**SEIS 752 March 17, 2015**

**# HW6-APIs**

**## PART1 –**

Using TWILLIO API – POST a message to your site.

- Use the discount code in the slide lectures for a $30 credit.

**## PART2 –**

**###OPTION 1:** Implement [one] Step by Step an OAuth Token exchange.

- https://developers.google.com/accounts/docs/OAuth2

- http://developer.linkedin.com/documents/authentication

- https://developers.facebook.com/docs/howtos/login/server-side-login/

AND Make at least 2 endpoint requests.

Display the results down a long page.

**###OPTION 2:** Choose, choose a public Web Service API {Twillio, Flickr, Amazon, YouTube, Google, etc } and write a page that will query the API and return results on your page.

- Parse XML, JSON or ?? Objects

- Recompile results into

- Image / Book Cover / Video Thumbnail

- Description

- Plus something else

- Tags

- GeoCode info

- Other?

- Parse and contain results on your application page.

**##Deliverable:**

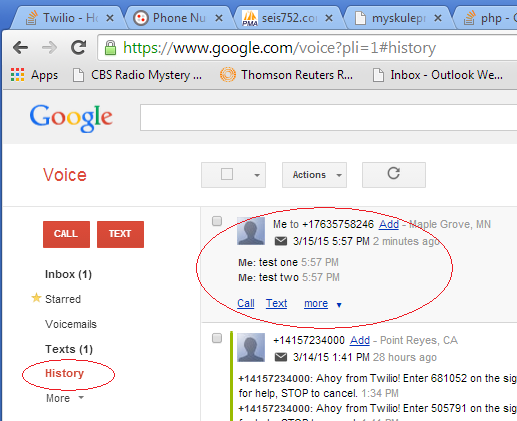
1. Fork this Repo, submit pull request to turn in

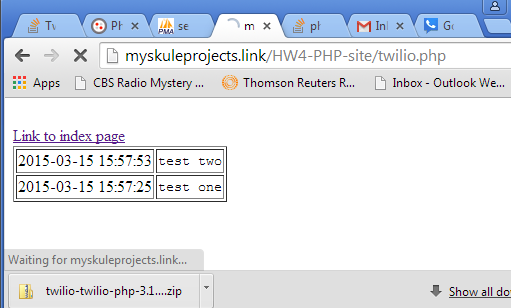
2. Include in the Repo a Description /Documentation of what you did.

***## PART1 –***  *Using TWILLIO API – POST a message to your site.*

I added the code from Hwk6 repo to my website. <http://myskuleprojects.link/HW4-PHP-site/index.php> has a link to my twilio page.

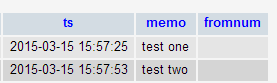
The next two screen shots show a couple texts being sent from Google voice and my twilio page in receiving them.



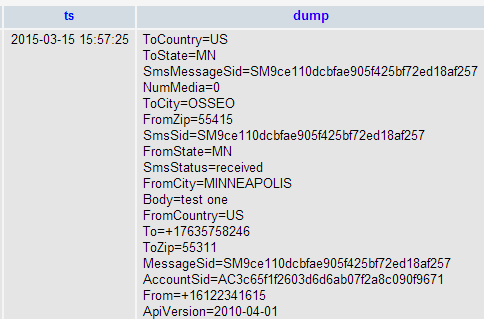


These screen shots show that my database is storing the messages.

SELECT \* FROM `twilio`



SELECT \* FROM `twiliotest`





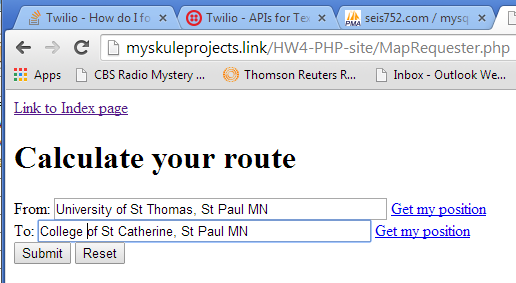
***###OPTION 2:*** *Choose, choose a public Web Service API and write a page that will query the API and return results on your page.*

My intent was to develop a page that could query Google Maps API and return directions. This is something we want to do for our project. So I went to Google’s documentation on its Maps API, but it was unusable. It seemed to refer me to another page, then another, then back to the first page. So, I googled for an example from another source.

