

# Demonic Possession of Browsers



BeEF issue #666

# Intros

- Who am I?
  - Mike Haworth
- What do I do?
  - Pentester for Aura Information Security
  - Contributor to BeEF project



# Same Origin Policy (SOP)

- What is SOP and why should I care?
- It's a rule enforced in the browser
- SOP is what stops a script on hacker.com from reading content on gmail.com

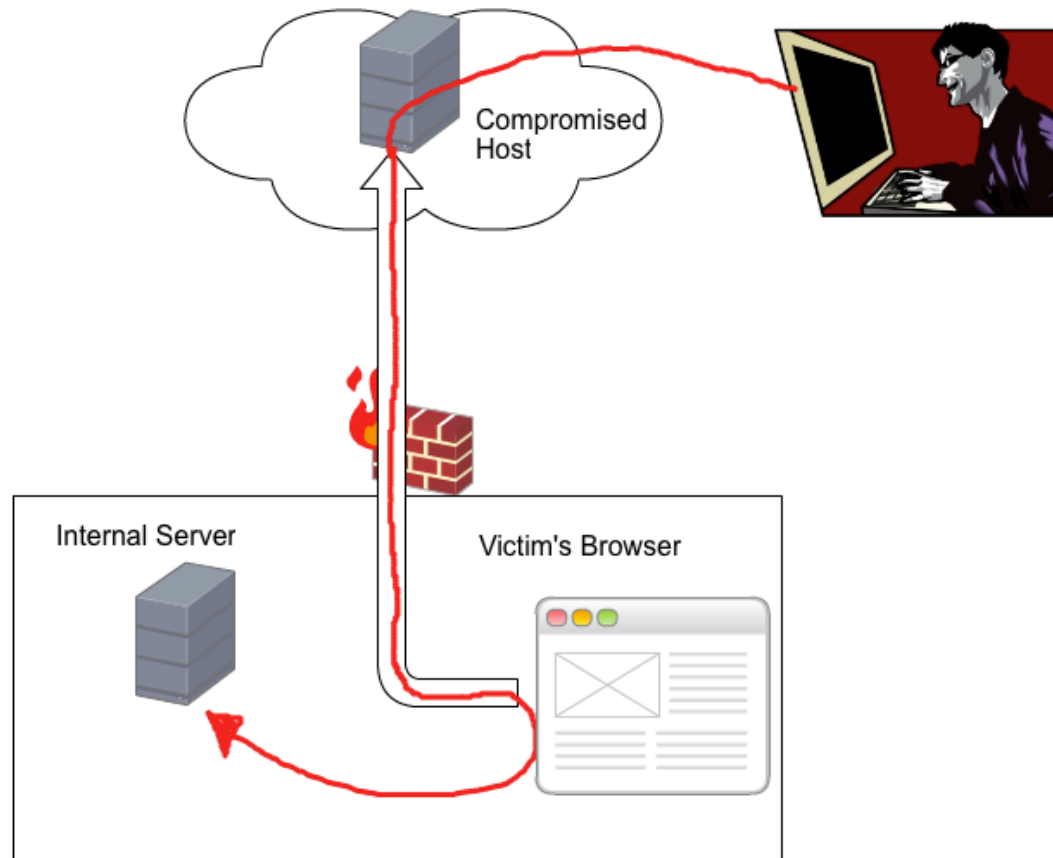
# SOP – what the docs say..

Same Origin Policy says that,  
Host, Protocol and Port must match...

URL	Outcome	Reason
<code>http://store.company.com/dir2/other.html</code>	Success	
<code>http://store.company.com/dir/inner/another.html</code>	Success	
<code>https://store.company.com/secure.html</code>	Failure	Different protocol
<code>http://store.company.com:81/dir/etc.html</code>	Failure	Different port
<code>http://news.company.com/dir/other.html</code>	Failure	Different host

