

Finding Gold in Your Cache



Exploring Browser Caching
By Corey Benninger, CISSP



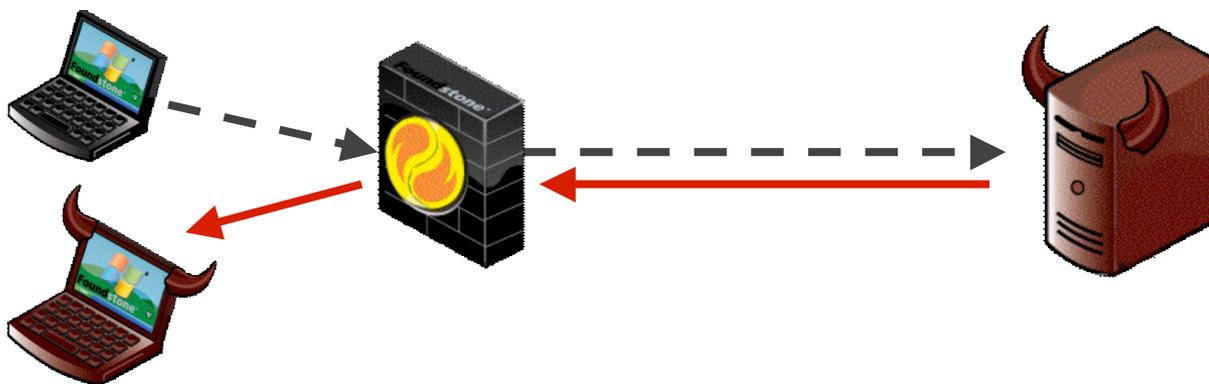
Show Me the Money

- » Credit card data from Firefox AutoComplete cache

```
156
157 Name = BackDays
158 Value = 60
159
160 Name = CCForm:CCNumberBox
161 Value = ██████████ 1000
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 = CheckInControl1:txtConfirmationNumber
177 Value = SITUAX
178
```

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

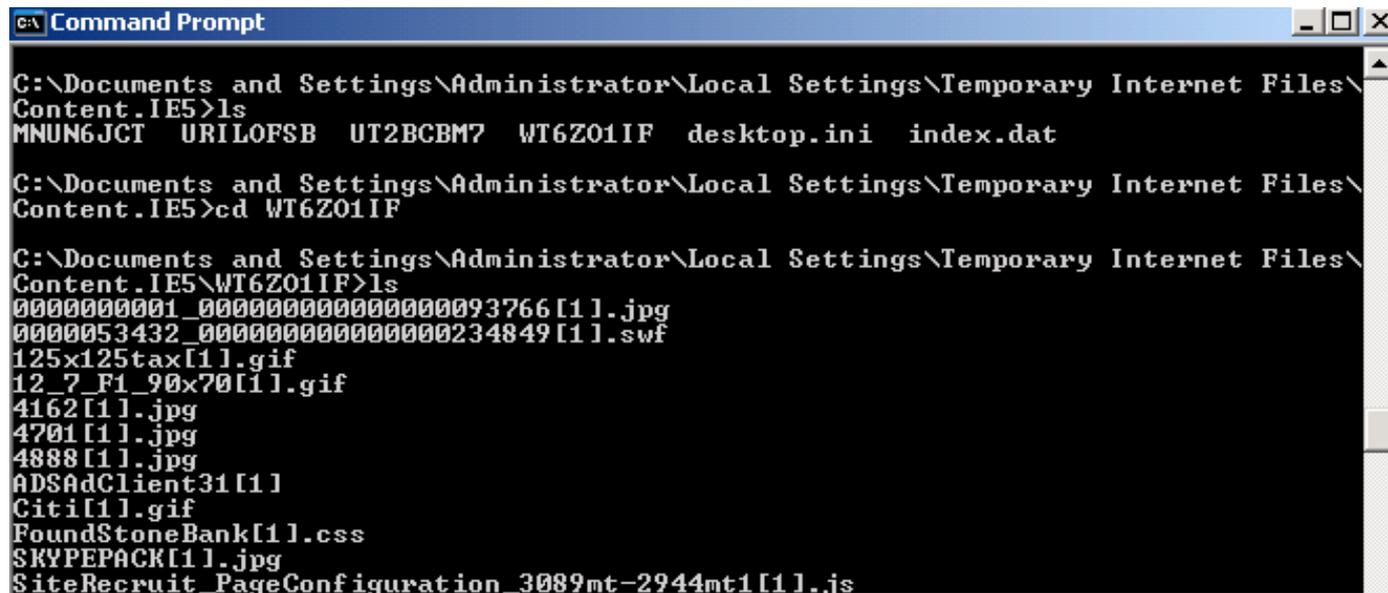
Old Skool Cache

- » 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.