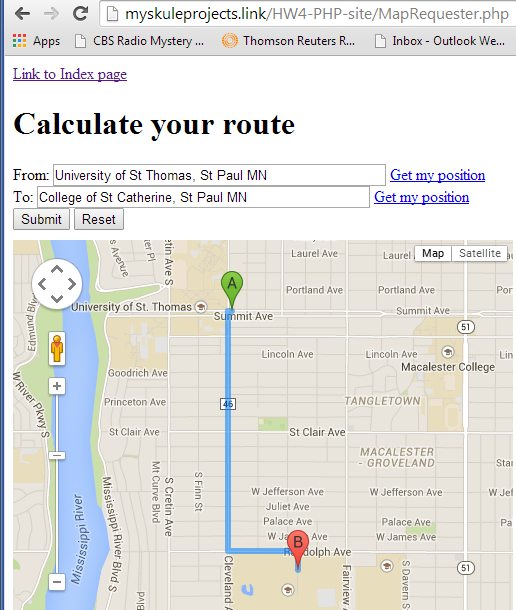
**Full Disclosure :**  The example I found was exactly what I wanted and it was complete. I can take no credit for it. Thecode came from **http://www.sitepoint.com/find-a-route-using-the-geolocation-and-the-google-maps-api/ ; it was written by Aurelio De Rosa .**

I did make some minor modifications like changing the URL’s, setting the default location to UST, and increasing length of the input boxes of the form.

Here is screenshot of my MapRequester page showing two locations entered.



This screen shot shows the map retuned from Google



***###OPTION 1:*** *Implement [one] Step by Step an OAuth Token exchange.*

*- https://developers.google.com/accounts/docs/OAuth2*

*- http://developer.linkedin.com/documents/authentication*

*- https://developers.facebook.com/docs/howtos/login/server-side-login/*

*AND Make at least 2 endpoint requests.*

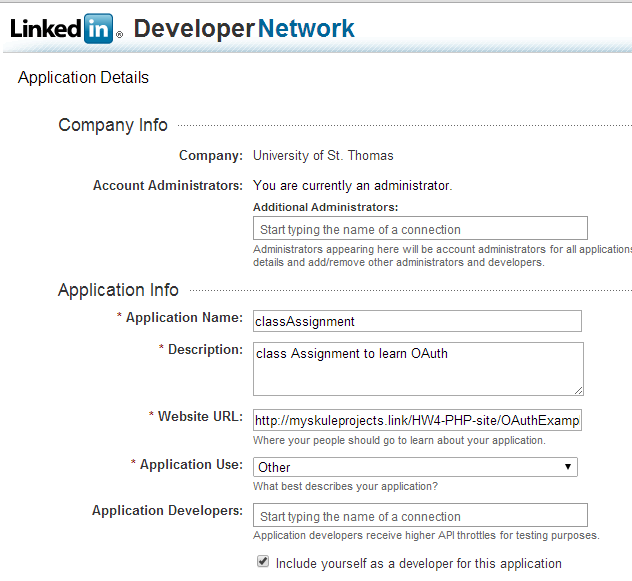
*Display the results down a long page.*

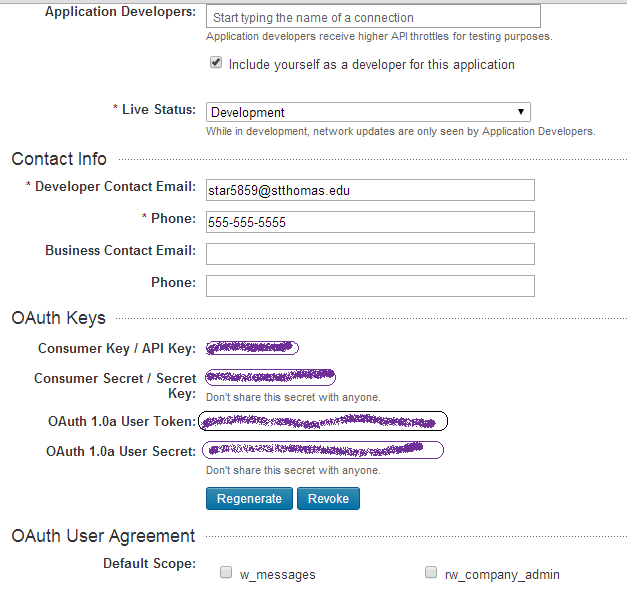
Since Option 2 turned out to be so little work on my part, I tried Option 1 also. I got a little overwhelmed by Google’s API’s , and moved on to investigate LinkedIn’s API’s. With fewer options, the documentation was more straight forward. I found some hints at <http://stackoverflow.com/questions/9935775/php-oauth-for-linkedin>, and a good example at