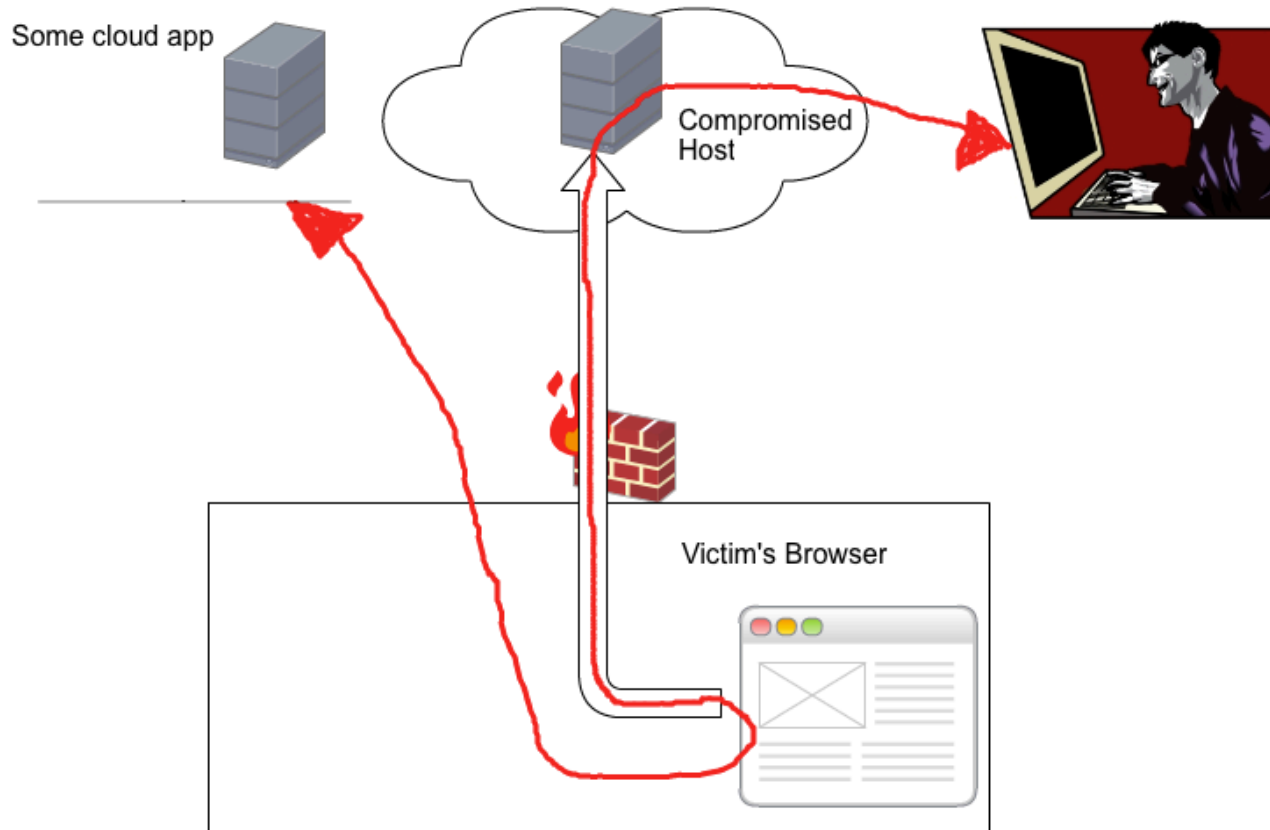
# Same Origin Policy (SOP)

- SOP, Its what stops this happening...



# Same Origin Policy (SOP)

... and this from happening.



# Ways to get an SOP bypass

- By browser issue:
  - Opera 12.02, location object bug
  - XSS into Chrome extensions
  - Dropbox, iOS
  - Safari
- By DNS, you control origin.
  - Not gonna cover this
- By WebApp issue: i.e. “Spoofing” origin via XSS
  - Or this

# Opera x-domain bug

- Overly broad access to location object of a child iframe
- Reported by Gareth Hayes ([thespanner.co.uk](http://thespanner.co.uk))



# Opera x-domain

```
iframe.contentWindow.location.constructor.prototype.  
  __defineGetter__.constructor('[]constructor.prototype.  
  join=function(){alert("PWND:"+document.body.innerHTML)}')();
```

Opera allows overwrite the array constructor of a framed page.

The bug is triggered when framed domain does `join()` on an array

# Logged in to Amazon.com

Amazon.com: Recommended for You - Opera

Opera Amazon.com: Rec... x

Secure www.amazon.com/gp/yourstore/home

amazon Join Prime

mike's Amazon.com | Today's Deals | Gift Cards | Help

Shop by Department Search All Go Hello, mike Your Account

Your Amazon.com Your Browsing History Recommended For You Amazon Betterizer Improve Your Recommendations Your Profile Lea...

