OWASP
Open Web Application
Security Project

OWASP Portland Chapter

Welcome to OWASP Portland's monthly chapter meeting!

OWASP
Open Web Application
Security Project

Twitter: @PortlandOWASP

Website: pdxowasp.org

Meetup: https://www.meetup.com/OWASP-Portland-Chapter/

Slack: owasp.slack.com #chapter-pdx

OWASP
Open Web Application Security Project

Next Chapter Meeting: Aug

Graph Theory for Security

Presented by Timothy Morgan

August 13th 2019 from 6–8pm

Hosted by: Simple 120 SE Clay St, Floor 2

Follow the Portland OWASP Meetup, Twitter, or email list for further details!

OWASP
Open Web Application Security Project

Project Focus: Amass

- In-depth DNS Enumeration and Network Mapping!

Information Gathering Techniques Used

- DNS, Scraping, Certificates, APIs, Web Archives

https://www.owasp.org/index.php/OWASP_Amass_Project

https://github.com/OWASP/Amass

OWASP
Open Web Application Security Project

Become A Member

- Support Web Application Security Education
- Get involved in OWASP Projects
- Direct Your Membership Dues to Your Home Chapter or Project You Care About

https://www.owasp.org/index.php/Membership

identiverse®

THE EASY (AND SECURE!) WAY TO BUILD JAVASCRIPT WEB APPS WITH OAUTH 2 & OIDC

Introduction

- Jake Feasel
- Developer Experience lead engineer at ForgeRock

- **AppAuthHelper** : https://www.npmjs.com/package/appauthhelper
- Wrapper for AppAuth for JS to assist with the full OAuth2 / OIDC token life-cycle.

- **OIDCSessionCheck**: https://www.npmjs.com/package/oidcsessioncheck

JavaScript library to assist with binding sessions between an OIDC OP and RP

identiverse®

Context

- JavaScript or "Single Page" applications
- OAuth 2 client / OIDC relying party
- REST calls to Resource Server Endpoints
- Client app driven by the resource owner

identiverse®

identiverse®

Best Current Practices

Important security concerns for web clients

Which Grant to Use: Implicit or Authorization Code?

- **https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-3.1.2**

- *The implicit grant (response type "token") ... [is] vulnerable to access token leakage and access token replay...*

- *[C]lients SHOULD NOT use the implicit grant (response type "token")...*

- *Clients SHOULD instead use the response type "code" (aka authorization code grant type)*

identiverse®

PKCE for non-Mobile?

- **https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-3.1.1**

- *Clients utilizing the authorization grant type MUST use PKCE [RFC7636] in order to (with the help of the authorization server) detect and prevent attempts to inject (replay) authorization codes into the authorization response.*

- *Note: although PKCE so far was recommended as a mechanism to protect native apps, this advice applies to all kinds of OAuth clients, including web applications.*

identiverse®

Renewing tokens

- **HTTP/1.1 401 Unauthorized**
- WWW-Authenticate: Bearer realm="example",
- error="invalid_token",
- error_description="The access token expired"

identiverse®

Use a Refresh Token?

- Server side Clients Use These
- Why Not Front-End Apps?

- Refresh Tokens Live For a Long Time
- Less Is More
- You May Not Need It

identiverse®

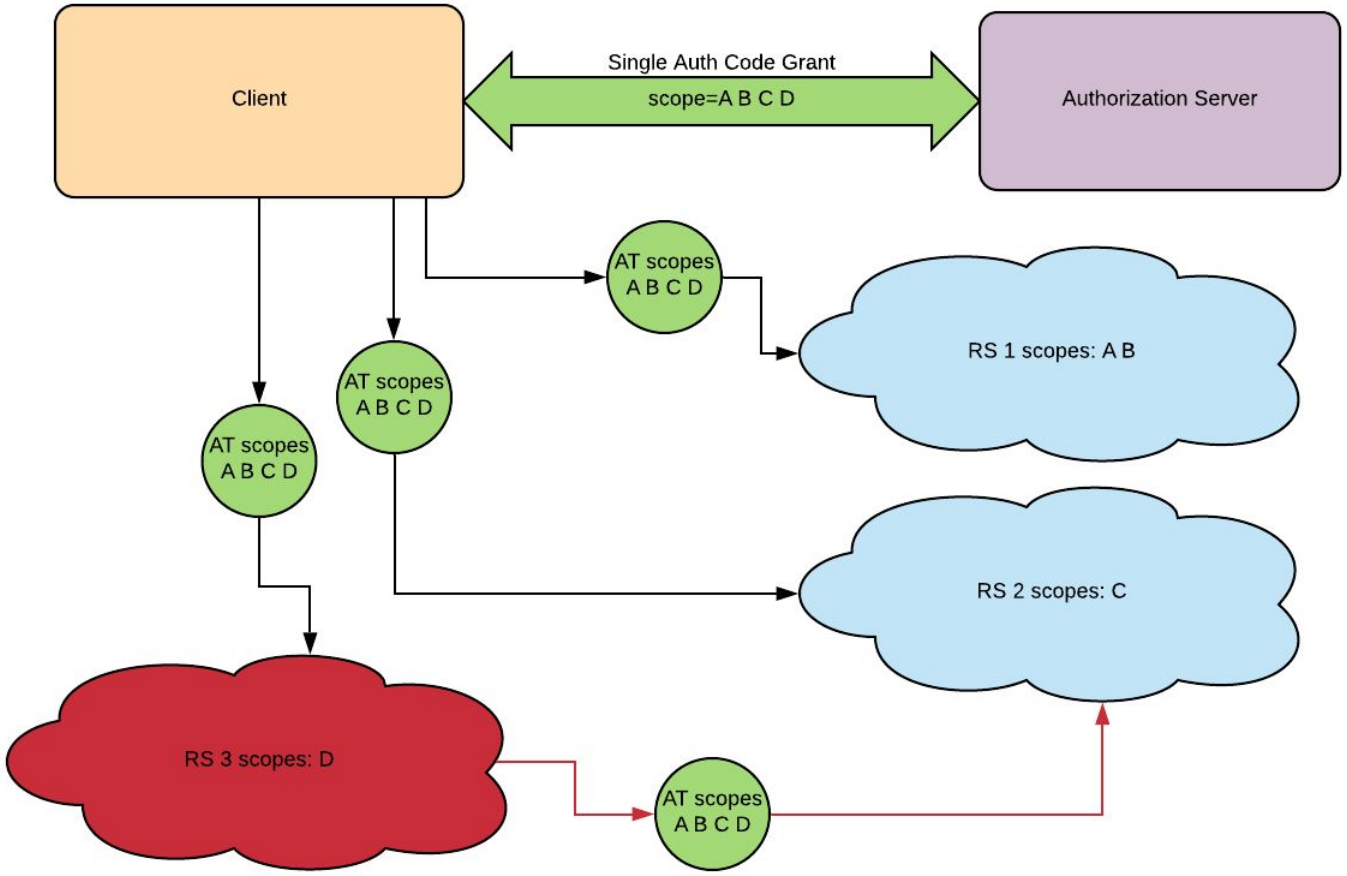
Silent Authz Code Grant in iFrames

- Established session in the AS
- Scope consent has to have been saved
- Access token lifetime shorter than the AS session lifetime.
- Access-token-bearing requests in the same browser as the AS session cookie.
- Include `prompt=none` in the call to the authorization endpoint
- Make the request in a hidden iFrame