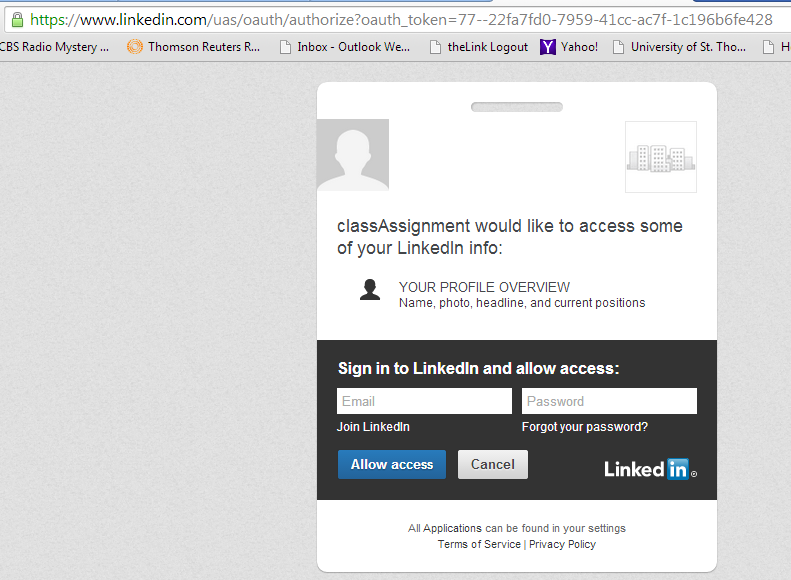
http://thinkdiff.net/linkedin/integrate-linkedin-api-in-your-site/. I tried following the second example in my website (citing the author in the code I pasted in). After setting up my application in the LinkedIn API system, I was able to send an oauth request to LinkedIn, but it only worked partially. The screen shots below show the request and response as well as what Fiddler captured. I suspect that the example’s code may be a bit out of date and some calling some deprecated methods.

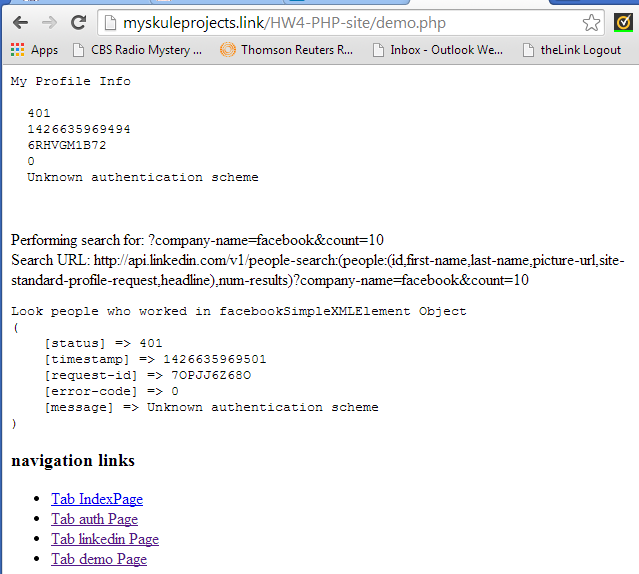
At this point I ran out of time, wrote up this document and checked everything in.

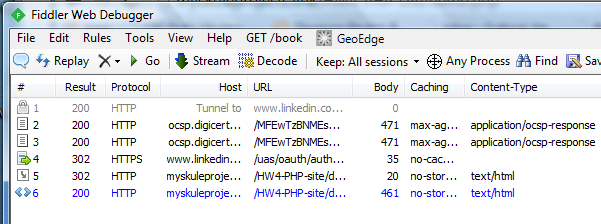
In my website, <http://myskuleprojects.link/HW4-PHP-site/index.php> has a link to the ‘auth’ (authorization) page.











