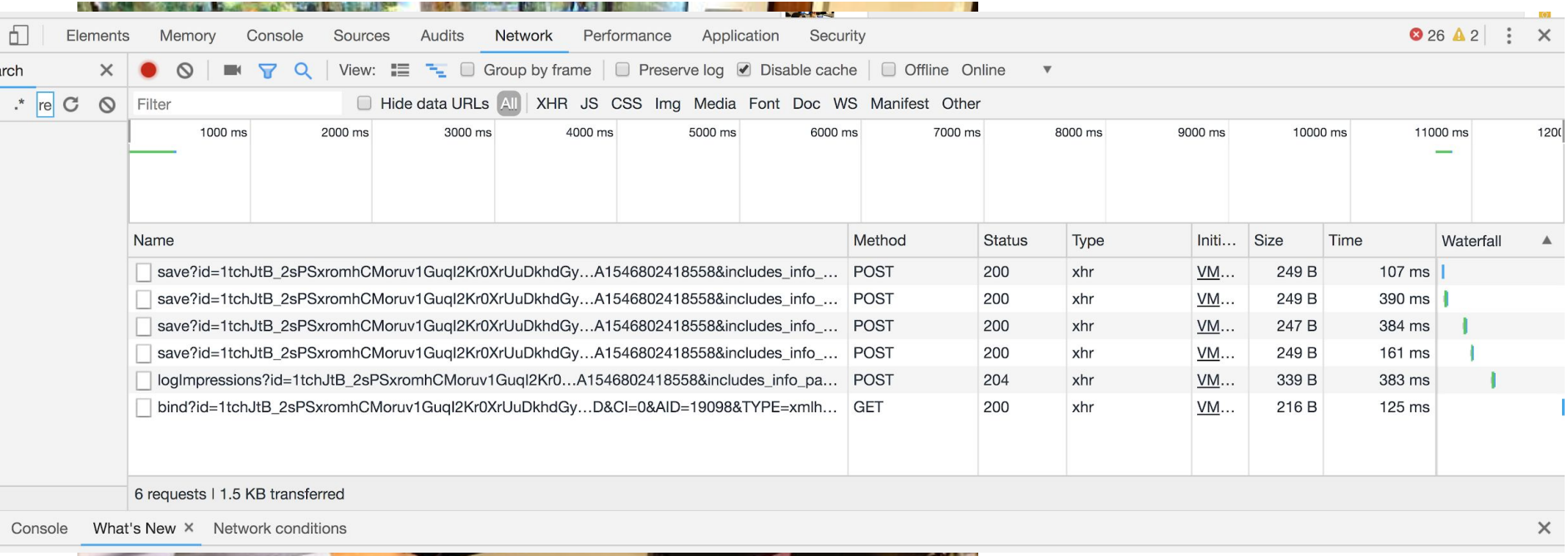
Web Security Shorts

A Healthy Skepticism for Browser Extensions

UNIVERSITY of WASHINGTON

But first... A quick story

But first... A quick story



Unexpected behavior

Request URL: https://xcvnid.vnjksuy.org/

Request Method: POST

Request Payload:

{ url: https://secure.uw.edu/app1/?t=15 }

Unexpected behavior

Request URL: https://xcvnid.vnjksuy.org/

Request Method: POST

Request Payload:

{ url: https://secure.uw.edu/app2/ }

Unexpected behavior

Request URL: https://xcvnid.vnjksuy.org/

Request Method: POST

Request Payload:

{ url: https://secure.uw.e

Compromised JavaScript Library?

Did someone break into our repo?

A more methodical approach

- Sent url for every url visited not just our secure app
- Not reproducible on a different computer
- Not reproducible in a different web browser (only Chrome)

Conclusion: Something specific about this particular Chrome install… chrome extension?

