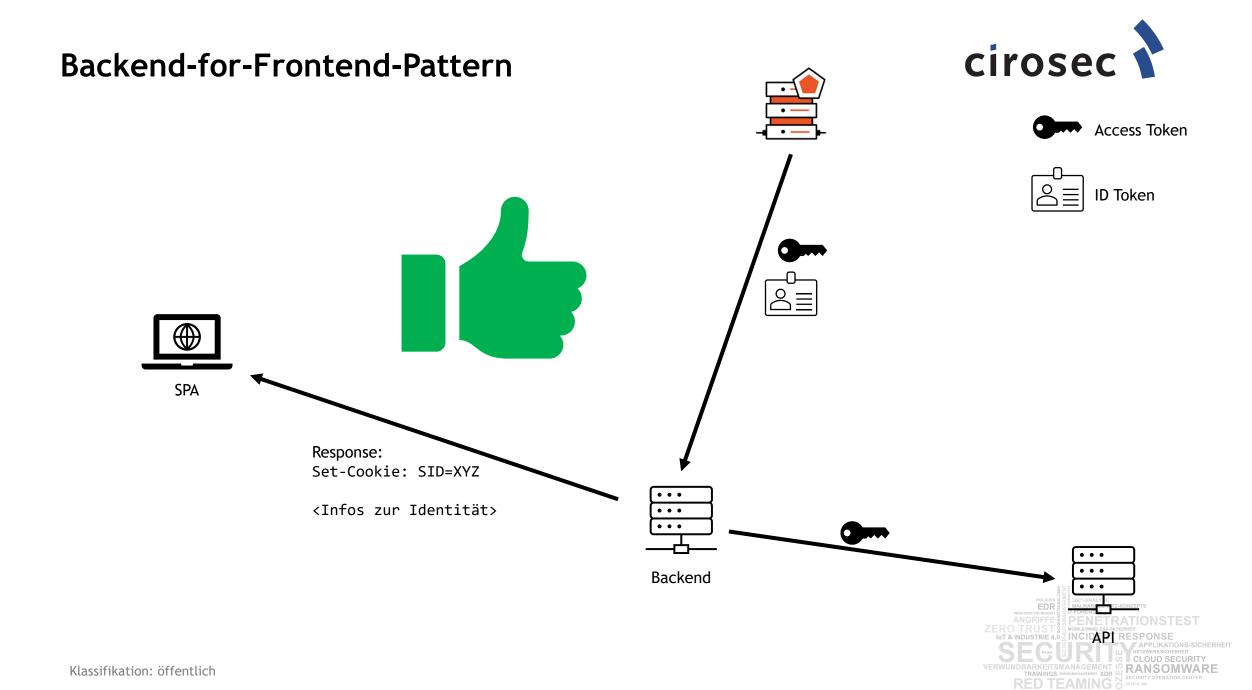








API

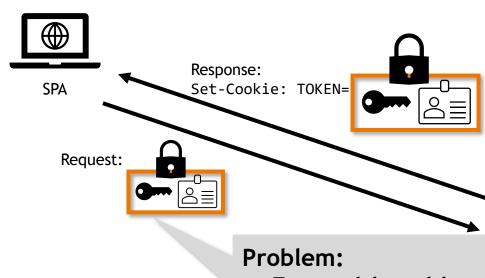


### **Token-Mediating Backend**

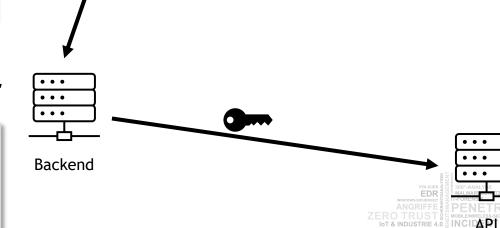








Zustandslos, d.h.
 Logout nicht
 wirksam

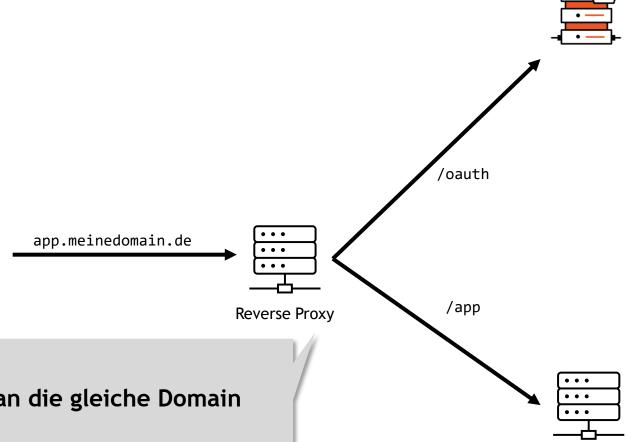


### Anwendung und IdP teilen sich eine Domain









Problem:

- · Cookies sind an die gleiche Domain gebunden
- XSS in /app hat Auswirkung auf IdP



POLICIES WAVE ANALYSE
EDR WINDOWS-SICHERHEIT IT-FORENSIK
ANGRIFFE WAVE PENETRATIONSTEST
ERO TRUST MOBILE/WIRELESS-SICHERHEIT
IOT & INDUSTRIE 4.0

SE WLAN LONG TO THE WORLD WAVE PENETRATIONS TO THE WORLD WAVE PENETRATION TO THE WORLD WAVE PENET

### Schutzmaßnahmen bei SPA



# Mögliche Schutzmaßnahmen für SPA (wenn Sie OAuth-Client sein müssen)



- Proof Key for Code Exchange (PKCE, RFC 7636)
  - Bindung von Authorization Codes an die Instanz des Clients, der den OAuth-Flow gestartet hat
- Demonstrating Proof of Possession (DPoP, 9449)
  - Bindung von Access und Refresh Token an den Besitz von Privaten Schlüsseln



### PKCE (Proof Key for Code Exchange)















HASH(Code Verifier) Code Challenge

Nachweis, dass Instanz des anfragenden und eintauschenden Clients "dieselbe" ist. (bis auf Weitergabe/Diebstahl des Code Verifier)

### Benjamin Häublein



#### cirosec GmbH

- https://www.cirosec.de/
- info@cirosec.de
- +49 7131 59455 0

### Vielen Dank für Ihre Aufmerksamkeit!