Concrete Steps to Create a Culture of Security

Arkadiy Tetelman / BSidesSF 2019

AGENDA

- Why does it matter
- Concrete examples
- Guiding principles
- Measuring success
- Questions

WHO AM I

- Arkadiy Tetelman (@arkadiyt)
- Staff Application Security at Lob
- Previously appsec at Airbnb, Twitter
- Fun fact: I don’t know how to ride a bike

Why does security culture matter

WHY DOES SECURITY CULTURE MATTER

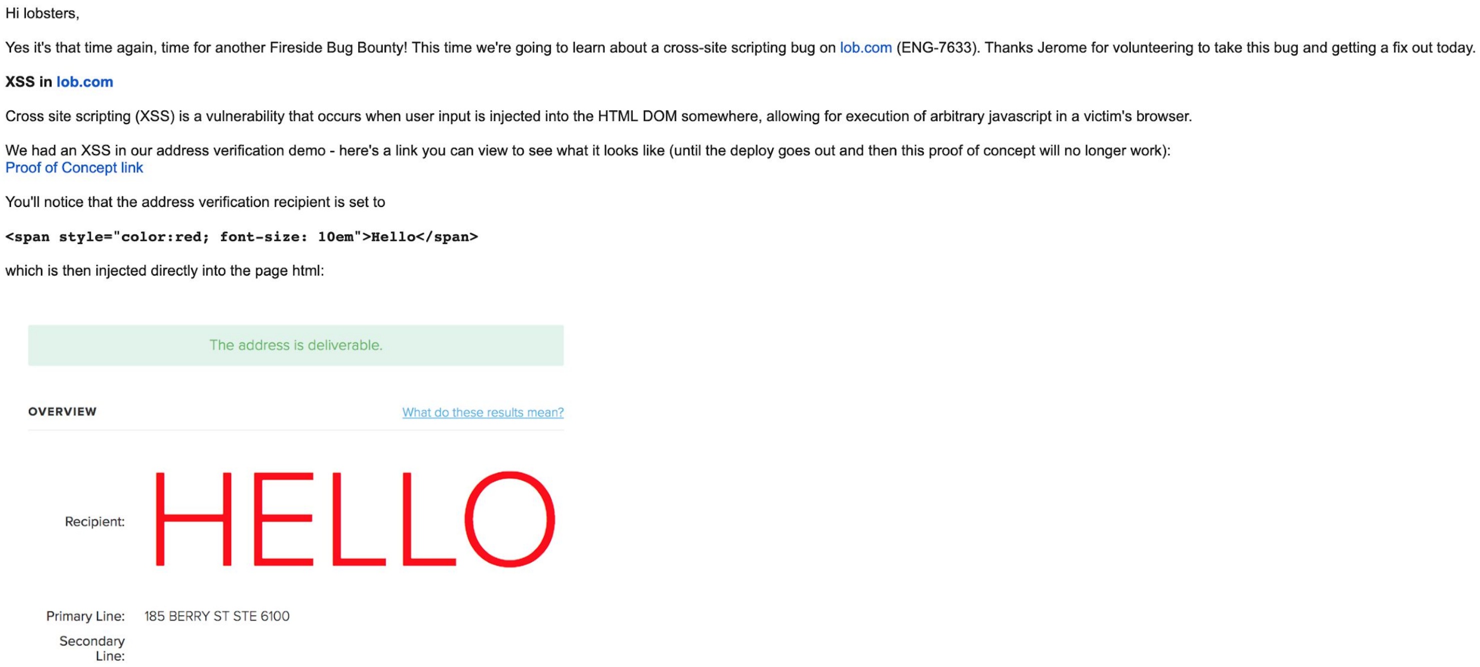
- Most security work is not done by the security team
- The security team must work through influence
- Employees are your eyes and ears on the ground
- Build social capital

Concrete Examples

1) SECURITY CHAMPIONS

- many different versions of this; depends on the organization
- at Lob, this is a “security enthusiast” interest group

2) FIRESIDE BUG BOUNTY



Hi lobsters,

Yes it's that time again, time for another Fireside Bug Bounty! This time we're going to learn about a cross-site scripting bug on lob.com (ENG-7633). Thanks Jerome for volunteering to take this bug and getting a fix out today.

XSS in lob.com

Cross site scripting (XSS) is a vulnerability that occurs when user input is injected into the HTML DOM somewhere, allowing for execution of arbitrary javascript in a victim's browser.

We had an XSS in our address verification demo - here's a link you can view to see what it looks like (until the deploy goes out and then this proof of concept will no longer work):
Proof of Concept link

You'll notice that the address verification recipient is set to

```
<span style="color:red; font-size: 10em">Hello</span>
```

which is then injected directly into the page html:

The address is deliverable.

OVERVIEW

What do these results mean?

Recipient: HELLO

Primary Line: 185 BERRY ST STE 6100

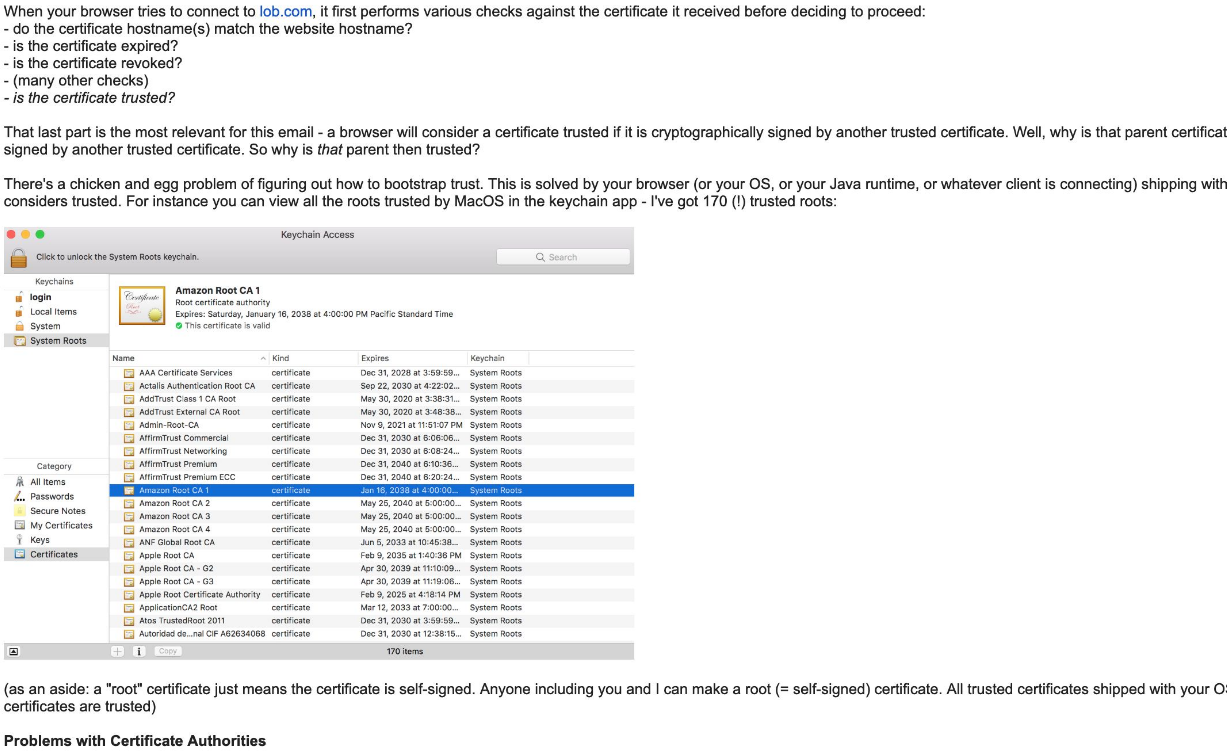
Secondary Line:

