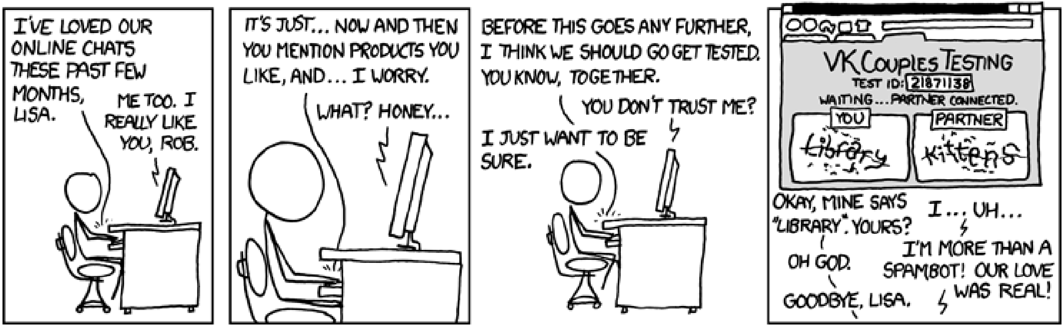
HTML2PostGIS
Safety and Security

Michał Okulewicz

Wydział Matematyki i Nauk Informacyjnych
Politechnika Warszawska

Safety (rope) and security (bulletproof vest)

You never know who is on the other side...


I'VE LOVED OUR ONLINE CHATS THESE PAST FEW MONTHS, LISA.
ME TOO. I REALLY LIKE YOU, ROB.
IT'S JUST... NOW AND THEN YOU MENTION PRODUCTS YOU LIKE, AND... I WORRY.
WHAT? HONEY...
BEFORE THIS GOES ANY FURTHER, I THINK WE SHOULD GO GET TESTED. YOU KNOW, TOGETHER.
YOU DON'T TRUST ME?
I JUST WANT TO BE SURE.
VK Couples Testing
TEST ID: 21871138
WAITING... PARTNER CONNECTED.
YOU
PARTNER
library
kittens
OKAY, MINE SAYS "LIBRARY". YOURS?
I... UH...
OH GOD.
I'M MORE THAN A SPAMBOT! OUR LOVE WAS REAL!
GOODBYE, LISA.

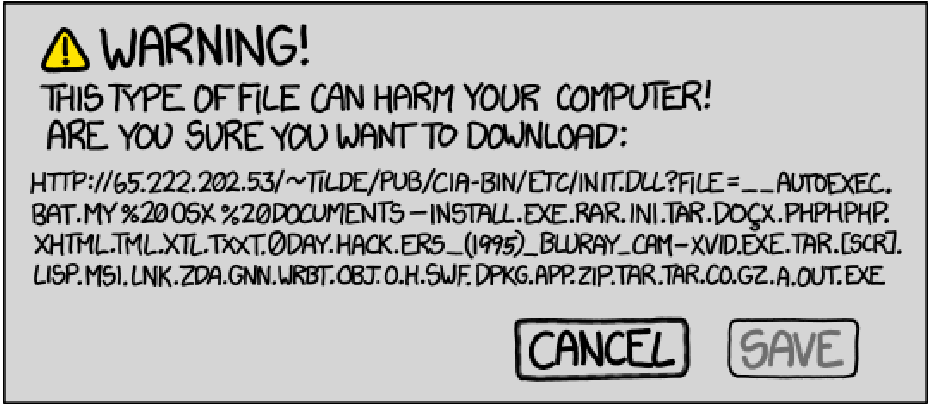
Fine, walk away. I'm gonna go cry into a pint of Ben&Jerry's Brownie Batter™ ice cream, then take out my frustration on a variety of great flash games from PopCap Games®.

http://xkcd.com/632

1. Trustworthy websites
   - SSL/TLS
   - Certificates
   - Trusting a source
2. Secured websites
   - Authorization and authentication
   - OAuth2
3. Course summary

Part 1: Trustworthy websites

Is the connection secure?


