



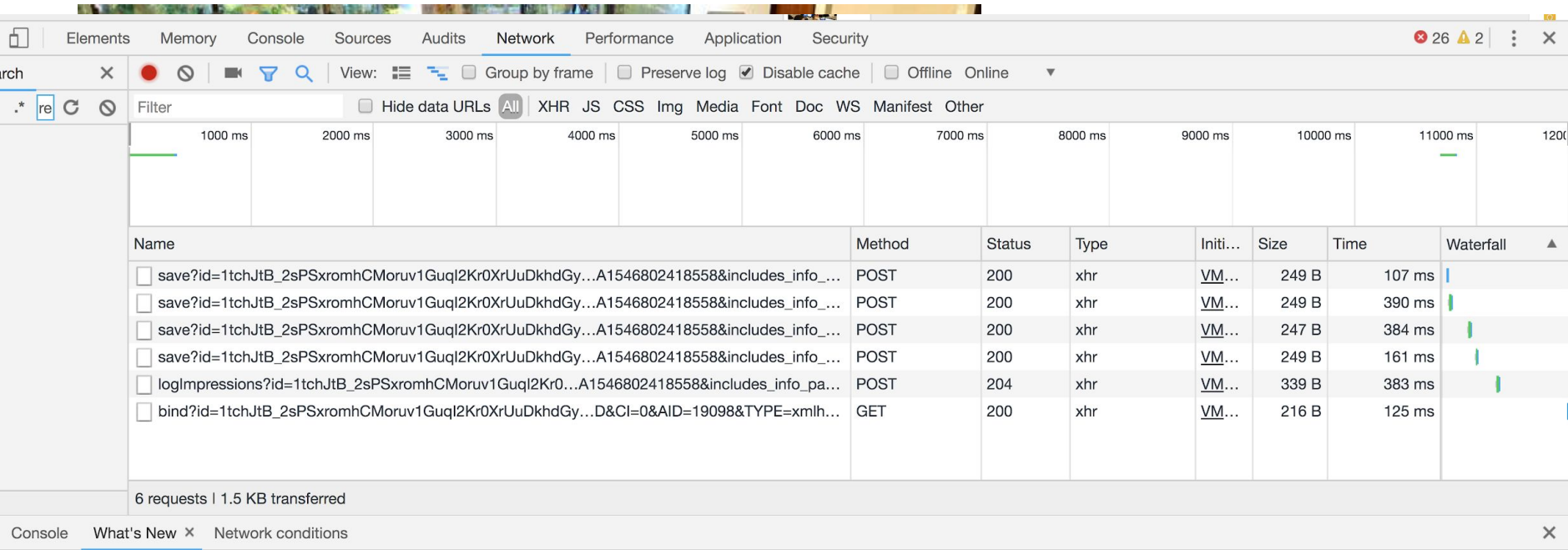
Web Security Shorts

A Healthy Skepticism for Browser Extensions

But first.. A quick story



But first.. A quick story



Network tab showing 6 requests. The requests are:

Name	Method	Status	Type	Initi...	Size	Time	Waterfall
<input type="checkbox"/> save?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0XrUuDkhdGy...A1546802418558&includes_info_...	POST	200	xhr	VM...	249 B	107 ms	
<input type="checkbox"/> save?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0XrUuDkhdGy...A1546802418558&includes_info_...	POST	200	xhr	VM...	249 B	390 ms	
<input type="checkbox"/> save?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0XrUuDkhdGy...A1546802418558&includes_info_...	POST	200	xhr	VM...	247 B	384 ms	
<input type="checkbox"/> save?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0XrUuDkhdGy...A1546802418558&includes_info_...	POST	200	xhr	VM...	249 B	161 ms	
<input type="checkbox"/> logImpressions?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0...A1546802418558&includes_info_pa...	POST	204	xhr	VM...	339 B	383 ms	
<input type="checkbox"/> bind?id=1tchJtB_2sPSxromhCMoruv1Guql2Kr0XrUuDkhdGy...D&CI=0&AID=19098&TYPE=xmlh...	GET	200	xhr	VM...	216 B	125 ms	

6 requests | 1.5 KB transferred



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.edu>



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

★★★★☆ 16,296

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



FURRY POCKY

Ncage

Labour opens up five-point poll lead over Tories

Conservative support drops to 26% after autumn statement, the party's lowest score since May last year

920 comments

Obama 'to overhaul Cuba relations'

Last updated 6m 45s ago

Like Barack Obama expected to make statement after release of 65-year-old US prisoner confirmed this morning

16 comments

LATEST

GP's diplomatic correspondent Matt Lee has happy news for cigar connoisseurs.
Gross releases: rolling coverage

• Cuba frees American prisoner Alan Gross

Drivers face smoking ban in cars

Last updated 15 minutes ago

Exclusive: Smoking in cars carrying children to become illegal in England next year

319 comments

Police halt girl's Syria flight

Last updated 14 minutes ago

Police stopped plane on runway at Heathrow to prevent 15-year-old from flying to Syria to join Islamist fighters

Migrant overstayer figures swell

Dramatic report by chief inspector of borders and migration, John Vines, details massive backlog of 993,640

2014

The year women won – or was it?

Find a job

Online dating

Most interesting worth meeting

Join Guardian Soulmates

Essential journalism skills

Sunday 14 January, London
LEARN the fundamentals of column-writing, pitching and digital storytelling from Joe Hootley, Polly Toynbee, Owen Jones and Becky Gardner
Price: £125
Learn more and book

More journalism courses from Guardian Masterclasses

Christmas charity appeal 2014

Christmas gift

Jeremy Deller

Sport

Sport quiz of the year 2014 – live!

Like Germany win the World Cup, Lewis Hamilton won the F1 title and Rory McIlroy was robbed, but were you paying attention?

- Rodgers confident Sterling will stay
- Bale still misses Cup tie to focus on fitness
- A day in the life of Southampton's Howe

Stretcher was asked for three times

Football: Petr Cech has taken of the Tugce lift when he clashed heads with the team-mate Karl Zouna at Derby County

- Zouna injury concerns Mourinho
- Eden Hazard sets Chelsea up for final four
- The Rumour Mill: Cech on loan to Liverpool?

Ten memorable football moments

Football: Eric van Persie to Sainsbury's bid, Paul Wilson joins the best, worst and controversial moments from

Millenials to Snake People

SECTIONS HOME SEARCH The New York Times SUBSCRIBE NOW LOG IN

OPINION Poor Little Rich Women EDITORIAL Hoousing Apartheid, American Style FRANK BRUM Greed and the Presidency MALREEN DOWD He Is Heavy. He's My Brother. PAID POST Bigger, Faster, and More Dating - Luxury Travel's New Frontier

NYU SCHOOL OF PROFESSIONAL STUDIES MAKE A DIFFERENCE U FIND YOUR FUTURE SELF >> APPLY NOW

GEORGE H. HEYMAN, JR. CENTER FOR PHILANTHROPY AND FUNDRAISING

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 effluvia: 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

MAKE A



DIFFERENCE



GEORGE H. HEYMAN, JR. CENTER FOR PHILANTHROPY AND FUNDRAISING



SCHOOL OF PROFESSIONAL STUDIES

FIND YOUR FUTURE SELF >> APPLY NOW

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

