

OAuth Abuse Detection & Incident Response Report

Author: Emmanuel Ajayi

Date: 30-Dec-2025

Executive Summary

This lab demonstrates how valid OAuth tokens can be **misused outside their intended context**, bypassing authentication controls.

Key takeaways:

- Token theft can grant access to sensitive data.
- Context-aware monitoring is critical.
- Mitigations include short-lived tokens, strict scope control, and behavioral monitoring.

Attack Narrative

Step 1: Legitimate OAuth Login

- User authenticates successfully via Flask OAuth app.

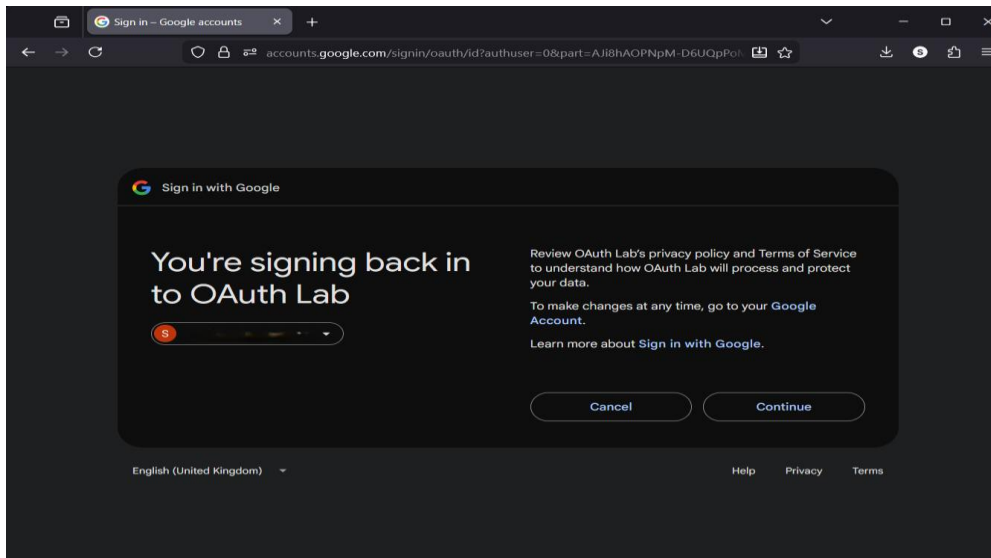


Figure 1: Successful OAuth login

Step 2: Access Token Issued

- OAuth server issues a valid access token with proper scopes.

Step 3: Token Exposure

- ```
python_OAuth
logs
auth.log
venv
.env
app.py
requirements.txt

1 -firefox/147.0", "data": {"access_token": "ya29.a0Aa/pCAB6A/ptGS...E9V7YmIMDEBGI-29LBjZyVDF-AUION/ggQ4l08agz9pr-PfofzoCrF-p8Lqgh
2
3 3101 Firefox/147.0", "data": {"id": "113192185949044927341", "email": "...", "verified_email": true, "name": "Ser Dte", "given_name":
4 000101 Firefox/147.0", "data": {"code": "4/OATX87IPMBsKwJw3y3...PGXIVvppl0vZDvrC1vr28kISoG"}}
5 -firefox/147.0", "data": {"access_token": "ya29.a0Aa/pCABFUG2GO...N28rNbttLDymDMpTq1gfTNULf3UZFNmp-WOTWUY9Z3ht-f5AgRytSB
6 3101 Firefox/147.0", "data": {"id": "113192185949044927341", "email": "...", "verified_email": true, "name": "Ser Dte", "given_name":
7 000101 Firefox/147.0", "data": {"code": "4/OATX87IP0vZU4v-lbgCF...7ZK_6kBtHebowdwtvB5JuA"}
8 -firefox/147.0", "data": {"access_token": "ya29.a0Aa/pCA_kBDgdpx...IxbknFG7VOFLCTEYssMTbXHSFRV4jou9f7miNo-goXgvZnyDIzl-Esyf
9 3101 Firefox/147.0", "data": {"id": "113192185949044927341", "email": "...", "verified_email": true, "name": "Ser Dte", "given_name":
10 000101 Firefox/147.0", "data": {"code": "4/OATX87IPDvtNAt3cqJnSxum...ZRVvg6hztXFNDPWFxf-yg}}
11 -firefox/147.0", "data": {"access_token": "ya29.a0Aa/pCA_SV6uzg...YGQ3ixiUrZQA8EPxyYngcrOUnIngasuj7cwMpf4PZrhqndsv1ktHJ5Xu
12 3101 Firefox/147.0", "data": {"id": "113192185949044927341", "email": "...", "verified_email": true, "name": "Ser Dte", "given_name":
13
```

