Web サービス Hack

～Web サービスの中身を覗いてみよう～

序章

朝なら「おはよウナギ」昼なら「こんにちワン」夜なら「こんばんワニ」

Mine です。

いろんなコトやっていて、いろんなこと書いてきた人ですが、今回はそのなかでも Web サービスの解析というのを紹介してみます。

なお、文化祭で配布する、紙のものでは一部の資料が見づらくなっているため、あとでデジタル版を配布できるようにします。

ついでに、タイトルでは「Web サービス Hack」となっているのですが、この hack というのは英和辞典で引くと「たたき切る」というのが一番初めに出てくる。そして、二番目ぐらいに「＜道など＞を切り開く、作る」というのがあるかと思う。コンピューターの世界で言う「Hack」というのはどちらかというと後者の意味が多いです。

コンピューターで様々な技術を駆使して革新的なものを作ったり、新たな技術を生み出したりと、そういったことに長けている人たちを「Hacker」と呼ぶ。そしてその Hacker というのは必然的にその分野で最先端を行く人となり、尊敬されます。

そういう文化を育んできたのがこのコンピューターの使い手たち、「Hacker」の文化なのです。

詳しくはググッて[1]みるとわかるかも。

ともあれ、今回はみささんと共に Web サービスを「切り開いて」いこうと思います。

Web サービスとは

Web サービスの解析を始める前に Web サービスがなにか理解していないと話にならない。

普段なら「ググれ」の一言で済ませてしまうのですが、部誌なのでちゃんと書きます。

(ついでに、４月時点での Wikipedia の「Web サービス」の項目は古くてアテにならない・・・もしかすると、みなさんが呼んでいる頃には僕とかが編集しているかも)

Web サービスとは「Web」という手段を用いて提供するサービスのことをいう。Web というのは、簡単に行ってしまえばみなさんが一般的に「インターネット」と呼んでいるものである。

---

[1] ググる：大手検索エンジン「Google」で検索することをいう。ちゃんと動詞として活用する。

こんなやつですね。

有名な Web サービスといえば Twitter や Facebook のような SNS[2]、Google や Yahoo が提供する検索エンジン、YouTube やニコニコ動画のような動画共有サービス、Amazon や Yahoo ショッピングのようなネットショッピング、Gmail や Windows Live メールのような Web メールなどなど、いろんな Web サービスがあります。

これらのサービスは、ブラウザを起動して、そのサイトにアクセスするだけで使えるため、手軽で、もしパソコンが壊れたり、買え買えたりしてもデータを紛失したり、移動させる必要がない。

---

[2] SNS：ソーシャル・ネットワーク・サービスの略。人同士のコミュニケーションを目的とされるサービス。

一見便利に見えるが、当然、そのサイトと通信しないといけないので、そこでセキュリティ上のリスクが生じる。

余談: ブラウザって何よ

先ほど、さりげなく「ブラウザ」という単語を出したが、読者の中にも「ブラウザって何？」っていう人がいるかと思うので、軽く解説します。

ブラウザは Web を閲覧するソフトウェアの事。

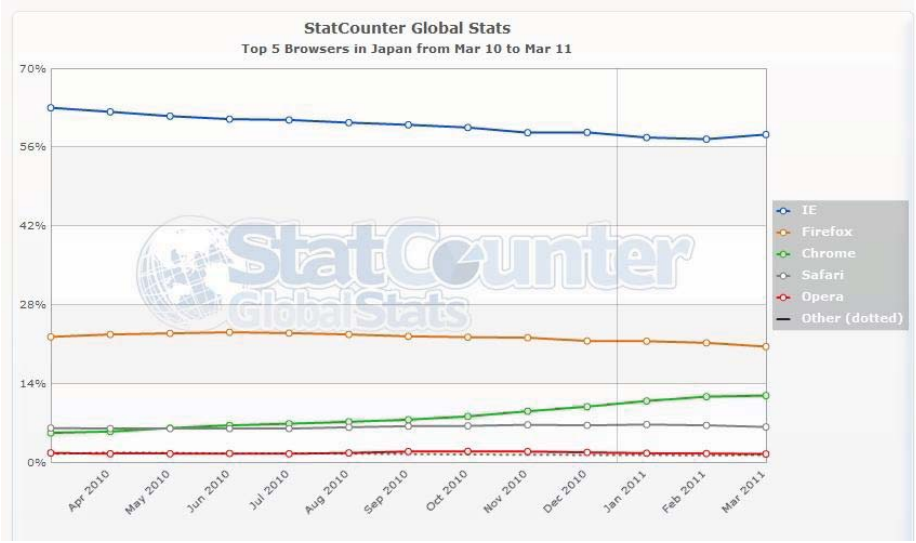
俗に「インターネット」と呼ばれるもの。コンピューターの世界で、認知度が高い割には、ほとんど正しい意味を知られていない単語は「インターネット」だろう。