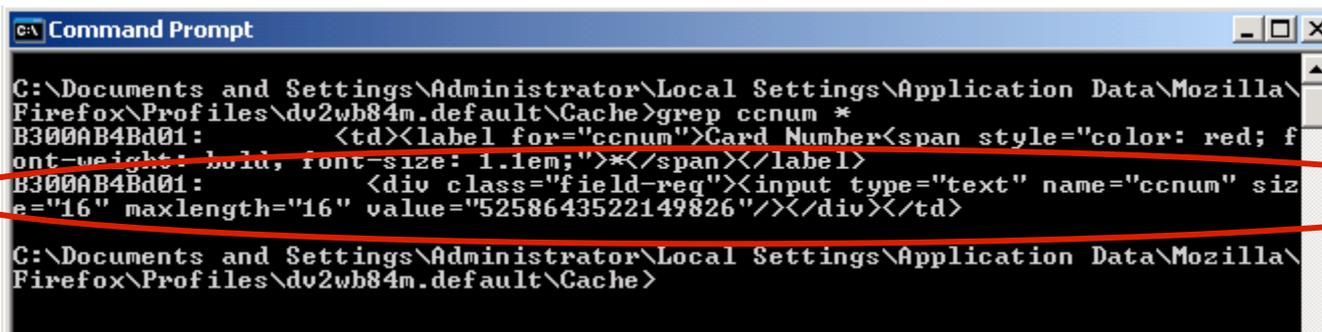
```
C:\> Command Prompt
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5>ls
MNUN6JCT  URILOFSB  UT2BCBM7  WT6Z01IF  desktop.ini  index.dat

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5>cd WT6Z01IF

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\WT6Z01IF>ls
0000000001_0000000000000000093766[1].jpg
0000053432_00000000000000000234849[1].swf
125x125tax[1].gif
12_7_F1_90x70[1].gif
4162[1].jpg
4701[1].jpg
4888[1].jpg
ADSAdClient31[1]
Citi[1].gif
FoundStoneBank[1].css
SKYPEPACK[1].jpg
SiteRecruit_PageConfiguration_3089mt-2944mt1[1].js
```

Will Grep for Gold

- » Grep for useful common input names
- » ***grep "ccnum\|ssn\|creditcard\|cc_num\|cvv" ****



```
C:\> Command Prompt
C:\Documents and Settings\Administrator\Local Settings\Application Data\Mozilla\Firefox\Profiles\dv2wb84m.default\Cache>grep ccnum *
B300AB4Bd01: <td><label for="ccnum">Card Number<span style="color: red; font-weight: bold, font-size: 1.1em;">*</span></label>
B300AB4Bd01: <div class="field-req"><input type="text" name="ccnum" size="16" maxlength="16" value="5258643522149826" /></div></td>
C:\Documents and Settings\Administrator\Local Settings\Application Data\Mozilla\Firefox\Profiles\dv2wb84m.default\Cache>
```



No Cache For You!

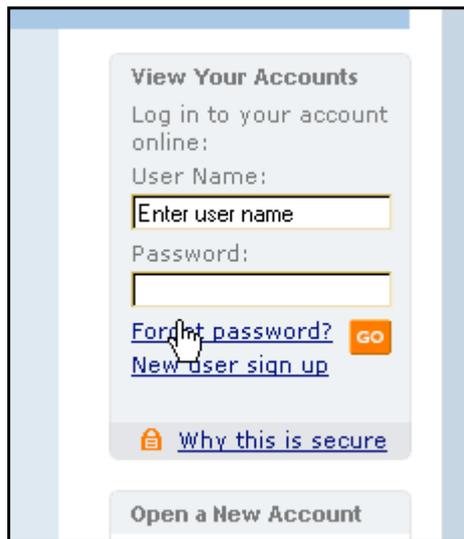
- » Sites should set proper cache control settings:
 - HTTP 1.1
 - Cache-Control: *no-store, no-cache, private*
 - HTTP 1.0
 - Pragma: *no-cache*
 - Expires: *-1 (or a past date)*

- » Do not redisplay full credit card, social security, or account numbers.