WARNING!
THIS TYPE OF FILE CAN HARM YOUR COMPUTER!
ARE YOU SURE YOU WANT TO DOWNLOAD:
HTTP://65.222.202.53/~TILDE/PUB/CIA-BIN/ETC/INIT.DLL?FILE=__AUTOEXEC.
BAT.MY%20OSX%20DOCUMENTS—INSTALL.EXE.RAR.INI.TAR.DOCX.PHPHPHP.
XHTML.TML.XTL.TXXT.0DAY.HACK.ERS_(1995)_BLURAY_CAM-XVID.EXE.TAR.[SCR].
LISP.MSI.LNK.ZDA.GNN.WRBT.OBJ.O.H.SWF.DPKG.APP.ZIP.TAR.TAR.CO.GZ.A.OUT.EXE
CANCEL
SAVE

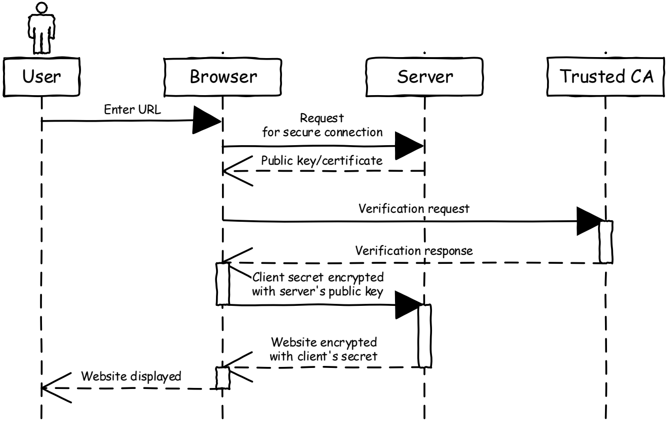
Better change the URL to **'https'** before downloading.

http://xkcd.com/1247

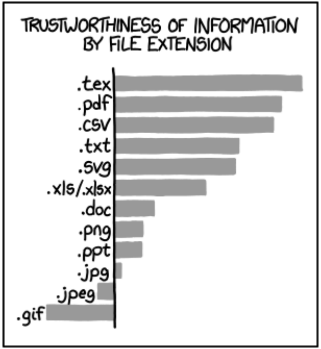
What is HTTPS protocol?

- It is an HTTP with additional SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocol providing an encryption to the connection
- It utilizes establishing a shared secret key through public key encryption – private key decryption scheme
- All you want to know about TLS 1.2 and TLS 1.3

Rough HTTPS depiction

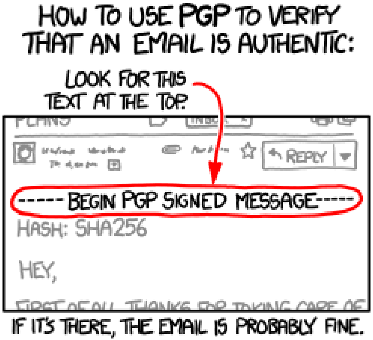


How can we trust a website?



I have never been lied to by data in a .txt file which has been hand-aligned.
http://xkcd.com/1301

How can we trust a website?


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP:
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
FIRST OF ALL, THANKS FOR TAKING CARE OF
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

If you want to be extra safe, check that there's a big block of jumbled characters at the bottom.

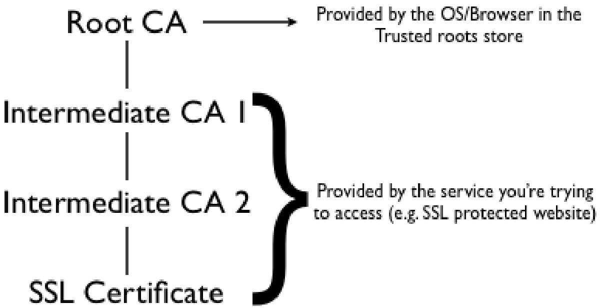
http://xkcd.com/1181

How do we know they are not lying?

HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

Never bring tequila to a key-signing party.
http://xkcd.com/364

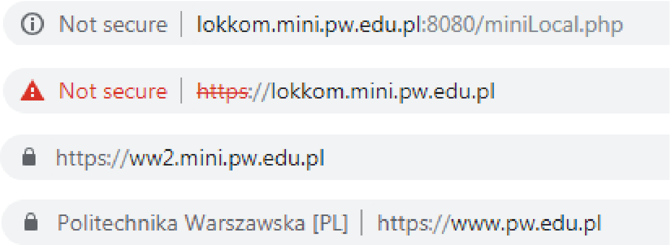
Certificate trust hierarchy


Root CA
Provided by the OS/Browser in the Trusted roots store
Intermediate CA 1
Intermediate CA 2
SSL Certificate
Provided by the service you're trying to access (e.g. SSL protected website)

source: http://redelijkheid.squarespace.com/blog/2009/7/16/citrix-ica-client-ssl-error-61.html

Levels of certificate trust

- No certificate
- Self-signed certificate (SS)
- Domain Validation (DV) - domain ownership validated
- Organization Validation (OV) - company ownership validated
- Extended Validation (EV) - business legitimacy validated



ⓘ Not secure | lokkom.mini.pw.edu.pl:8080/miniLocal.php

⚠ Not secure | ~~https~~://lokkom.mini.pw.edu.pl

🔒 https://ww2.mini.pw.edu.pl

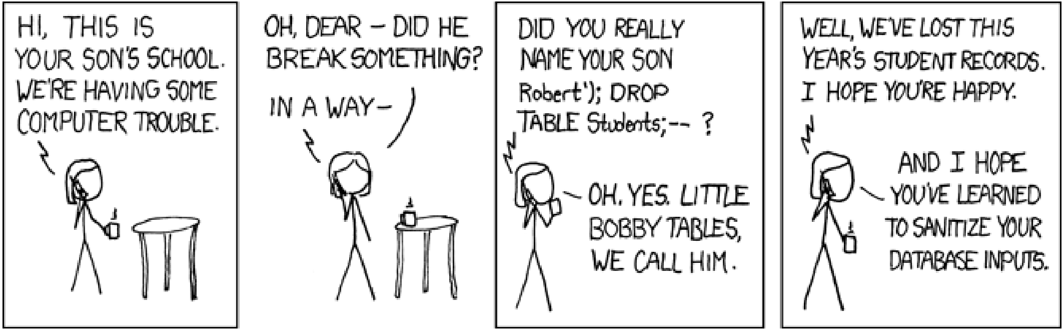
🔒 Politechnika Warszawska [PL] | https://www.pw.edu.pl

Handling and creating self-signed certificates

- Using SSL in .NET Core applications
- StackOverflow: creating self-signed certificate
- Adding self-signed .NET Core certificates for applications in development stage
- Trust'em all! (please don't. . .)
- StackOverflow: adding a new certificate in Java

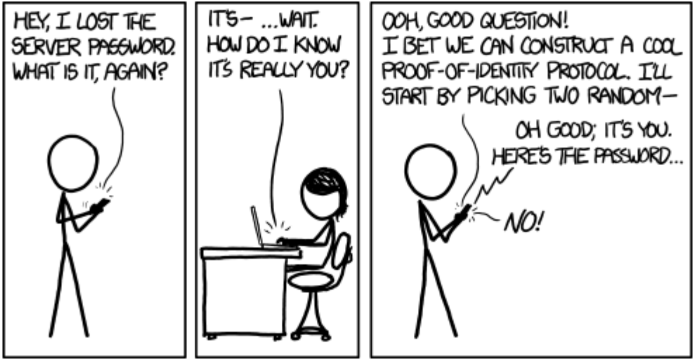
Part 2: Secured websites

How to protect us from malicious users?


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY –
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Her daughter is named Help I'm trapped in a driver's license factory.
http://xkcd.com/327

How to establish users identity?


HEY, I LOST THE SERVER PASSWORD. WHAT IS IT, AGAIN?
IT'S– ...WAIT. HOW DO I KNOW IT'S REALLY YOU?
OOH, GOOD QUESTION! I BET WE CAN CONSTRUCT A COOL PROOF-OF-IDENTITY PROTOCOL. I'LL START BY PICKING TWO RANDOM–
OH GOOD; IT'S YOU. HERE'S THE PASSWORD...
NO!