identiverse®

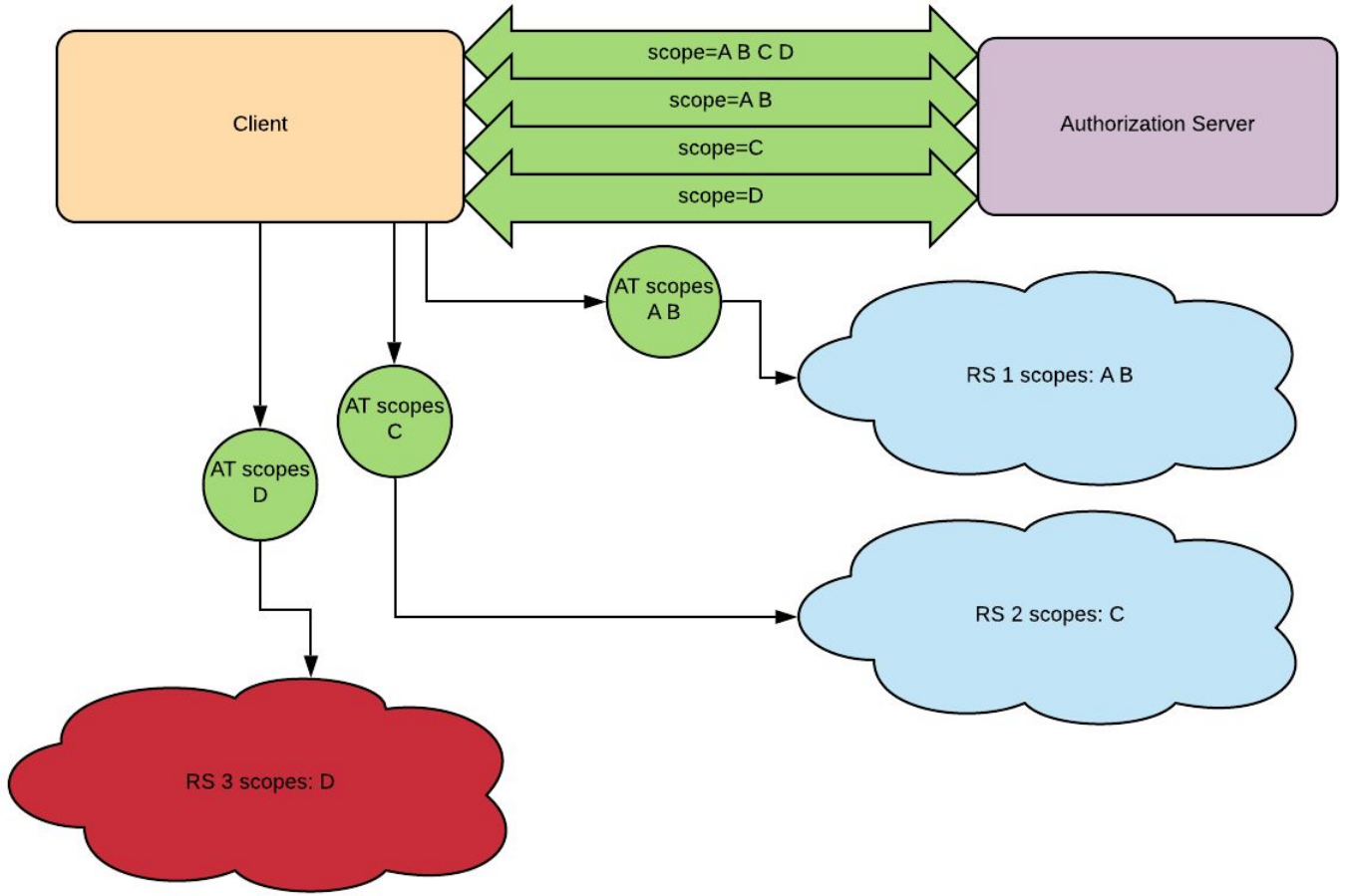
Access Token Leakage

- **https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-4.8**



identiverse®

Counter-measure for token leakage



IDP-Initiated Logout

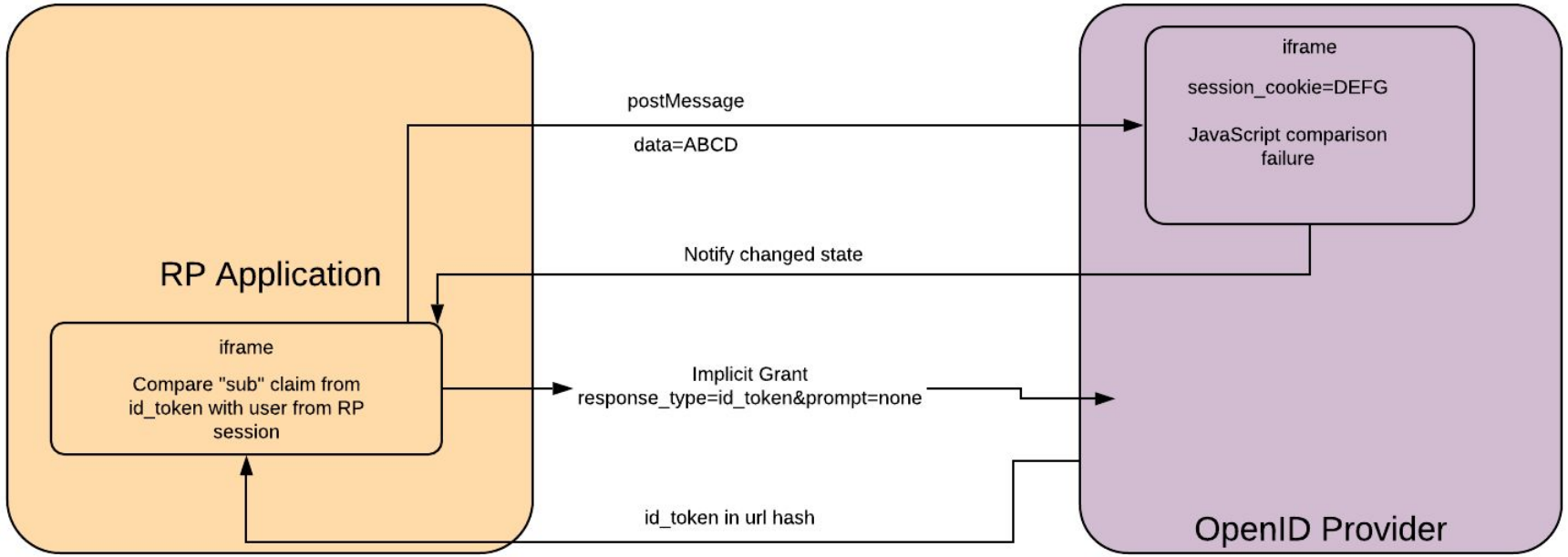
- **https://openid.net/specs/openid-connect-session-1_0.html**

- *To do so, it is **possible to repeat the Authentication Request with prompt=none**. However, this causes network traffic and this is **problematic on the mobile devices that are becoming increasingly popular**. Therefore, once the session is established with the Authentication Request and Response, it is desirable to be able to check the login status at the OP without causing network traffic by **polling a hidden OP iframe from an RP iframe with an origin restricted postMessage** as follows....*

- .

