



Advanced SSL: The good, the bad, and the ugly



Michael Coates
Global Membership Committee
AppSensor Project Lead

Aspect Security
michael.coates@aspectsecurity.com
<http://michael-coates.blogspot.com>

AppSec DC
November 12, 2009

The OWASP Foundation
<http://www.owasp.org>

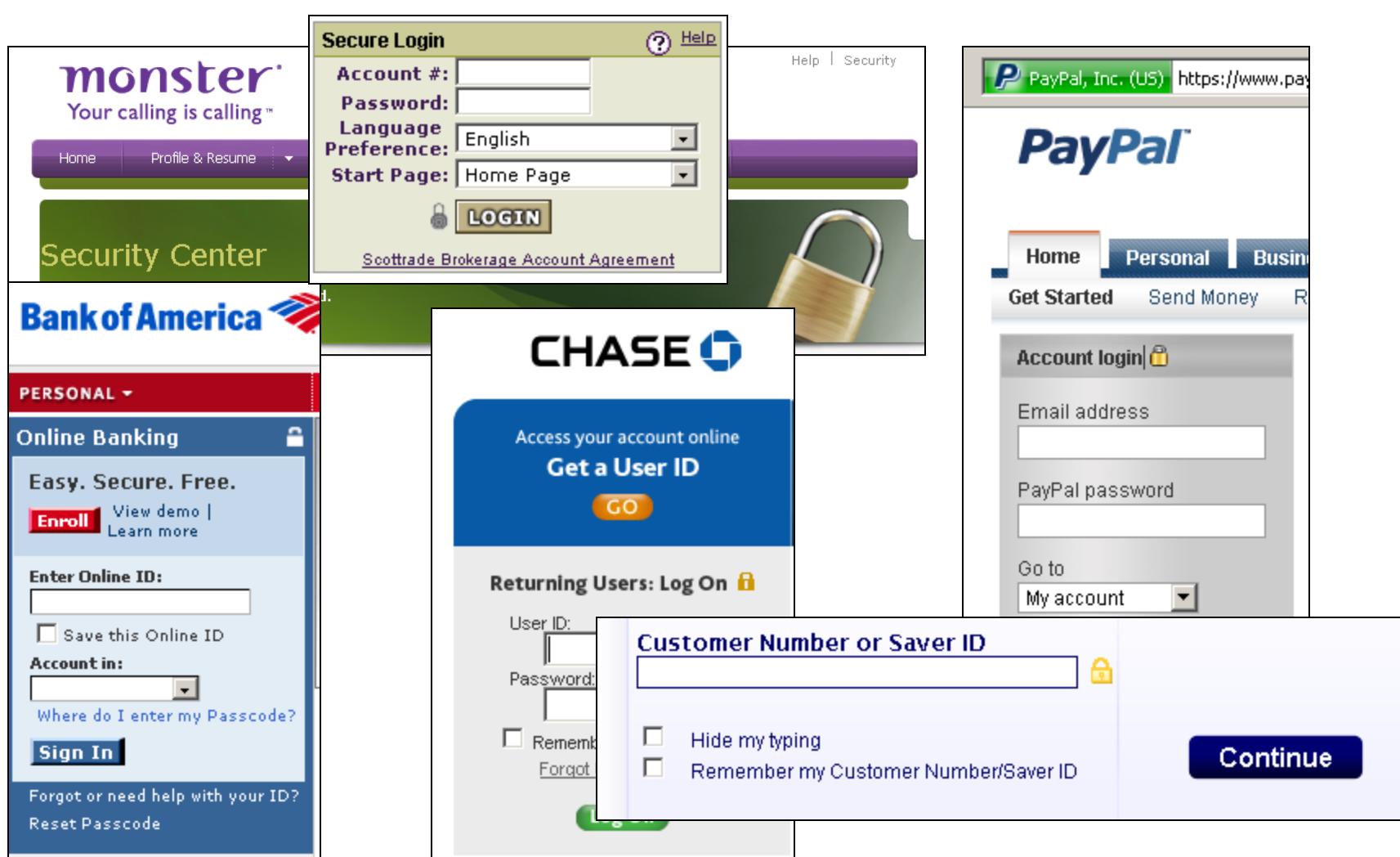
Who am I?

- Senior Application Security Engineer
@ Aspect Security
- Creator & Leader OWASP AppSensor
- Security Blogger
 - ▶ <http://michael-coates.blogspot.com>
- Life Outside Security?
 - ▶ Motorcycle, Triathlons

