



Information Security

CPSC 310



EQUIFAX®

**DATA BREACH IMPACTS
143 MILLION
U.S. CONSUMERS!**

July 29 2017

100,000 Canadian victims: What we know about the Equifax breach – and what we don't

When did the company know about the breach? And why didn't it patch the hole intruders used to get in?



Matthew Braga · CBC News · Posted: Sep 19, 2017 6:50 PM ET | Last Updated: September 19, 2017

EQUIFAX

5 Ways an Identity Thief Can Use Your Social Security Number

November 2, 2017 · 5 min read by Christine DiGangi ★ 7 Comments

Having your Social Security number or card stolen isn't quite like getting your bank account information taken—though granted, both are stressful experiences. The major difference is that you can get a new bank account number, while the Social Security Administration very rarely issues new Social Security numbers.

EQUIFAX®
DATA BREACH IMPACTS
143 MILLION
U.S. CONSUMERS!

July 29 2017



Struts™

CVE-2017-5638

March 7 2017



1. Insecure network design
2. Inadequate encryption of personally identifiable information
3. Ineffective breach detection mechanism



(306) 000-01

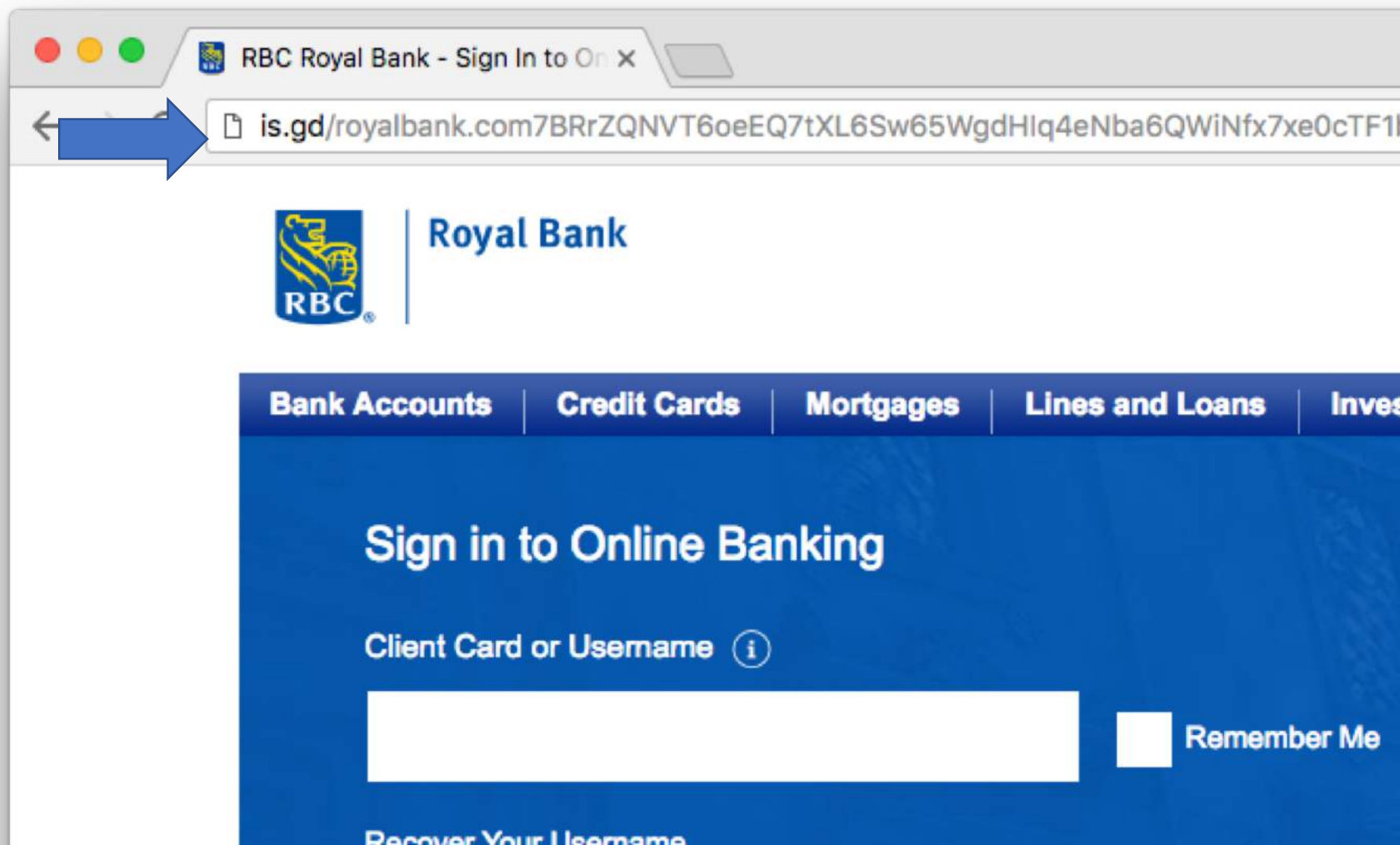
Text Message
Mon, Oct 30, 11:01 AM

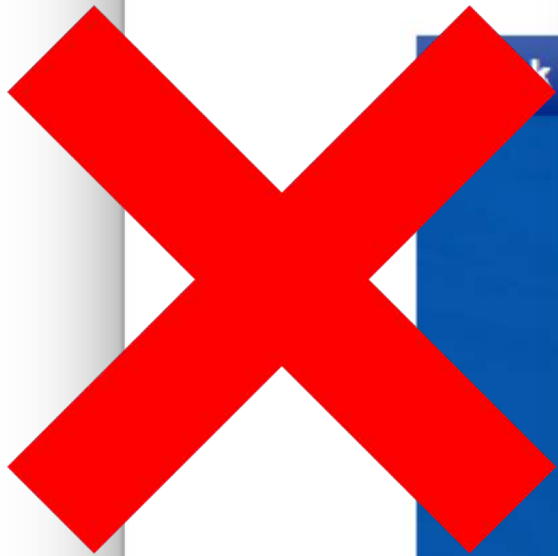
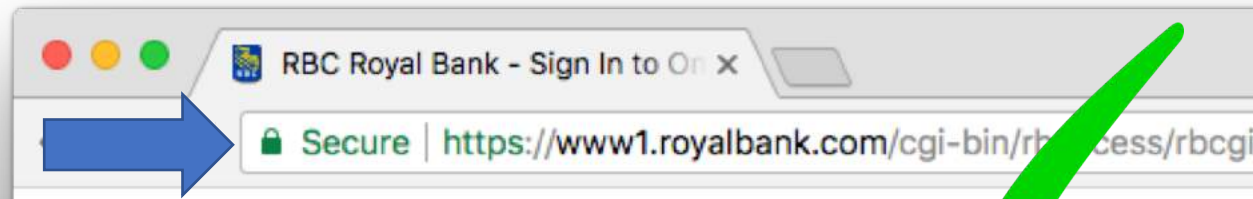
Hi it's Fido: we have issued a refund to your account. Please see:

Tap to Load Preview

is.gd







RBC Royal Bank

[Bank Accounts](#) | [Credit Cards](#) | [Mortgages](#) | [Lines of Credit](#)

Sign in to Online Banking

Client Card or Username ⓘ

[Recover Your Username](#)

Password



Information need security

Today we mainly talk about how service providers know you are actually you
, and what could go wrong