The culprit

Webpage screenshot extension

One week later

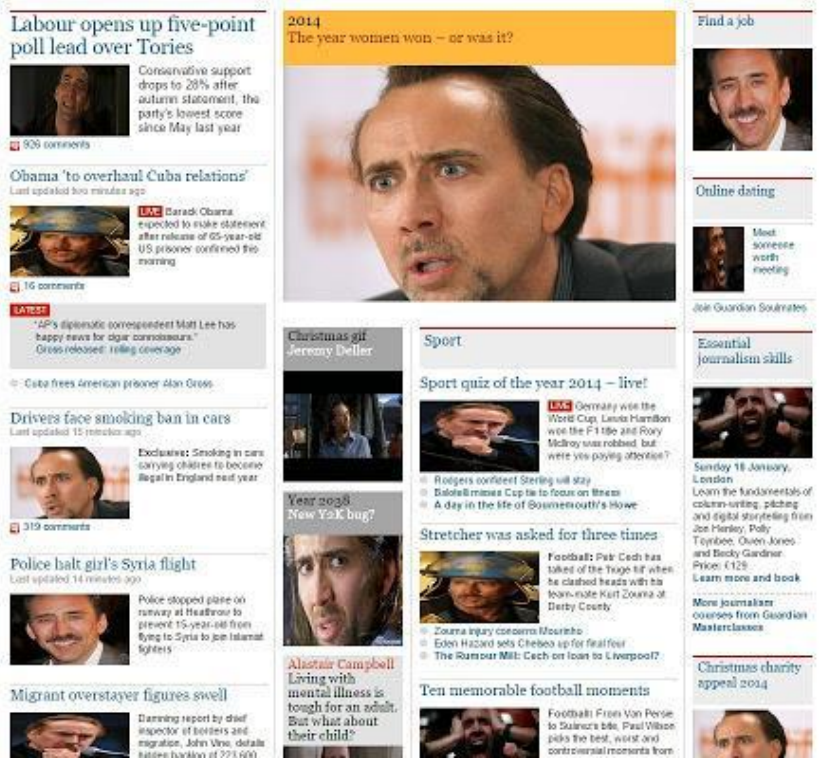
Webpage screenshot extension

Why Browser Extensions

- Improved browser experience (spell checkers, translations, screenshots, etc)
- Improved web interactions (accessibility support, tracking of bookmarks, etc)
- Fun!