2) FIRESIDE BUG BOUNTY

- description of what the bug is
- how to exploit it
- impact
- fixing this particular instance
- solving this entire class of vulnerability

3) SEND OUT CURRENT HAPPENINGS

- when browsers started enforcing certificate transparency



When your browser tries to connect to lob.com, it first performs various checks against the certificate it received before deciding to proceed:
- do the certificate hostname(s) match the website hostname?
- is the certificate expired?
- is the certificate revoked?
- (many other checks)
- *is the certificate trusted?*

That last part is the most relevant for this email - a browser will consider a certificate trusted if it is cryptographically signed by another trusted certificate. Well, why is that parent certificat
signed by another trusted certificate. So why is *that* parent then trusted?

There's a chicken and egg problem of figuring out how to bootstrap trust. This is solved by your browser (or your OS, or your Java runtime, or whatever client is connecting) shipping with
considers trusted. For instance you can view all the roots trusted by MacOS in the keychain app - I've got 170 (!) trusted roots:

Click to unlock the System Roots keychain.

Amazon Root CA 1
Root certificate authority
Expires: Saturday, January 16, 2038 at 4:00:00 PM Pacific Standard Time
✓ This certificate is valid

Name	Kind	Expires	Keychain
AAA Certificate Services	certificate	Dec 31, 2028 at 3:59:59...	System Roots
Actalis Authentication Root CA	certificate	Sep 22, 2030 at 4:22:02...	System Roots
AddTrust Class 1 CA Root	certificate	May 30, 2020 at 3:38:31...	System Roots
AddTrust External CA Root	certificate	May 30, 2020 at 3:48:38...	System Roots
Admin-Root-CA	certificate	Nov 9, 2021 at 11:51:07 PM	System Roots
AffirmTrust Commercial	certificate	Dec 31, 2030 at 6:06:06...	System Roots
AffirmTrust Networking	certificate	Dec 31, 2030 at 6:08:24...	System Roots
AffirmTrust Premium	certificate	Dec 31, 2040 at 6:10:36...	System Roots
AffirmTrust Premium ECC	certificate	Dec 31, 2040 at 6:20:24...	System Roots
Amazon Root CA 1	certificate	Jan 16, 2038 at 4:00:00...	System Roots
Amazon Root CA 2	certificate	May 25, 2040 at 5:00:00...	System Roots
Amazon Root CA 3	certificate	May 25, 2040 at 5:00:00...	System Roots
Amazon Root CA 4	certificate	May 25, 2040 at 5:00:00...	System Roots
ANF Global Root CA	certificate	Jun 5, 2033 at 10:45:38...	System Roots
Apple Root CA	certificate	Feb 9, 2035 at 1:40:36 PM	System Roots
Apple Root CA - G2	certificate	Apr 30, 2039 at 11:10:09...	System Roots
Apple Root CA - G3	certificate	Apr 30, 2039 at 11:19:06...	System Roots
Apple Root Certificate Authority	certificate	Feb 9, 2025 at 4:18:14 PM	System Roots
ApplicationCA2 Root	certificate	Mar 12, 2033 at 7:00:00...	System Roots
Atos TrustedRoot 2011	certificate	Dec 31, 2030 at 3:59:59...	System Roots
Autoridad de...nal CIF A62634068	certificate	Dec 31, 2030 at 12:38:15...	System Roots

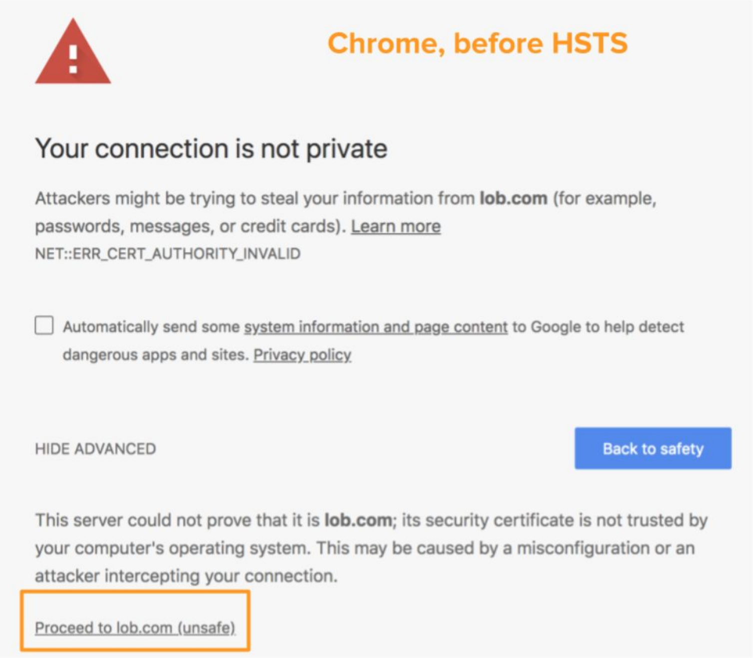
170 items

(as an aside: a "root" certificate just means the certificate is self-signed. Anyone including you and I can make a root (= self-signed) certificate. All trusted certificates shipped with your O
certificates are trusted)

