Finding Gold in Your Cache

Exploring Browser Caching
By Corey Benninger, CISSP
Show Me the Money

» Credit card data from Firefox AutoComplete cache

```xml
156 Name = BackDays
157 Value = 60
158
160 Name = CCForm:CCNumberBox
161 Value = ********
162 Value = 1000
163
164 Name = CCForm:ZipCodeBox
165 Value = 10003
166
167 Name = CCNum
168 Value = ********3610
169
170 Name = Card_CCNUMBERNEW
171 Value = ********3610
172
173 Name = ChallengeAnswer
174 Value = Black
175
176 Name = CheckInControll:txtConfirmationNumber
177 Value = S1TUAK
```

This is a Client Side Attack…

» These caching issues relate to an attacker directly targeting an end user’s computer
» Most of these attacks do not require Administrator/Root level access
» Both Firefox and Internet Explorer averaged more than one new vulnerability per month in 2005*

* Data from Secunia Vulnerability Reports for Microsoft Internet Explorer 6.x and Mozilla Firefox 1.x
This is Instant Gratification…

» No need to wait for a key logger to capture data
» No need to trick a user into visiting a “trusted” website
» End user does not even need to be online or using the system
Old Skool Cache

» All your Favorite Bookmarks
  – Bookmarks to any “hard to remember” URLs (like your hidden Admin site)

» The Browser History remembers every site you visit
  – The URL of your Bank, Web Mail service, MySpace pages…

» Parameters in the URL can be cached
  – Usernames, Session IDs, Account numbers
  – Confidential information should be sent using POST, not GET, requests
Down and Dirty in the File System

» The browser can save numerous files (HTML, JPG, JS, SWF…) to the standard browser cache directory.
» Non-Session cookies can also be saved to disk.
Will Grep for Gold

» Grep for useful common input names
» `grep “ccnum|ssn|creditcard|cc_num|cvv”` *
No Cache For You!

» Sites should set proper cache control settings:
  – HTTP 1.1
    • Cache-Control: no-store, no-cache, private
  – HTTP 1.0
    • Pragma: no-cache
    • Expires: -1 (or a past date)

» Do not redisplay full credit card, social security, or account numbers.
All Your RAM are Belong to Us….

» A Normal Credential check

Whisper Sweet HTTP in My Ear.

Request:
POST /myaccount.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg
Referer: https://mybanksite.com/login2.asp
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 1.1.4322) Paros/3.1.2-Foundstone
Host: mybanksite.com
username=88903&password=p8ssWOrd%21&submit=submit

Response:
HTTP/1.1 200 OK
Date: Tue, 11 Apr 2006 01:06:19 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Pragma: no-cache
Content-Length: 49606
Content-Type: text/html
Expires: Tue, 11 Apr 2006 01:05:19 GMT
Cache-control: no-cache
Rollin’ with HTTP

» A Normal Credential check

username=bob&password=p@ssw0rd!
Haven’t I Seen You Here Before?

» A Normal Credential check

http://mybank/Login.html

http://mybank/myAccount.html
username=bob&password=p@ssw0rd!
The Vulcan Mind Meld

» Search the Memory for your favorite parameter names or URLs:
   username, password, ccnum, ssn, login, etc…
You AutoComplete Me…

![Google Autocomplete Example](image_url)
Password AutoComplete is so 1999
Rules of Form AutoComplete (... you do not talk about autocomplete)

- Form Autocomplete can only save data for input types of “text”
- Data is saved based on the “name” of the field and not limited to the URL it was entered on
- User input is required to retrieve Autocomplete data

```html
<input type="text" name="email" value=""/>
```
You AutoComplete Me Too…
Where Did it Go?

» Internet Explorer: In the Registry

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

» Firefox: In a File

C:\Documents and Settings\{username}\Application Data\Mozilla\Firefox\Profiles\default.{random}\formhistory.dat
Hungry Like the FireFox

» C:\Documents and Settings\{username}\Application Data\Mozilla\Firefox\Profiles\default.{random}\formhistory.dat
dumpAutoComplete

» Convert any FireFox “formhistory” file to XML, then parse for gold.
You May Have Data in Your AutoComplete Cache If …

» Your Credit Card Number was entered on:
  – Online Stores
  – Airline Reservation Sites
  – Hotel Reservation Sites

» Your Social Security Number was entered on:
  – Identity Theft Complaint Forms (hosted on government sites)
  – Online Resume Submissions (to a government agency)
  – Housing Applications with Universities
Chocolate and Peanut Butter Demo

» (Putting it all together.)
I’ve Fallen and I Can’t Get Up!

Simple countermeasures can prevent this data from being cached regardless of browser settings

» Disabling AutoComplete
  – Add `autocomplete="off"` to form objects or input fields when sending confidential information

» Redirect Login Forms
  – Issue a “301 Moved Permanently”, “302 Temporarily Moved”, or “303 See Other” redirect response to pages posting confidential information
These are Not the Droids You’re Looking For

» How sites can turn off AutoComplete

```html
<form action="login" method="POST" AUTOCOMPLETE="off">
  <input type="text" name="username">Name
  <input type="password" name="Password">Password
  <input type="Submit" name="Login">
</form>

<form action="SignUpForm" method="POST">
  <input type="text" name="username"> Name
  <input type="text" name="address"> Address
  <input type="text" name="ccnum" AUTOCOMPLETE="off"> Card Num
  <input type="Submit" name="Submit">
</form>
```
Whisper More Sweet HTTP in My Ear.

POST /login2.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg
Referer: https://mybanksite.com/login.asp
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
LR 1.1.422) Paros/3.1.2-Foundstone
Host: mybanksite.com
username=89703&password=p8ssWrd%21&submit=submit

GET /myaccount.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg
Referer: https://mybanksite.com/login.asp
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
LR 1.1.4322) Paros/3.1.2-Foundstone
Host: mybanksite.com
Cache-Control: no-cache

HTTP/1.1 301 Moved Permanently
Date: Tue, 11 Apr 2006 01:05:56 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Location: myaccount.asp
Content-Length: 0
Content-Type: text/html
Cache-control: private

HTTP/1.1 200 OK
Date: Tue, 11 Apr 2006 01:05:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Pragma: no-cache
Content-Length: 49777
Content-Type: text/html
Expires: Tue, 11 Apr 2006 01:04:57 GMT
Cache-control: no-cache
Finding Gold in Your Cache

Corey Benninger – Corey.Benninger@Foundstone.com

dumpAutoComplete - http://www.foundstone.com/resources/freetools.htm