ブラウザ戦争というブラウザ同士のシェア闘いが過去に繰り広げられたが、ちょうど今、第二次ブラウザ戦争とも言える戦いが繰り広げられている。新しい Web の技術「HTML5」「CSS 3」「SVG」の使用策定が W3C によって進められており、この仕様をめぐる争いが第二次ブラウザ戦争をヒートアップさせている。

その一辺を見せるためにもちょっとブラウザのシェアを紹介しよう。

まずは日本でのシェア(2011 年 3 月時点)

http://gs.statcounter.com/ のデータを参考にさせていただいた



印刷すると見えないかもしれないですがすいません

シェアトップは Microsoft 社の Internet Explorer。現行最新バージョンは 9(日本では東日本大震災の影響で、執筆時点では正式リリースを行っていないが、文化祭時点では公開されている予定である)。シェアは 60%弱といったところ。

続いて Mozilla Foundation(非営利団体)の Firefox。現行最新バージョンは 4。リリーススケジュールが変更になり、6/21 に 5 がリリース予定だ。シェアは 20%強。

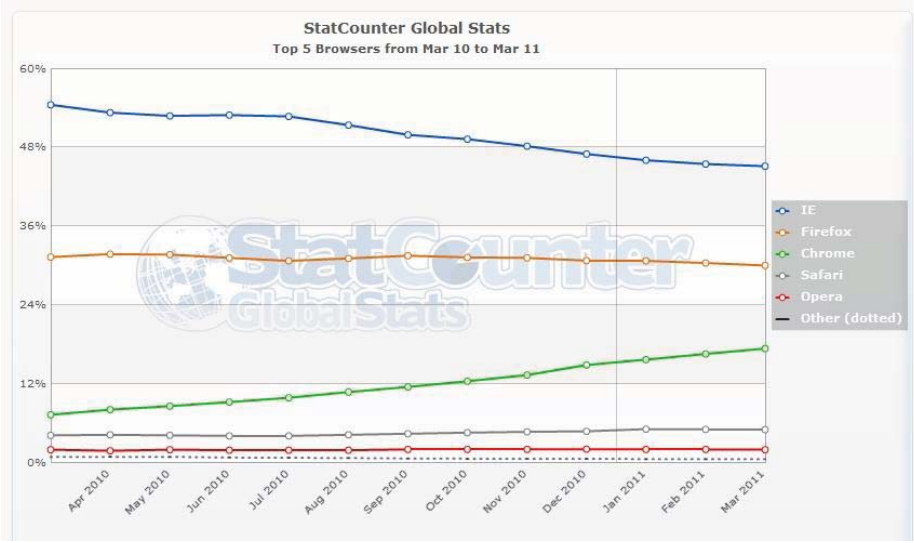
三位は Google 社の Chrome。現行最新バージョンは 10。シェアは 10%強。