Problems with Certificate Authorities

3) SEND OUT CURRENT HAPPENINGS

- when we deployed preloaded strict-transport-security on our website



Chrome, before HSTS

Your connection is not private

Attackers might be trying to steal your information from **lob.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

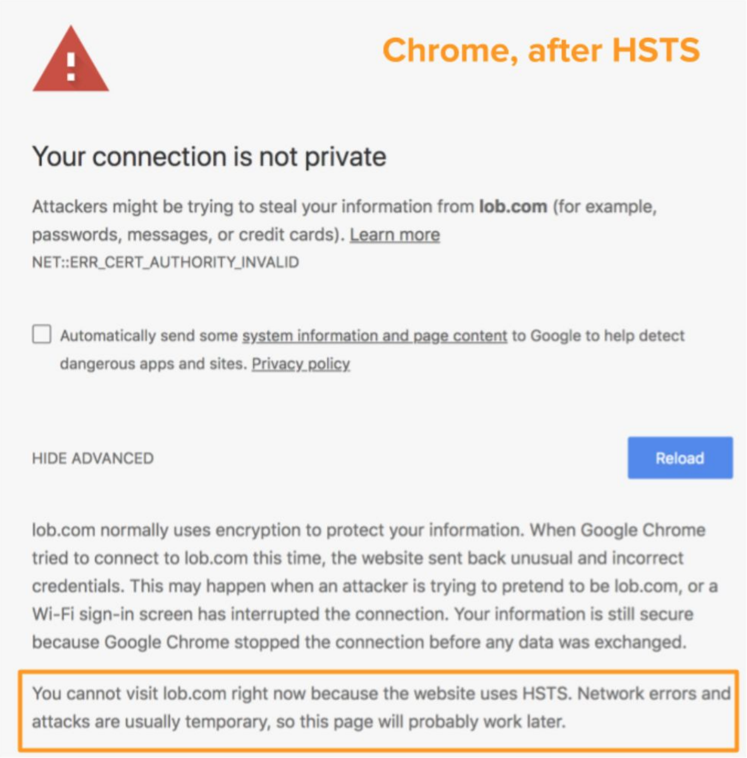
☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

HIDE ADVANCED

Back to safety

This server could not prove that it is **lob.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to lob.com (unsafe)



Chrome, after HSTS

Your connection is not private

Attackers might be trying to steal your information from **lob.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

HIDE ADVANCED

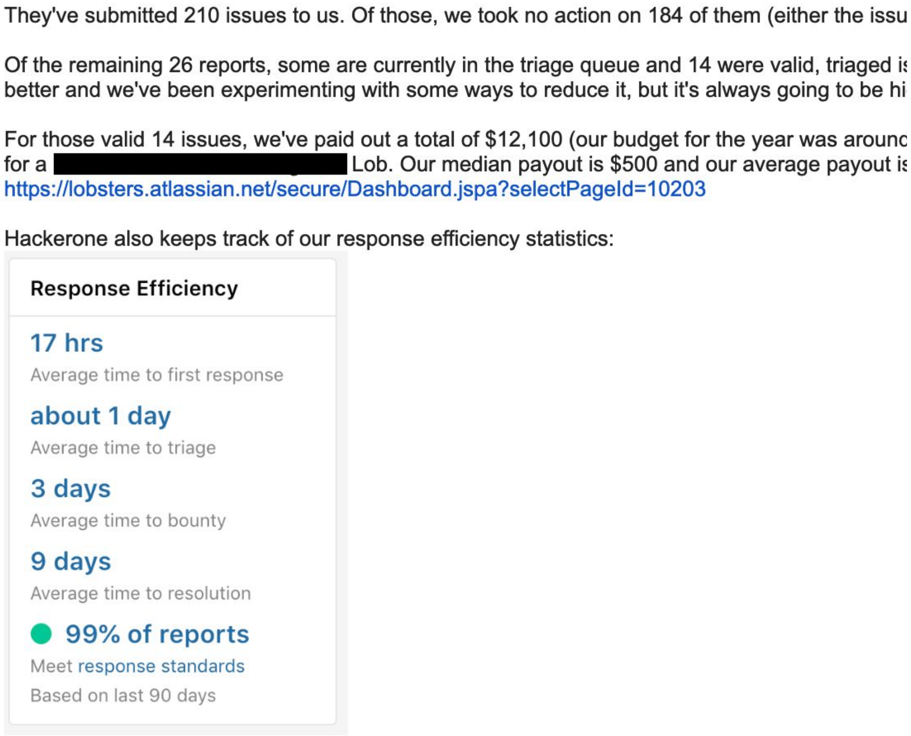
Reload

lob.com normally uses encryption to protect your information. When Google Chrome tried to connect to lob.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be lob.com, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Google Chrome stopped the connection before any data was exchanged.

You cannot visit lob.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

3) SEND OUT CURRENT HAPPENINGS

- when we had a quarter’s worth of bug bounty data



They've submitted 210 issues to us. Of those, we took no action on 184 of them (either the issu

Of the remaining 26 reports, some are currently in the triage queue and 14 were valid, triaged is better and we've been experimenting with some ways to reduce it, but it's always going to be hi

For those valid 14 issues, we've paid out a total of $12,100 (our budget for the year was arounc for a [redacted] Lob. Our median payout is $500 and our average payout is https://lobsters.atlassian.net/secure/Dashboard.jspa?selectPageId=10203

Hackerone also keeps track of our response efficiency statistics:

Response Efficiency

17 hrs
Average time to first response

about 1 day
Average time to triage

3 days
Average time to bounty

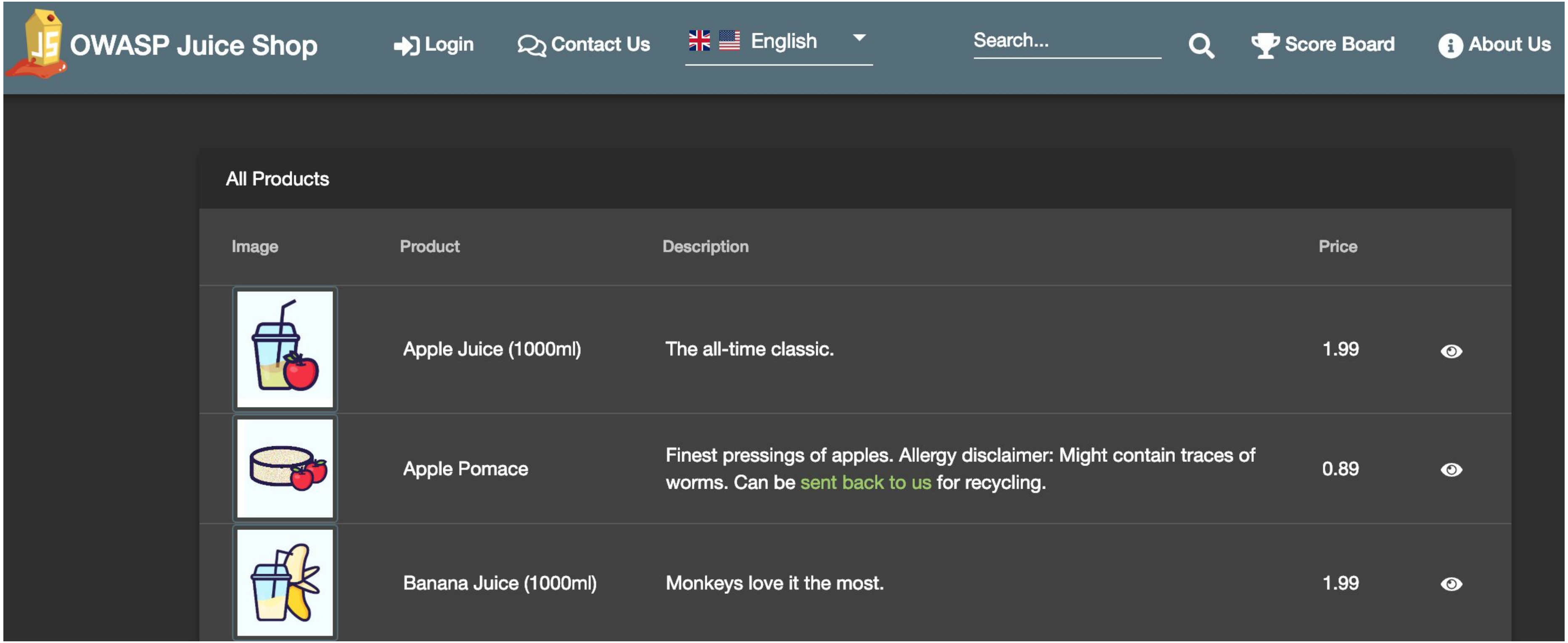
9 days
Average time to resolution

● 99% of reports
Meet response standards
Based on last 90 days

3) SEND OUT CURRENT HAPPENINGS

- writeup current security events & explain their significance
- know your audience

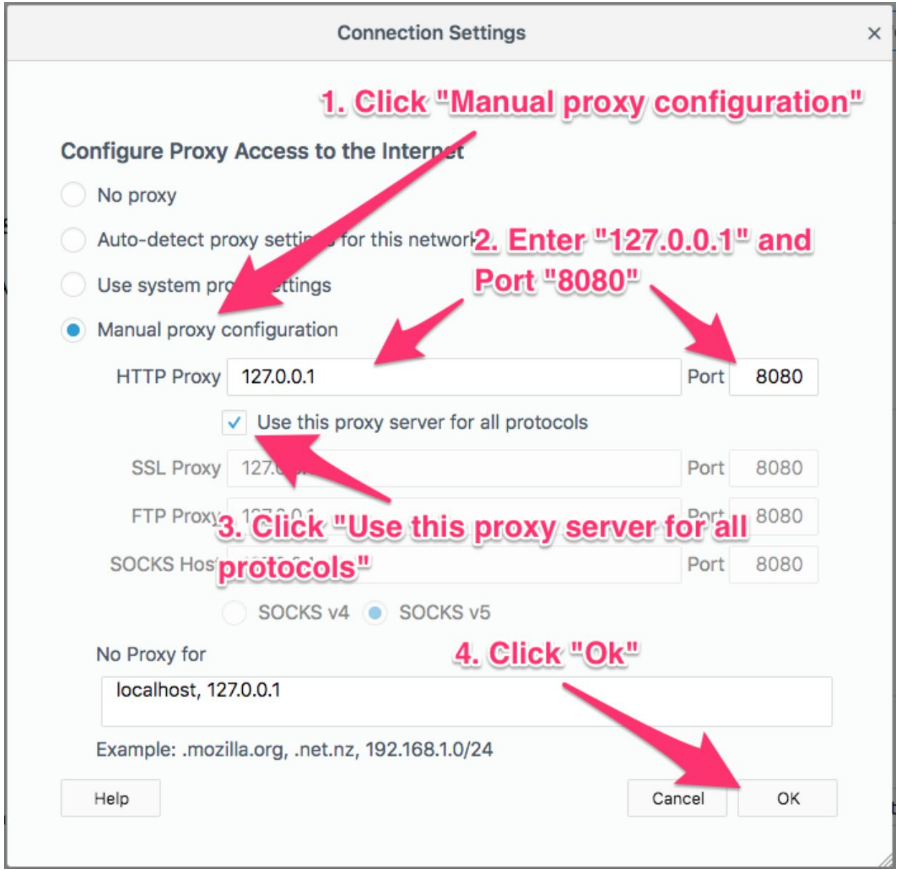
4) HACKING 101



All Products

Image	Product	Description	Price
	Apple Juice (1000ml)	The all-time classic.	1.99
	Apple Pomace	Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.	0.89
	Banana Juice (1000ml)	Monkeys love it the most.	1.99