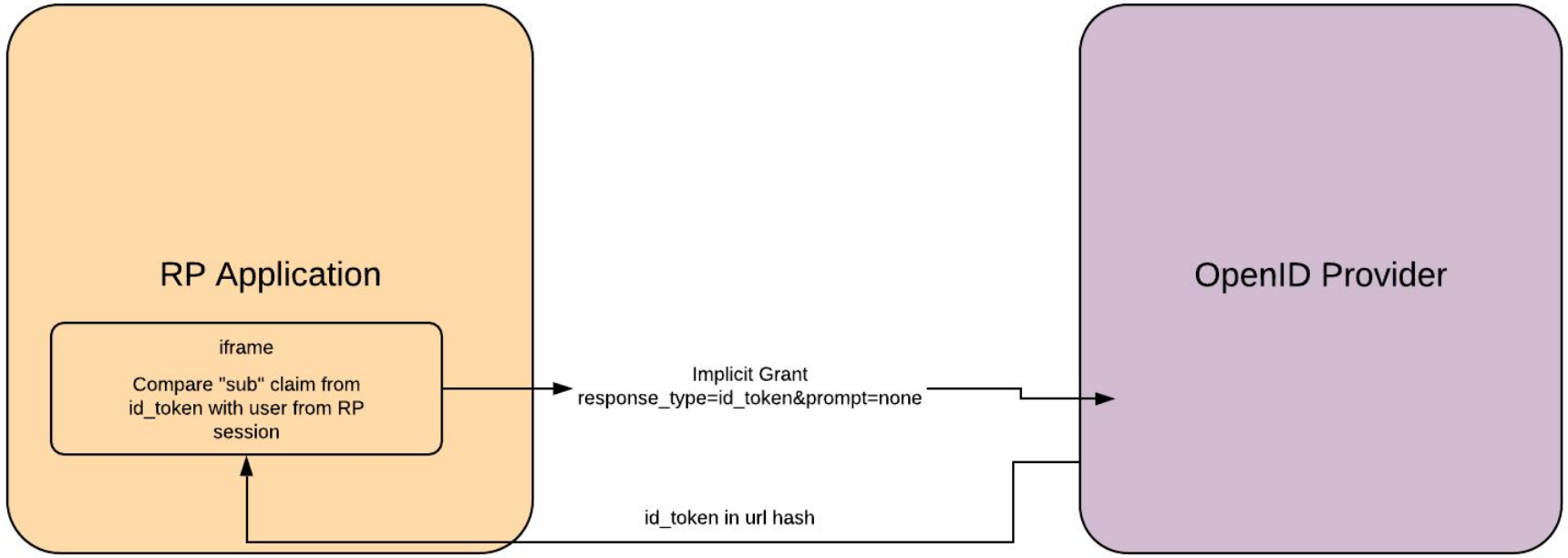
identiverse®

OIDC Spec Session Monitoring Proposal



identiverse®

OIDC Session Monitoring Simplified



identiverse®

identiverse®

Libraries to make it easy

Tools you can use today

OIDCSessionCheck

- **https://www.npmjs.com/package/oidcsession**

```
var sessionCheck = new SessionCheck({
    clientId: "myClientId",
    opUrl: "https://login.sample.forgeops.com/oauth2/authorize",
    subject: claims.sub,
    invalidSessionHandler: function () {
        logout();
    },
    cooldownPeriod: 5
});

// check with every captured event
document.addEventListener("click", function () {
    sessionCheck.triggerSessionCheck();
});
document.addEventListener("keypress", function () {
    sessionCheck.triggerSessionCheck();
});
```

identiverse®

AppAuth

AppAuth

Native App SDK for OAuth 2.0 and OpenID Connect implementing modern best practices

AppAuth for Android

AppAuth for iOS and macOS

AppAuth for JS

- Open Source (Apache 2.0)
- Backed by Google
- PKCE
- JS version is generic (not just for browser apps)

identiverse®

AppAuthHelper

- **https://www.npmjs.com/package/appauthhelper**

```
AppAuthHelper.init({
    clientId: "appAuthClient",
    authorizationEndpoint: "https://default.iam.example.com/am/oauth2/authorize",
    tokenEndpoint: "https://default.iam.example.com/am/oauth2/access_token",
    revocationEndpoint: "https://default.iam.example.com/am/oauth2/token/revoke",
    endSessionEndpoint: "https://default.iam.example.com/am/oauth2/endSession",
    resourceServers: {
        "https://default.iam.example.com/am/oauth2/userinfo": "profile",
        "https://default.iam.example.com/rs": "custom_scope1 custom_scope2"
    },
    tokensAvailableHandler: function (claims) {
        // Start making RS requests
        // fetch("https://default.iam.example.com/am/oauth2/userinfo").then(...)
    }
});
AppAuthHelper.getTokens();
```

identiverse®

RS requests are easy, right?

```
var deferred = $.ajax({
    url: "https://rs.example.com/me",
    headers: {
        "Authorization": "Bearer " + getAccessToken()
    }
});
```

identiverse®

What about expired tokens?

```
var deferred = $.Deferred(),
    requestDetails = function (token) {
        return {
            url: "https://rs.example.com/me",
            headers: {
                "Authorization": "Bearer " + getAccessToken()
            }
        };
    };

$.ajax(requestDetails()).then(deferred.resolve, function (jqXHR) {
    if (getAuthHeaderError(jqXHR) === "invalid_token") {
        refreshAccessToken().then(function () {
            $.ajax(requestDetails())
                .then(deferred.resolve, deferred.reject);
        }, deferred.reject);
    } else {
        deferred.reject(jqXHR);
    }
```

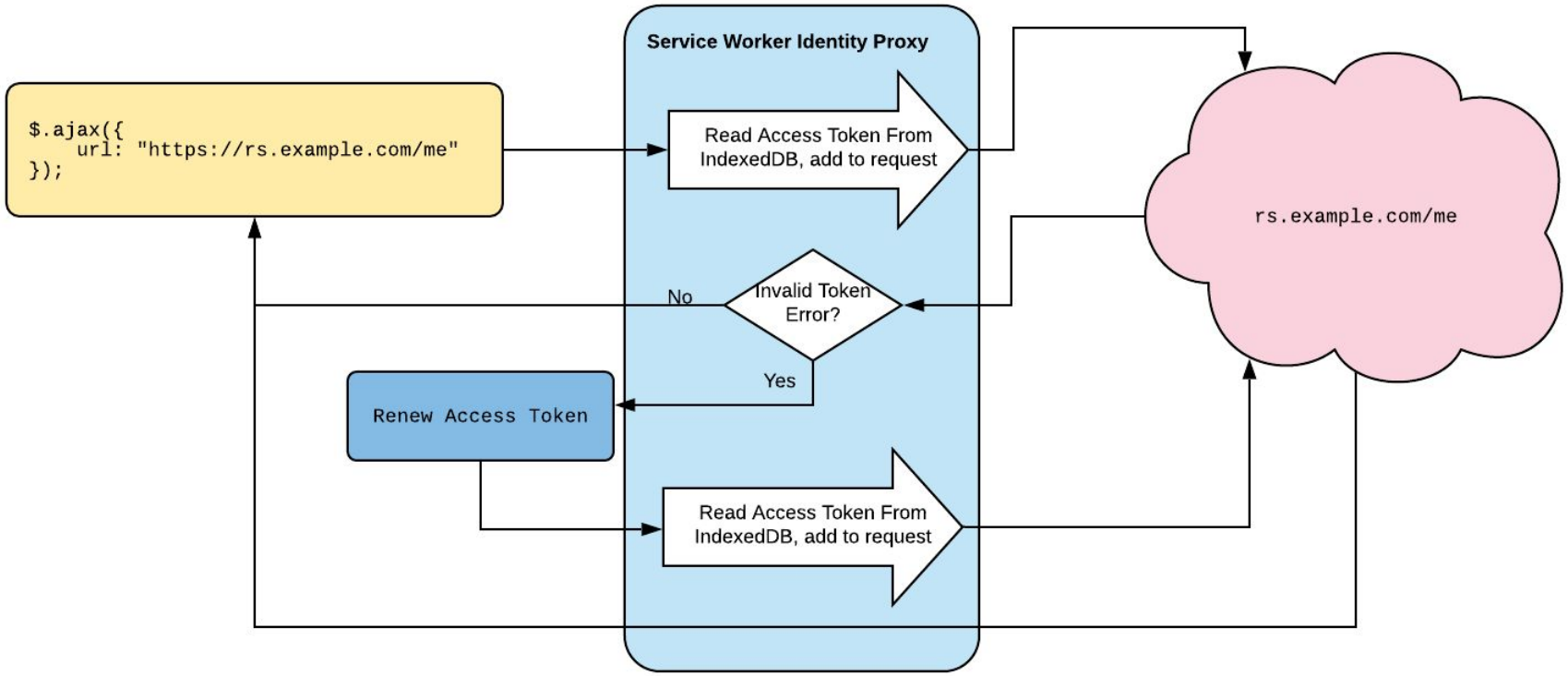
identiverse®

What if it wasn’t your problem?

```
var deferred = $.ajax({
   url: "https://rs.example.com/me"
});
```

