

# OAuth 2.0 Security Best Current Practice

draft-ietf-oauth-security-topics

## Status

John Bradley, Andrey Labunets,  
Daniel Fett, Torsten Lodderstedt

IETF-102  
July 19 2018, Montreal

# What is it?

- Comprehensive overview on open OAuth security topics
- Systematically captures and discusses these security topics and respective mitigations
- Recommends security best current practice

# Structure

- 1. Introduction . . . . . [3](#)
- 2. Recommendations . . . . . [4](#)
  - [2.1. Protecting redirect-based flows . . . . . \[4\]\(#\)](#)
  - [2.2. Token Replay Prevention . . . . . \[5\]\(#\)](#)
- 3. Attacks and Mitigations . . . . . [5](#)
  - [3.1. Insufficient redirect URI validation . . . . . \[5\]\(#\)](#)
    - [3.1.1. Attacks on Authorization Code Grant . . . . . \[6\]\(#\)](#)
    - [3.1.2. Attacks on Implicit Grant . . . . . \[7\]\(#\)](#)
    - [3.1.3. Proposed Countermeasures . . . . . \[8\]\(#\)](#)
  - [3.2. Code or State Leakage from Client or AS via Referrer Headers . . . . . \[9\]\(#\)](#)
    - [3.2.1. Proposed Countermeasures . . . . . \[9\]\(#\)](#)
  - [3.3. Attacks through the Browser History . . . . . \[10\]\(#\)](#)
    - [3.3.1. Code in Browser History . . . . . \[10\]\(#\)](#)
    - [3.3.2. Access Token in Browser History . . . . . \[10\]\(#\)](#)
  - [3.4. Mix-Up . . . . . \[11\]\(#\)](#)
    - [3.4.1. Attack Description . . . . . \[11\]\(#\)](#)
    - [3.4.2. Countermeasures . . . . . \[13\]\(#\)](#)
  - [3.5. Code Injection . . . . . \[14\]\(#\)](#)
    - [3.5.1. Proposed Countermeasures . . . . . \[16\]\(#\)](#)
  - [3.6. Cross Site Request Forgery . . . . . \[17\]\(#\)](#)
    - [3.6.1. Proposed Countermeasures . . . . . \[17\]\(#\)](#)
  - [3.7. Access Token Leakage at the Resource Server . . . . . \[18\]\(#\)](#)
    - [3.7.1. Access Token Phishing by Counterfeit Resource Server \[18\]\(#\)](#)
      - [3.7.1.1. Metadata . . . . . \[18\]\(#\)](#)
      - [3.7.1.2. Sender Constrained Access Tokens . . . . . \[19\]\(#\)](#)
      - [3.7.1.3. Audience Restricted Access Tokens . . . . . \[22\]\(#\)](#)
    - [3.7.2. Compromised Resource Server . . . . . \[23\]\(#\)](#)
  - [3.8. Open Redirection . . . . . \[24\]\(#\)](#)
    - [3.8.1. Authorization Server as Open Redirector . . . . . \[24\]\(#\)](#)
    - [3.8.2. Clients as Open Redirector . . . . . \[24\]\(#\)](#)
  - [3.9. TLS Terminating Reverse Proxies . . . . . \[25\]\(#\)](#)

} Recommendations

} Threat Analysis and Discussion of potential Counter Measures

# Recommendations

- Exact redirect URI matching at AS (token leakage, mix-up)
- Avoid any redirects or forwards, which can be parameterized by URI query parameters (open redirection, token/code leakage)
- One-time use tokens carried in the STATE parameter for XSRF prevention
- AS-specific redirect URIs (mix-up)
- Clients shall use PKCE (or nonce) to prevent code injection
- Use of TLS-based methods for sender constraint access tokens
- Use end-to-end TLS whenever possible

# Status

- Some review feedback during/after IETF-101 (-05)
- Incorporated feedback into latest revision (-06)
  - Reworked text on open redirection (esp. redirect behavior of AS in case of erroneous requests)
  - Reworked section on mix up (thanks to our new co-author Daniel Fett)
  - replaced text intended to inform WG discussion by recommendations to implementors (turned draft into BCP)
- No further (reasonable) feedback
- Two open proposals, otherwise ready to proceed

# Adopt proposals? WG Feedback needed!

- **Audience restriction** - Johan Peeters proposed an additional section on the value of audience/action restricted access tokens

<https://www.ietf.org/mail-archive/web/oauth/current/msg18117.html>

- **Crypto Agility** - Doug McDorman proposed an additional section on crypto agility.

<https://www.ietf.org/mail-archive/web/oauth/current/msg18118.html>