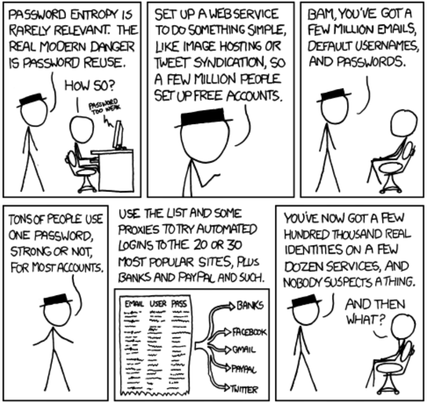
Not sure why I just taught everyone to flawlessly impersonate me to pretty much anyone I know. Just remember to constantly bring up how cool it is that birds are dinosaurs and you'll be set.

http://xkcd.com/1121

Typical cases of establishing users identity

- User–password pair
- Hardware tokens
- Security questions (who are those people? what is your mother’s maiden name?)
- One-time password (OTP) (e.g. delivered by SMS)

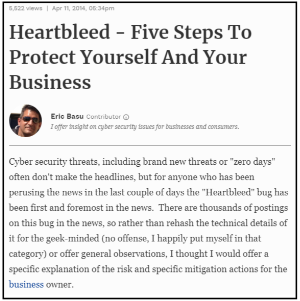
Can we be really secure?


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.
TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.
USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.
EMAIL USER PASS
BANKS
FACEBOOK
GMAIL
PAYPAL
TWITTER
YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.
AND THEN WHAT?

...

http://xkcd.com/792

Can we be really secure?



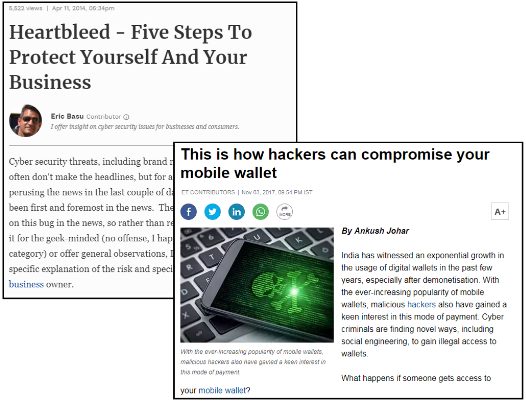
5,522 views | Apr 11, 2014, 05:34pm

Heartbleed - Five Steps To Protect Yourself And Your Business

Eric Basu Contributor ⓘ
I offer insight on cyber security issues for businesses and consumers.

Cyber security threats, including brand new threats or "zero days" often don't make the headlines, but for anyone who has been perusing the news in the last couple of days the "Heartbleed" bug has been first and foremost in the news. There are thousands of postings on this bug in the news, so rather than rehash the technical details of it for the geek-minded (no offense, I happily put myself in that category) or offer general observations, I thought I would offer a specific explanation of the risk and specific mitigation actions for the business owner.

Can we be really secure?



5,522 views | Apr 11, 2014, 05:34pm

Heartbleed - Five Steps To Protect Yourself And Your Business

Eric Basu Contributor ⓘ
I offer insight on cyber security issues for businesses and consumers.

Cyber security threats, including brand r
often don't make the headlines, but for a
perusing the news in the last couple of da
been first and foremost in the news. The
on this bug in the news, so rather than re
it for the geek-minded (no offense, I hap
category) or offer general observations, I
specific explanation of the risk and speci
business owner.

This is how hackers can compromise your mobile wallet

ET CONTRIBUTORS | Nov 03, 2017, 09.54 PM IST

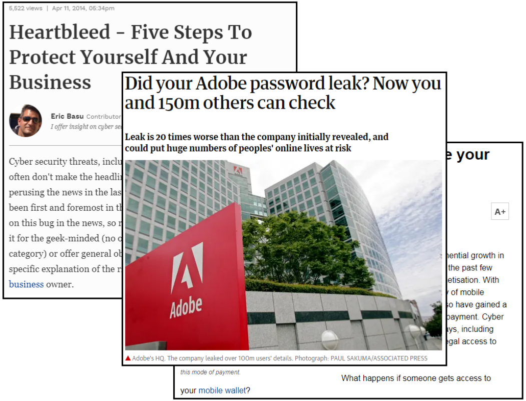
By Ankush Johar

India has witnessed an exponential growth in the usage of digital wallets in the past few years, especially after demonetisation. With the ever-increasing popularity of mobile wallets, malicious hackers also have gained a keen interest in this mode of payment. Cyber criminals are finding novel ways, including social engineering, to gain illegal access to wallets.