次に Safari、Opera と続く。

日本のだけを見ると、Internet Explorer 安泰に見えるかもしれない。

ところが

世界のシェアを覗いてみると日本とはかなり違ったことになっている。

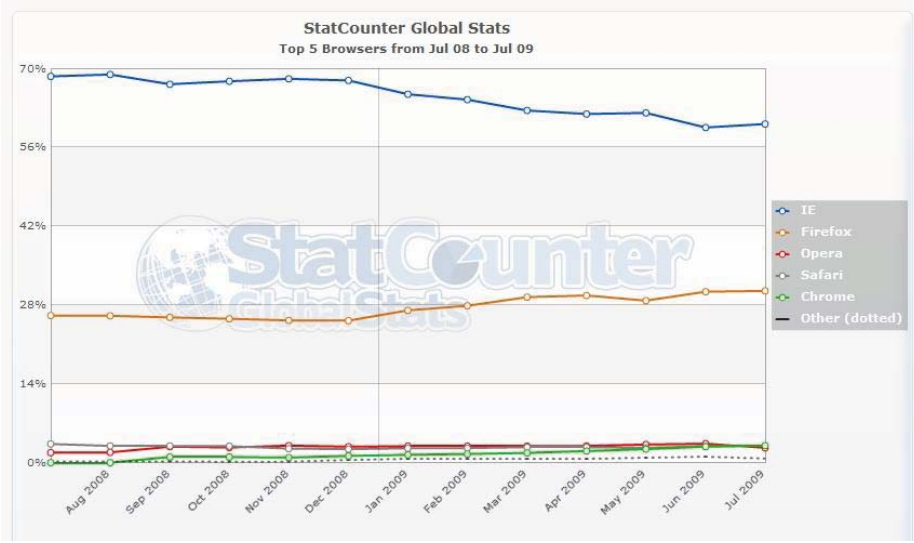


分かりやすいように 2011 年 3 月時点の値を表にしてみる。

ブラウザ名	日本でのシェア	世界でのシェア
Internet Explorer	58.25%	45.11%
Firefox	20.62%	29.98%
Chrome	11.91%	17.73%

世界でのシェアを長いスケールで見ると、第一次ブラウザ戦争で勝利を収めた Internet Explorer を Firefox が一気に侵略をはじめ、直後、Chrome が両者のシェアをジリジリ奪いながら成長しているといった辺りだ。

そう考えると、**かなり日本は遅れている**。実は、まだ Chrome が登場したばかりの 2008 年 7 月～2009 年 7 月の世界でのシェアのグラフに特に IE の様子が近いのだ。



ここまで日本が鈍感なのは、日本人としては結構悔しい話。

Web サービスの解析の準備

さて、早速 Web サービスの解析にとりかかろうと思うのですが、そこで必要なソフトをインストールしてもらいましょう。

なお、OS は Windows を想定しています。

(以下、様々な開発用ソフトウェアを使用しますが、普段使用しているコンピューターにインストールすると、普段の作業に支障が出る可能性があります。また、この記事に書かれている内容を実行して、何かしらの問題が発生しても、保証できません。)

Fiddler

インストールしたパソコン上での HTTP、設定次第では HTTPS 通信をキャプチャして解析するツール。Web サービスの解析には必須。

Windows 専用です。

http://www.fiddler2.com/fiddler2/

Firefox & Firebug & Firecookie

燃える狐に燃えるバグに燃える COOKIE です。

今回は使いませんが、Fiddler と違い、ブラウザでの表示内容や、JavaScript などの制御も行えます。が、通信解析向けではないので、今回のような場合は Fiddler が使えない環境での代替策ととってください。

Firefox は先ほど出てきたブラウザですが、Firebug はその Firefox のアドオン。そして Firecookie は Firebug のアドオン。