Your Amazon.com

Featured Recommendations Books Electronics Kindle eBooks Music Sports & Outdoors Recom

Books

THE BASICS OF HACKING AND PENETRATION

The Web Application Hacker's Handbook


HACKING 2ND EDITION

NMAP NETWORK SCANNING

# Malicious site frames Amazon, steals data

← → ↻ 🔑 Web 172.16.1.186/opera-poc.html

## iframe

 Join Prime | mike's Amazon.com | Today's Deals | Gift Cards | Help


Shop by Department Search All Go

### Change Account Settings

**Name:** mike haworth  
**E-mail:** mike.haworth@gmail.com  
**Password:** \*\*\*\*\*  
**Mobile Phone Number:** 555555555

[Edit](#)

**JavaScript**

 <www.amazon.com>

555555555

Stop executing scripts on this page [OK](#)

# Opera bug

- Pros:
  - Its in a browser so can get data from logged in apps
- Cons:
  - Patched (post 12.02)
  - Victim domain must do [].join() to trigger bug
  - Must be able to iframe victim (X-FRAME-OPTIONS)
  - Opera browser warnings for internal sites ☹️

# XSS into Chrome Extensions

Steps:

- 1) Enumerate chrome extensions remotely
- 2) Find vulnerable extension
- 3) Inject BeEF
- 4) Can access anything extension can access
- 5) Can do lots of other stuff that's out of scope for this talk

# Chrome Extension Example

- RSS feed reader chrome extension
- Extension reads pages, provides button to subscribe to RSS in page
- Can get our JS into the context of the extension, via page

```
<link title="Slashdot RSS" data-bbox="55 730 942 781" /><img src=x onerror=badness()..
```

# XSS of Chrome Extensions

- Pros:
  - Can get *waaaay* more than just SOP bypass
  - Access to all tabs potential for RCE if using NPAPI
- Cons:
  - Content Security Policy will be enforced in 2013

More: <http://blog.kotowicz.net/>

# Stealing files outta Dropbox

- iOS app allows JavaScript to read local files!  
(via XMLHttpRequest for file://)
- Don't even have to know filename as there is a plist that contains a list of cached files  
(thanks!)