All Your RAM are Belong to Us....

» A Normal Credential check

<http://mybank/Login.html>

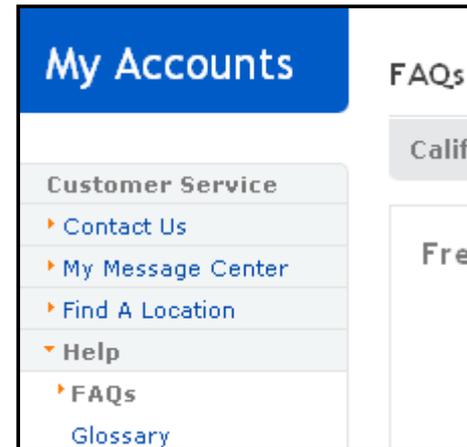


View Your Accounts
Log in to your account online:
User Name:

Password:

[Forgot password?](#)
[New user sign up](#)
 [Why this is secure](#)

<http://mybank/myAccount.html>



My Accounts

- Customer Service
 - Contact Us
 - My Message Center
 - Find A Location
 - Help
 - FAQs
 - Glossary

FAQs
Califo
Fred

Whisper Sweet HTTP in My Ear.

```
Requests Responses Trap Filters Scan Options
Header
POST /myaccount.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pj
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 N
LR 1.1.4322) Paros/3.1.2-Foundstone
Host: mybanksite.com
username=88903&password=p@sswOrd%21&submit=submit
```

```
Requests Responses Trap Filters Scan Options
Header
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: 49806
Content-Type: text/html
Expires: Tue, 11 Apr 2006 01:05:19 GMT
Cache-control: no-cache
```

Rollin' with HTTP

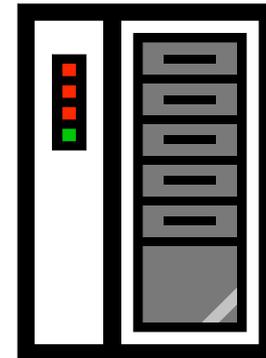
» A Normal Credential check

View Your Accounts
Log in to your account online:
User Name:

Password:

[Forgot password?](#)
[New user sign up](#)

username=bob&password=p@ssw0rd!



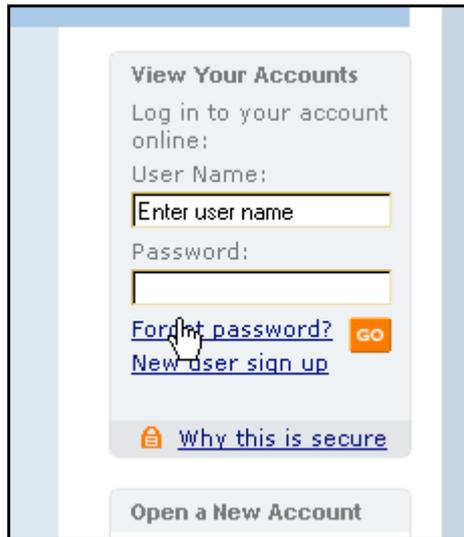
My Accounts FAQs
Califo
Fred
Customer Service
▸ Contact Us
▸ My Message Center
▸ Find A Location
▾ Help
▸ FAQs
Glossary

200 OK

Haven't I Seen You Here Before?

» A Normal Credential check

<http://mybank/Login.html>

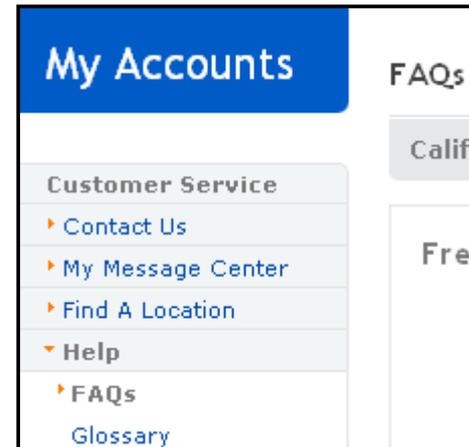


The screenshot shows a login form with the following elements:

- View Your Accounts** (Section Header)
- Log in to your account online:
- User Name:
- Password:
- [Forgot password?](#)
- [New user sign up](#)
- [Why this is secure](#)
-

<http://mybank/myAccount.html>

[username=bob&password=p@ssw0rd!](#)



The screenshot shows a navigation menu with the following items:

- My Accounts** (Section Header)
- FAQs
- Califo
- Customer Service
 - Contact Us
 - My Message Center
 - Find A Location
 - Help
 - FAQs
 - Glossary
- Fred

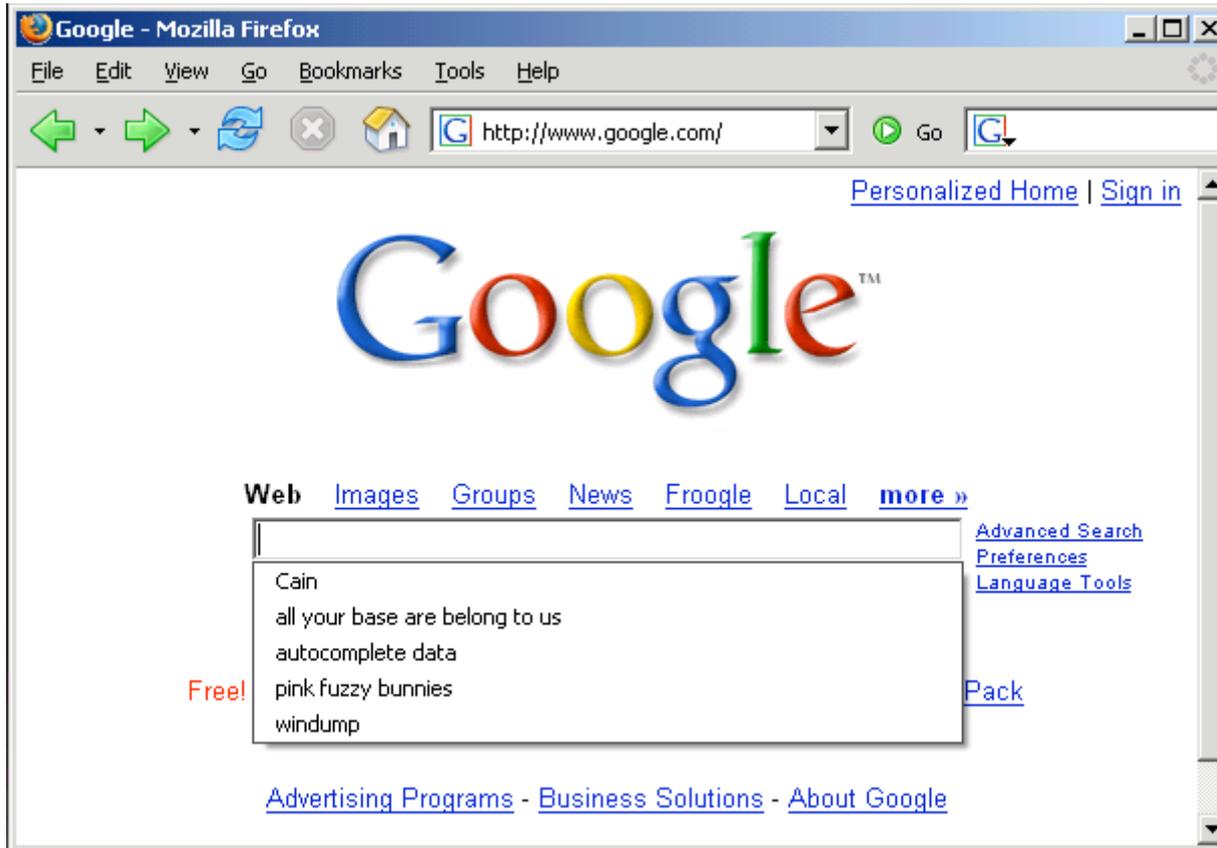


The Vulcan Mind Meld

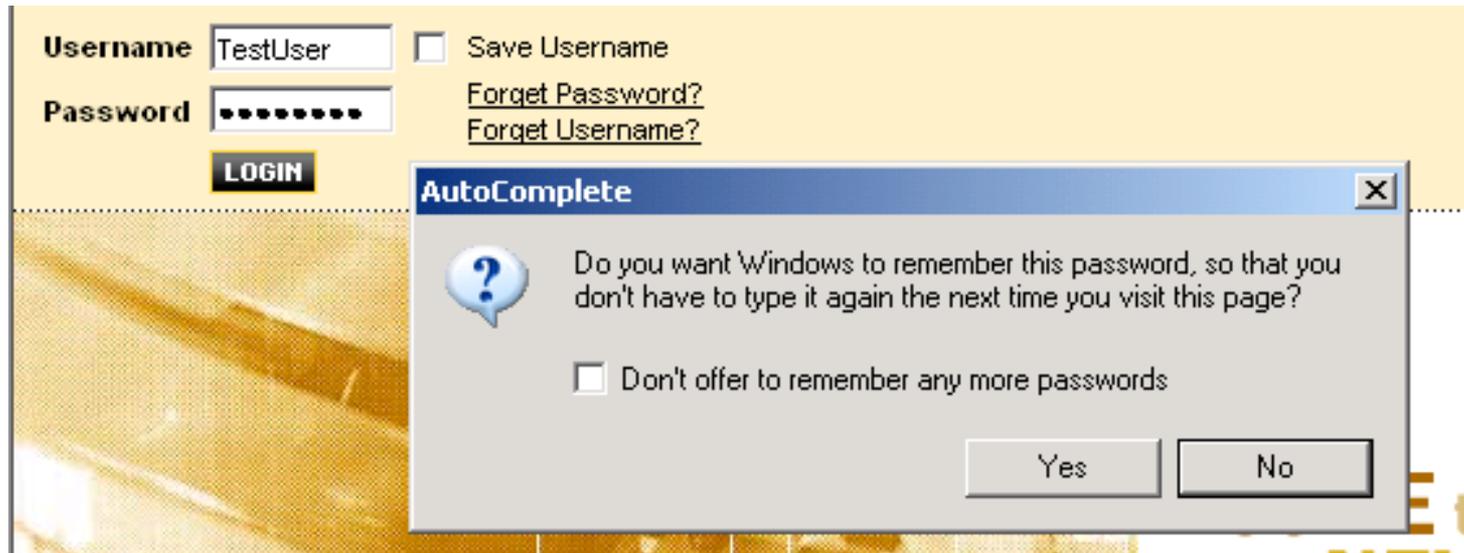
- » Search the Memory for your favorite parameter names or URLs: username, password, ccnum, ssn, login, etc...

00171C10	21 00 00 00 61 00 70 00	70 00 6C 00 69 00 63 00	!...a.p.p.l.i.c.
00171C20	61 00 74 00 69 00 6F 00	6E 00 2F 00 78 00 2D 00	a.t.i.o.n./x.-
00171C30	77 00 77 00 77 00 2D 00	66 00 6F 00 72 00 6D 00	w.w.w.-f.o.r.m.
00171C40	2D 00 75 00 72 00 6C 00	65 00 6E 00 63 00 6F 00	-u.r.l.e.n.c.o.
00171C50	64 00 65 00 64 00 01 00	00 00 32 00 00 00 75 73	d.e.d....2...us
00171C60	65 72 6E 61 6D 65 3D 38	38 39 30 33 26 70 61 73	ername=88903&pas
00171C70	73 77 6F 72 64 3D 70 40	73 73 77 30 72 64 25 32	sword=p@ssw0rd%2
00171C80	31 26 73 75 62 6D 69 74	3D 73 75 62 6D 69 74 00	l&submit=submit.
00171C90	0B 00 00 00 8A AD AC AB	21 00 00 00 68 00 74 00!-~«!...h.t.
00171CA0	74 00 70 00 73 00 3A 00	2F 00 2F 00 6D 00 79 00	t.p.s...//.m.y.
00171CB0	62 00 61 00 6E 00 6B 00	73 00 69 00 74 00 65 00	b.a.n.k.s.i.t.e.
00171CC0	2E 00 63 00 6F 00 6D 00	2F 00 6C 00 6F 00 67 00	..c.o.m./l.o.g.
00171CD0	69 00 6E 00 32 00 2E 00	61 00 73 00 70 00 0C 00	i.n.2...a.s.p...

You AutoComplete Me...