identiverse®

Service Worker as an Identity Proxy




```
resourceServers: {
    "https://default.iam.example.com/am/oauth2/userinfo": "profile email",
    "https://default.iam.example.com/me": "custom_scope1 custom_scope2"
},
```

identiverse®

Service Worker Code Sample

```
self.addEventListener("fetch", (event) => {
    if (self.appAuthConfig &&
        typeof self.appAuthConfig.resourceServers === "object" &&
        Object.keys(self.appAuthConfig.resourceServers).length) {

        var resourceServer = Object.keys(self.appAuthConfig.resourceServers)
            .filter((rs) => event.request.url.indexOf(rs) === 0)[0];

        if (resourceServer) {
            event.respondWith(new Promise((resolve, reject) => {
                self.addAccessTokenToRequest(event.request, resourceServer)
                    .then((rsRequest) => fetch(rsRequest))
                    .then((resp) => {
                        // Watch for retry-able errors as described by https://tools.ietf.org/html/rfc6750#section-3
                        if (!resp.ok && self.getAuthHeaderDetails(resp.headers)["error"] === "invalid_token") {
                            let promise = self.waitForRenewedToken(resourceServer)
                                .then(() => self.addAccessTokenToRequest(event.request, resourceServer))
                                .then((freshRSRequest) => fetch(freshRSRequest));

                            self.messageChannel.postMessage({
                                "message":"renewTokens",
                                "resourceServer": resourceServer
                            });
                            return promise;
                        } else {
                            return resp;
                        }
                    })
                    .then(resolve, reject);
            }));
        }
    }
    return;
});
```