アドオンのアドオンというなんとも複雑な立ち位置

Mozilla Firefox

http://mozilla.jp/firefox/

Firebug (Firefox で開いてください)

http://goo.gl/FcbRe

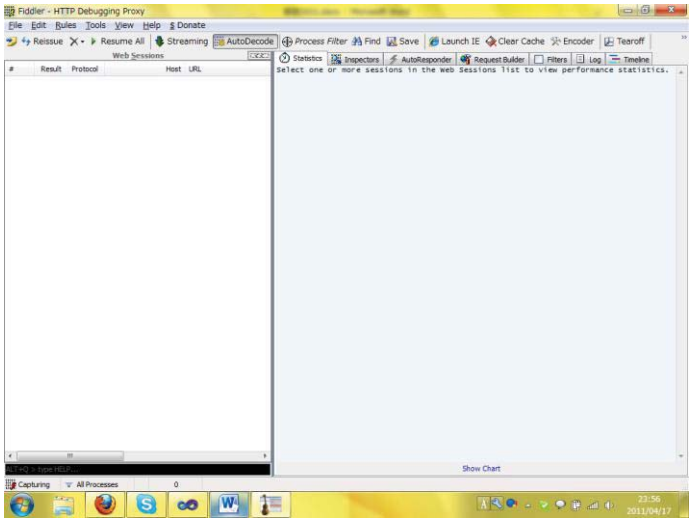
Firecookie(Firefox で開いてください)

http://goo.gl/2Wauk

上から順番にインストールすると、まあ、最低限の環境は出来上がるかと思います。

いざ実践

Fiddler2 を起動すると、いきなり意味不明な画面が出てくるかと思います。



さて、Firefox で Google のトップページを開いて F12 でキャプチャを止めます。

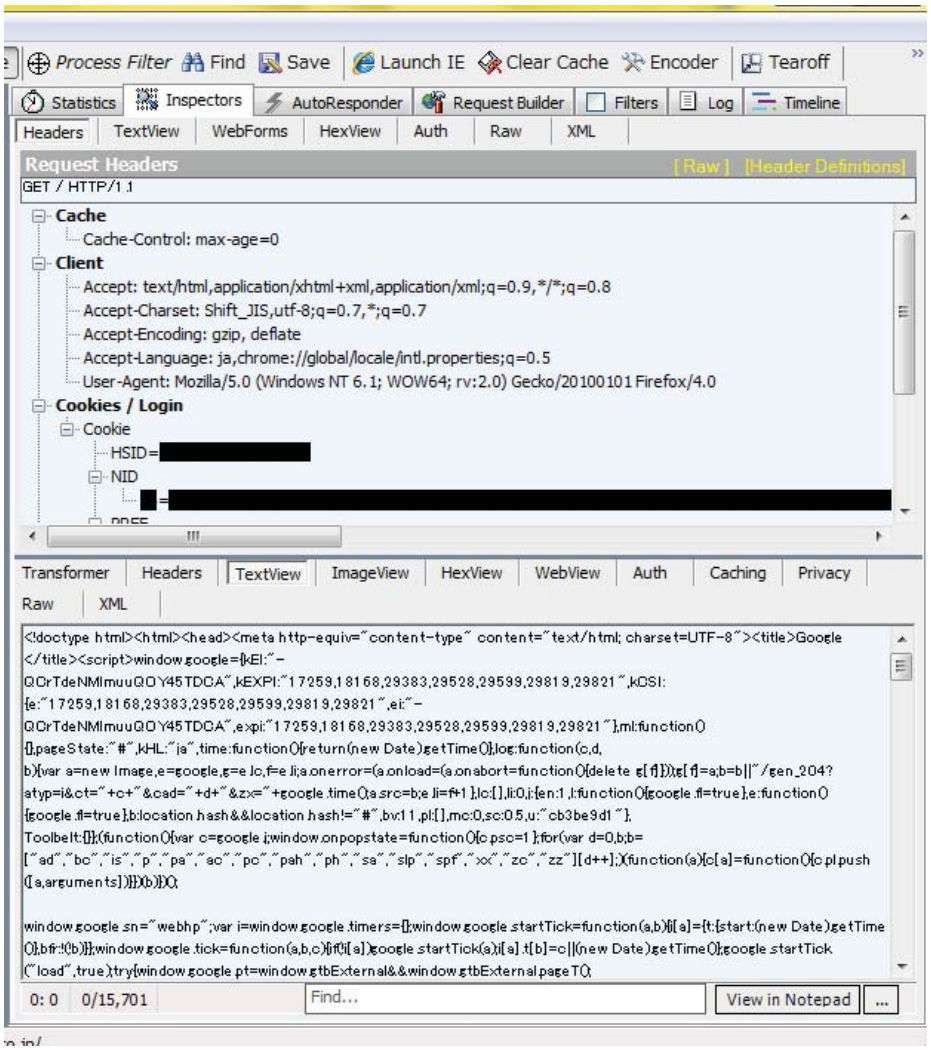
#	Result	Protocol	Host	URL
1	200	HTTP	www.google.co.jp	/
2	200	HTTP	toolbarqueries.goo...	/tbr?features=WH:Rank&
3	304	HTTP	www.google.co.jp	/intl/en_com/images/srpr/
4	304	HTTP	www.google.co.jp	/images/srpr/nav_logo39.
5	304	HTTP	www.google.co.jp	/extern_js/f/CgJqYRICan
6	304	HTTP	www.google.co.jp	/extern_chrome/96edd23
7	204	HTTP	clients1.google.co.jp	/generate_204
8	304	HTTP	www.google.co.jp	/ig/cp/get?hl=ja&gl=jp&b