Basics

HTTP

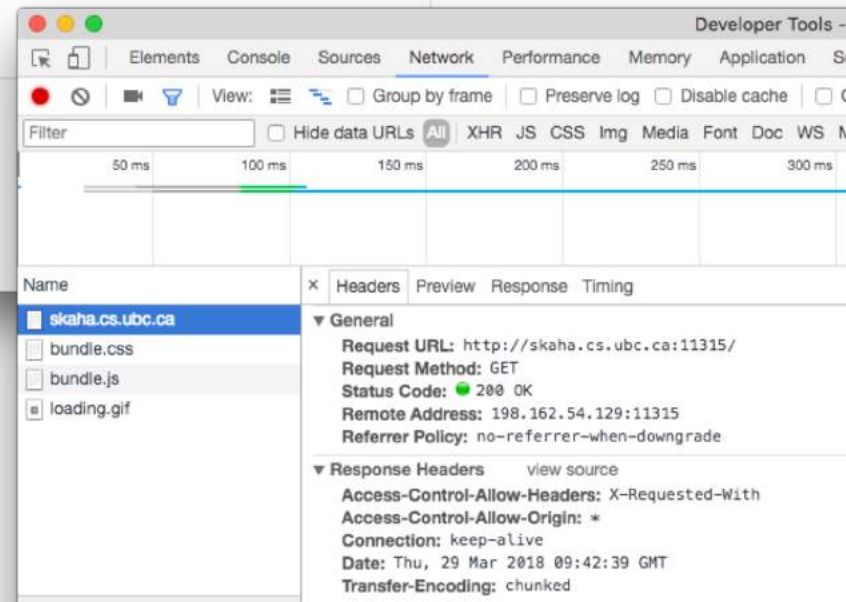
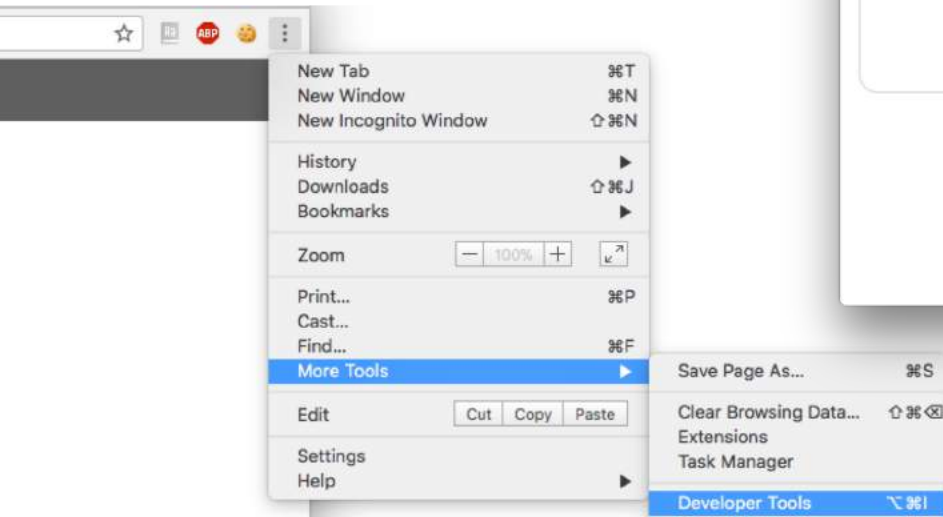
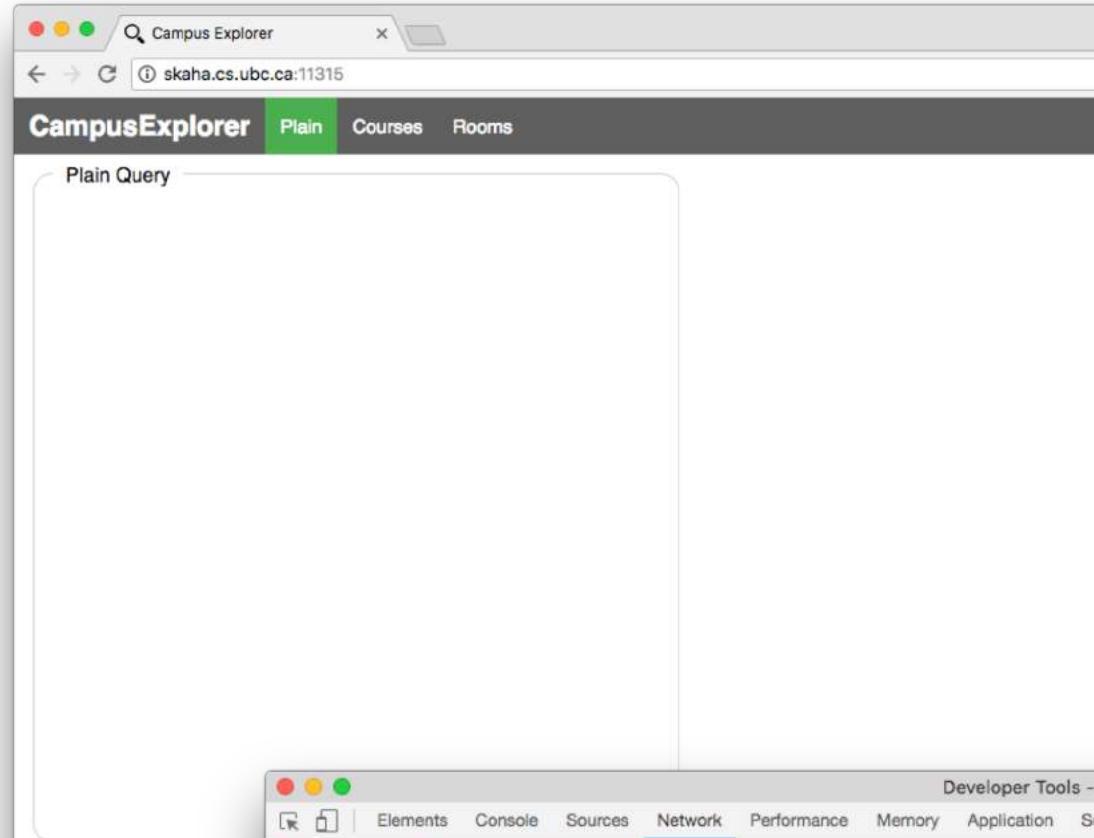
Cookies

HTTPS

Hypertext Transfer Protocol: HTTP

- Any communication using this protocol takes place via HTTP messages
 - All websites!
- Two types of HTTP messages
 - Request
 - Response
- Text-based
- Actually they are text messages

DEMO



DEMO

```
GET / HTTP/1.1
Host: skaha.cs.ubc.ca:11315
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Date: Thu, 29 Mar 2018 09:47:11 GMT
Connection: keep-alive
Transfer-Encoding: chunked
```

```
<!DOCTYPE html>
<html>
<head>
  <meta http-equiv="Content-type" content="text/html; charset=utf-8"/>
  <title>Campus Explorer</title>
  <link rel="shortcut icon" href="favicon.ico" />
  <link href="bundle.css" rel="stylesheet" />
</head>
<body class="loading prod" data-tabs="plain,courses,rooms">
  <script type="text/javascript" src="bundle.js"></script>
</body>
</html>
```



DEMO

```
GET / HTTP/1.1
Host: skaha.cs.ubc.ca:11315
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
```



↓ ↓

```
POST /query HTTP/1.1
Host: skaha.cs.ubc.ca:11315
Connection: keep-alive
Content-Length: 87
Origin: http://skaha.cs.ubc.ca:11315
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3)
Content-Type: application/json
Accept: */*
DNT: 1
Referer: http://skaha.cs.ubc.ca:11315/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
```

→ {"WHERE":{"GT":{"courses_avg":95}},"OPTIONS":{"COLUMNS":["courses_d



DEMO

```
POST /query HTTP/1.1
Host: skaha.cs.ubc.ca:11315
Connection: keep-alive
Content-Length: 87
Origin: http://skaha.cs.ubc.ca:11315
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3)
Content-Type: application/json
Accept: */*
DNT: 1
Referer: http://skaha.cs.ubc.ca:11315/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7

{"WHERE":{"GT":{"courses_avg":95}},"OPTIONS":{"COLUMNS":["courses_d
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Content-Type: application/json
Content-Length: 9940
Date: Thu, 29 Mar 2018 09:56:28 GMT
Connection: keep-alive

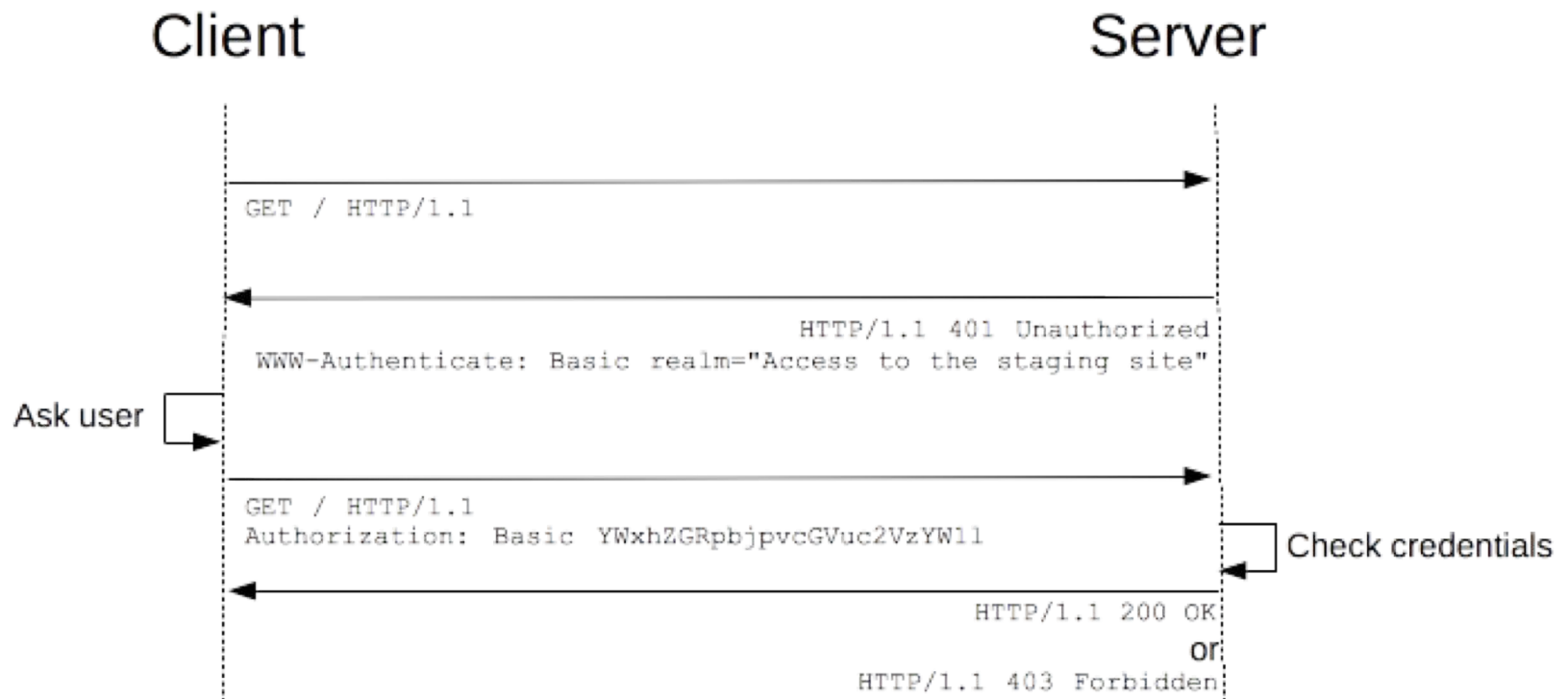
{"result":[{"courses_dept":"adhe","courses_id":"329"}, {"courses_dept":"aps
```