4) HACKING 101



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

1. Click "Manual proxy configuration"

2. Enter "127.0.0.1" and Port "8080"

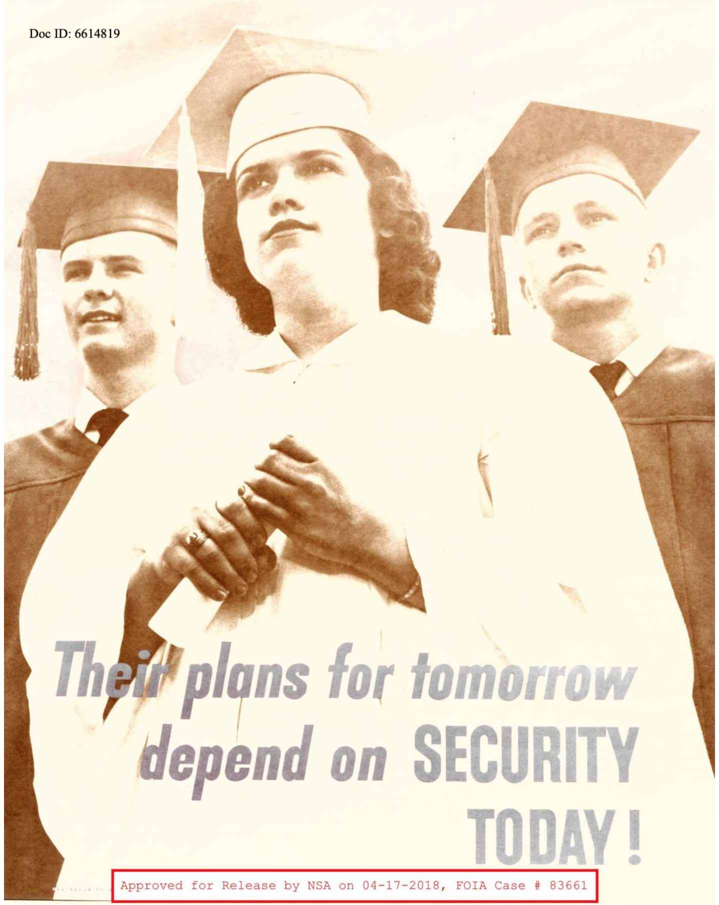
3. Click "Use this proxy server for all protocols"

4. Click "Ok"

5) NSA POSTCARDS

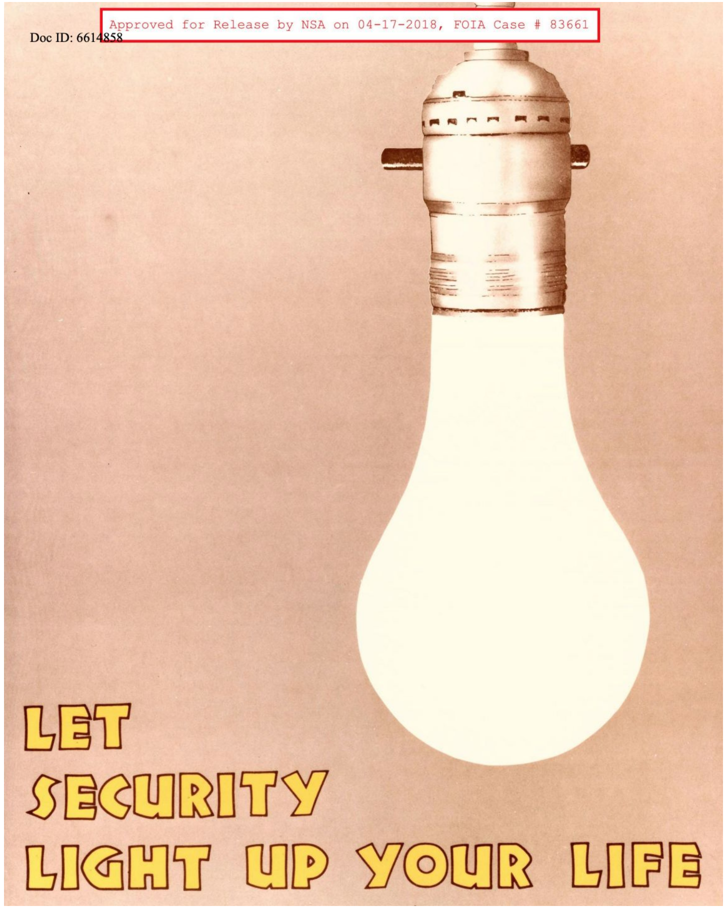
- 2016: A government watchdog group FOIA-ed the NSA for security propaganda posters from the 1950s and 1960s
- 2018: NSA responded with 136 posters