左側がこんな感じになったかと思います。

実は Google のトップページを読み込むだけで、そこにある画像やその他のプログラムなどをダウンロードする必要があります。

ここで重要なのは Host と URL です。この二つでどこにアクセスしているのかがわかります。

試しに一番上の Host: www.google.co.jp URL: / をクリックしてみましょう。



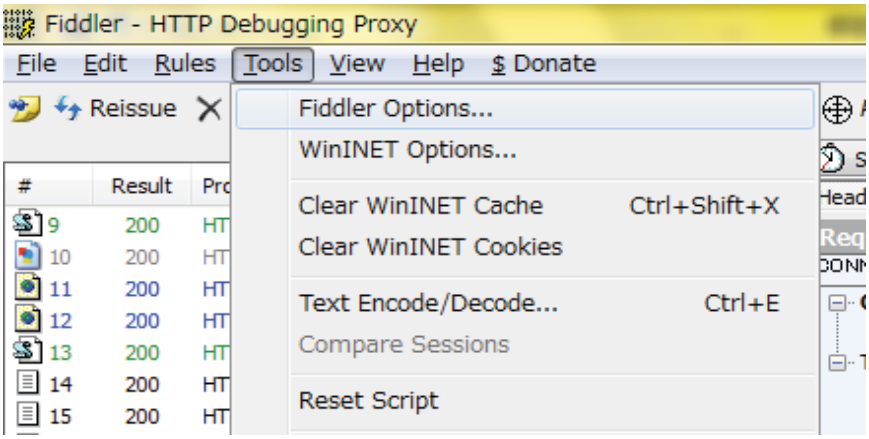
その後、右側の Inspectors タブを開き、下部の TextView をクリックするとこんな感じになるかと思います。

早速一部黒く塗りつぶした部分がありますが、これらの情報はアカウントを侵略するときの鍵のひとつにもなります。

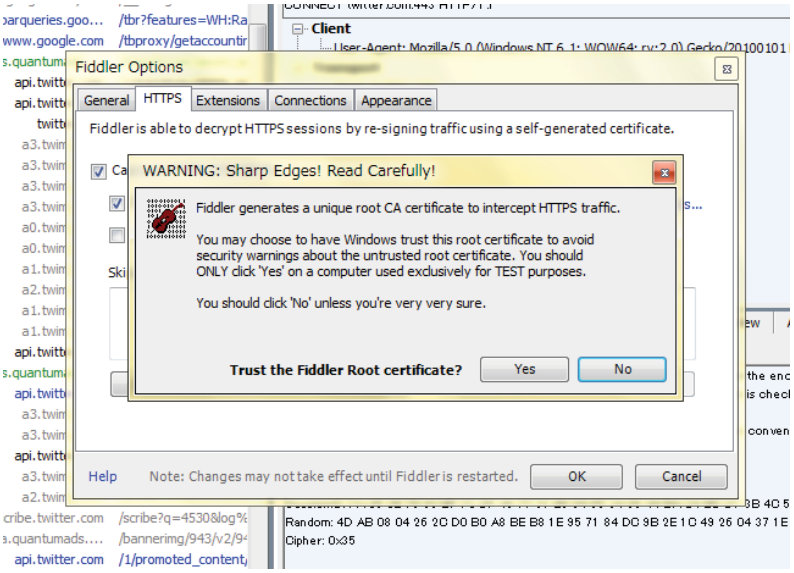
現時点ではまだ直接侵略できるほどの情報ではないですが、現時点で重要なのは先ほど表示した情報はすべて**暗号化せずに通信している**ということ。