CONNECT <www.linkedin.com:443> HTTP/1.1

**(1)**

Host: [www.linkedin.com](file:///C:\University%20of%20St%20Thomas\SEIS752\week6\www.linkedin.com)

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36

A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.3 (TLS/1.2)

Random: 86 C1 DE AC 87 5E 2A 38 EF 6B 1B 95 47 CF 21 A3 9D A2 70 4E D5 CA 6D 80 CA E4 37 B3 0C D5 3A AD

"Time": 11/26/2061 7:14:46 PM

SessionID: 62 7B 5E DD E0 16 46 72 F0 B1 40 1F 58 C0 C8 FB D5 19 BF CC E8 FA EB BA 44 0F A7 C0 B0 C1 EC C2

Extensions:

server\_name [www.linkedin.com](file:///C:\University%20of%20St%20Thomas\SEIS752\week6\www.linkedin.com)

0x0017 empty

SessionTicket empty

signature\_algorithms sha512\_rsa, sha512\_ecdsa, sha384\_rsa, sha384\_ecdsa, sha256\_rsa, sha256\_ecdsa, sha224\_rsa, sha224\_ecdsa, sha1\_rsa, sha1\_ecdsa

status\_request OCSP - Implicit Responder

NextProtocolNegotiation empty

SignedCertTimestamp (RFC6962) empty

ALPN http/1.1, spdy/3.1, h2-14

channel\_id(GoogleDraft) empty

ec\_point\_formats uncompressed [0x0]

elliptic\_curves secp256r1 [0x17], secp384r1 [0x18], secp521r1 [0x19]

Ciphers:

[CC14] TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[CC13] TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

[CC15] Unrecognized cipher - See <http://www.iana.org/assignments/tls-parameters/>

[C02B] TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

[C02F] TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[009E] TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[C00A] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

[C014] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA

[0039] TLS\_DHE\_RSA\_WITH\_AES\_256\_SHA

[C009] TLS1\_CK\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA

[C013] TLS1\_CK\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

[0033] TLS\_DHE\_RSA\_WITH\_AES\_128\_SHA

[C007] TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA

[C011] TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA

[009C] TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

[0035] TLS\_RSA\_AES\_256\_SHA

[002F] TLS\_RSA\_AES\_128\_SHA

[0005] SSL\_RSA\_WITH\_RC4\_128\_SHA

[0004] SSL\_RSA\_WITH\_RC4\_128\_MD5

[000A] SSL\_RSA\_WITH\_3DES\_EDE\_SHA

[00FF] TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

Compression:

[00] NO\_COMPRESSION

HTTP/1.1 200 Connection Established

FiddlerGateway: Direct

StartTime: 19:19:23.584

Connection: close

Encrypted HTTPS traffic flows through this CONNECT tunnel. HTTPS Decryption is enabled in Fiddler, so decrypted sessions running in this tunnel will be shown in the Web Sessions list.

Secure Protocol: Tls

Cipher: Aes 128bits

Hash Algorithm: Sha1 160bits

Key Exchange: ECDHE\_RSA (0xae06) 256bits

== Server Certificate ==========

[Subject]

CN=www.linkedin.com, O=LinkedIn Corporation, L=Mountain View, S=California, C=US

[Issuer]

CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US

[Serial Number]

0CDAB5274A872B20731372F6B4F95F15

[Not Before]

12/19/2013 6:00:00 PM

[Not After]

12/30/2016 6:00:00 AM

[Thumbprint]

A33BB54CBC57513F94A3C288A64A02C5F68D4057

**(2)**

GET <http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAH9o%2BtuynXIiEOLckvPvJE%3D> HTTP/1.1

Accept: \*/\*

User-Agent: Microsoft-CryptoAPI/6.0

Host: ocsp.digicert.com

Connection: Keep-Alive

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: max-age=515657

Content-Type: application/ocsp-response

Date: Wed, 18 Mar 2015 00:19:24 GMT

Etag: "55089623-1d7"

Expires: Tue, 24 Mar 2015 12:19:24 GMT

Last-Modified: Tue, 17 Mar 2015 21:01:23 GMT

Server: ECS (ord/4CFC)