Password AutoComplete is so 1999



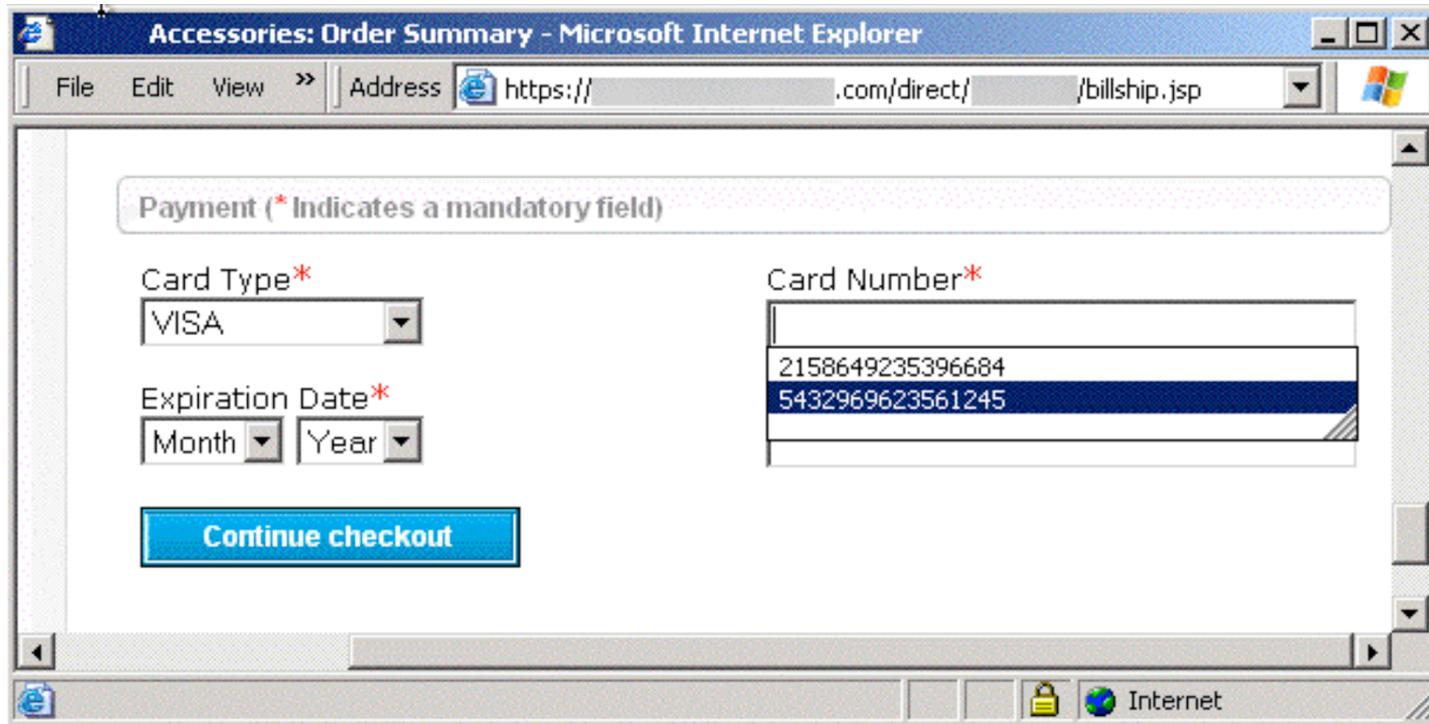


Rules of Form AutoComplete (... you do not talk about autocomplete)

- » 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

```
<input type="text" name="email" value="">
```

You AutoComplete Me Too...





Where Did it Go?