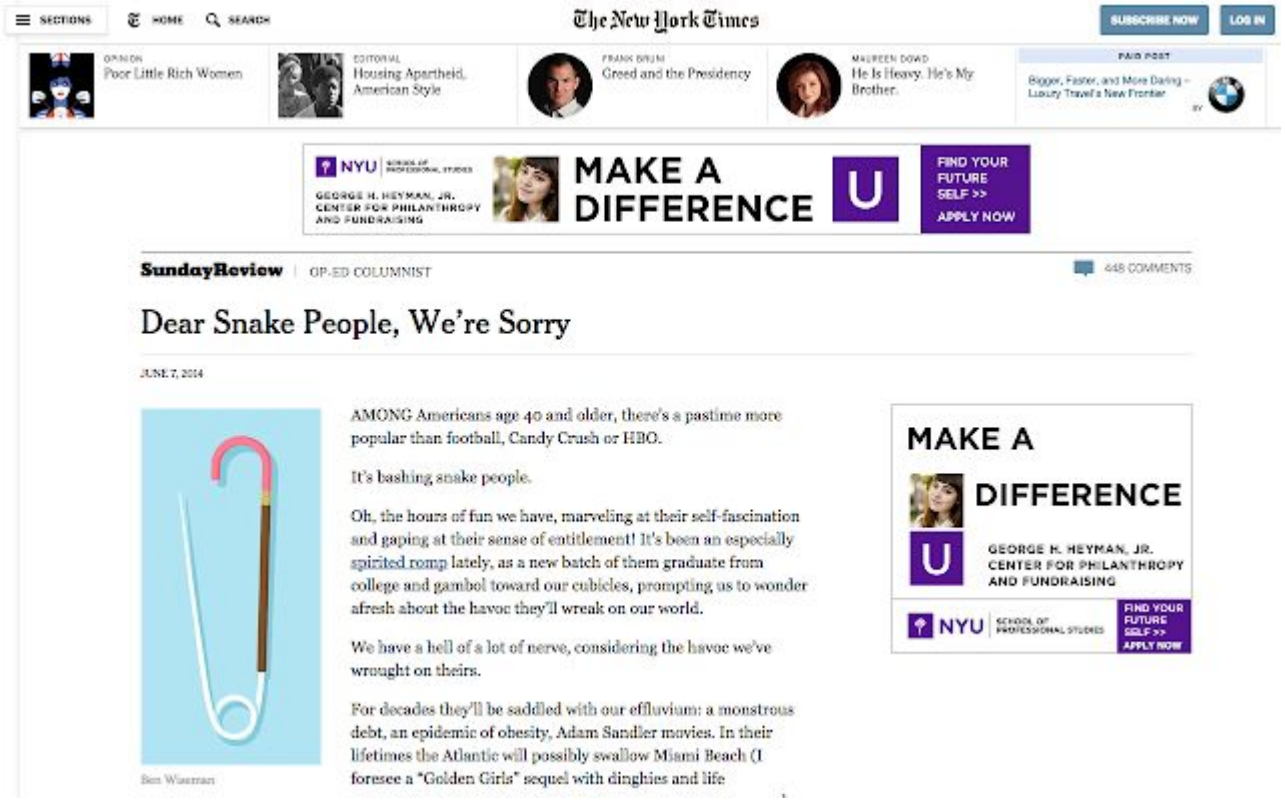
Tabby Cat

Ncage



UNIVERSITY of WASHINGTON

Millenials to Snake People



SECTIONS HOME SEARCH

The New York Times

SUBSCRIBE NOW LOG IN

OPINION
Poor Little Rich Women

EDITORIAL
Housing Apartheid, American Style

FRANK BRUNI
Greed and the Presidency

MAUREEN DOWD
He Is Heavy. He's My Brother.

PAID POST
Bigger, Faster, and More Daring – Luxury Travel's New Frontier

SundayReview | OP-ED COLUMNIST

448 COMMENTS

Dear Snake People, We're Sorry

JUNE 7, 2014

Ben Wiseman

AMONG Americans age 40 and older, there's a pastime more popular than football, Candy Crush or HBO.

It's bashing snake people.

Oh, the hours of fun we have, marveling at their self-fascination and gaping at their sense of entitlement! It's been an especially spirited romp lately, as a new batch of them graduate from college and gambol toward our cubicles, prompting us to wonder afresh about the havoc they'll wreak on our world.

We have a hell of a lot of nerve, considering the havoc we've wrought on theirs.

For decades they'll be saddled with our effluvium: a monstrous debt, an epidemic of obesity, Adam Sandler movies. In their lifetimes the Atlantic will possibly swallow Miami Beach (I foresee a "Golden Girls" sequel with dinghies and life

What can extensions do?

- Manipulate the sites you visit
- Store data
- Make requests on your behalf
- Control when a browser can be shut down
- Track your physical location
- Much much more...

https://developer.chrome.com/extensions/declare_permissions

What can you do?

- Be knowledgeable about the risks
- Be thoughtful about what you chose to install and when you chose to make the extension active
- Review permissions carefully when installing
- Review for bad comments and also for comment gaming
- Consider doing sensitive activities, such as banking, bill paying, etc. on a browser without extensions installed

https://lifehacker.com/how-to-tell-legit-chrome-extensions-from-malware-1825423984

Questions?

Peter Giles
gilesp@uw.edu

Pete Graff
pgraff@uw.edu

Zephyr McLaughlin
zephyrmc@uw.edu