では、暗号化されている部分を見るにはどうすればいいのでしょう。

Fiddler の設定を変えます。



メニューバーの Tools から Fiddler Options...というのをクリックします。



HTTPS タブを開いて、”Capture HTTPS CONNECTs”と”Decrypt HTTPS traffic”にチェックを入れます。すると上のようにダイアログが出るので、Yes を押すと、「セキュリティ警告」というダイアログがさらに出てくるので、「はい」をクリックします。

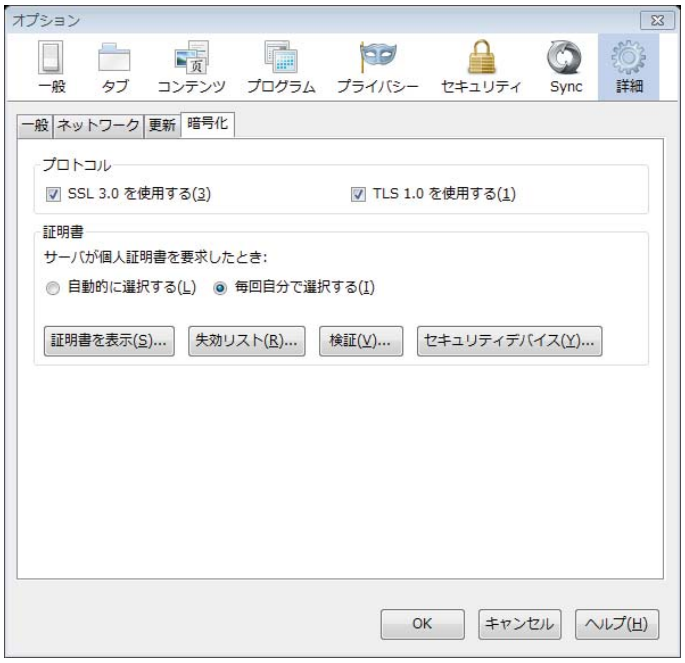
このままブラウジングをしようとすると、証明書エラーがたくさん出てしまい、まともにサイトを見ることができません。

実は Fiddler はこの時点で「中間者攻撃」という攻撃を自らのコンピューターに仕掛けることで、正攻法では解読不能な(とされている)暗号を解読しています。

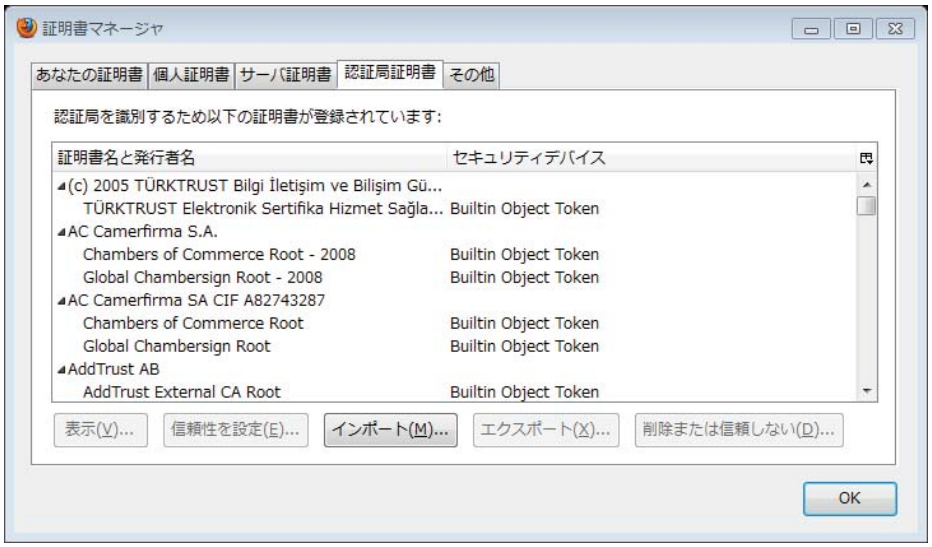
当然、そういう攻撃に対する対処法も存在するため、一筋縄では解読させてくれません。