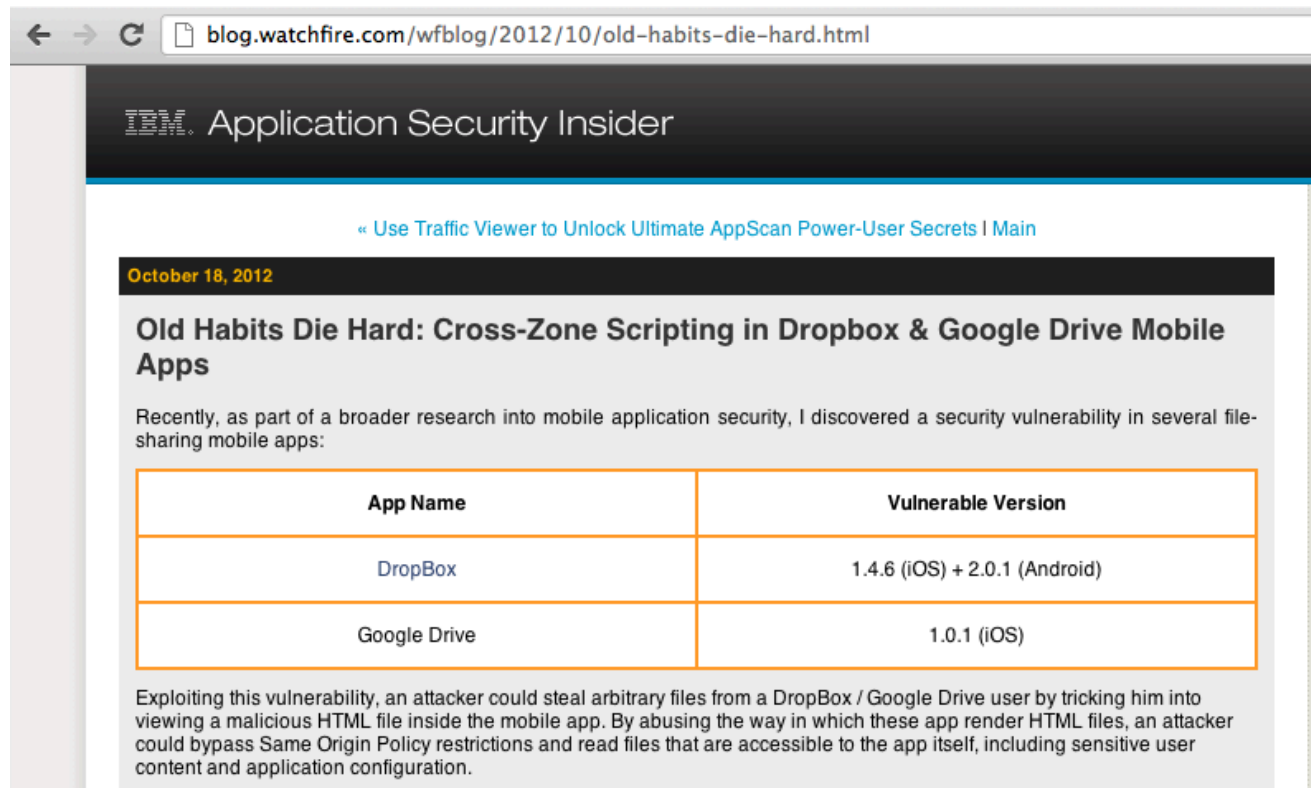


# Steal files out of Dropbox with BeEF

<http://www.youtube.com/watch?v=enKM1LWeLJk>

# Stealing files outta Dropbox

- Bug disclosed and fixed ☹️



The screenshot shows a web browser window with the address bar displaying `blog.watchfire.com/wfblog/2012/10/old-habits-die-hard.html`. The page header includes the IBM logo and the text "Application Security Insider". A navigation link reads "« Use Traffic Viewer to Unlock Ultimate AppScan Power-User Secrets | Main". The article is dated "October 18, 2012" and has the title "Old Habits Die Hard: Cross-Zone Scripting in DropBox & Google Drive Mobile Apps". The text below the title states: "Recently, as part of a broader research into mobile application security, I discovered a security vulnerability in several file-sharing mobile apps:". A table follows, listing the vulnerable versions for Dropbox and Google Drive. Below the table, the text explains that an attacker could steal files by tricking a user into viewing a malicious HTML file, bypassing Same Origin Policy restrictions.

App Name	Vulnerable Version
DropBox	1.4.6 (iOS) + 2.0.1 (Android)
Google Drive	1.0.1 (iOS)

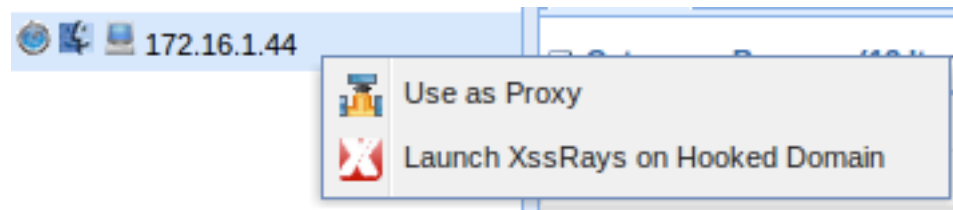
Exploiting this vulnerability, an attacker could steal arbitrary files from a DropBox / Google Drive user by tricking him into viewing a malicious HTML file inside the mobile app. By abusing the way in which these app render HTML files, an attacker could bypass Same Origin Policy restrictions and read files that are accessible to the app itself, including sensitive user content and application configuration.

# Dropbox bug

- Pros:
  - Access local files
  - Access sites on internal network
- Cons:
  - Not in a browser, no data from logged in apps.
  - Requires victim to open attacker's file in Dropbox app on iOS device.

# How does this all relate to BeEF issue #666?

- BeEF has a 'use victim as proxy' feature.



- Nice, but of limited use as need an XSS in this domain in the first place.
  - i.e. we are limited by SOP


# BeEF Issue #666


GitHub, Inc. [US] <https://github.com/beefproject/beef/issues/666>



mike-at-aura opened this issue 6 months ago

## Allow BeEF proxy to do cross-domain requests

 mike-at-aura is assigned

Milestone: 0.4.3.5-alpha 

Currently the BeEF proxy prevents cross-domain requests by design.