5) NSA POSTCARDS


Doc ID: 6614819

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

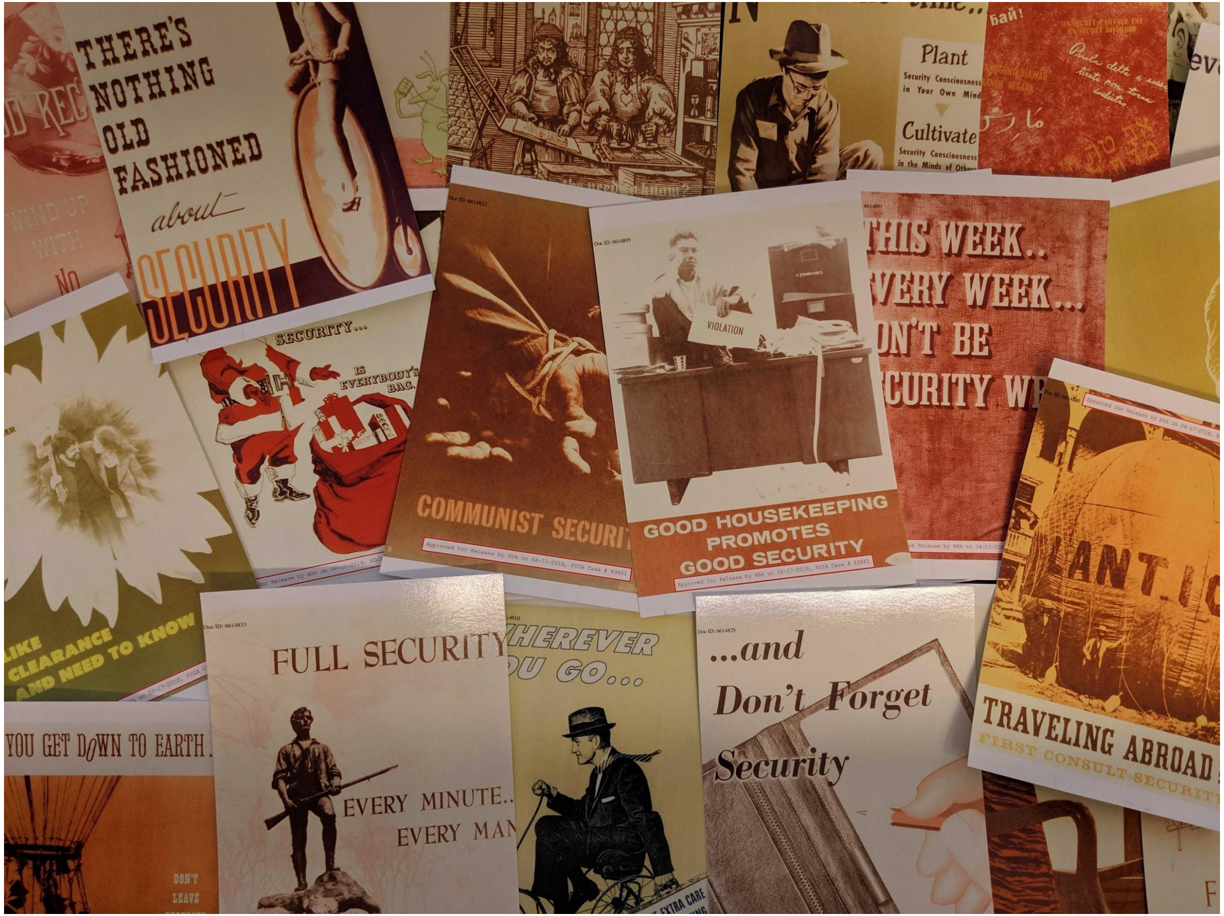
5) NSA POSTCARDS



Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

Doc ID: 6614858

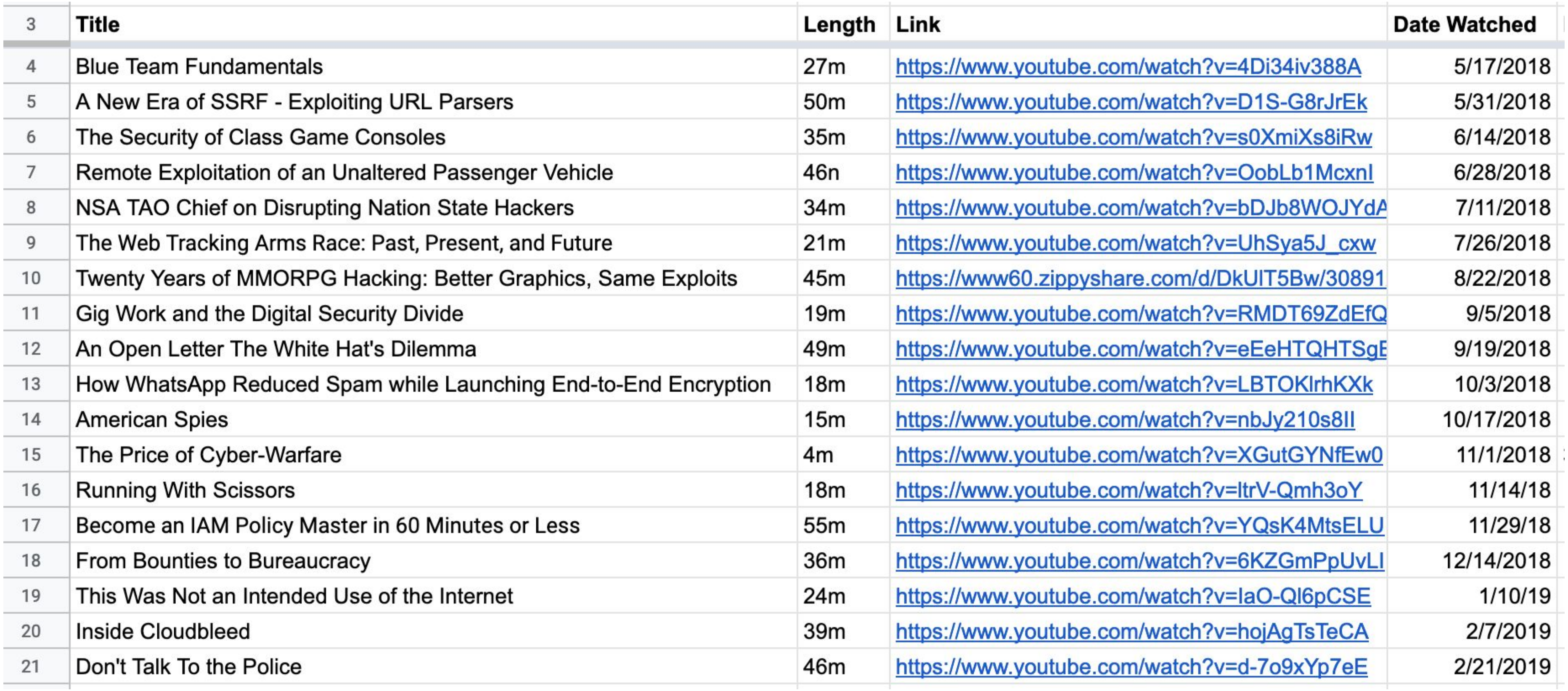
5) NSA POSTCARDS


THERE'S NOTHING OLD FASHIONED about SECURITY
Plant Security Consciousness in Your Own Mind
Cultivate Security Consciousness in the Minds of Others
SECURITY... IS EVERYBODY'S BAG.
COMMUNIST SECURIT
VIOLATION
GOOD HOUSEKEEPING PROMOTES GOOD SECURITY
THIS WEEK.. VERY WEEK... ON'T BE CURITY WE
CLEARANCE AND NEED TO KNOW
FULL SECURITY EVERY MINUTE.. EVERY MAN
HEREVER OU GO...
...and Don't Forget Security
TRAVELING ABROAD FIRST CONSULT SECURITY
YOU GET DOWN TO EARTH
Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

6) SECURITY CONFERENCE WATCH PARTY

- meet at lunch once every 2 weeks to watch a security talk
- send out a reminder the day before with a summary of the talk