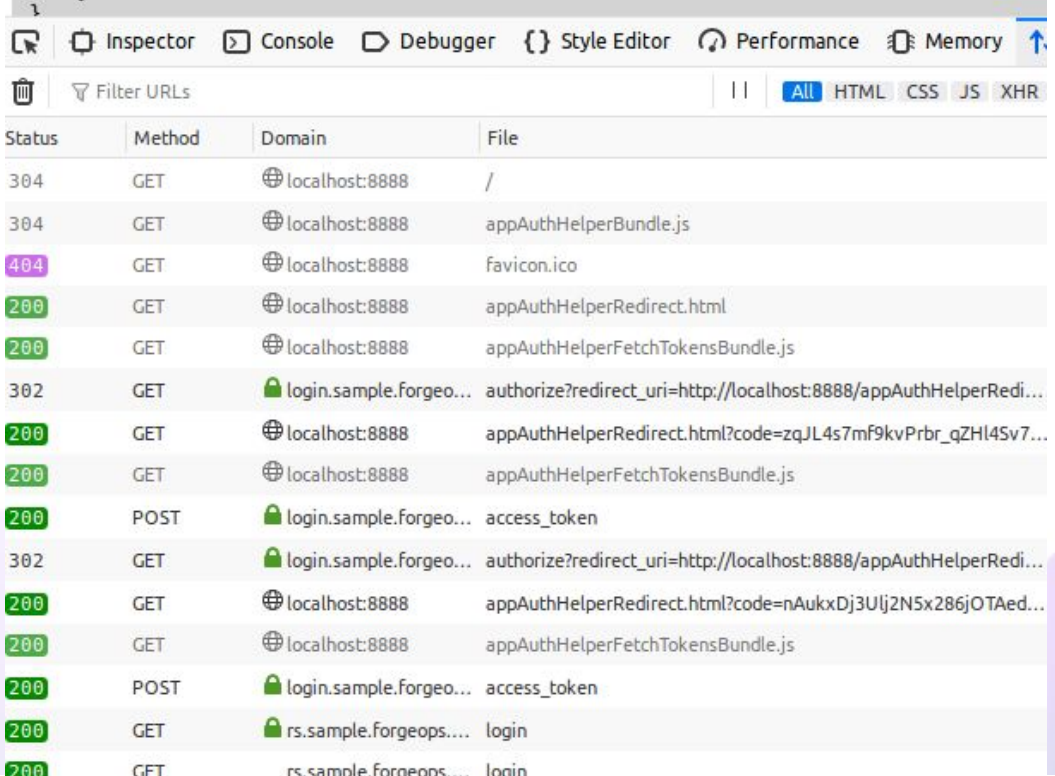
identiverse®

identiverse®

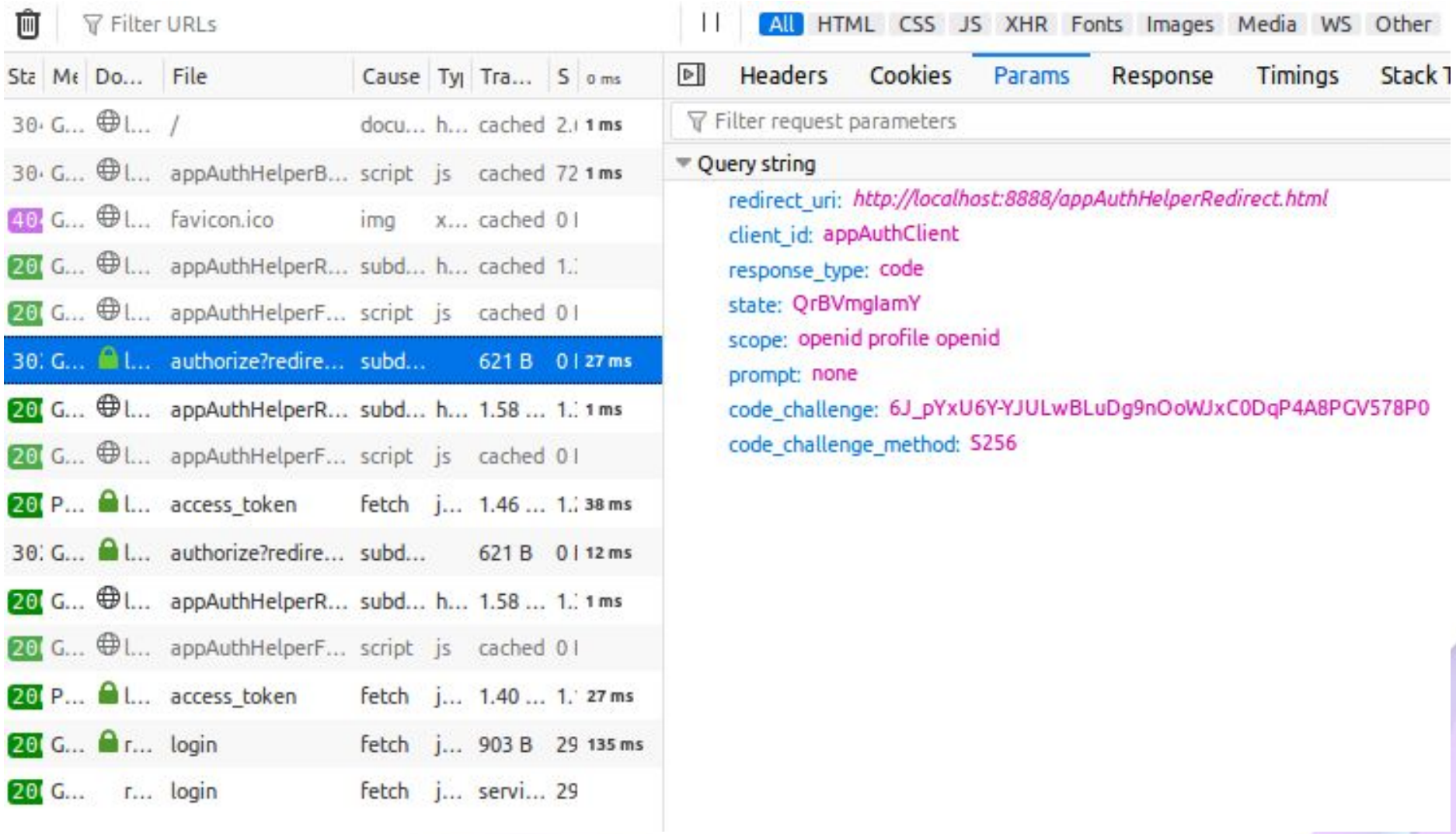
Demo

Walk-through of an example application

```
tokensAvailableHandler: function (claims) {
    Promise.all([
        fetch("https://rs.sample.forgeops.com/openidm/info/login").then((resp) => resp.json())
    ]).then((responses) => {
        document.getElementById('userDetails').innerText = JSON.stringify({
            "info/login": responses[0]
        }, null, 4);
    });
}
```

identiverse®



identiverse®

Request URL: https://login.sample.forgeops.com/oauth2/authorize?redirect_uri=http://localhost:8888/appAuthHelperRe
response_type=code&state=QrBVmgIamY&scope=openid profile openid&prompt=none&code_challenge=6J_pYxU6Y-YJULwBLuDg
code_challenge_method=S256
Request method: GET
Remote address: 192.168.99.100:443
Status code: 302 Found
Version: HTTP/2.0
Referrer Policy: no-referrer-when-downgrade

Filter headers

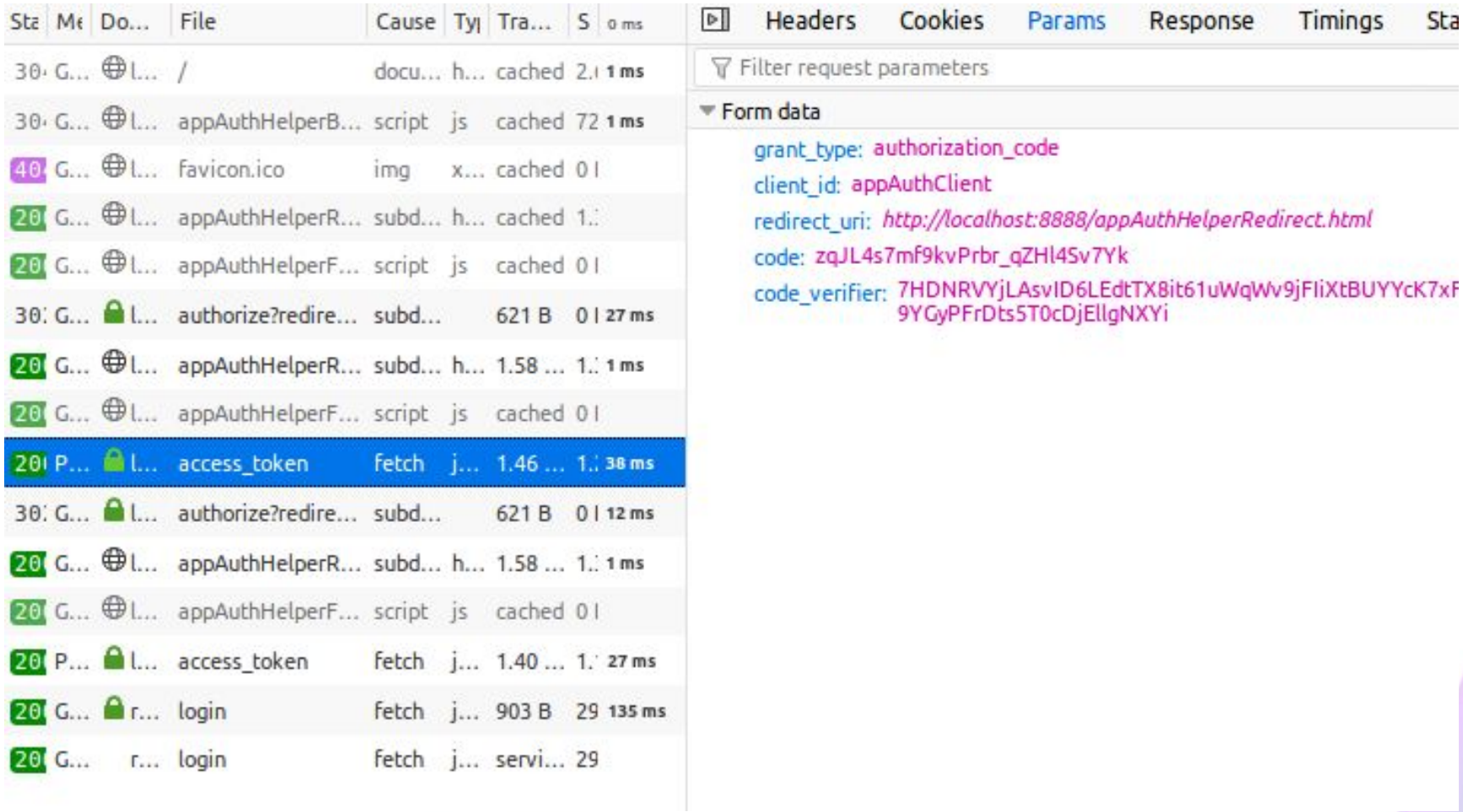
Response headers (621 B)

```
HTTP/2.0 302 Found
server: nginx/1.15.9
date: Thu, 20 Jun 2019 20:32:53 GMT
content-length: 0
location: http://localhost:8888/appAuthHelperRedirect.html?code=zqJL4s7mf9kvPrbr_qZHl4Sv7Yk&iss=https%3A%2F%2F
x-frame-options: SAMEORIGIN
pragma: no-cache
cache-control: no-store
accept-ranges: bytes
vary: Accept-Charset, Accept-Encoding, Accept-Language, Accept
access-control-allow-origin: *
access-control-allow-methods: PUT,GET,POST,HEAD,PATCH,DELETE
access-control-allow-headers: authorization,x-requested-with
X-Firefox-Spdy: h2
```