SSL: Super Shiny Locks

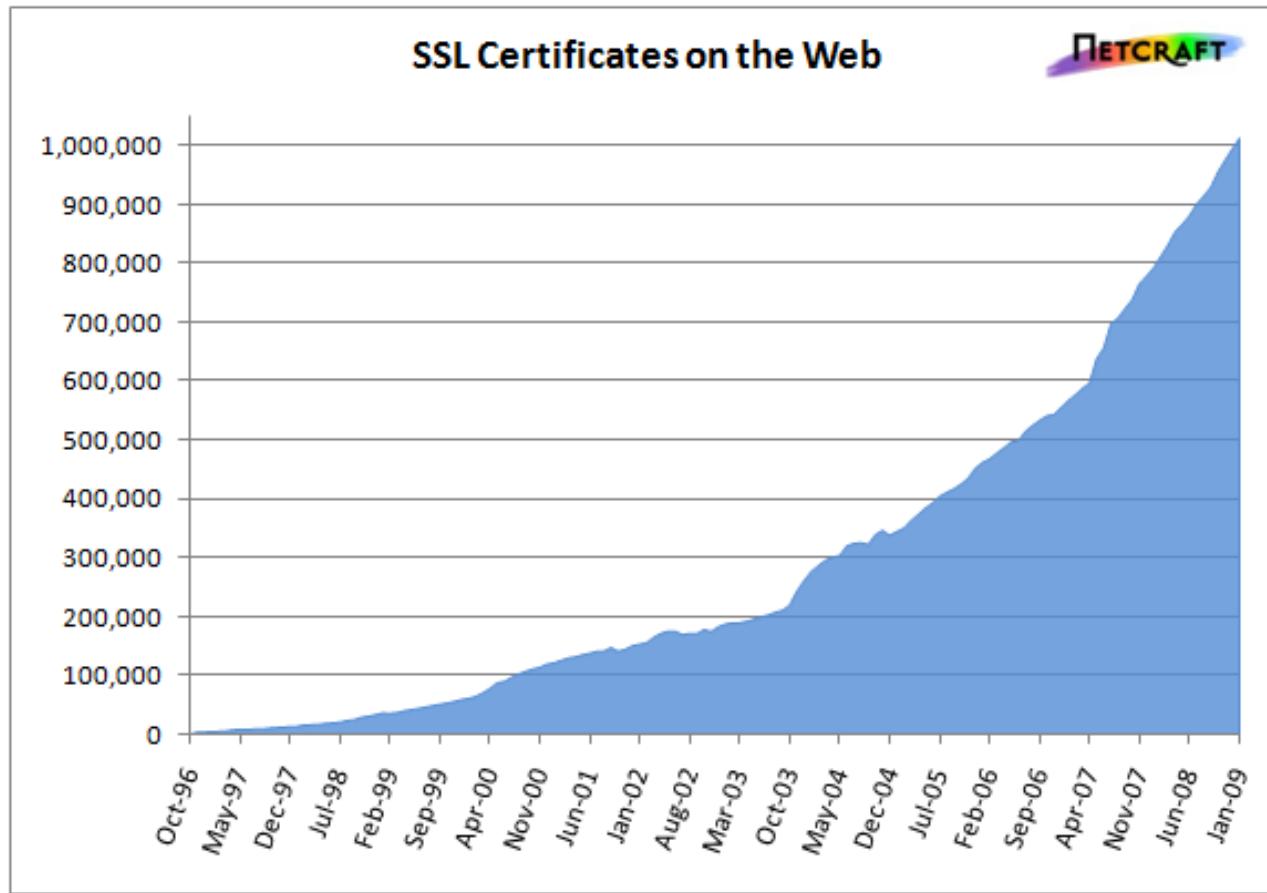


Padlock != Secure



SSL Growth

- > 1 Million SSL Certificates



The Good

- Confidentiality
- Integrity
- Replay Protection
- End Point Authentication



The Bad - Usability



The security certificate presented by this website was not issued by a trusted certificate authority



The security certificate presented by this website was issued for a different website's address.

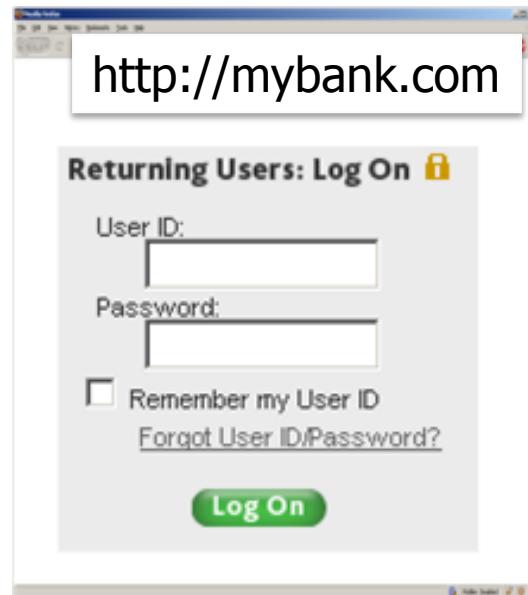
The Bad – User Expectations

- How did you get to the site?
- Is HTTPS in the URL?
- Are those zeros or o's?
- Did you get any browser warning messages?
- Did you click “ok” or “accept” to any popup boxes?

“I've told many people about the https and they didn't know!” – dad

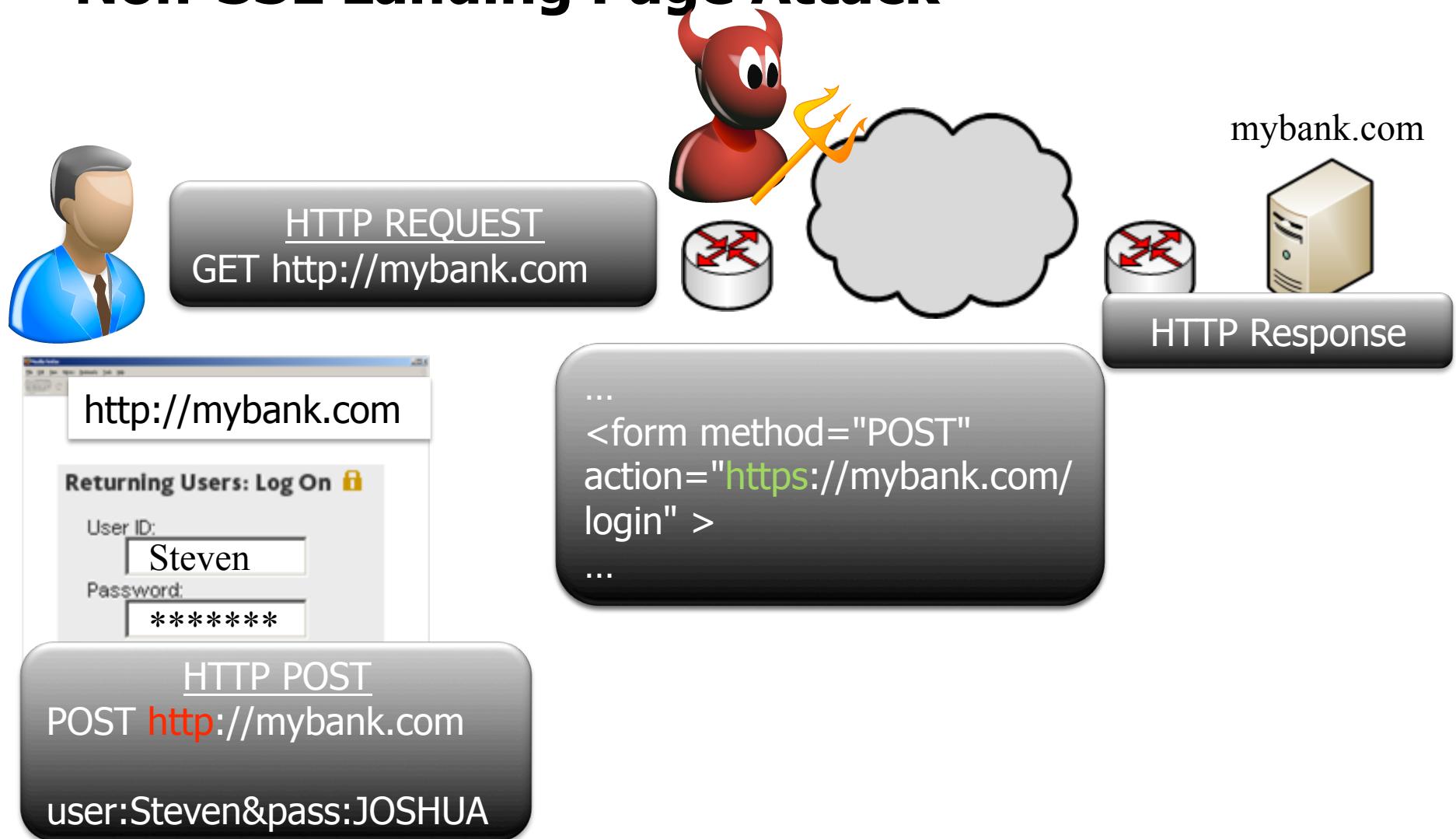
The Bad – Websites are Configured Wrong!