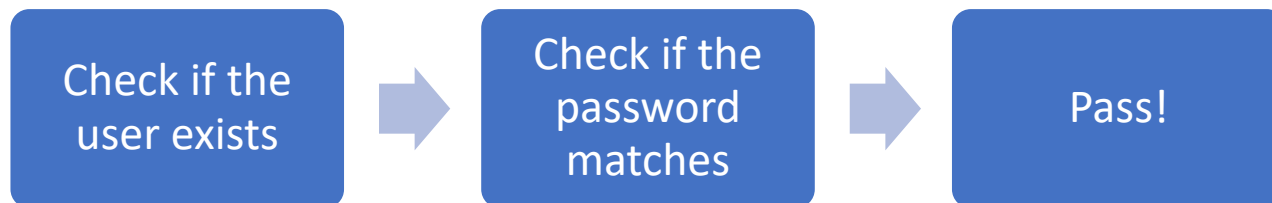
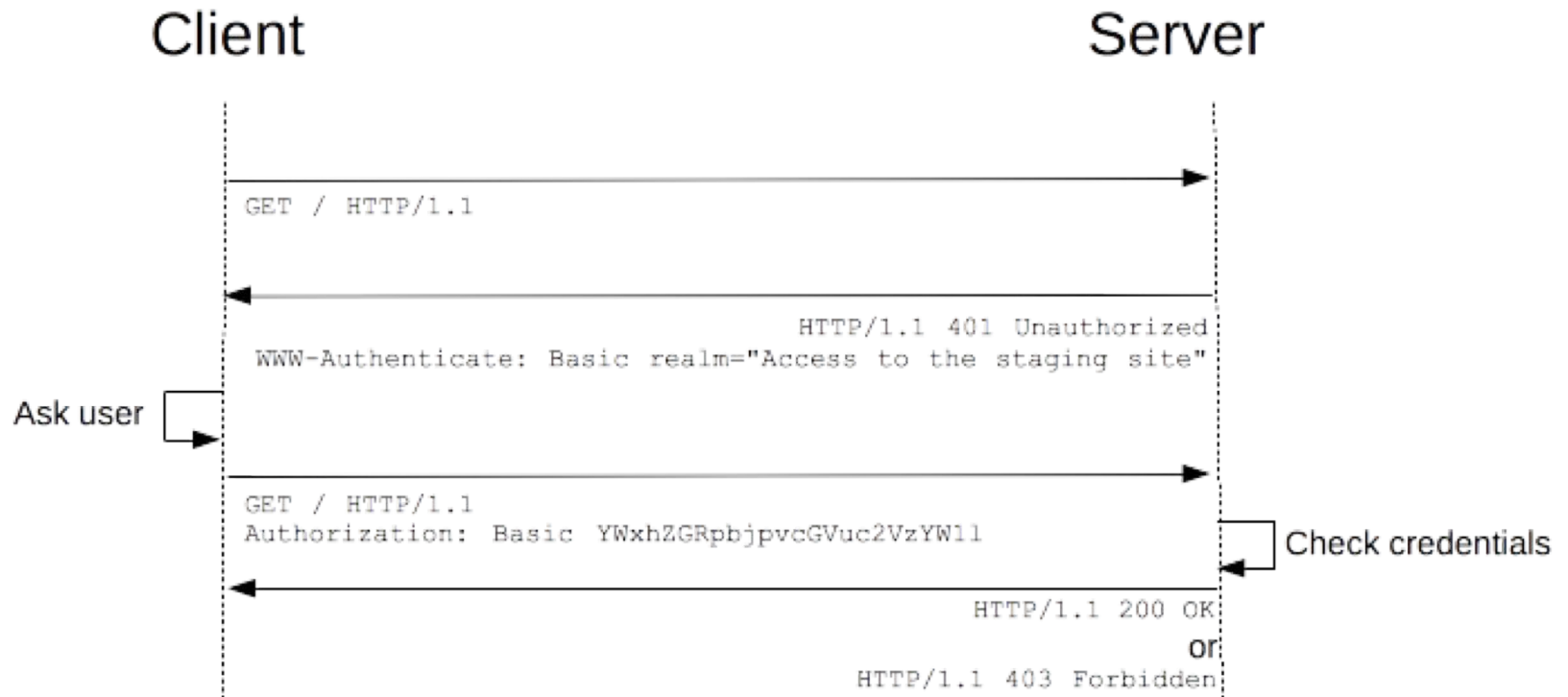
What if

I want to protect a website?

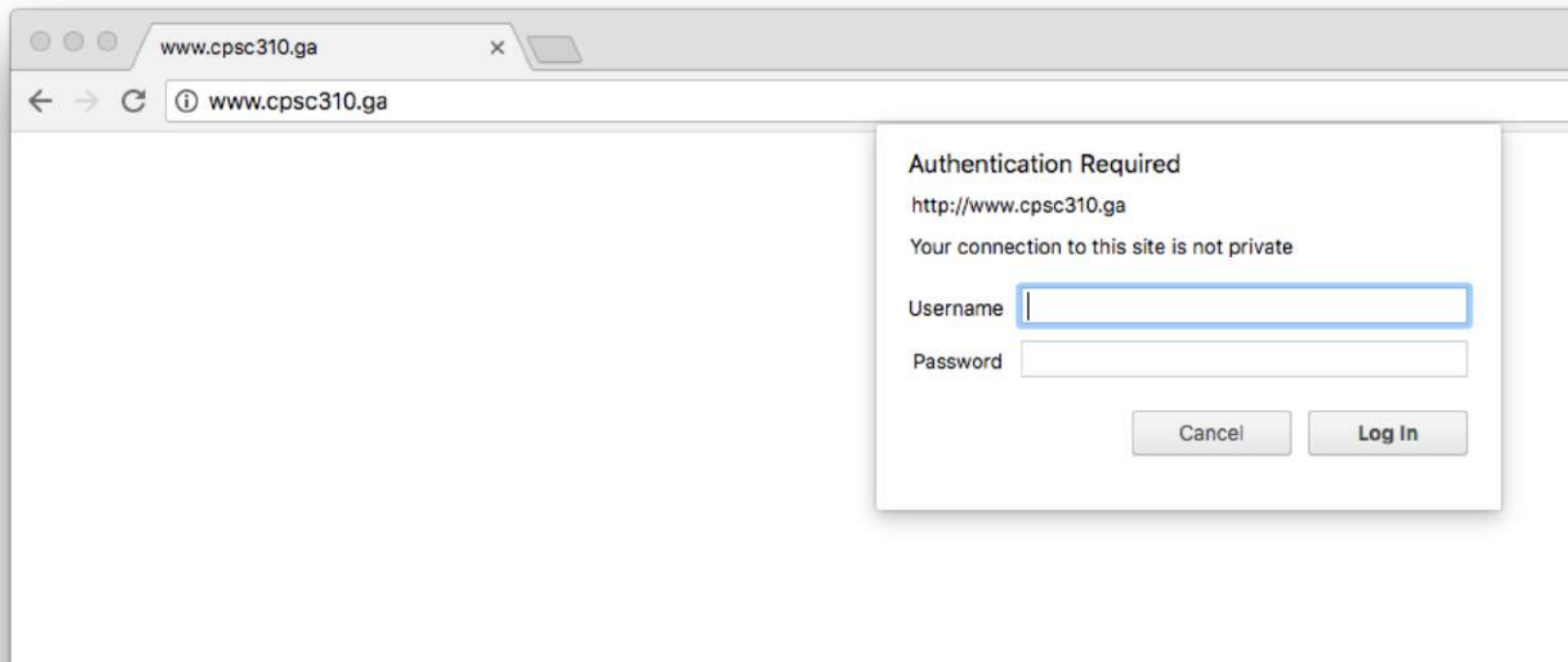
HTTP Basic Authentication



HTTP Basic Authentication



DEMO



DEMO

User: goodguy

Pass: letmein

```
GET / HTTP/1.1
Host: www.cpsc310.ga
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic Z29vZGd1eTpsZXRtZWlu
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_
Accept: text/html,application/xhtml+xml,application/xml;
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
```