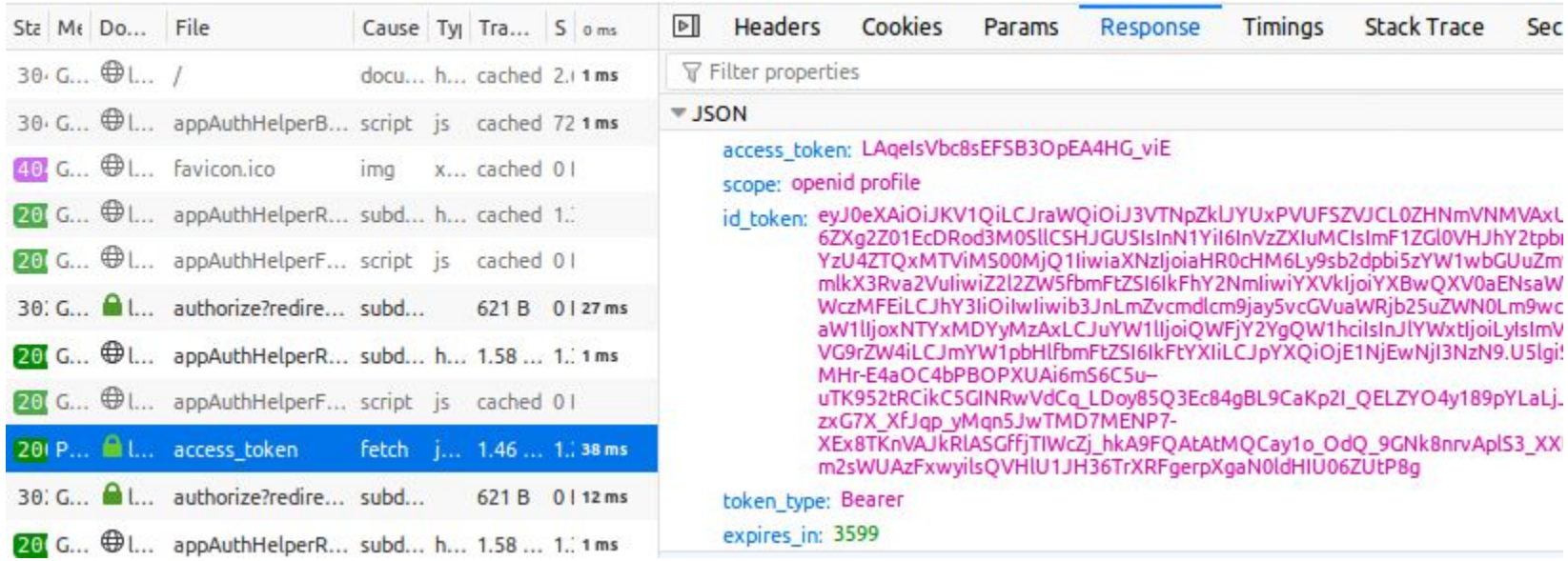
Request headers (855 B)

```
Host: login.sample.forgeops.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://localhost:8888/
Connection: keep-alive
Cookie: route=59372b3ea79657fbe7c765171526fdef07a57509; amlbcookie=01; iPlanetDirectoryPro=Qamslikf2RkZoZIVAPe
Upgrade-Insecure-Requests: 1
```