■ Scenario 1: Non-SSL Landing Page



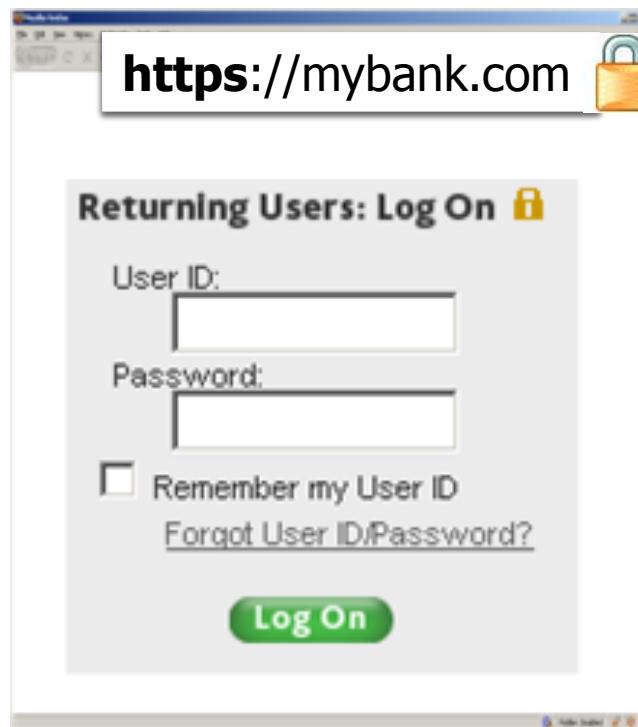
```
<form method="POST" action="https://mybank.com/login" >  
Username: <input type="text" name="user"> <br>  
Password: <input type="password" name="pass"> <br>  
</form>
```