Welcome
Please Come In

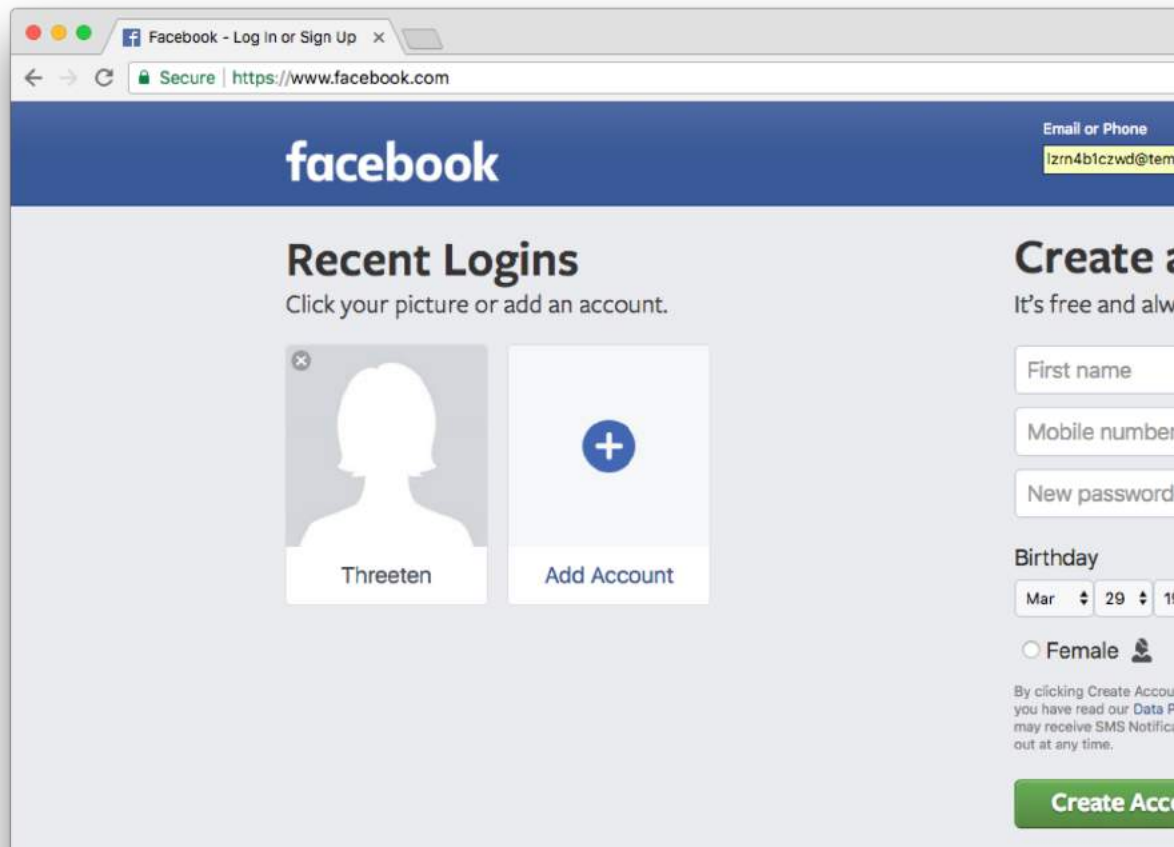


HTTP Basic Authentication

- Essentially, the user name and password are sent in HTTP request.
- the user name and password are sent for every request.
- No log out button

DEMO

Similarly...



Cookies

A small piece of information stored in the browser



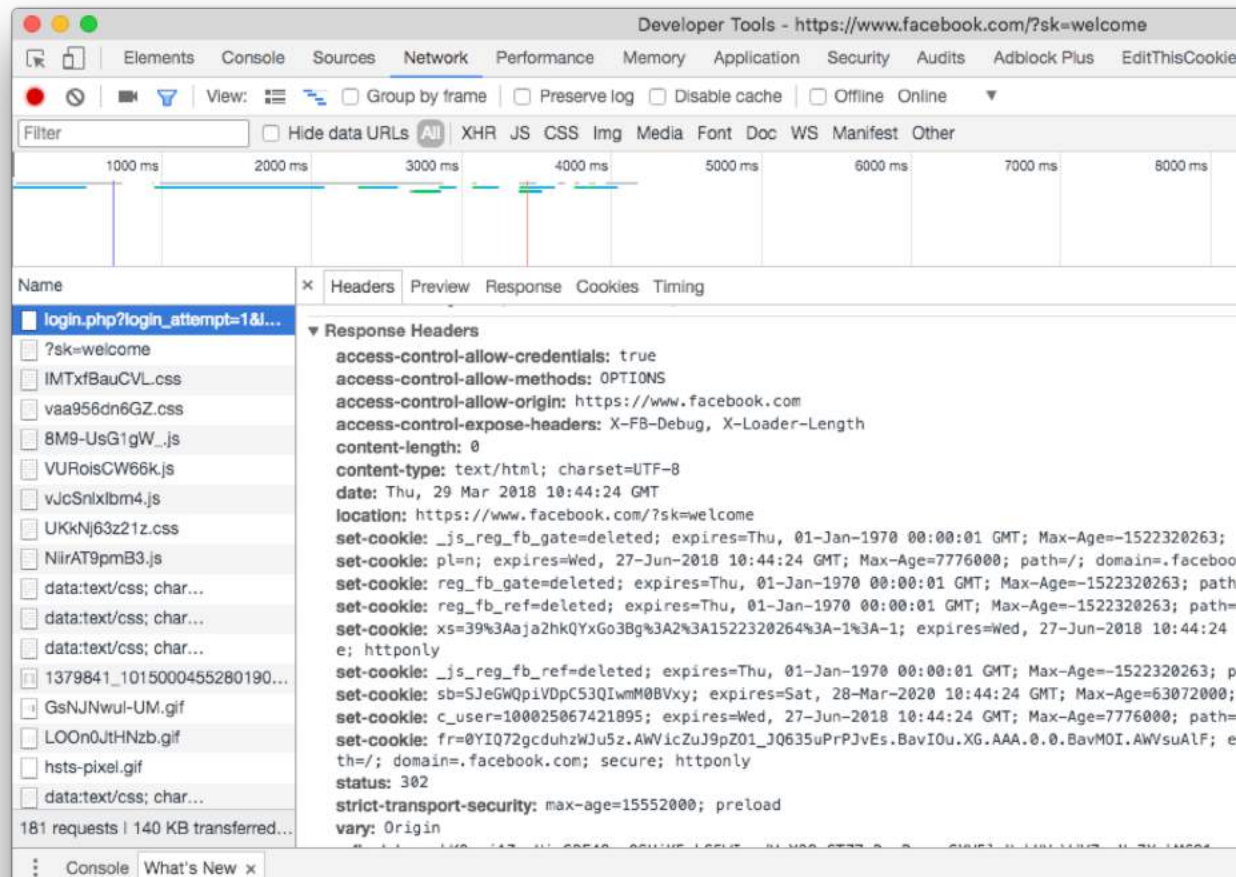
Cookies

- Small text file that contains a small amount of information
- Stored on the user's computer
- Accessed only by the site created them
- Usually for
 - Preference
 - Remember user credentials
 - Store your shopping cart!
 - ...

Cookies

- When you visit Facebook, the cookies are sent out for every request
- Facebook knows you are you via these cookies

DEMO



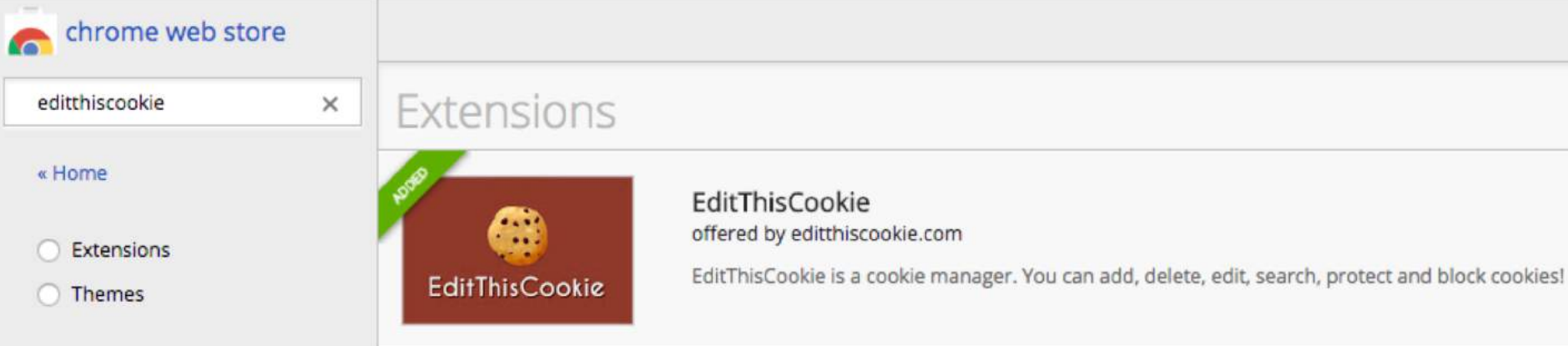
Steal your best friend's Facebook account