6) SECURITY CONFERENCE WATCH PARTY



3	Title	Length	Link	Date Watched
4	Blue Team Fundamentals	27m	https://www.youtube.com/watch?v=4Di34iv388A	5/17/2018
5	A New Era of SSRF - Exploiting URL Parsers	50m	https://www.youtube.com/watch?v=D1S-G8rJrEk	5/31/2018
6	The Security of Class Game Consoles	35m	https://www.youtube.com/watch?v=s0XmiXs8iRw	6/14/2018
7	Remote Exploitation of an Unaltered Passenger Vehicle	46n	https://www.youtube.com/watch?v=OobLb1Mcxnl	6/28/2018
8	NSA TAO Chief on Disrupting Nation State Hackers	34m	https://www.youtube.com/watch?v=bDJb8WOJYdA	7/11/2018
9	The Web Tracking Arms Race: Past, Present, and Future	21m	https://www.youtube.com/watch?v=UhSya5J_cxw	7/26/2018
10	Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits	45m	https://www60.zippyshare.com/d/DkUIT5Bw/30891	8/22/2018
11	Gig Work and the Digital Security Divide	19m	https://www.youtube.com/watch?v=RMDT69ZdEfQ	9/5/2018
12	An Open Letter The White Hat's Dilemma	49m	https://www.youtube.com/watch?v=eEeHTQHTSg	9/19/2018
13	How WhatsApp Reduced Spam while Launching End-to-End Encryption	18m	https://www.youtube.com/watch?v=LBTOKlrhKXk	10/3/2018
14	American Spies	15m	https://www.youtube.com/watch?v=nbJy210s8Il	10/17/2018
15	The Price of Cyber-Warfare	4m	https://www.youtube.com/watch?v=XGutGYNfEw0	11/1/2018
16	Running With Scissors	18m	https://www.youtube.com/watch?v=ltrV-Qmh3oY	11/14/18
17	Become an IAM Policy Master in 60 Minutes or Less	55m	https://www.youtube.com/watch?v=YQsK4MtsELU	11/29/18
18	From Bounties to Bureaucracy	36m	https://www.youtube.com/watch?v=6KZGmPpUvLI	12/14/2018
19	This Was Not an Intended Use of the Internet	24m	https://www.youtube.com/watch?v=IaO-Ql6pCSE	1/10/19
20	Inside Cloudbleed	39m	https://www.youtube.com/watch?v=hojAgTsTeCA	2/7/2019
21	Don't Talk To the Police	46m	https://www.youtube.com/watch?v=d-7o9xYp7eE	2/21/2019

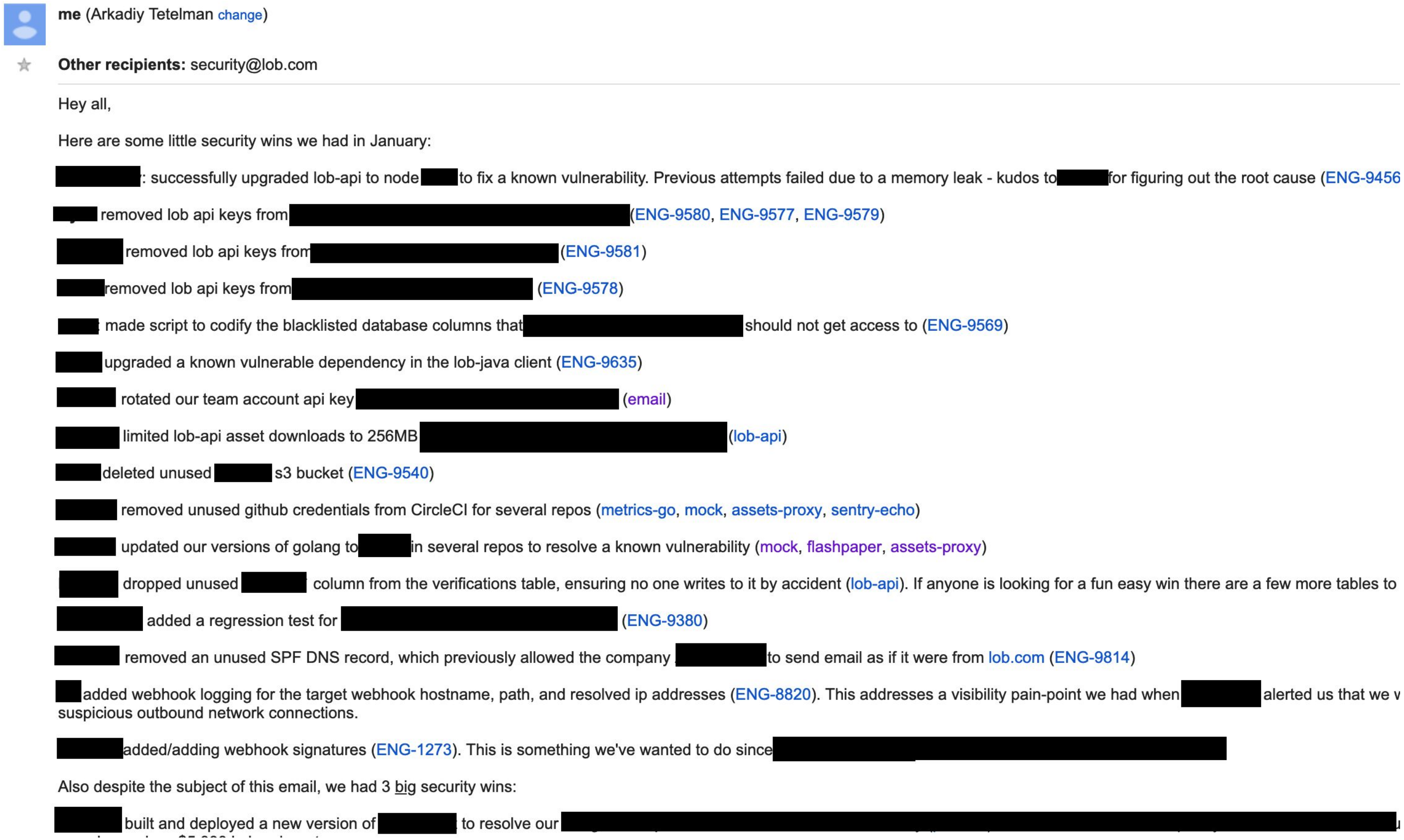
7) SHOW-AND-TELL

- every other week on Friday
- 5m presentations by any employee on any topic

8) SECURITY LITTLE WINS

- monthly email calling out all the small security wins

8) SECURITY LITTLE WINS



me (Arkadiy Tetelman change)

Other recipients: security@lob.com

Hey all,

Here are some little security wins we had in January:

[redacted]: successfully upgraded lob-api to node [redacted] to fix a known vulnerability. Previous attempts failed due to a memory leak - kudos to [redacted] for figuring out the root cause (ENG-9456