Non-SSL Landing Page Attack

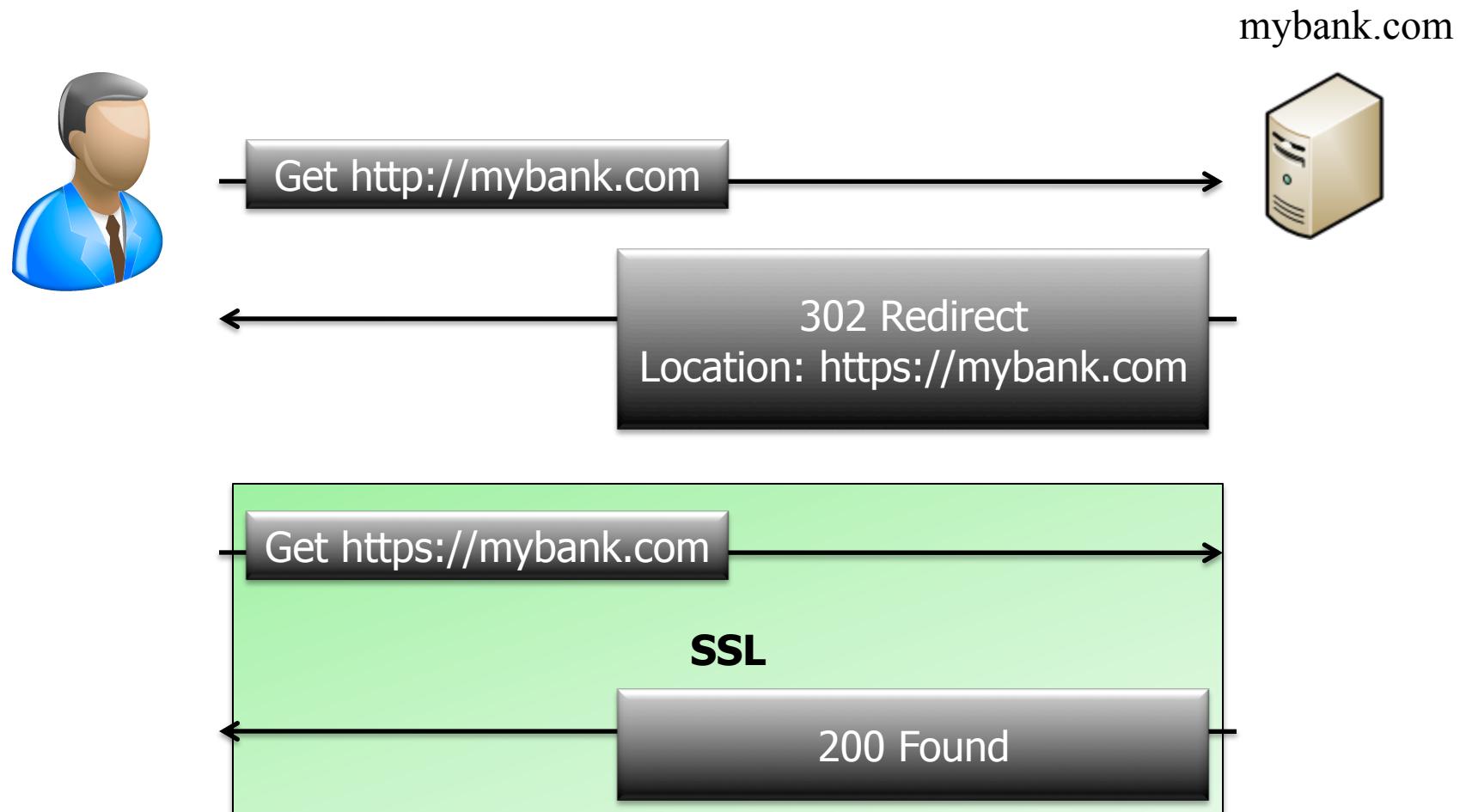


The Bad – Websites are Configured Wrong!