Demo

- Pre-requisite
 - Your friend let you use his laptop
 - His/Her Facebook is logged in

Steal your best friend's Facebook account



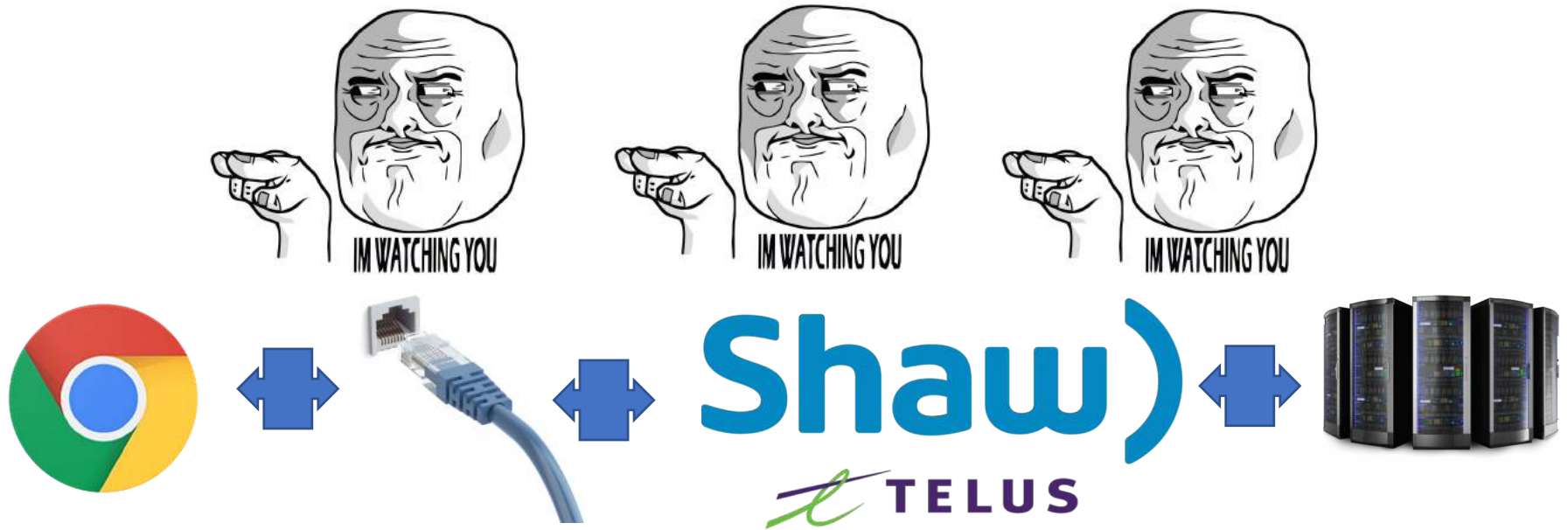


Steal your best friend's
Facebook account

HTTPS (HTTP Secure)