ですので、今回は Fiddler の攻撃を許可する設定を行います。

先程の Fiddler Options の画面で Export Fiddler Root Certificate to Desktop をクリックすると、デスクトップに FiddlerRoot.cer というファイルが出来ます。



Firefox のオプションから詳細を開き、暗号化を開き、下の「証明書を表示」ボタンをクリックします。



下のインポートボタンをクリックし、先程のファイルを開きます。

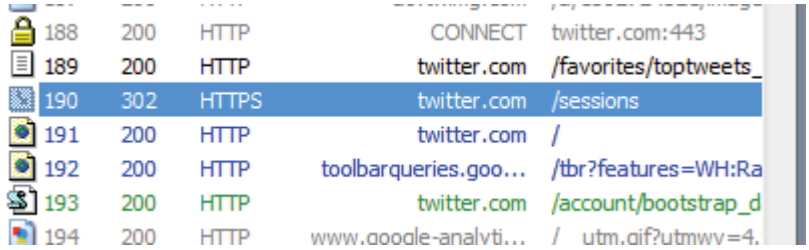
こんな画面になりましたら、一番上にだけチェックを入れて OK をクリックします。

OK で設定画面を閉じると暗号化された HTTPS 通信ものぞくことができます。

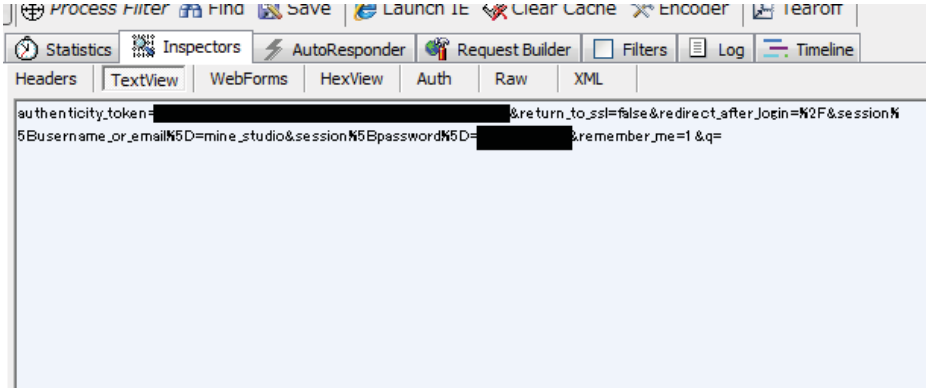
この後は暗号を解読されるとどんなにヤバいのかを実感できるかと思います。

例えば、Twitter にログインしてみると・・・・

左部が流れていきますので、その中から下のようなのを選びます。



その後、右の上側の Inspectors の TextView を開きますと・・・・



黒く塗りつぶした部分(下の方)にもろパスワードが書かれています。

上側の塗りつぶした部分もここからアカウントを乗っ取れることができるデータです。

暗号化を紐解くと当然ながらパスワードが出てきてしまいます。

数学的には解読不能でもシステム的な脆弱性から・・・

では、暗号を解読されることはあるのでしょうか？

当然あります。HTTPS 通信で使われる公開暗号鍵と言われる暗号化方式を使っています。

数学界隈の人でもこの公開暗号鍵に関して詳しい人も多いかと思います。(というよりは、暗号分野は数学寄りの分野なので当然ですが)