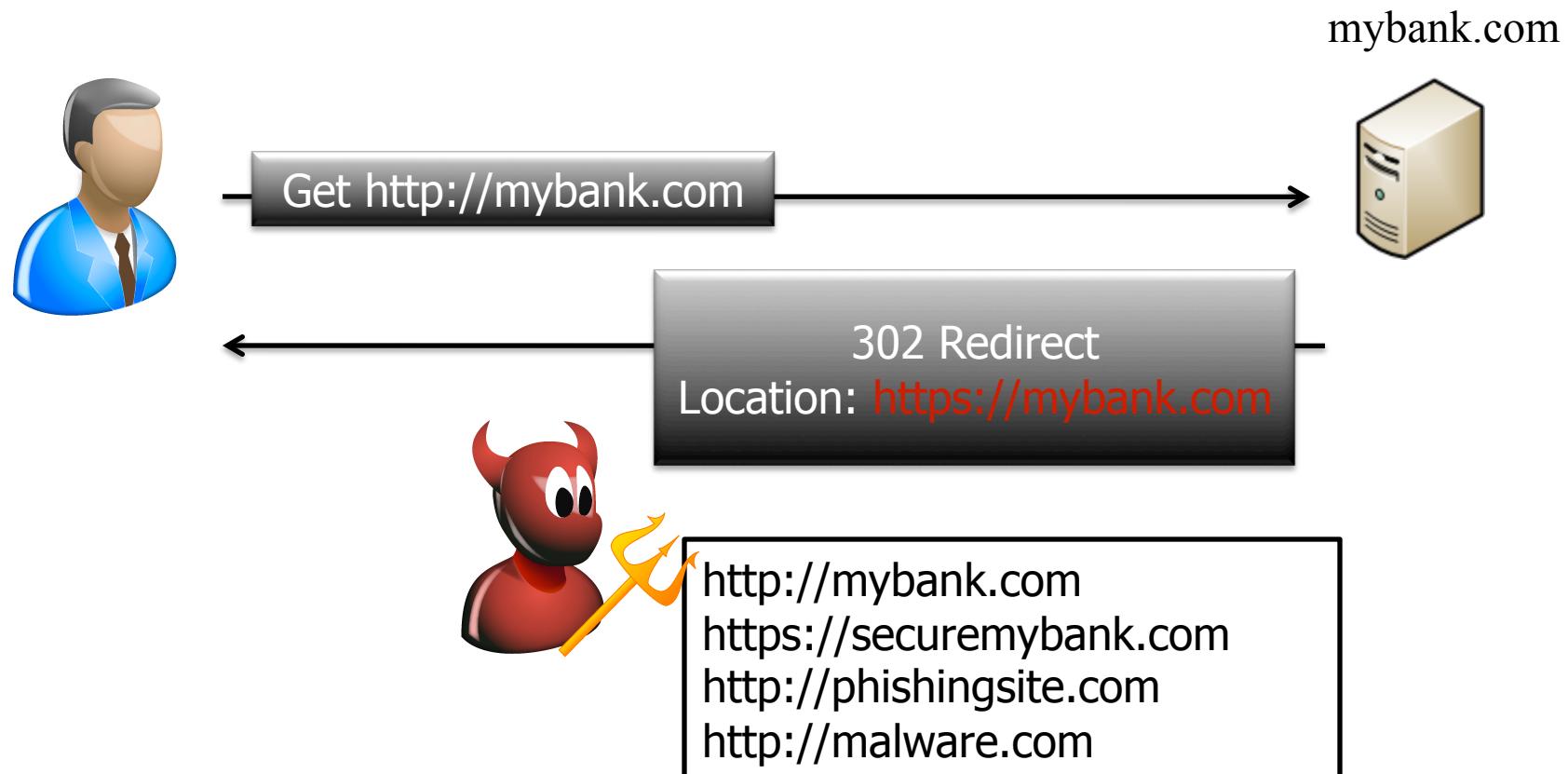
■ Scenario 2: HTTP to HTTPS redirects



HTTP to HTTPS redirects

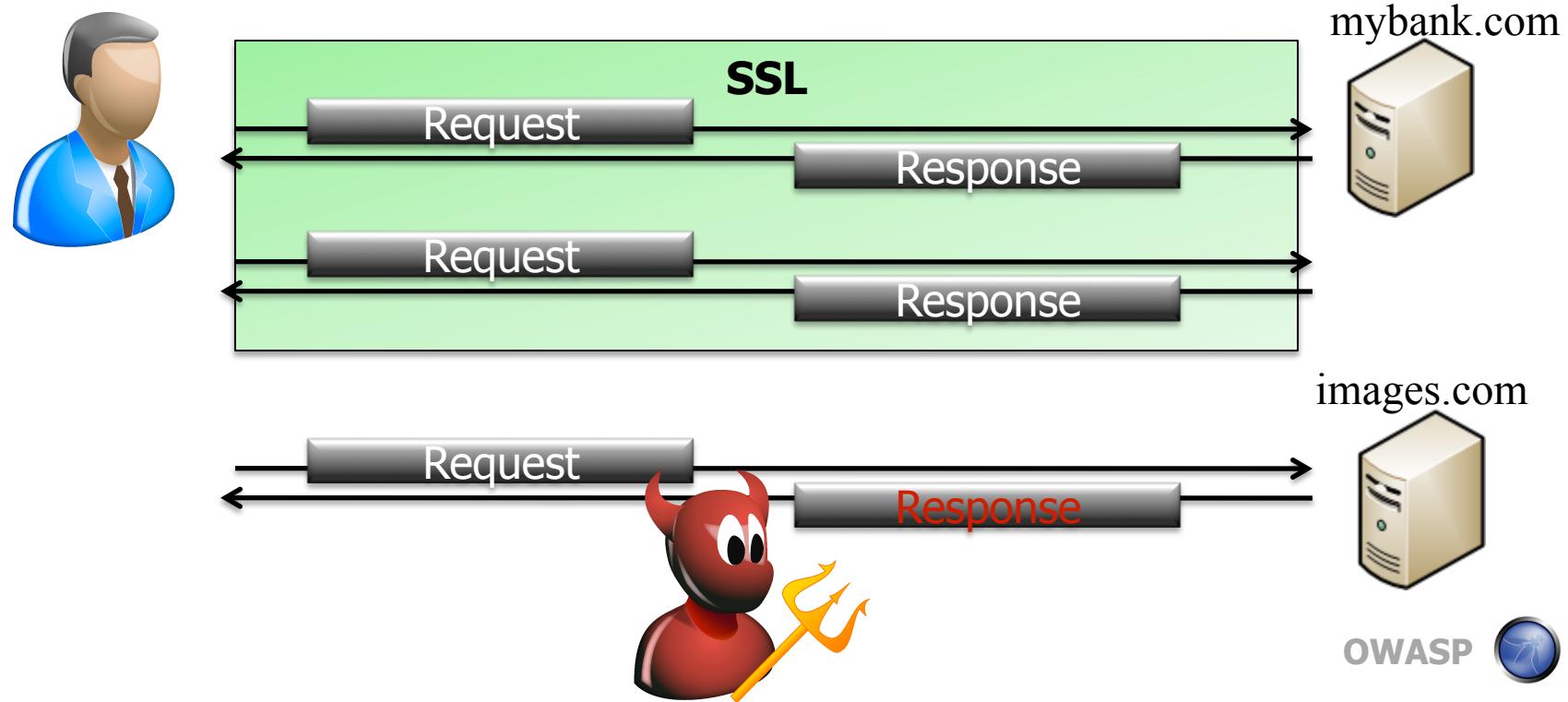
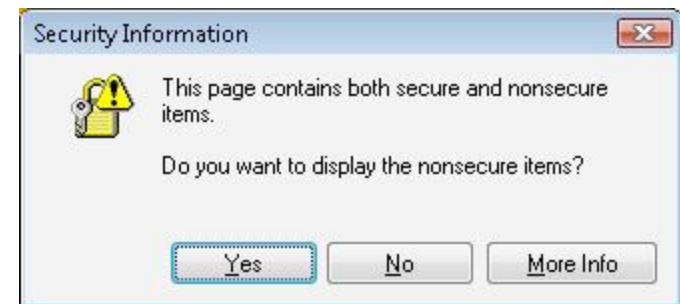


HTTP to HTTPS redirects



The Bad – Websites are Configured Wrong!

■ Scenario 3: Mixed Content



The Bad – Not All SSL is equal

■ View Ciphers by Strength

```
openssl ciphers <strength> -v
```

■ Test Server:

```
openssl s_client -connect site.com:443 -cipher <strength>
```

■ Test Client:

```
openssl s_server -www -cert cacert.pem -key cakey.pem
```

<strength>=NULL|LOW|MEDIUM|HIGH|FIPS

FIPS Approved Ciphers

*ADH-AES256-SHA
DHE-RSA-AES256-SHA
DHE-DSS-AES256-SHA
AES256-SHA
ADH-AES128-SHA
DHE-RSA-AES128-SHA
DHE-DSS-AES128-SHA
AES128-SHA
ADH-DES-CBC3-SHA
EDH-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA
DES-CBC3-SHA*

