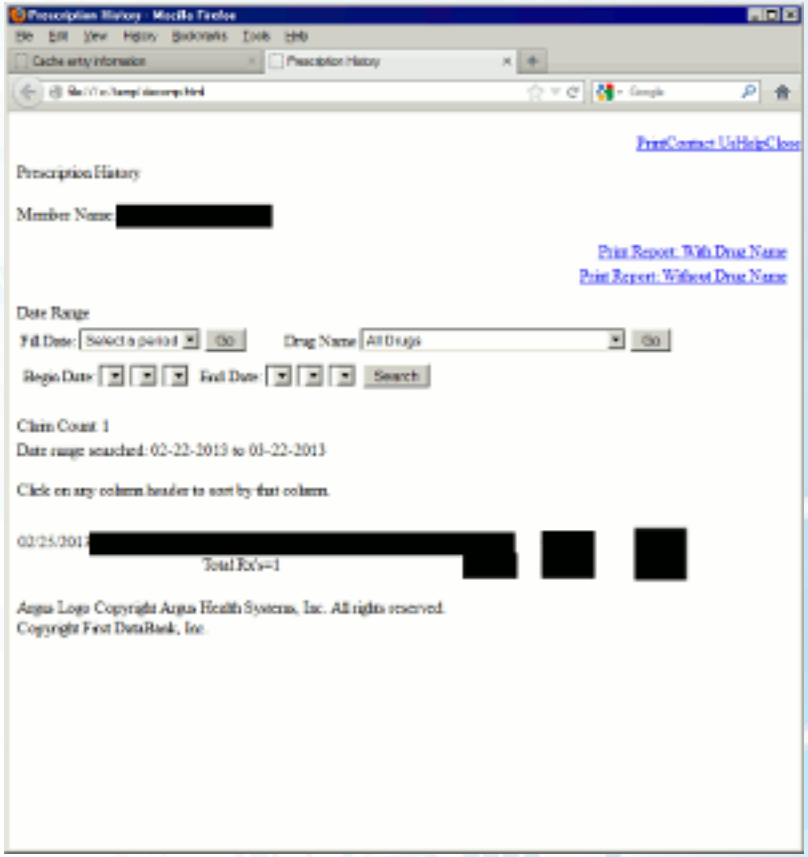
C.R.E.A.M. – Cache Rules Evidently Ambiguous, Misunderstood

Jacob Thompson
Security Analyst
Independent Security Evaluators
jthompson@securityevaluators.com

Payroll Statement from ADP

- Name
- Address
- Last four of SSN
- Last four of bank acct.

Prescription Claims from Argus



- Name
- Medication names and dosages

Credit Report from Equifax

EQUIFAX

Equifax 3-Bureau Credit Report and Scores as of March 13, 2013

Name: [redacted]

Confirmation Number: [redacted]

Section Title	Section Description
1. Credit Score	Summary, Understanding Your Score, How Lenders See You
2. Credit Report	Personal, Credit, Account, Inquiry, Public and Dispute Information

CREDIT SCORE

Section Title	Section Description
1. Credit Score Summary	Summary of how your score rates
2. Understanding Your Score	Summary of factors that are affecting your score
3. Your Loan Risk Rating	The bottom line on how lenders may view your credit risk

Credit Score Summary

Where You Stand

Equifax	Experian	TransUnion
728 Very Good	773 Excellent	728 Very Good

The Equifax Credit Score™ ranges from 280-850. Higher scores are viewed more favorably.

Your 3 credit scores are calculated by Equifax using the information contained in your Equifax, Experian, and TransUnion credit reports.

Equifax & TransUnion: Your score is considered **very good**. Based on this score, you should be able to qualify for credit with competitive interest rates, and a wide variety of credit offers should be available to you.

Experian: Your score is considered **excellent**. Based on this score, you should be able to qualify for some of the lowest interest rates available and a wide variety of competitive credit offers should be available to you.