たしかに数学的に考えると、暗号の解読には途方もない時間がかかり、現実的には不可能という結論が出てきます。(最近こちら方面でも動きがありますが割愛)

しかし、そもそもの鍵を詐称するというシステム的なトリックで、解読しなくても通信内容が分かってしまいます。そこで、鍵の身元を確認する技術もあり、先ほどの証明書エラーのようなエラーで攻撃をブロックします。

ですが・・・・

例えば、Chrome だと中間者攻撃を受けていることを把握すると、このような画面になるのですが、ここでよくわからずに「このまま続行」をクリックすると、ものの見事に暗号化したはずのものの中身が筒抜けになります。

実際のところ、特に企業内のシステムで、証明書の設定を間違えたままで、こういうエラーが出るが、無視してくれと言われている方もいるかと思いますが、これはとても危険な行為だということを理解してください。

モバイルの時代への突入とコンプライアンスとの衝突

完璧に余談臭たっぷりですが、お付き合い下さい m(__)m

一気にレベルが上がるので今回は割愛いたしましたが、先程の Fiddler での HTTPS トラフィックの解析は実は、インストールしたコンピューターのみならず、別のコンピューターの通信も見ることができます。

たとえ相手が携帯電話であってもです。

Android セキュリティ部の部長をやっているので、こちらに関しても少し書かせていただきます。

今、Android や iOS といったスマートフォン OS、並びに各種スマートフォンが浸透しています。そして、それらのスマートフォンを企業の IT 戦略として導入しようという動きが特に大企業を中心に動いています。

しかし、スマートフォンを導入するということは、当然、スマートフォンに企業の機密情報などが入ることになりますし、スマートフォンから情報が抜かれると、個人情報漏洩問題などが起こり、コンプライアンス違反だ、と騒がれることになります。

特にコンプライアンス問題は大企業にとっては大変な問題で、マスコミで一旦取り上げられてしまうと、もう手の付けようありません。

さすがに社名は出せませんが、大企業を中心にスマートフォンのコンプライアンス問題や情報漏洩問題を解決し、「安全に」導入しようと集まって

います。私も立ち会っているのですが、クラッカーからの攻撃の話題になった途端にノートパソコンの話題とループし始めて、議論が進まない。

大企業へのスマートフォンの導入にはかなりの壁があるというのが実情です。

まとめ 通信内容から新たな切り口が見えてくる

今回の記事では、Web サービス Hack の触りの触りぐらいまでしか説明しなかったですが、「Fiddler」というツールの存在と「暗号化はちょっとした不注意から簡単に解読される」ということを覚えておけば、のちのち役に立つかもしれないといったところです。

特に後者は出先で無線 LAN スポットなどを使用するときには気をつけてください。

怪しいダイアログがでたらすぐに使用をやめる。

特に空港での偽装 LAN スポットによるクレジットカードの情報やメールの情報の抜き取りの被害が後を絶ちません。

そして、これを気に、通信内容をのぞくという「キャプチャ」に興味を持った人は是非私にメールなり Twitter なりで声をかけてみてください。

さらに詳しい説明をしたり、サイトを紹介できるかもしれません。

又、灘校生でしたら、ぜひパソコン研究部にも立ち寄ってみてください。

灘校生以外の人でも、学生の方でしたら、セキュリティ＆プログラミングキャンプという、経産省が開催する学生向けの IT 技術者育成合宿が夏休みに開催されます。

書類選考を突破する必要がありますが、参加できると日本の IT のトップを走る人たちの直接の指導を受けられるだけでなく、未来の日本の IT を担う人たちと友だちになれます。

私もそのキャンプを卒業し、そこで教えてもらったこと、そこで手にいれた人間関係は今でも生きています。

今は意味不明な Fiddler のキャプチャですが、意味がわかると楽しいものです。

ではこの辺りで

65 回生 Mine

Mail: naclubkaityo@gmail.com

Twitter: @mine_studio