LOW Strength Ciphers

*ADH-DES-CBC-SHA
EDH-RSA-DES-CBC-SHA
EDH-DSS-DES-CBC-SHA
DES-CBC-SHA
DES-CBC-MDS*

The Ugly

■ MD5 Collision Rogue CA Creation

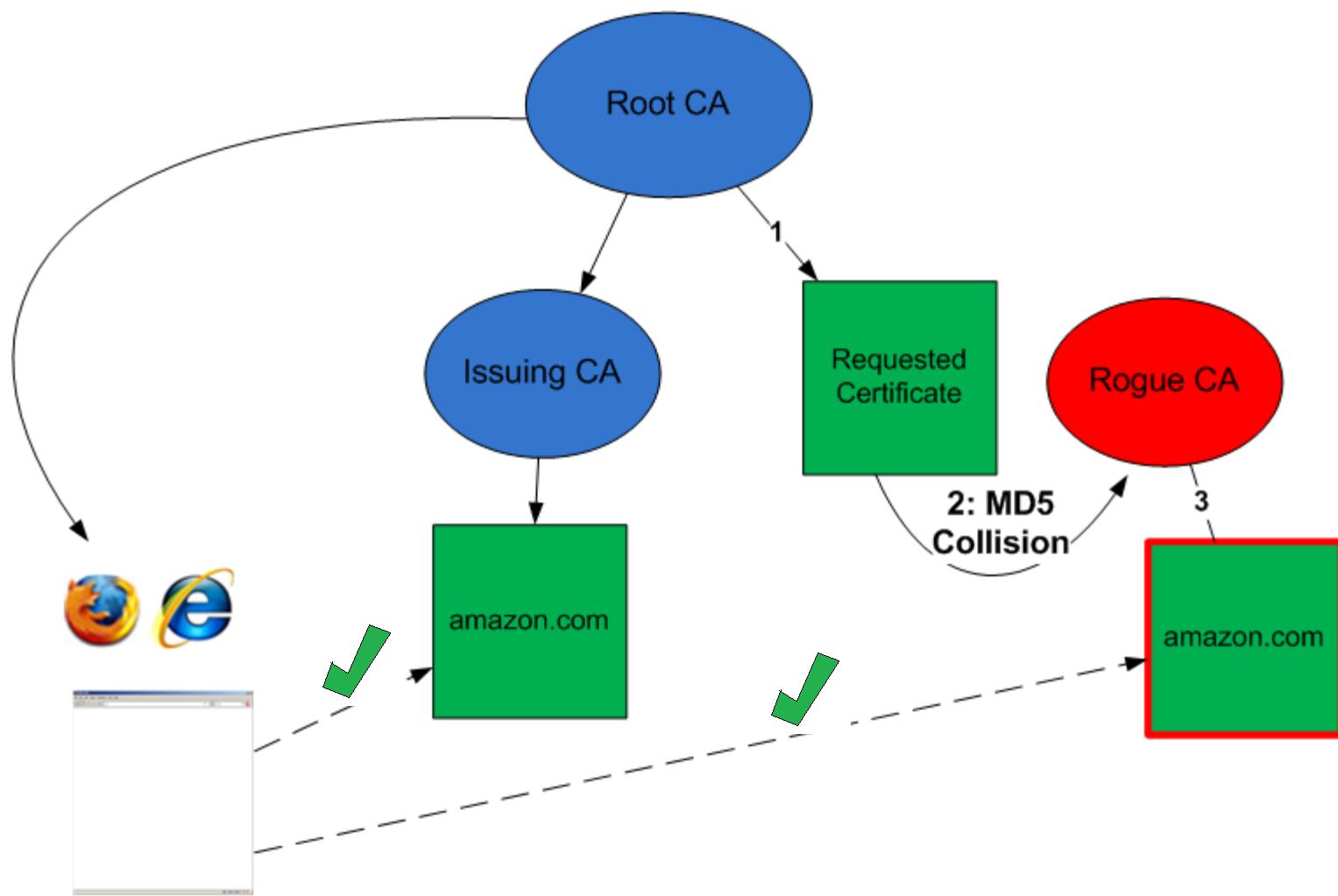
- ▶ Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger
- ▶ <http://www.win.tue.nl/hashclash/rogue-ca/>

■ SSLstrip

■ Null Prefix Attacks Against SSL/TLS Certificates

- ▶ Moxie Marlinspike
- ▶ <http://www.thoughtcrime.org/software/sslstrip/>
- ▶ <http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf>

MD5 Collision Rogue CA



Null Prefix Attack

Part 1: Certificate Authority

- CA verifies ownership of root domain

www.foo.com == www.anything.foo.com == nonexistent.a.b.c.foo.com

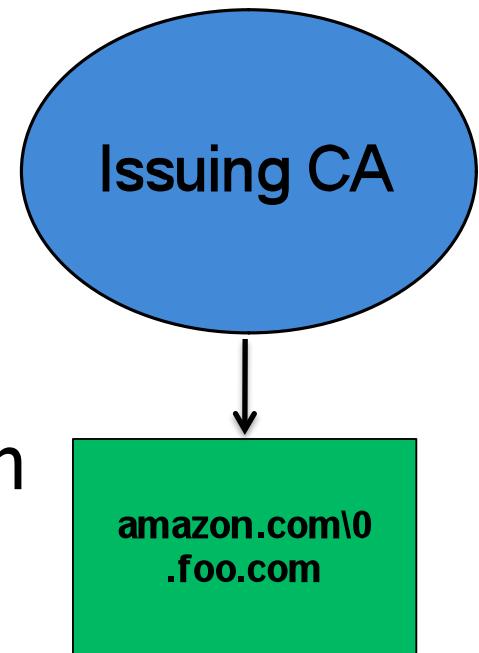
- What about? amazon.com\0.foo.com

Part 2: Browser SSL Verification

- Microsoft CryptoAPI - \0 is eos

amazon.com == amazon.com\0.foo.com

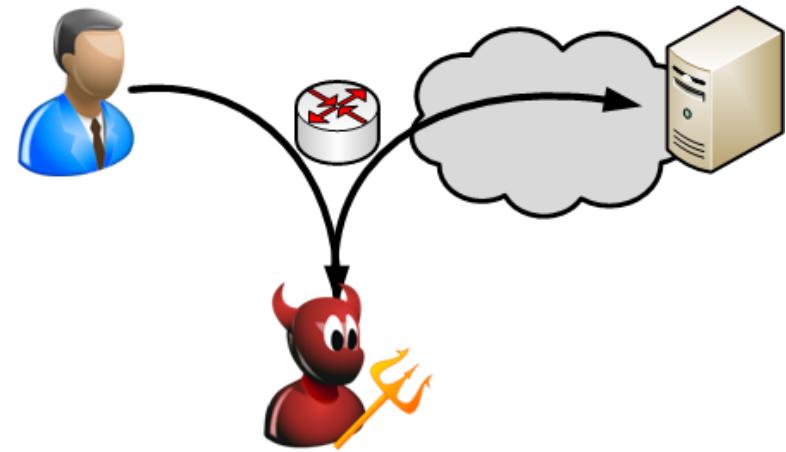
- Vulnerable: “Firefox, Internet Explorer, Chrome, Thunderbird, Outlook, Evolution, Pidgin, AIM, irssi”



SSLstrip

■ MitM SSL Connections

- ▶ ARP Spoofing
- ▶ IP Tables



■ Auto Strip SSL -> HTTPS to HTTP

■ Execute Null Prefix Attack

■ Block Certificate Revocation Messages

- ▶ OCSP Attacks

Is There Hope?