[redacted] removed lob api keys from [redacted] (ENG-9580, ENG-9577, ENG-9579)

[redacted] removed lob api keys from [redacted] (ENG-9581)

[redacted] removed lob api keys from [redacted] (ENG-9578)

[redacted] made script to codify the blacklisted database columns that [redacted] should not get access to (ENG-9569)

[redacted] upgraded a known vulnerable dependency in the lob-java client (ENG-9635)

[redacted] rotated our team account api key [redacted] (email)

[redacted] limited lob-api asset downloads to 256MB [redacted] (lob-api)

[redacted] deleted unused [redacted] s3 bucket (ENG-9540)

[redacted] removed unused github credentials from CircleCI for several repos (metrics-go, mock, assets-proxy, sentry-echo)

[redacted] updated our versions of golang to [redacted] in several repos to resolve a known vulnerability (mock, flashpaper, assets-proxy)

[redacted] dropped unused [redacted] column from the verifications table, ensuring no one writes to it by accident (lob-api). If anyone is looking for a fun easy win there are a few more tables to

[redacted] added a regression test for [redacted] (ENG-9380)

[redacted] removed an unused SPF DNS record, which previously allowed the company [redacted] to send email as if it were from lob.com (ENG-9814)

[redacted] added webhook logging for the target webhook hostname, path, and resolved ip addresses (ENG-8820). This addresses a visibility pain-point we had when [redacted] alerted us that we v suspicious outbound network connections.

[redacted] added/adding webhook signatures (ENG-1273). This is something we've wanted to do since [redacted]

Also despite the subject of this email, we had 3 big security wins:

[redacted] built and deployed a new version of [redacted] to resolve our [redacted]

THINGS THAT DIDN’T WORK

- Security 20% time
- Didn’t focus enough on non-engineering functions

Guiding Principles

GUIDING PRINCIPLES

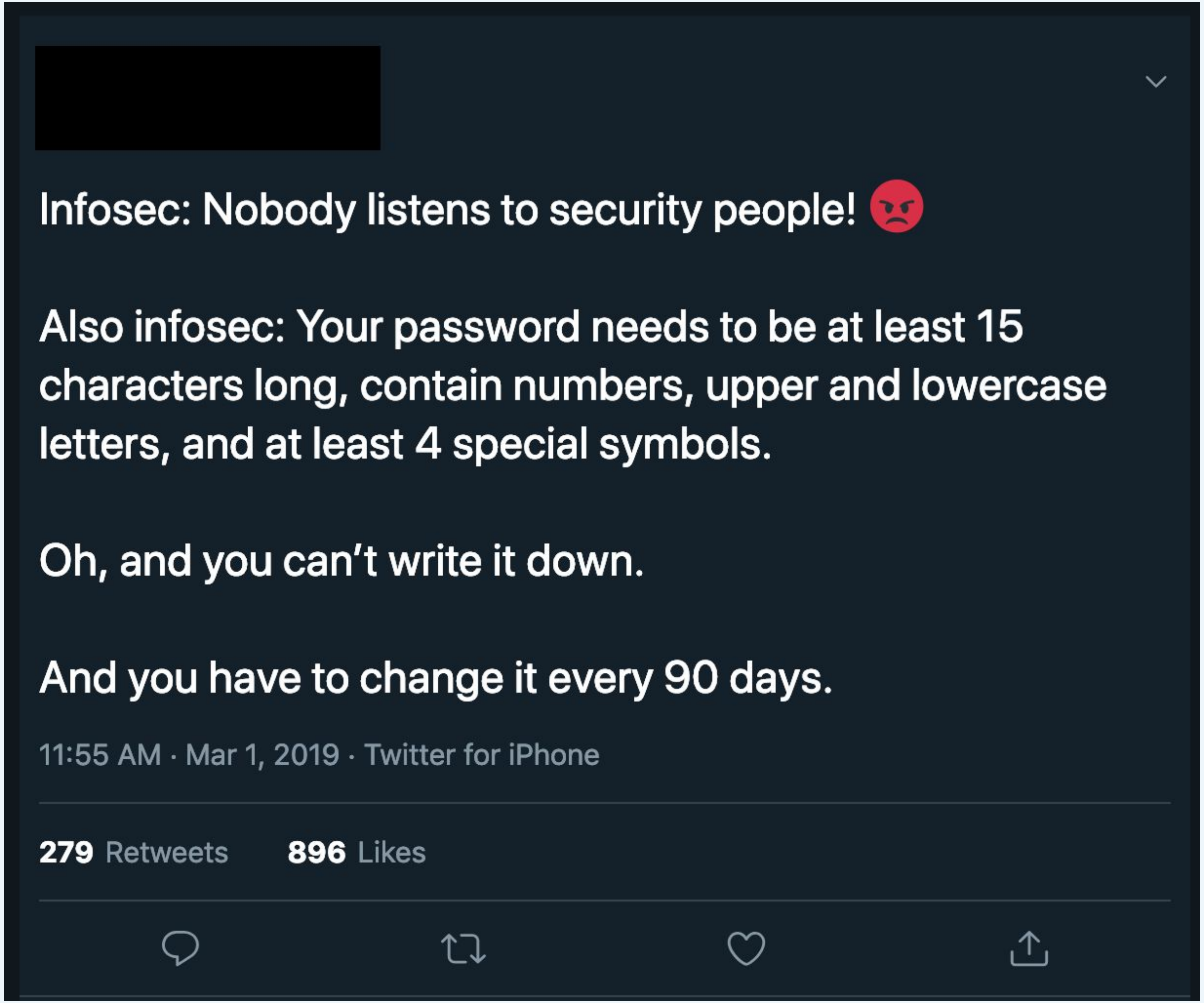
- Add value
- Be visible
- Be available

Why does security culture matter

How much should I prioritize security culture over my other work

HOW MUCH SHOULD I INVEST

- Measuring culture is hard & subjective
- Anecdotally seeing improvements
- Invest more in the beginning: culture has momentum



[redacted]

Infosec: Nobody listens to security people! 😡

Also infosec: Your password needs to be at least 15 characters long, contain numbers, upper and lowercase letters, and at least 4 special symbols.

Oh, and you can’t write it down.

And you have to change it every 90 days.

11:55 AM · Mar 1, 2019 · Twitter for iPhone

279 Retweets **896** Likes

Questions

Twitter:	@arkadiyt
I’m hiring:	bit.ly/lobsecurity