X-Cache: HIT

Content-Length: 471

0 \_

\_ \_ 0 \_ \_ +\_\_\_\_ 0\_\_\_ \_ 0 \_ 0 \_\_\_\_ P5V L f \_\_× = U\_\_20150317200000Z0s0q0I0 \_\_+\_\_\_\_\_ \_\_ Q\_\_2 }Q \_b\_U \_\_\_ P5V L f \_\_× = U\_\_\_ n uȈC rKϼ \_\_20150317200000Z \_\_\_20150324200000Z0

\_ \* H

\_\_  
\_ \_ \_\_ q' ' \_W 2 \_R \\_

/ a6\_uC s,\*HU x B+G e \_ \_] 4\_Lbǋ \_> y # B~|WB ; T 2\_ 3\_ 9\_ ; \_ U PH X,bx g @ /\_a \_ ~ 6C 7p b \_ hL N k 6 r wEFY m#\_W \_ Gs \_G k \_\_B\_Vw \_ \_ \_ ۧ:\_ Y \_ \_ \_ B R O 5 \_ ԽD \_ )z

**(3)**

GET <http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEAzatSdKhysgcxNy9rT5XxU%3D> HTTP/1.1

Accept: \*/\*

User-Agent: Microsoft-CryptoAPI/6.0

Host: ocsp.digicert.com

Connection: Keep-Alive

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: max-age=516707

Content-Type: application/ocsp-response

Date: Wed, 18 Mar 2015 00:19:24 GMT

Etag: "5508a062-1d7"

Expires: Tue, 24 Mar 2015 12:19:24 GMT

Last-Modified: Tue, 17 Mar 2015 21:45:06 GMT

Server: ECS (ord/269D)

X-Cache: HIT

Content-Length: 471

0 \_

\_ \_ 0 \_ \_ +\_\_\_\_ 0\_\_\_ \_ 0 \_ 0 \_\_\_\_ a\_ 1a /( F8 , \_\_20150317213000Z0s0q0I0 \_\_+\_\_\_\_\_ \_\_\_\_ z \_ ' 5΃  
C

\_\_\_ a\_ 1a /( F8 , \_\_

ڵ'J + s\_r \_\_ \_\_20150317213000Z \_\_\_20150324214500Z0

\_ \* H

\_\_  
\_ \_ \_\_ djO g 1l\_ %N7 r `TL " ? { L

Fב Q&6u M2 | Q\_ v q f ` ! ~ и p\_ ` <\_ ܕ 腱

- "

Oe C |#Z t [&& F9 \_I, ɺ H 鯵 \_ K䣥\_Jl . T\_% q } I -. \_\_! Ճ\_ 8 \_ ) wk

1b 7 [ #\_\_mă p \_ Z#\_ M u G ?T = c r re R \_9 /gB/

(4)

POST <https://www.linkedin.com/uas/oauth/authorize/submit> HTTP/1.1

Host: [www.linkedin.com](file:///C:\University%20of%20St%20Thomas\SEIS752\week6\www.linkedin.com)

Connection: keep-alive

Content-Length: 445

Cache-Control: max-age=0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Origin: <https://www.linkedin.com>

User-Agent: Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Referer: <https://www.linkedin.com/uas/oauth/authorize?oauth_token=77--7c77951b-7fd1-4700-8bcc-5ac1721fb796>

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.8

Cookie: lidc="b=LB21:g=199:u=1:i=1426635873:t=1426722273:s=AQFYNtlQ7V6f03YzShtwi5P0VewnTTKl"; JSESSIONID="ajax:2246175690956348726"; visit="v=1&G"; bcookie="v=2&e341a47f-727f-4b60-8c47-bfa96e874a86"; bscookie="v=1&201503172344345b05f9d1-a24e-4534-85ee-78c79f3ff168AQHUNTR92kxNViIYgc3z8ef4mnFh8Ot2"; leo\_auth\_token="GST:8KirH582hnzx4YjEybXH\_n8ez8LTbY6kTiSM8KfAsnLxZYI\_qhz5EO:1426637927:ccb5ae32c333f700aa361d76365cc0ee17bf0b1d"; lang="v=2&lang=en-us"

isJsEnabled=true&session\_key=js24816%40yahoo.com&session\_password=%7EPLds\_593&duration=0&authorize=Allow+access&extra=&access=-3&agree=true&oauth\_token=77--7c77951b-7fd1-4700-8bcc-5ac1721fb796&email=&appId=&csrfToken=ajax%3A2246175690956348726&sourceAlias=0\_8L1usXMS\_e\_-SfuxXa1idxJ207ESR8hAXKfus4aDeAk&client\_ts=1426637963423&client\_r=%3A161134884%3A776856703%3A693399167&client\_output=0&client\_n=161134884%3A776856703%3A693399167&client\_v=1.0.1