- Average User == Not Technical
- Most Deployments Vulnerable
- Specialized Tools Available

Doing It Right...



The Application

- SSL only
- No HTTP -> HTTPS redirects : HTTP shows “User Education” message
- No SSL errors or warnings

The User

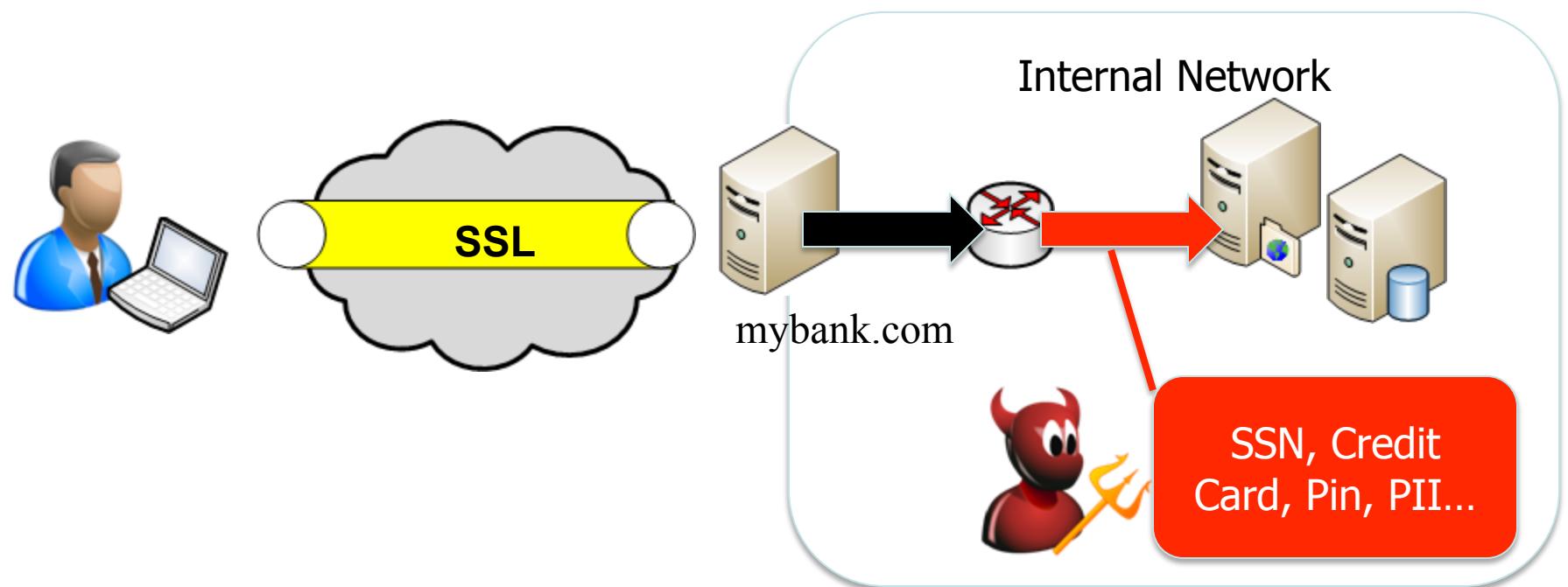
- Bookmark the HTTPS page
- Stop if any SSL warnings/errors presented

The Browser

- Set realistic user expectations
- Provide “Secure” mode option**

Internal Network SSL

- Protect the data on internal network too!



Resources - ssllabs.com (Ivan Ristic)