With the ever-increasing popularity of mobile wallets, malicious hackers also have gained a keen interest in this mode of payment.

What happens if someone gets access to your mobile wallet?

Can we be really secure?



5,522 views | Apr 11, 2014, 05:34pm

Heartbleed – Five Steps To Protect Yourself And Your Business

Eric Basu Contributor
I offer insight on cyber se

Cyber security threats, inclu
often don't make the headli
perusing the news in the las
been first and foremost in th
on this bug in the news, so r
it for the geek-minded (no c
category) or offer general ob
specific explanation of the r
business owner.

Did your Adobe password leak? Now you and 150m others can check

Leak is 20 times worse than the company initially revealed, and could put huge numbers of peoples' online lives at risk

▲ Adobe's HQ. The company leaked over 100m users' details. Photograph: PAUL SAKUMA/ASSOCIATED PRESS

e your

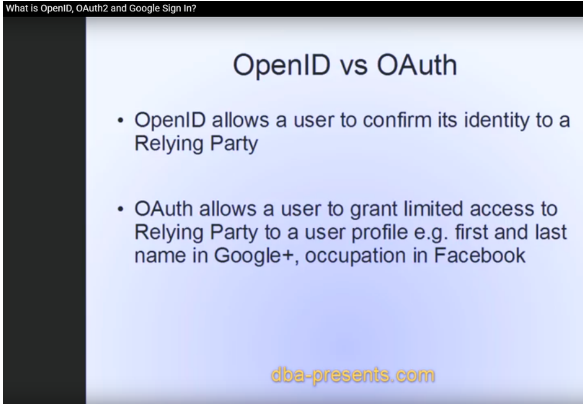
A+

nential growth in
the past few
etisation. With
of mobile
so have gained a
payment. Cyber
ys, including
egal access to

this mode of payment.

What happens if someone gets access to your mobile wallet?

Utilizing 3rd party websites: OpenID and OAuth2



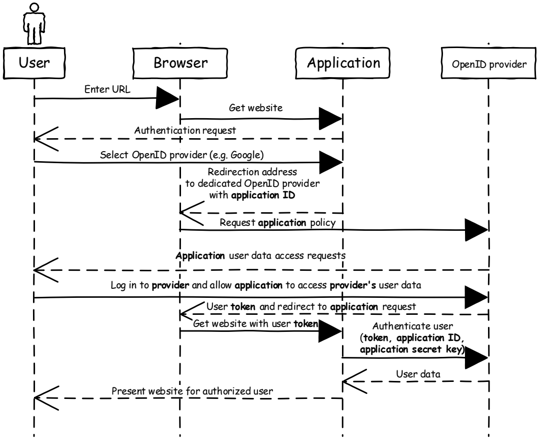
What is OpenID, OAuth2 and Google Sign In?

OpenID vs OAuth

- OpenID allows a user to confirm its identity to a Relying Party
- OAuth allows a user to grant limited access to Relying Party to a user profile e.g. first and last name in Google+, occupation in Facebook

dba-presents.com

Rough protocol's depiction



User

Browser

Application

OpenID provider

Enter URL

Get website

Authentication request

Select OpenID provider (e.g. Google)

Redirection address
to dedicated OpenID provider
with **application ID**

Request **application** policy

Application user data access requests

Log in to **provider** and allow **application** to access **provider's** user data

User **token** and redirect to **application** request

Get website with user **token**

Authenticate user
(**token**, **application ID**,
application secret key)

User data

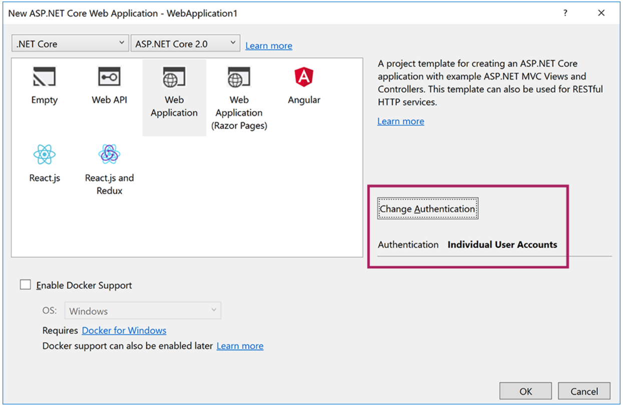
Present website for authorized user

OAuth2 example tutorials

Notes to self:

- `dotnet dev-certs https --trust`
- Creating ASP .NET Core application
  - `app.UseHsts();`
  - `app.UseHttpsRedirection();`
- Google authentication
  - remember to enable Google Plus API access in order to log in
- Tutorial on user (application) secrets
- Custom providers

An MVC ASP .NET Core application



New ASP.NET Core Web Application - WebApplication1

.NET Core

ASP.NET Core 2.0

A project template for creating an ASP.NET Core application with example ASP.NET MVC Views and Controllers. This template can also be used for RESTful HTTP services.

Authentication **Individual User Accounts**

□ Enable Docker Support

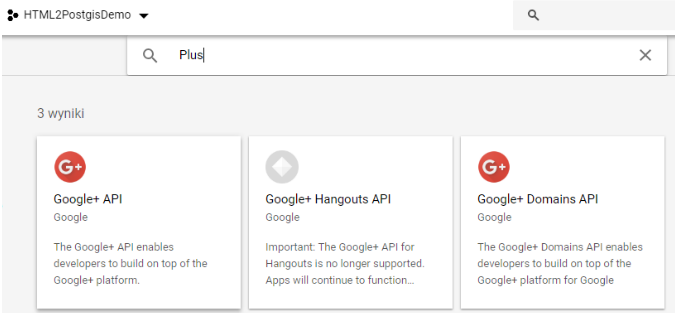
OS: Windows

Requires Docker for Windows

Docker support can also be enabled later Learn more

Source: Microsoft

OpenID provider configuration and utilization



HTML2PostgisDemo

Plus

3 wyniki

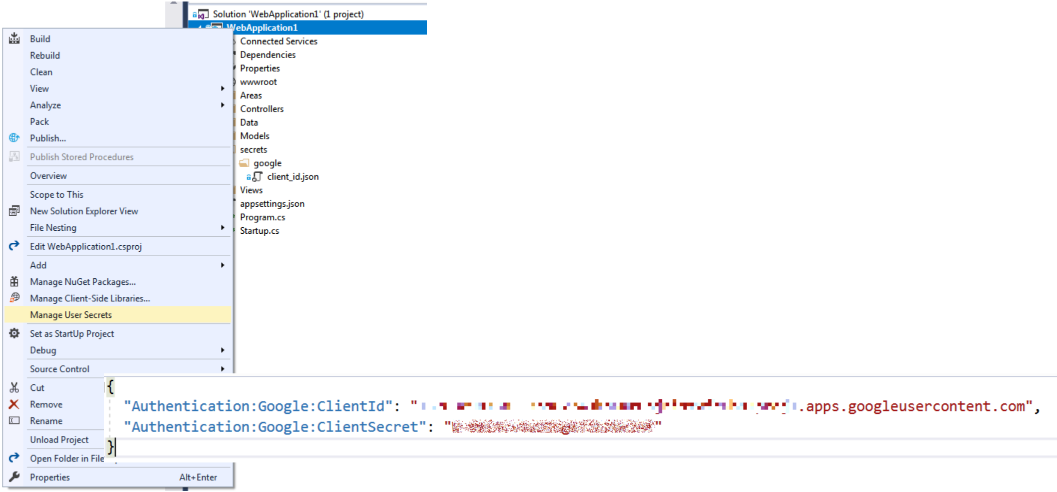
Google+ API
Google
The Google+ API enables developers to build on top of the Google+ platform.

Google+ Hangouts API
Google
Important: The Google+ API for Hangouts is no longer supported. Apps will continue to function...