- » Internet Explorer: In the Registry

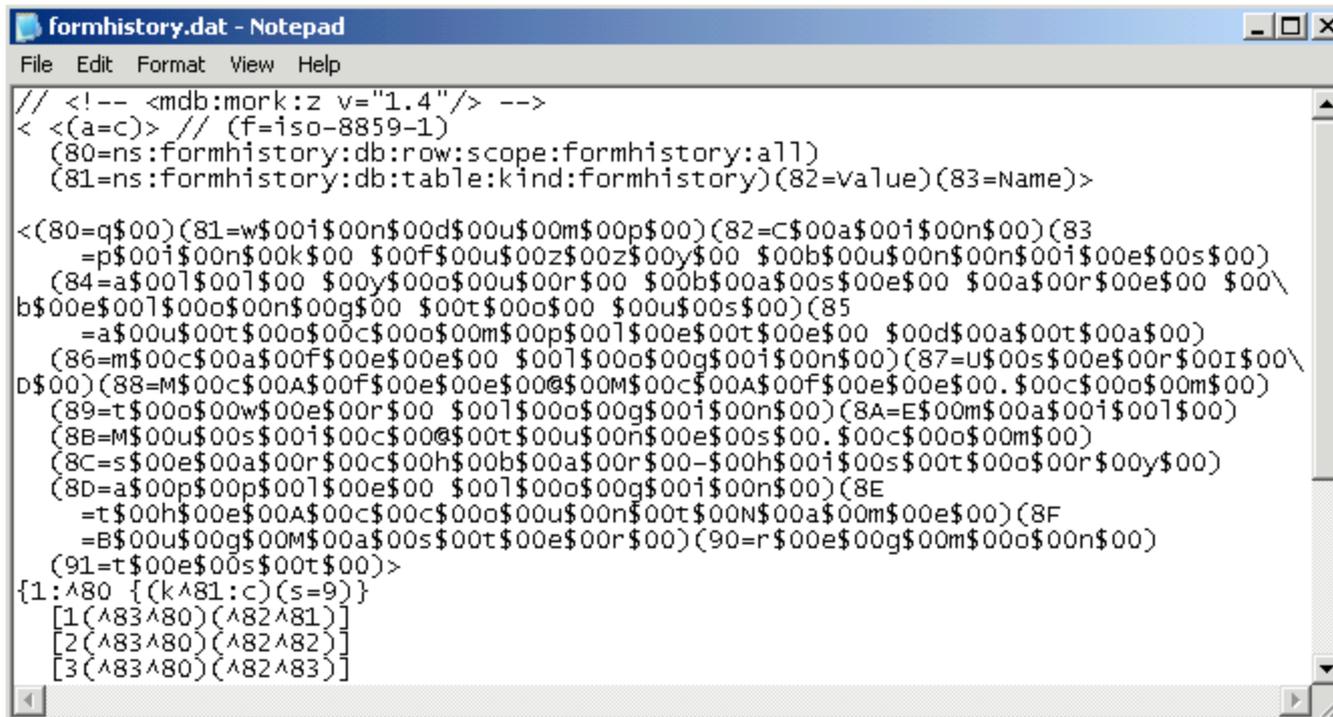
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