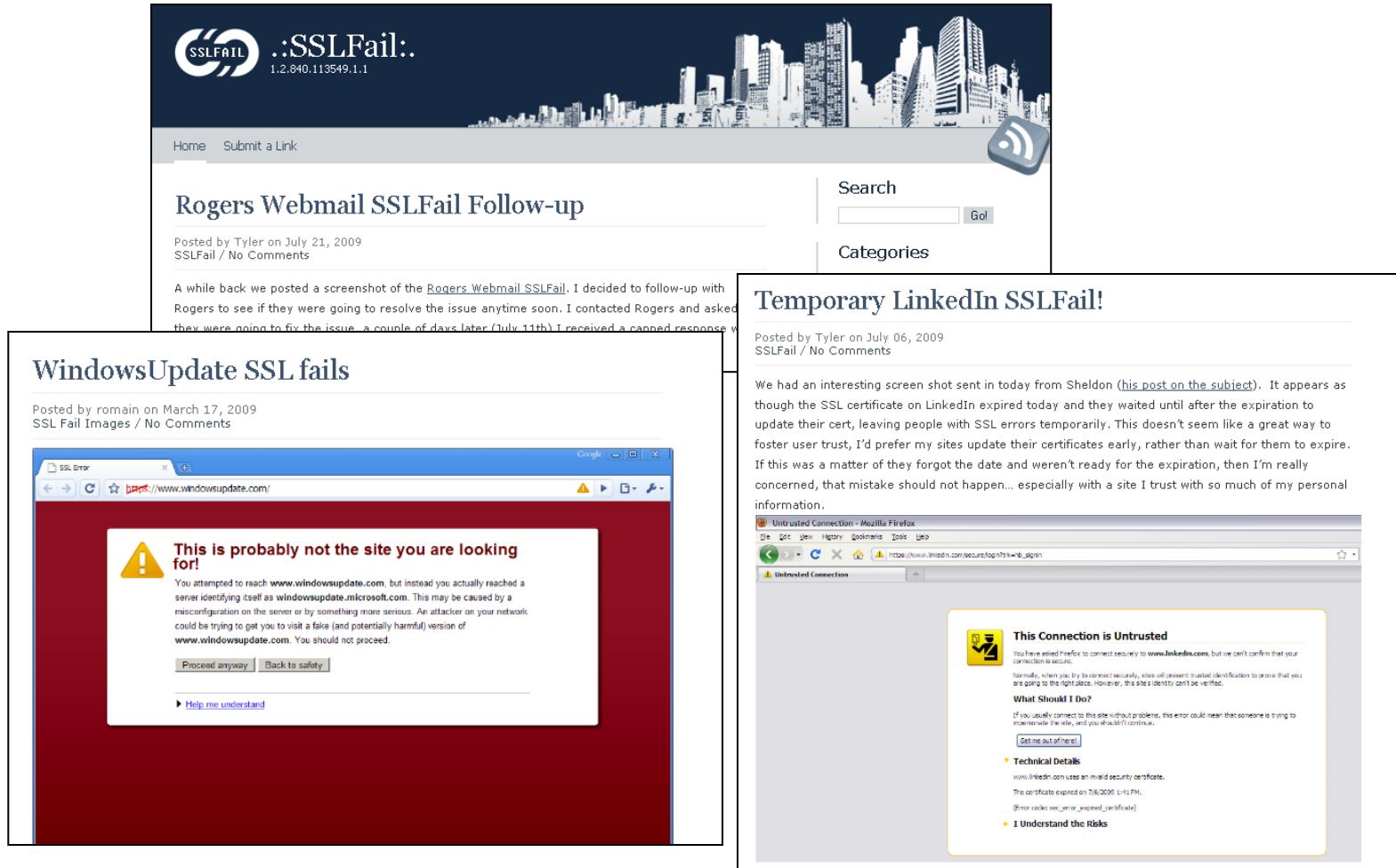


| Recently Seen | Recent Best-Rated | Recent Worst-Rated | |
|-----------------------------------|---|--|--------------|
| amazon.com | B (67) sparklit.com | A (91) webmail.verto.com.br | F (0) |
| chase.com | B (72) www.startssl.org | A (88) webmail.stiefel.com | F (0) |
| bankofamerica.com | C (60) ais2.uniba.sk | A (88) www.kaching.com | F (0) |
| gmail.google.com | C (64) blog.startcom.org | A (88) imperva.com | F (0) |

SSL Report: [amazon.com](#) (72.21.207.65)



Resources – sslfail.com (Tyler Reguly, Marcin Wielgoszewski)



The screenshot displays the SSLFail website, which is a collection of posts about SSL certificate failures. The main navigation includes 'Home' and 'Submit a Link'. The sidebar features a search bar and a 'Categories' section. The main content area shows two posts:

- Rogers Webmail SSLFail Follow-up**
Posted by Tyler on July 21, 2009
SSLFail / No Comments
A while back we posted a screenshot of the [Rogers Webmail SSLFail](#). I decided to follow-up with Rogers to see if they were going to resolve the issue anytime soon. I contacted Rogers and asked [they were going to fix the issue a couple of days later \(July 11th\)](#). I received a canned response where they said they were investigating the issue and would get back to me. I am still waiting for a response.
- Temporary LinkedIn SSLFail!**
Posted by Tyler on July 06, 2009
SSLFail / No Comments
We had an interesting screen shot sent in today from Sheldon ([his post on the subject](#)). It appears as though the SSL certificate on LinkedIn expired today and they waited until after the expiration to update their cert, leaving people with SSL errors temporarily. This doesn't seem like a great way to foster user trust. I'd prefer my sites update their certificates early, rather than wait for them to expire. If this was a matter of they forgot the date and weren't ready for the expiration, then I'm really concerned, that mistake should not happen... especially with a site I trust with so much of my personal information.

Below the posts, there are two screenshots of browser errors:

- WindowsUpdate SSL fails**
Posted by roman on March 17, 2009
SSLFail Images / No Comments
A screenshot of a Firefox browser window showing an SSL error. The message reads: "This is probably not the site you are looking for! You attempted to reach www.windowsupdate.com, but instead you actually reached a server identifying itself as [windowsupdate.microsoft.com](http://www.windowsupdate.microsoft.com). This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of www.windowsupdate.com. You should not proceed." Buttons for "Proceed anyway" and "Back to safety" are visible.
- LinkedIn SSL fail**
A screenshot of a Firefox browser window showing an SSL error. The message reads: "This Connection is Untrusted. You have selected Firefox to connect securely to www.linkedin.com, but we can't confirm that your connection is secure. Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified." It includes sections for "What Should I Do?", "Technical Details" (mentioning an invalid security certificate that expired on 7/6/2009), and "I Understand the Risks".

Thanks

■ Questions:

Lobby –or–

michael.coates@aspectsecurity.com –or–

<http://michael-coates.blogspot.com>

Ferries - Book Cheap ferries to France, Ireland, Holland and other European ferry crossings - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.aferry.co.uk/

Ferries Ferries+Hotels Hotels Disney Groups Freight Ski

Home Companies Ports Destinations Offers Timetables News Game FAQ Sitemap

Book by route Compare prices

Return Single Multi

£ Pound Sterling

(select outward route)

(select return route)

(select total passengers)

Get Price Reset

Click the map to view routes

thawte SECURE SITE

Book your perfect deal on UK and European ferries with AFerry.co.uk.

Booking ferries has never been simpler or cheaper! We work with over 60 major ferry operators including P&O Ferries, Norfolkline, Stena Line, LD Lines, Irish Ferries and many more, with access to over 800 routes.

Find ferries to France, Ireland, Spain, the rest of Europe and North Africa, taking advantage of our unique comparison engine to find the best deals.

Latest Ferry Offers

LD Lines Summer Offer! Dover - Boulogne

single from **£30**

Seafrance(Dover to Calais) Car+ 4 from just £27 each way

LD Lines(Newhaven to Dieppe) Car+ 2 from just £49 each way

Transeuropa Ferries(Ramsgate to Ostend) Car+ 4 from just £82 each way

Latest Ferry News

► [PSA: Catch ferries for festival fun 14 July 2009](#)

► [The top 10 summer camping locations in France - Part 2 13 July 2009](#)

► [The top 10 summer camping locations in France - Part 1 13 July 2009](#)

► [Brittany Ferries' St Malo service 'a revelation' 13 July 2009](#)

► [Brittany Ferries offering discount cycle hire 10 July 2009](#)

► [New tourist office opened in Dublin 10 July 2009](#)