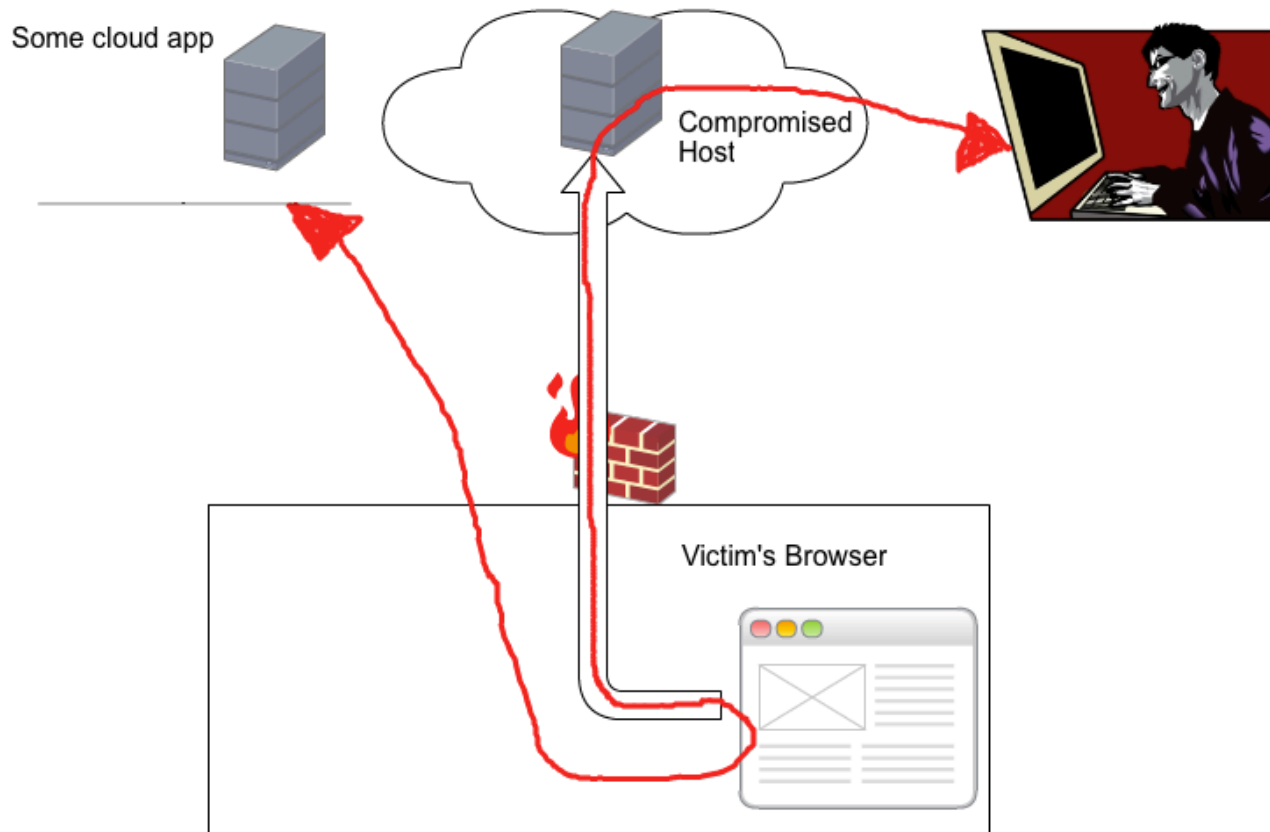
When an SOP bypass is possible it would be beneficial to be able to do cross-domain requests.

This could allow a hooked browser to serve as a proxy into an internal network.

Got the Proxy working for Cross-Domain requests!

# BeEF Cross Domain Proxy

Attacker proxies requests via victims browser



# BeEF Cross Domain Proxy

<http://www.youtube.com/watch?v=ZO7VGCjBtFQ>

# BeEFs Proxy feature

- It can be really slow
- Not that practical
- Be nice if you could just pull down Gmail messages or something useful...



# Use SOP Bypass to read gmail with BeEF

<http://www.youtube.com/watch?v=FVS8UFC-hKA>

# Safari ~~bug~~ feature

- Pros:
  - Access anything user is logged into in Safari
  - Access local files
  - It's a feature! (reported in 2k7 and still in 6.0)
- Cons:
  - Requires “spearphish” vector, user must open file from attacker

fin.