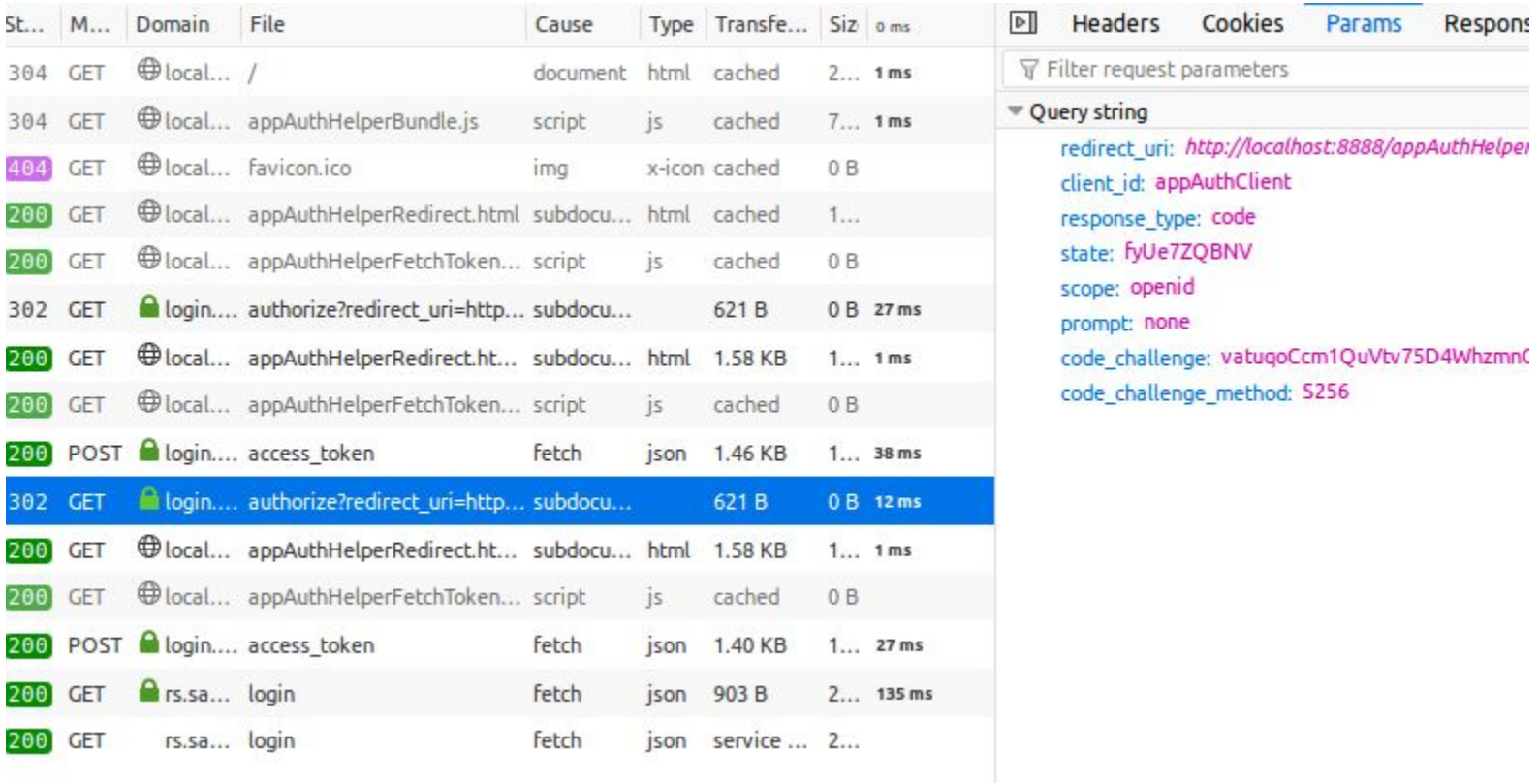
identiverse®



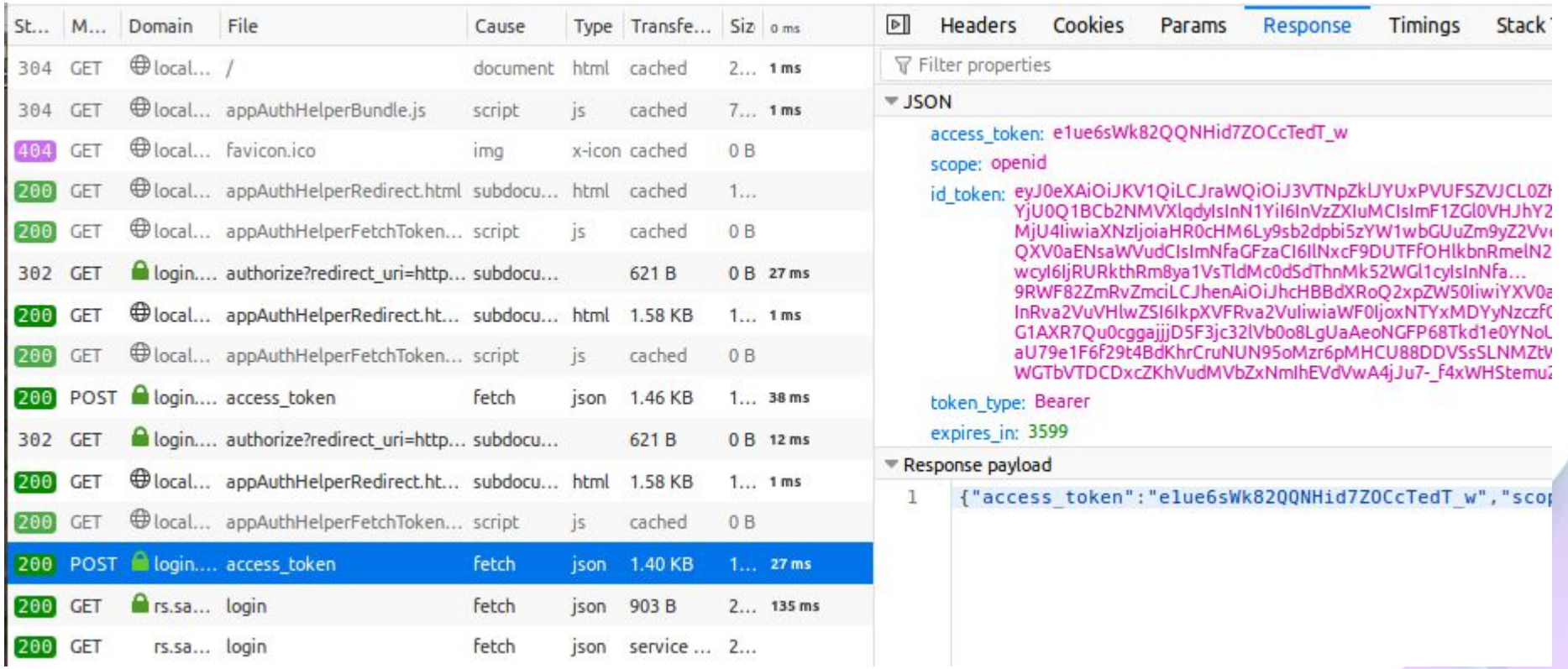
identiverse®



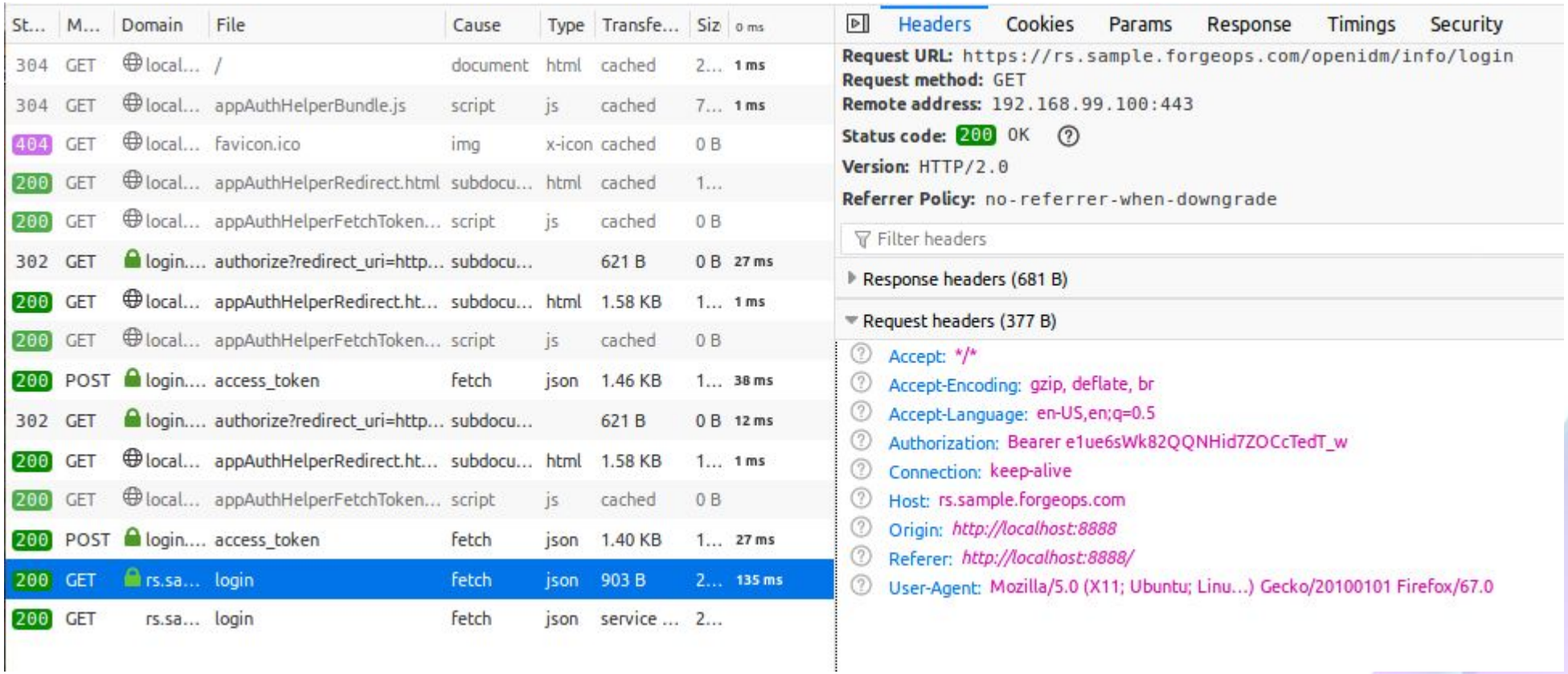
identiverse®



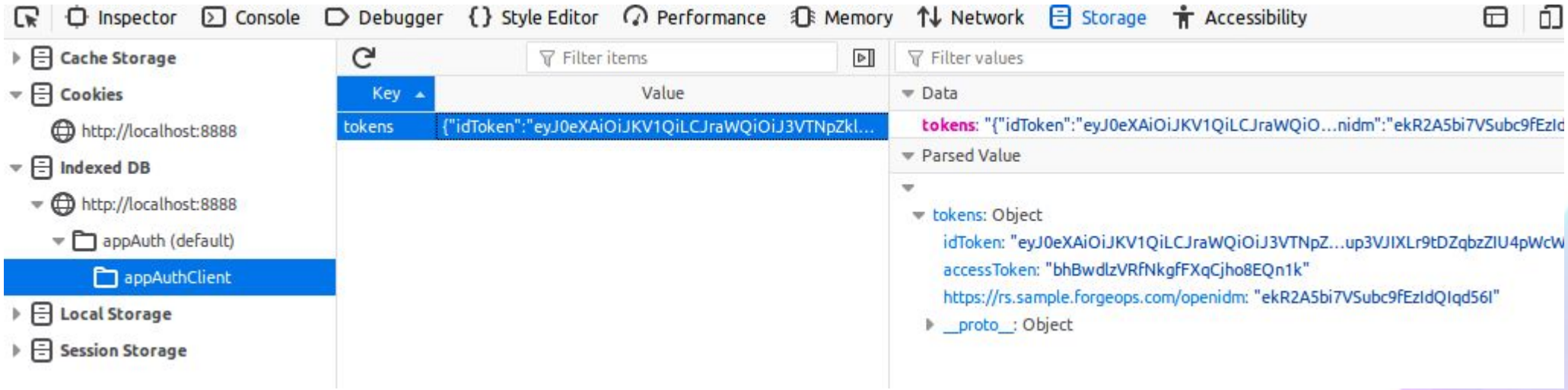
identiverse®



identiverse®



identiverse®



identiverse®

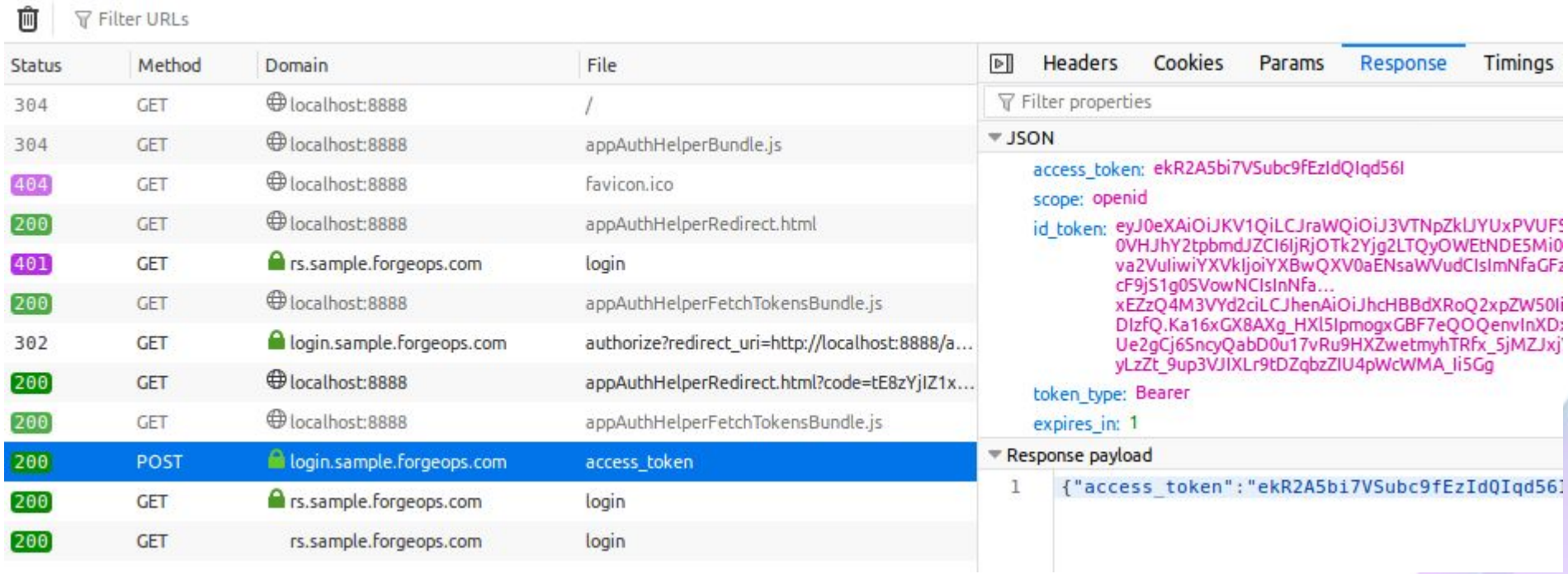
Request URL: https://rs.sample.forgeops.com/openidm/info/login
Request method: GET
Remote address: 192.168.99.100:443
Status code: 401 Unauthorized
Version: HTTP/2.0
Referrer Policy: no-referrer-when-downgrade

Filter headers

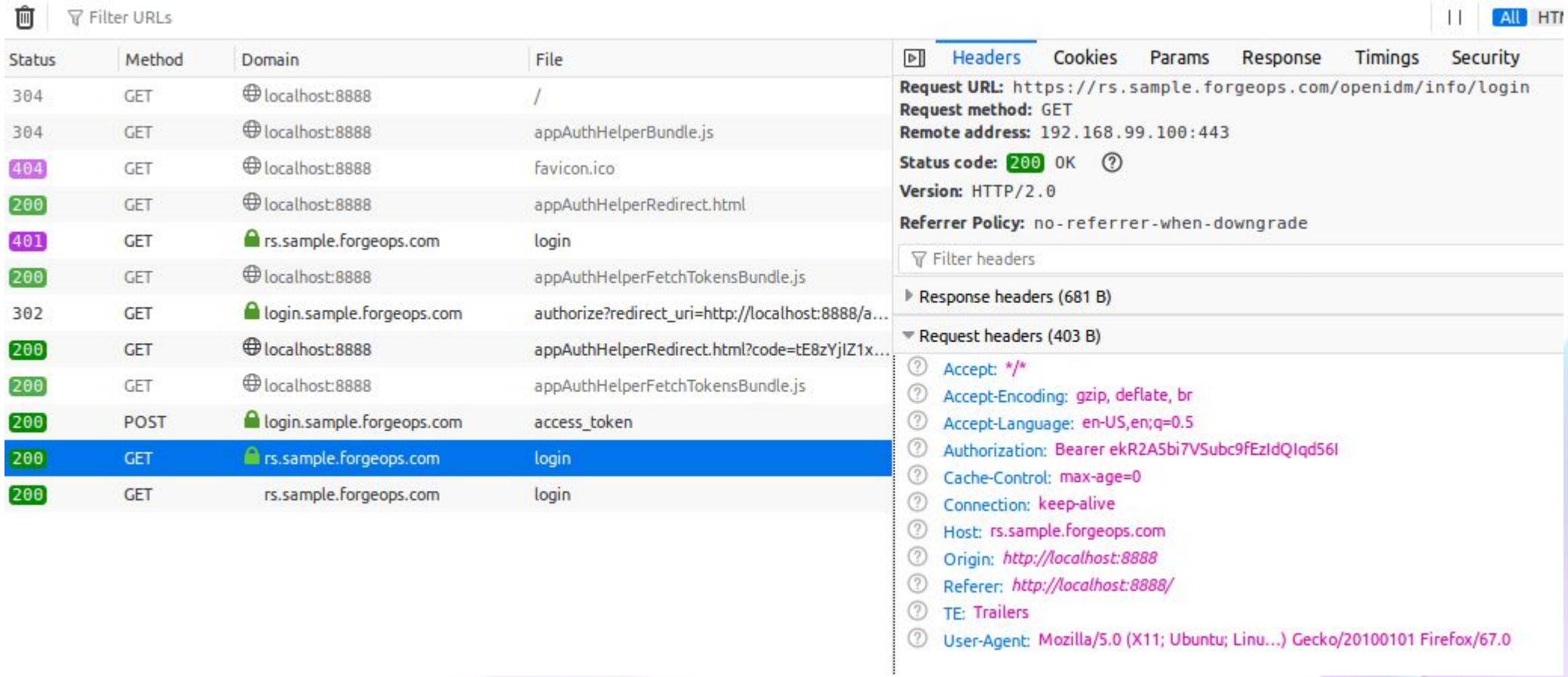
Response headers (697 B)

```
HTTP/2.0 401 Unauthorized
server: nginx/1.15.9
date: Thu, 20 Jun 2019 21:00:23 GMT
content-length: 0
set-cookie: INGRESSCOOKIE=f9714211a5c6084e034bbcb6bcd3b981; Path=/; Secure; HttpOnly
www-authenticate: Bearer realm="OpenIG",error_description="The access token provided is expired, revoked, malformed, or invalid for other reasons.",error="invalid_token"
```

identiverse®



identiverse®



identiverse®

- **AppAuthHelper** : https://www.npmjs.com/package/appauthhelper
- Wrapper for AppAuth for JS to assist with the full OAuth2 / OIDC token life-cycle.

- **OIDCSessionCheck**: https://www.npmjs.com/package/oidcsessioncheck
- JavaScript library to assist with binding sessions between an OIDC OP and RP

- Twitter: **@jakefeasel**
- https://github.com/**jakefeasel**
- https://www.linkedin.com/in/**jake-feasel**/

identiverse®


identiverse®
CELEBRATING
identiverse
10 YEARS
ANNIVERSARY