- » 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

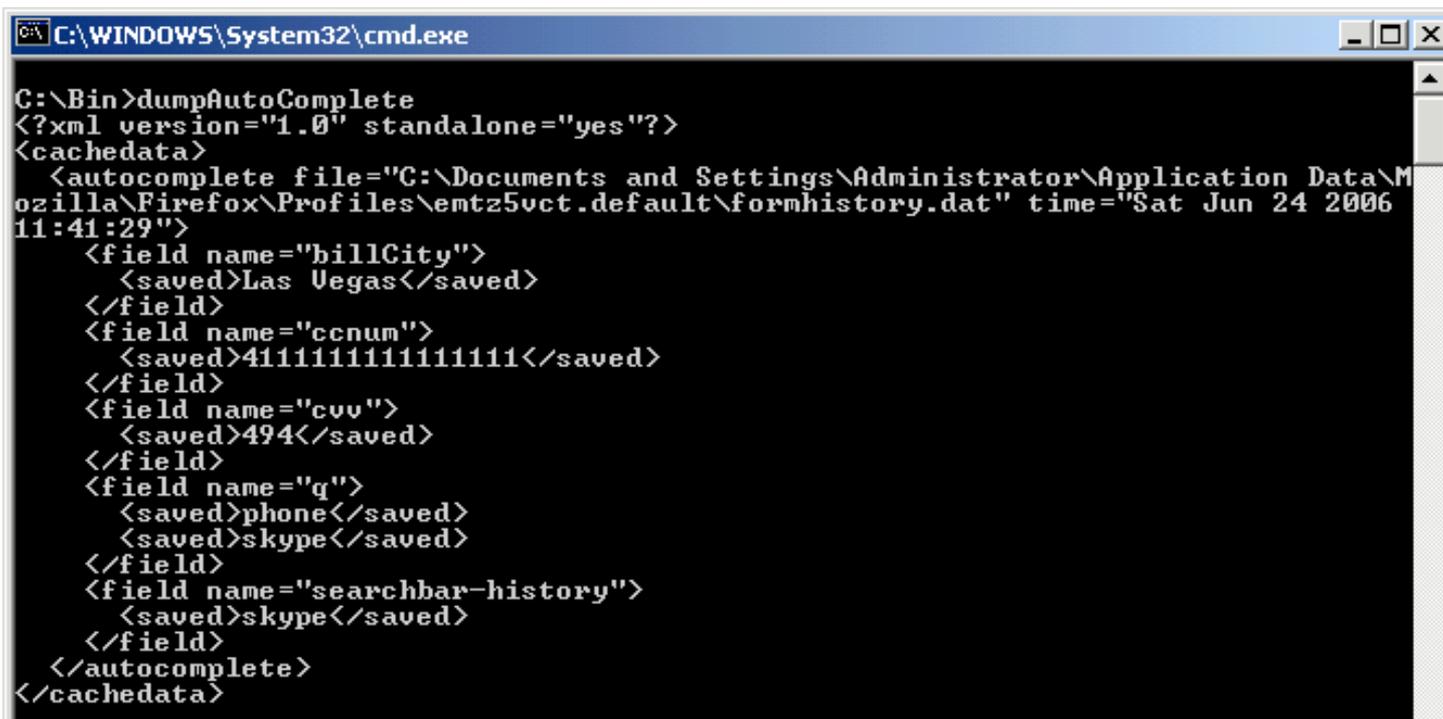


```
formhistory.dat - Notepad
File Edit Format View Help
// <!-- <mdb:mork:z v="1.4"/> -->
< <(a=c)> // (f=iso-8859-1)
(80=ns:formhistory:db:row:scope:formhistory:all)
(81=ns:formhistory:db:table:kind:formhistory)(82=value)(83=Name)>

<(80=q$00)(81=w$00i$00n$00d$00u$00m$00p$00)(82=c$00a$00i$00n$00)(83
=p$00i$00n$00k$00 $0f$00u$00z$00z$00y$00 $0b$00u$00n$00n$00i$00e$00s$00)
(84=a$00l$00l$00 $00y$00o$00u$00r$00 $00b$00a$00s$00e$00 $00a$00r$00e$00 $00\
b$00e$00l$00o$00n$00g$00 $00t$00o$00 $00u$00s$00)(85
=a$00u$00t$00o$00c$00o$00m$00p$00l$00e$00t$00e$00 $00d$00a$00t$00a$00)
(86=m$00c$00a$00f$00e$00e$00 $00l$00o$00g$00i$00n$00)(87=u$00s$00e$00r$00i$00\
d$00)(88=M$00c$00A$00f$00e$00e$00@ $00M$00c$00A$00f$00e$00e$00.$00c$00o$00m$00)
(89=t$00o$00w$00e$00r$00 $00l$00o$00g$00i$00n$00)(8A=E$00m$00a$00i$00l$00)
(8B=M$00u$00s$00i$00c$00@ $00t$00u$00n$00e$00s$00.$00c$00o$00m$00)
(8C=s$00e$00a$00r$00c$00h$00b$00a$00r$00-$00h$00i$00s$00t$00o$00r$00y$00)
(8D=a$00p$00p$00l$00e$00 $00l$00o$00g$00i$00n$00)(8E
=t$00h$00e$00A$00c$00c$00o$00u$00n$00t$00N$00a$00m$00e$00)(8F
=B$00u$00g$00M$00a$00s$00t$00e$00r$00)(90=r$00e$00g$00m$00o$00n$00)
(91=t$00e$00s$00t$00)>
{1: ^80 {(k ^81:c)(s=9)}
[1(^83^80)(^82^81)]
[2(^83^80)(^82^82)]
[3(^83^80)(^82^83)]
```

dumpAutoComplete

- » Convert any FireFox “formhistory” file to XML, then parse for gold.



```
C:\WINDOWS\System32\cmd.exe

C:\Bin>dumpAutoComplete
<?xml version="1.0" standalone="yes"?>
<cachedata>
  <autocomplete file="C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\emtz5vct.default\formhistory.dat" time="Sat Jun 24 2006 11:41:29">
    <field name="hillCity">
      <saved>Las Vegas</saved>
    </field>
    <field name="ccnum">
      <saved>4111111111111111</saved>
    </field>
    <field name="cvv">
      <saved>494</saved>
    </field>
    <field name="q">
      <saved>phone</saved>
      <saved>skype</saved>
    </field>
    <field name="searchbar-history">
      <saved>skype</saved>
    </field>
  </autocomplete>
</cachedata>
```



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

```
<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.

```
Requests Responses Trap Filters Scan Options
Header
POST /login2.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, ima
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; Wind
LR 1.1.4322) Paros/3.1.2-Foundstone
Host: mybanksite.com

username=89703&password=p@sswOrd%21&submit=submit
```

```
Requests Responses Trap Filters Scan Options
Header
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
```

```
Requests Responses Trap Filters Scan Options
Header
GET /myaccount.asp HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/j
Referer: https://mybanksite.com/login.asp
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6
LR 1.1.4322) Paros/3.1.2-Foundstone
Host: mybanksite.com
Cache-Control: no-cache
```

```
Requests Responses Trap Filters Scan Options
Header
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>