## Step 4: Token Abuse

- ```
> curl -H "Authorization: Bearer ya29.a0.../C3-SV6ZUzXNRH4UP3kuArYfoMFKJ3uQWmzslZgNVC..."  
FFHXhk_gcdTUMLUkFoaq3Qv_rf7f1SV2vsDHGHywflc:sZtIE8c-8oh3vQBMyfgjd8MYvsn9...  
refresh_token": "1103GFyBPgwAhlCGyIARAAGv19nBT-LP1RDgzJKUJUV...  
https://userinfo.email.openid?https://www.googleapis...  
DNLOGMSYmuYzVFNlDiuOWMdj3mj1FMDUwTYTxTK2KMGylC...  
FI2NP9MH1xOTtSdXNlyJMbOmYnmIUyXBwc5yb29bnBGVA...  
adovdcvds55jb20LcC...XIHTMXtOTLTODU...  
CT1BFVEGD4V2z55jb20LcC=tmshBWW101TZtXRHR1...  
GVGRKrf3BNldzd2NS4SYVtJ1o2TYtYr1mdpmvXuX2...  
VHWHg1-82E54VFVVj3xeAN29JRKEvHEBEFA7ezhe3eX880ygdJ-EHWLSLUaG6FSRSHGxOPT9ndemdlIL-BRBBcgNmZVU3utAk591AgUYLbd  
ZLPJBMh5JAstNYK-qPMKAUEZ5hZnP1xz2soLxJ_x8QeyY40v-Ah91tckFCSZW6JDc8-CpGG6j--WLIRNGj_QH1OKHzPa_WMU-5NEWzn1zGXQyZBYhm  
ISA": https://www.googleapis.com/oauth2/v1/userinfo  
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535  
curl: (3) URL rejected: Bad hostname  
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535  
curl: (7) Failed to connect to 0.0.0.1 port 80 after 1 ms: Could not connect to server  
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535  
curl: (3) URL rejected: Malformed input to a URL function  
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535  
curl: (3) URL rejected: Bad hostname  
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535  
curl: (6) Could not resolve host: ey3bhG6ci0J5uZu211niIsImtpzC2IGtJ05NmQuMdhLOGM3YmUxyUZFN2INDiOWOUZDVjMJf1MDUwTYTXtK...  
YL2FY291bnRZLmdvbWdsZs55jb20LcCJhenAI0iIZNDc5MDV2NDUUXMDATAjF5OtDpa2NONDFI2n2pMMHXTOTtSDXNlyJMbOmYnmIUyXBwc5yn
```

Indicators of Compromise (IOCs)

- ## Detection & Mitigation

Detection Strategies:

- Monitor token usage patterns (IP, device, frequency)
- Trigger alerts for abnormal behavior

Mitigation Measures:

- Short-lived access tokens
- Enforce strict scopes
- Eliminate plaintext token logging
- Revoke suspicious tokens immediately
- Implement behavior-based monitoring

Flow Diagram



Flow-diagram.png

Conclusion

- Authentication success does not equal security.
- Tokens can be abused even when login is legitimate.
- Continuous monitoring, anomaly detection, and proper token hygiene are key to defense.