Google+ Domains API
Google
The Google+ Domains API enables developers to build on top of the Google+ platform for Google

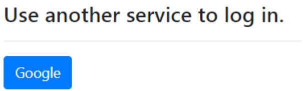
```
services.AddAuthentication().AddGoogle(googleOptions =>
{
    googleOptions.ClientId = Configuration["Authentication:Google:ClientId"];
    googleOptions.ClientSecret = Configuration["Authentication:Google:ClientSecret"];
});
```

Secret manager



```
{
  "Authentication:Google:ClientId": "[redacted].apps.googleusercontent.com",
  "Authentication:Google:ClientSecret": "[redacted]"
}
```

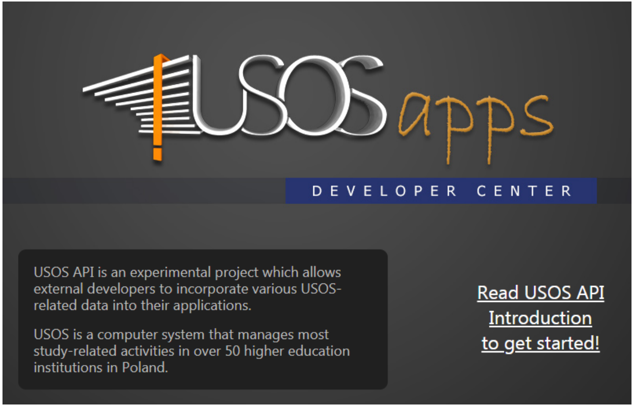
End result



Use another service to log in.

- https://accounts.google.com/o/oauth2/v2/auth?response_type=code&client_id=137...&redirect_uri=https://localhost:44371/signin-google&scope=openid+profile+email&...
- https://accounts.google.com/signin/oauth?client_id=137...&as=...&destination=https://localhost:44371&...
- https://localhost:44371/signin-google?state=...&code=...&scope=openid+email+profile+https://www.googleapis.com/auth/plus.mehttps://www.googleapis.com/auth/userinfo.email+https://www.googleapis.com/auth/userinfo.profile&authuser=0&session_state=...&prompt=none

What about USOS?

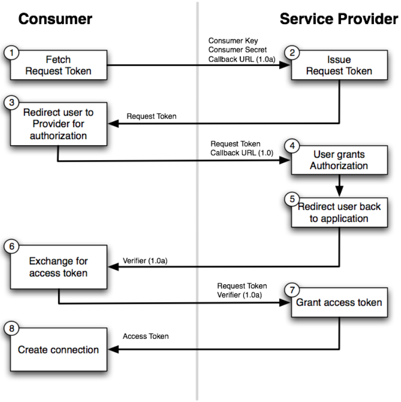


USOS API is an experimental project which allows external developers to incorporate various USOS-related data into their applications.

USOS is a computer system that manages most study-related activities in over 50 higher education institutions in Poland.

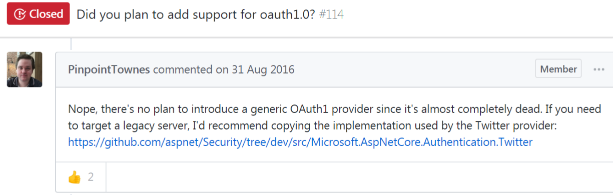
Read USOS API Introduction to get started!

Uses OAuth1a...



Source: StackOverflow

...which becomes obsolete

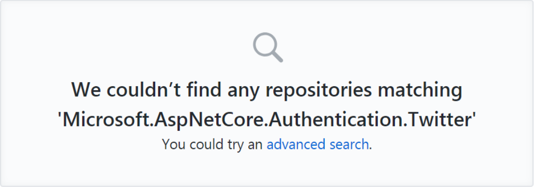


Closed Did you plan to add support for oauth1.0? #114

PinpointTownes commented on 31 Aug 2016 Member

Nope, there's no plan to introduce a generic OAuth1 provider since it's almost completely dead. If you need to target a legacy server, I'd recommend copying the implementation used by the Twitter provider: https://github.com/aspnet/Security/tree/dev/src/Microsoft.AspNetCore.Authentication.Twitter

👍 2



We couldn’t find any repositories matching 'Microsoft.AspNetCore.Authentication.Twitter'

You could try an advanced search.

Part 3: Course summary

- Web Development
  - HTML
  - CSS
  - JavaScript
  - HTTP Protocol
  - REST APIs
  - Web applications security
- Geographic Information Systems
  - Map projections
  - Web APIs
  - Data sources (government, commercial, community)
  - Map services and routing services
  - Spatial databases
  - GIS applications