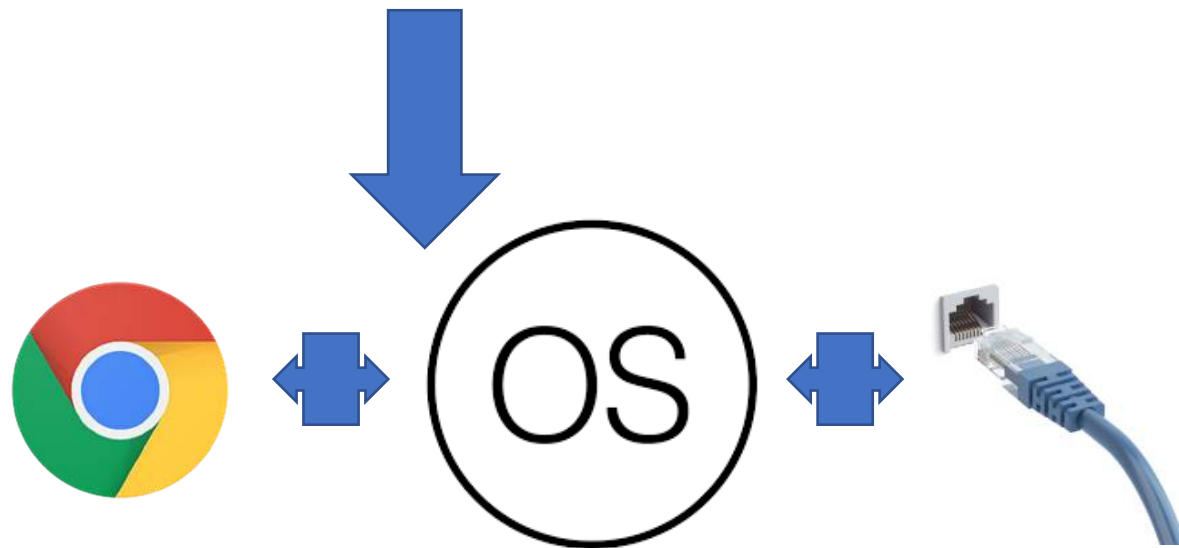
Previous DEMO



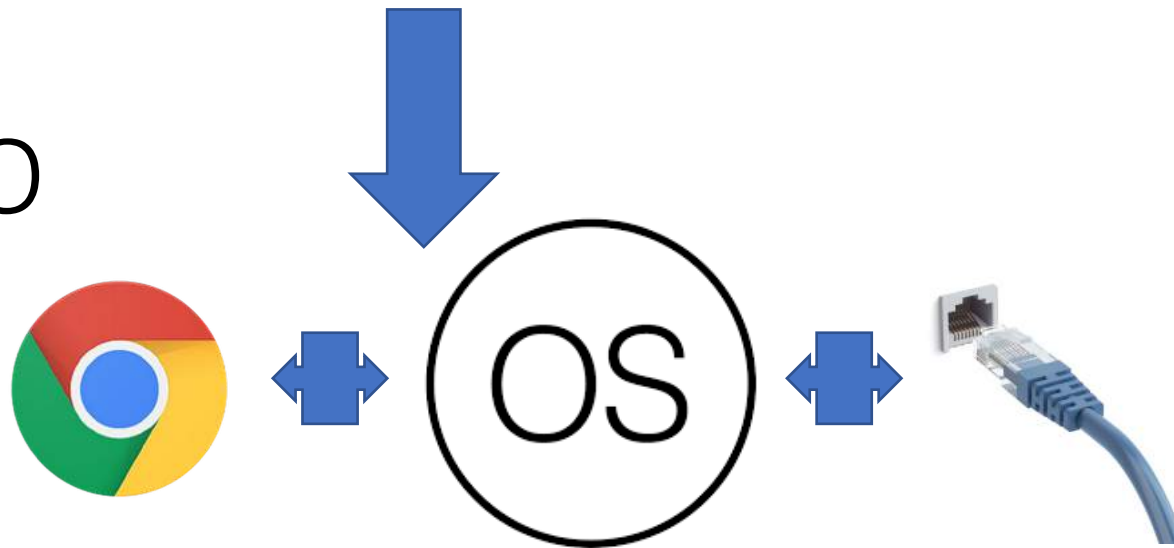


If you are visiting a HTTP site

DEMO



DEMO

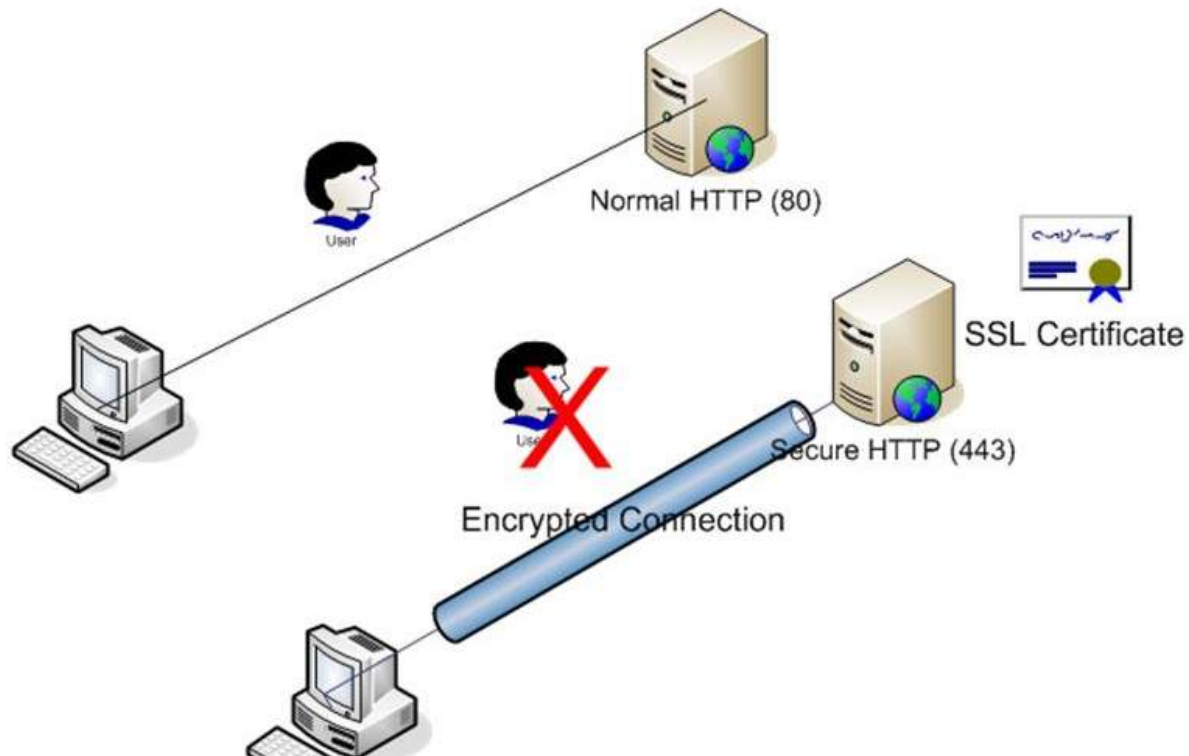


MAN-IN-THE-MIDDLE ATTACK



HTTPS

HTTP vs HTTPS



Message encrypted by the public key can only be decrypted by the private key

Public Key

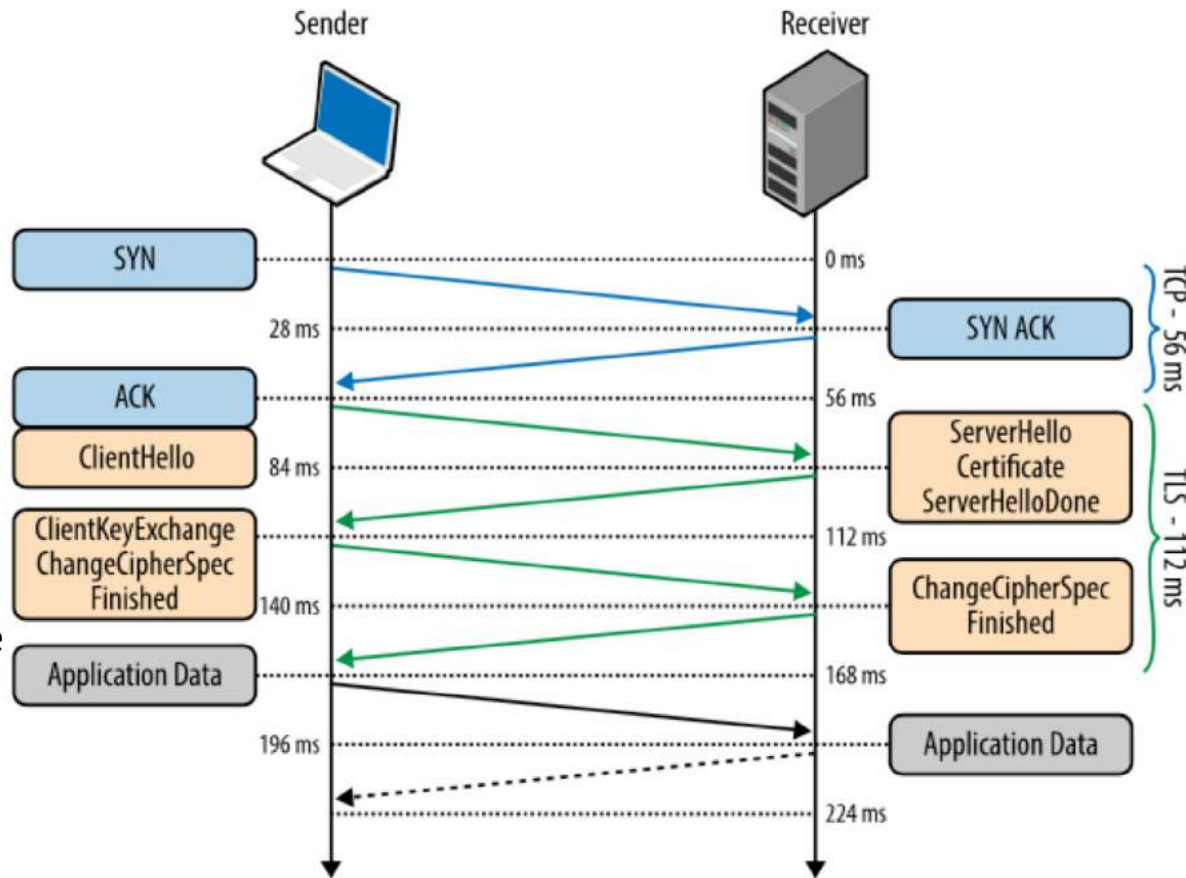
Private Key



HTTPS

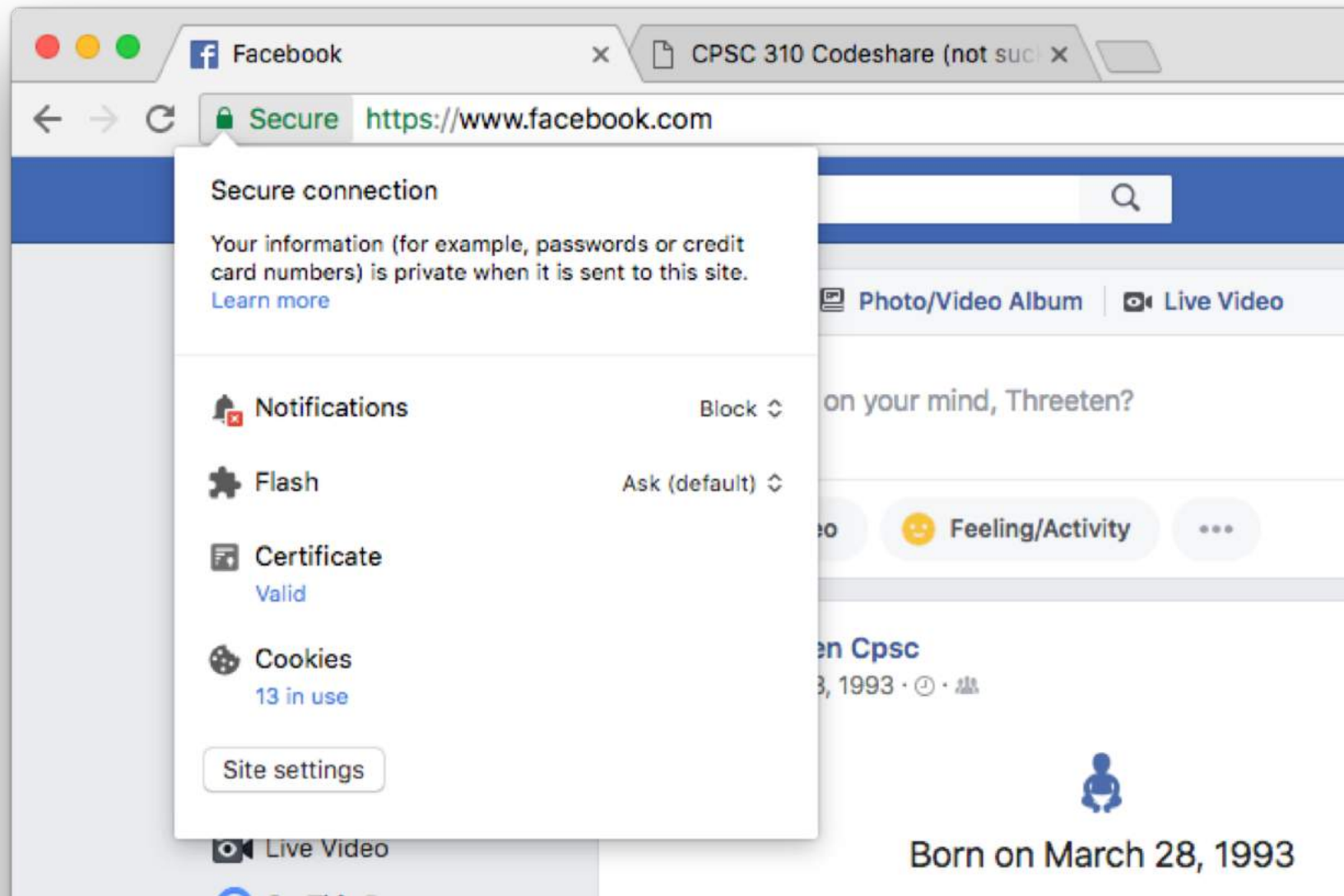


This key will be
used to encrypt the
application data

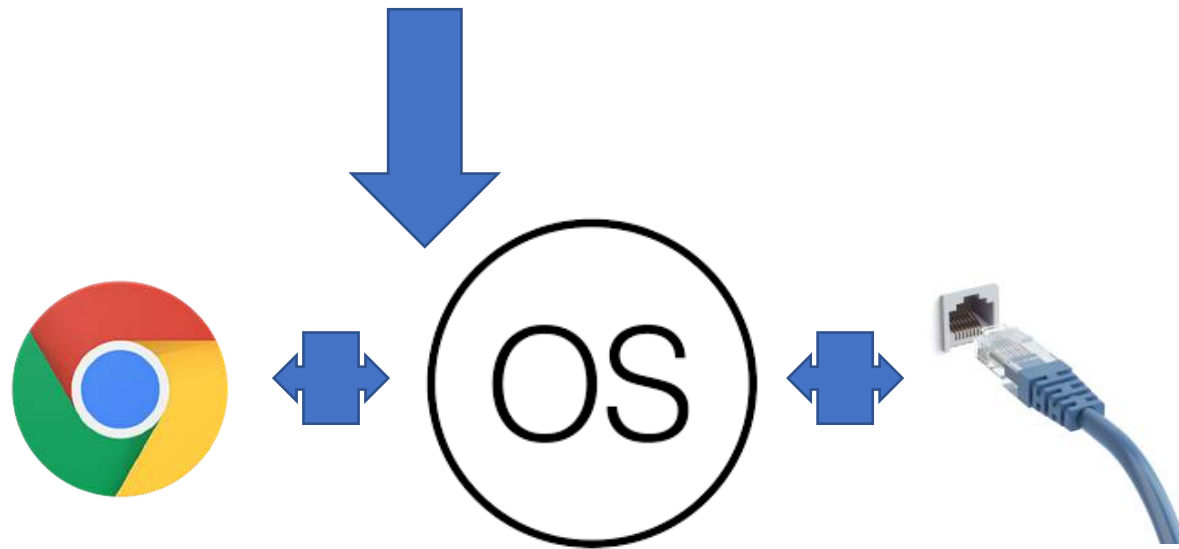


Now only we two can see the content

HTTPS




Try again for HTTPS



Man-in-the-middle attack


HTTPS Costs



[All](#) [News](#) [Shopping](#) [Videos](#) [Images](#) [More](#) [Settings](#) [Tools](#)

About 3,910,000 results (0.42 seconds)

\$5.99 SSL Certificates | Buy Now & Get 1st Month Free

 marketing.networksolutions.com/SSL ▼

Secure Your Website & Boost SEO Ranking. Buy Now & Get Your First Month Free!
Services: Domain Names, Website Hosting, Private Registration, SSL Certificates


Search for Domain Names

Find Your Perfect Domain Name!
Search Available Domains Now

Premium Domains

Search Premium Domains, Bid Expired
Domains & Place Certified Offers

\$1/month GoDaddy SSL | Secure Your Site With GoDaddy

 ca.godaddy.com/SSL_Certificate ▼

Get the Strongest Encryption on the Market & Help Make Your Customers Feel Safe.
2048-bit Encryption · Unlimited Server Coverage · Issued in Minutes