HTTP/1.1 302 Found

Server: Apache-Coyote/1.1

P3P: CP="CAO CUR ADM DEV PSA PSD OUR"

Location: <http://myskuleprojects.link/HW4-PHP-site/demo.php?oauth_token=77--7c77951b-7fd1-4700-8bcc-5ac1721fb796&oauth_verifier=20581>

Content-Language: en-US

Content-Encoding: gzip

Vary: Accept-Encoding

Date: Wed, 18 Mar 2015 00:19:25 GMT

X-FS-UUID: 77249db5ab6fcc13d03c548c6d2b0000

X-Li-Fabric: PROD-ELA4

Strict-Transport-Security: max-age=0

Set-Cookie: \_lipt=deleteMe; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

Set-Cookie: leo\_auth\_token="GST:9tUtlNDNO\_OulXh7LhUt4hygas55MaueIo3SMoyQjs514rY77RRCoL:1426637965:e70c5db3326b89000224201ebb81e84710983700"; Version=1; Max-Age=1799; Expires=Wed, 18-Mar-2015 00:49:25 GMT; Path=/

Set-Cookie: sl="delete me"; Version=1; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

Set-Cookie: sl="delete me"; Version=1; Domain=.www.linkedin.com; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

Set-Cookie: s\_leo\_auth\_token="delete me"; Version=1; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/

Set-Cookie: lang="v=2&lang=en-us"; Version=1; Domain=linkedin.com; Path=/

Pragma: no-cache

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Cache-Control: no-cache, no-store

Transfer-Encoding: chunked

Connection: keep-alive

X-Li-Pop: prod-lva1

X-LI-UUID: dySdtatvzBPQPFSMbSsAAA==

a\_ \_ a\_ 0

**(5)**

GET <http://myskuleprojects.link/HW4-PHP-site/demo.php?oauth_token=77--7c77951b-7fd1-4700-8bcc-5ac1721fb796&oauth_verifier=20581> HTTP/1.1

Host: myskuleprojects.link

Connection: keep-alive

Cache-Control: max-age=0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36

Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-US,en;q=0.8

Cookie: PHPSESSID=llTjeNaM2q9u0b2nywPwo2

HTTP/1.1 302 Moved Temporarily

Date: Wed, 18 Mar 2015 00:19:26 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Location: <http://myskuleprojects.link/HW4-PHP-site/demo.php>

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 20

Keep-Alive: timeout=2, max=100

Connection: Keep-Alive

Content-Type: text/html

\_ \_ \_\_

**(6)**

GET <http://myskuleprojects.link/HW4-PHP-site/demo.php> HTTP/1.1

Host: myskuleprojects.link

Connection: keep-alive

Cache-Control: max-age=0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36

Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-US,en;q=0.8

Cookie: PHPSESSID=llTjeNaM2q9u0b2nywPwo2

HTTP/1.1 200 OK

Date: Wed, 18 Mar 2015 00:19:27 GMT

Server: Apache

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 461

Keep-Alive: timeout=2, max=99

Connection: Keep-Alive

Content-Type: text/html

\_ \_ \_ RɎ @\_ # \_J\_"[\_7 x  
\_ ( , G ce ( 6 4 8 \_4 }JnU \* 4&\_g hu\_\_ WyP wY + Z(\_ Q \_ TeB 铿p 6\f P\_c L \_ V:q "bMS' `\_ na#J$ lv7? yĮD\_ WC / d x ~ r\_ \_ 4\_&A n r5 d' R $ ( H Ns,1b 0 /@ ^\_K" e tIkC \ 9 \_ 2Ue ٗ S +u| F x\_

[ {\ \_S J

! H \_Q

:f\_ @ߖ\_

" \_BӮm  
 \_ \_ i4 . Z\_J dЙ\_Y\_ H^ < f8 dS\_Z7 \_\_ WD N 49\_ ( |~X \_tLi` q\_$ w \_ \_ ? \_ ; fs\_pո N\_ gK\_U \_ O c } \_&L \_