Range	280 - 559	560 - 659	660 - 724	725 - 759	760 - 850

- Name
- Credit score
- Credit report

Types of Cached Sensitive Data

- Name
- Postal Address
- Email Address
- Phone Number
- Date of birth
- Last 4 digits of SSN
- Bank account numbers
- Check images
- Credit card account numbers
- Stock positions and balances
- Insurance policy numbers, amounts
- VINs
- Life insurance beneficiaries
- Medical prescriptions

Reliably Prevent Disk Caching

- Use two HTTP headers (not meta tags):
- Pragma: no-cache
  - IE 8 and earlier with HTTP/1.0 servers
- Cache-Control: no-store
  - All other cases

How to Fail at Preventing Caching

- Cache-Control: no-cache
  - Not standard
  - Works in IE 4-9
  - Broken in IE 10
- Pragma: no-cache
  - Only works in IE
- Cache-Control: private
  - Not for browsers
- Cache-Control in meta tags
  - Not recognized in any browser
- Cache-Control with HTTP/1.0
  - Broken in IE 4-8

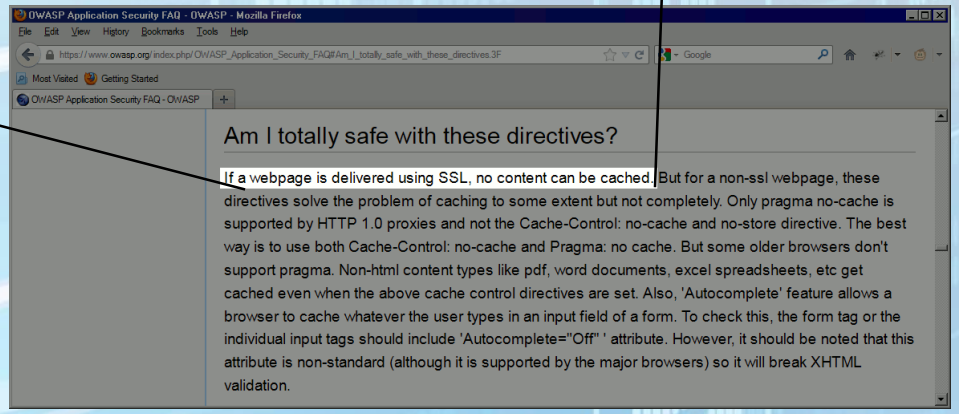
History of Disk Caching Policies

- Never cache HTTPS
  - Netscape 1, 3+
  - Mozilla
  - Firefox 1, 2
  - Safari
- Opt-in
  - Firefox 3, 3.5
- Non-standard opt-out
  - Netscape 2
  - IE 3
- Generous opt-out
  - IE 4-8
  - IE 9
  - IE 10
- Strict standards compliance
  - Chrome
  - Firefox 4+

Misunderstandings of Caching

- Google:
  - “browsers do not cache ssl”
  - “browsers do not cache https”

If a webpage is delivered using SSL, no content can be cached.



Browser Developers

- Favorite quote from Mozilla bug 531801:

> I'm on MoCo's security team :)
> Among sites that don't use cache-control:no-store, the correlation between "SSL" and "sensitive" is very low.

Recommendations

- Update web standards
- Fix web applications
- Fix bad documentation
- Fix browsers (maybe?)
- Try our demo site for yourself:
  https://demo.securityevaluators.com

Questions?

- Full report:
  http://securityevaluators.com/content/case-studies/caching/
- Demo:
  https://demo.securityevaluators.com/

A History Lesson

- 1995
  - Netscape 1 does not disk cache HTTPS content
- 1996
  - Netscape 2 is opt out: caches *unless* Pragma: no-cache header or meta tag is set
  - IE 3 copies Netscape opt-out behavior
  - Netscape 3 reverts, does not cache by default

A History Lesson (cont.)

- 1997
  - RFC 2068 introduces Cache-Control header
  - IE 4 supports Cache-Control when sent by an HTTP/1.1 server
  - Cache-Control: no-cache prevents disk caching in IE
  - Pragma: no-cache remains supported
- 1998
  - Mozilla scraps Netscape code; begins rewrite
  - Pragma: no-cache support lost in rewrite

A History Lesson (cont.)

- 2000
  - Netscape 6 released, does not cache
  - Pragma: no-cache is lost (but no one notices)
  - Apache SSL bug workaround introduced; breaks Cache-Control support in IE 4-8
- 2003
  - Safari released; never caches

A History Lesson (cont.)

- 2008
  - Firefox 3 is opt-in: caches *only* if Cache-Control: public is set
  - Chrome is opt-out: caches *unless* Cache-Control: no-store is set
  - Chrome does not support Pragma: no-cache
- 2010
  - Apache trunk patched; Cache-Control breakage now restricted to IE 4, 5

A History Lesson (cont.)

- 2011
  - Firefox 4 adopts Chrome's opt-out caching by default
  - IE 9 accepts Cache-Control headers over HTTP/1.0
- 2013
  - IE 10 caches despite Cache-Control: no-cache
  - ISE tests 30 HTTPS sites; 21 fail to set Cache-Control: no-store on sensitive data
  - IE 8 Cache-Control support still broken by Apache software in latest CentOS