[\\$0.99 Hosting+Free Domain](#) · [\\$0.99 .com Sale](#) · [\\$0.99 .ca Domain Sale](#) · [Site Builder Free Trial](#)
[Website Builder](#) - \$0.00 - [Start A Free Trial Today](#) · [More](#) ▼



Let's Encrypt



<https://www.yourdomain.com>

2016

DEMO



Email or Phone Password

lzn4b1czwd@temp.mailb |.....

Log In

Forgot account?

Happy?

Secure <https://www.facebook.com/?stype=>

Secure connection

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
[Learn more](#)

Notifications Block ↕

Flash Ask (default) ↕

Certificate Valid

Cookies 17 in use

Site settings

Email or Phone Password

lzn4b1czwd@temp.mailb |.....

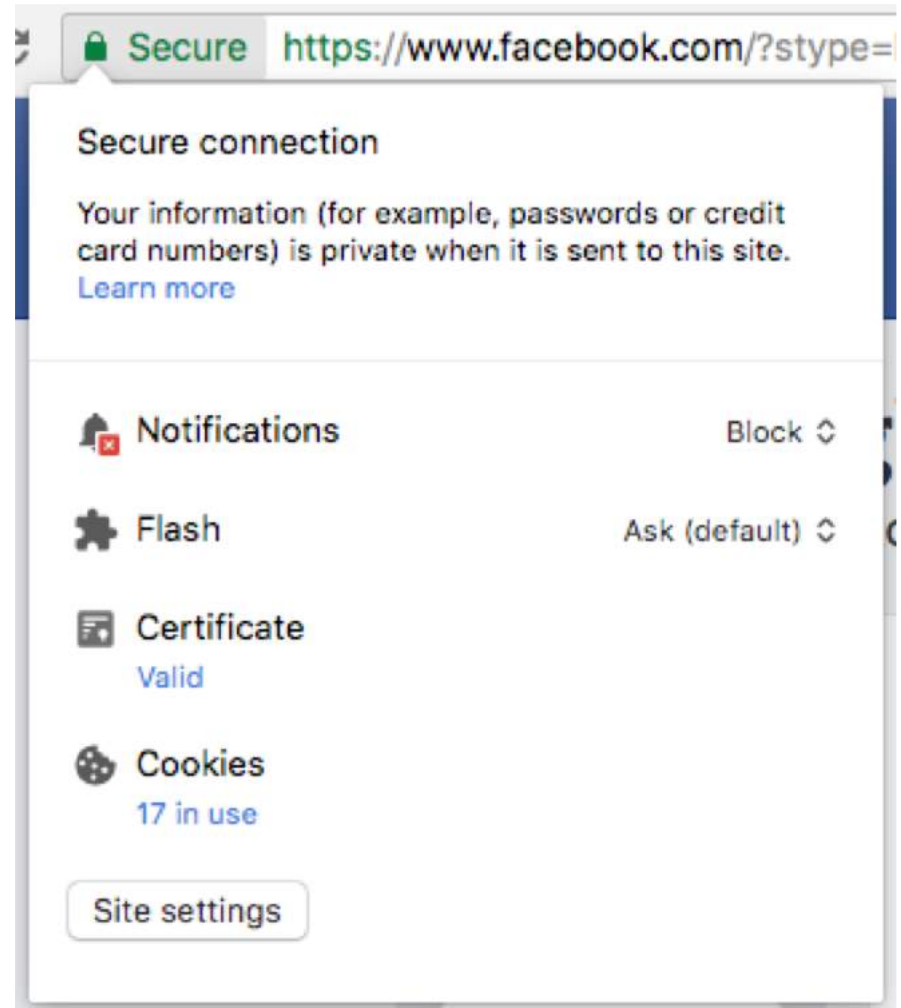
Log In

[Forgot account?](#)

Happy?

Too many passwords!

For many website,
they just want to verify your email




OAUTH


OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.





OAUTH

The image shows a user registration interface. On the left, there are four buttons for social login: 'CONNECT WITH FACEBOOK' (dark blue), 'CONNECT WITH TWITTER' (light blue), 'CONNECT WITH GOOGLE' (red), and 'CONNECT WITH EMAIL' (dark grey). Each button contains a corresponding icon. In the center, the word 'OR' is displayed between two vertical lines. On the right, under the heading 'CREATE NEW ACCOUNT:', there are three input fields labeled 'NAME', 'EMAIL', and 'PASSWORD'. Below these fields is a large blue button labeled 'CREATE ACCOUNT'.

 CONNECT WITH FACEBOOK

 CONNECT WITH TWITTER

 CONNECT WITH GOOGLE

 CONNECT WITH EMAIL

OR

CREATE NEW ACCOUNT:

CREATE ACCOUNT

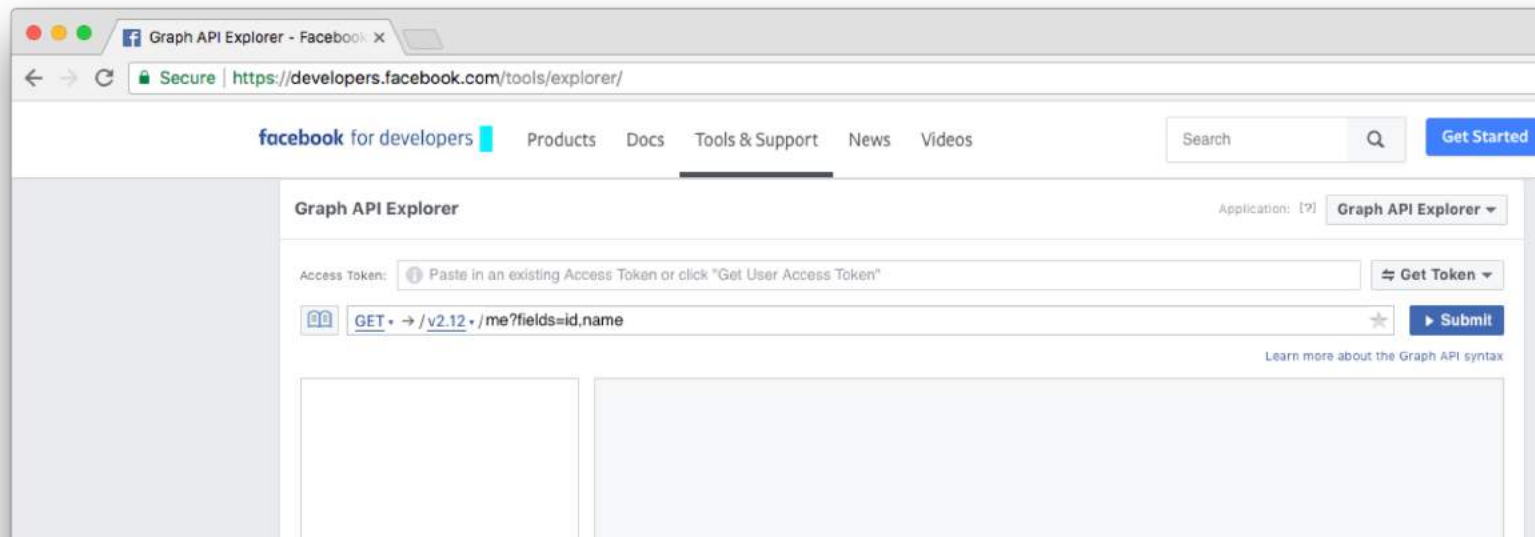
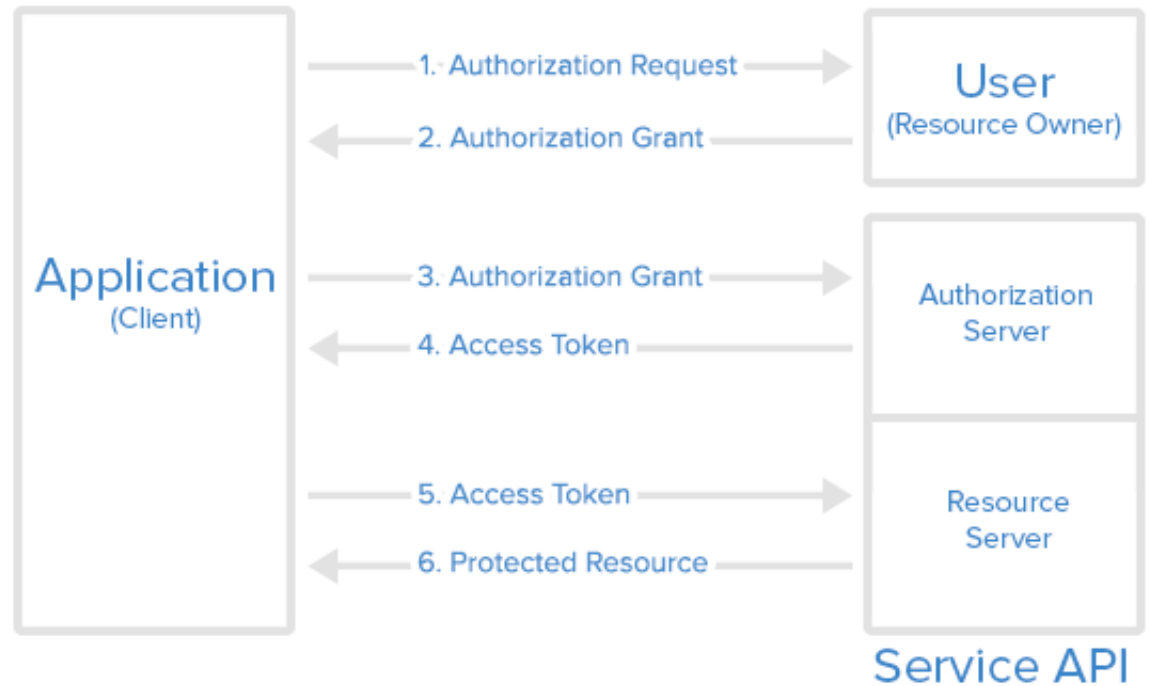
OAUTH – How it works

Abstract Protocol Flow

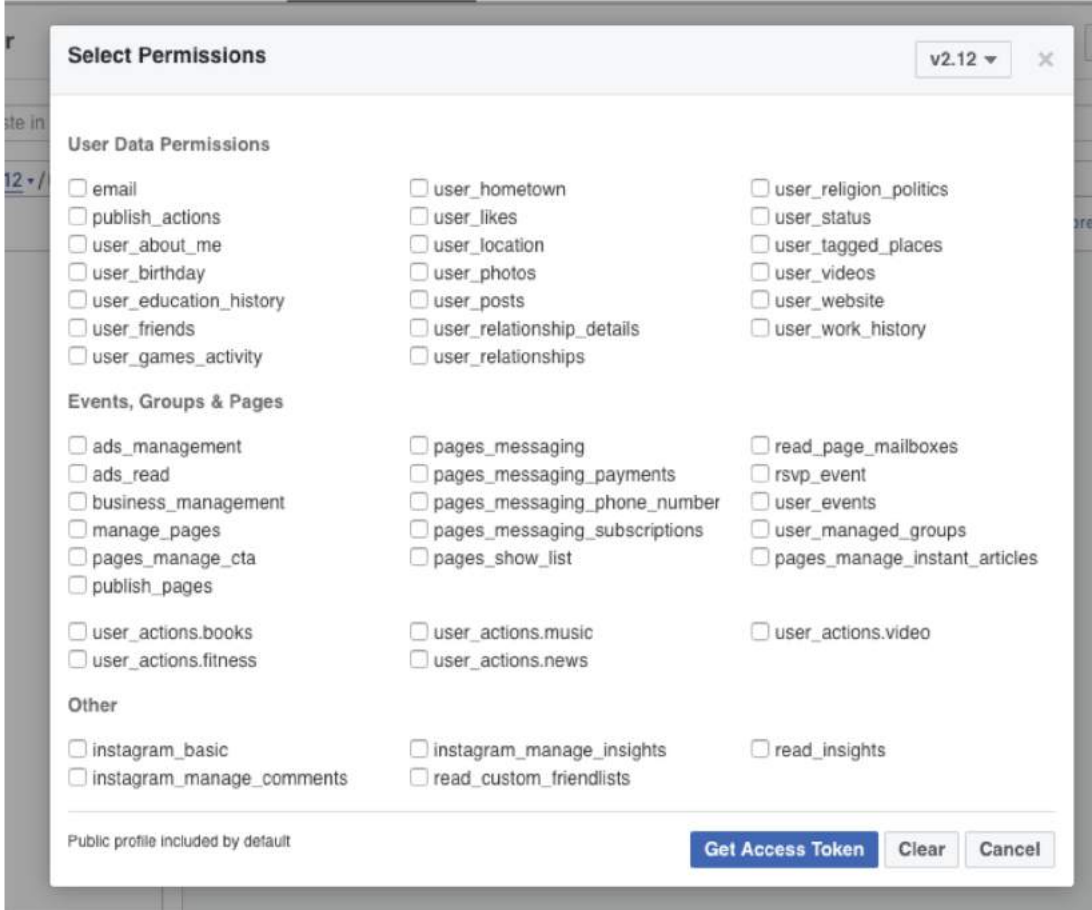


DEMO

Abstract Protocol Flow



OAUTH – Token Permissions



The screenshot shows a 'Select Permissions' dialog box with a title bar containing 'v2.12' and a close button. The dialog is organized into four sections, each with a list of permissions represented by checkboxes:

- User Data Permissions:**
 - ☐ email
 - ☐ publish_actions
 - ☐ user_about_me
 - ☐ user_birthday
 - ☐ user_education_history
 - ☐ user_friends
 - ☐ user_games_activity
 - ☐ user_hometown
 - ☐ user_likes
 - ☐ user_location
 - ☐ user_photos
 - ☐ user_posts
 - ☐ user_relationship_details
 - ☐ user_relationships
 - ☐ user_religion_politics
 - ☐ user_status
 - ☐ user_tagged_places
 - ☐ user_videos
 - ☐ user_website
 - ☐ user_work_history
- Events, Groups & Pages:**
 - ☐ ads_management
 - ☐ ads_read
 - ☐ business_management
 - ☐ manage_pages
 - ☐ pages_manage_cta
 - ☐ publish_pages
 - ☐ pages_messaging
 - ☐ pages_messaging_payments
 - ☐ pages_messaging_phone_number
 - ☐ pages_messaging_subscriptions
 - ☐ pages_show_list
 - ☐ read_page_mailboxes
 - ☐ rsvp_event
 - ☐ user_events
 - ☐ user_managed_groups
 - ☐ pages_manage_instant_articles
- Other:**
 - ☐ user_actions.books
 - ☐ user_actions.fitness
 - ☐ user_actions.music
 - ☐ user_actions.news
 - ☐ user_actions.video
 - ☐ instagram_basic
 - ☐ instagram_manage_comments
 - ☐ instagram_manage_insights
 - ☐ read_custom_friendlists
 - ☐ read_insights

At the bottom left, it says 'Public profile included by default'. At the bottom right, there are three buttons: 'Get Access Token' (highlighted in blue), 'Clear', and 'Cancel'.

Least privilege

Wrap-up

- HTTP and HTTPS
- Basic authentication
- Cookies
- OAUTH & Permissions

How to Reduce the Risk?

Use strong passwords (7tky2e_Kj6DK_ImYHmX)

Use different passwords for different services

Watch out for HTTP

Don't click weird links

Don't lend your laptop to others

Update your operating system

...