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
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

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

which is then injected directly into the page html:

The address is deliverable.

**OVERVIEW**

<table>
<thead>
<tr>
<th>Recipient:</th>
<th>HELLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Line:</td>
<td>185 BERRY ST STE 6000</td>
</tr>
<tr>
<td>Secondary Line:</td>
<td></td>
</tr>
</tbody>
</table>

What do these results mean?
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 certificate 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:

(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 OS certificates are trusted)

Problems with Certificate Authorities
3) SEND OUT CURRENT HAPPENINGS

- when we deployed preloaded strict-transport-security on our website
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 issues were not sufficiently severe or it was too much effort to fix them). Of the remaining 26 reports, some are currently in the triage queue and 14 were valid, triaged into problems. We’re seeing a slow improvement and we’ve been experimenting with some ways to reduce it, but it’s always going to be high.

For those 14 valid issues, we’ve paid out a total of $12,100 (our budget for the year was around $150,000). Our median payout is $500 and our average payout is $665. We used a third-party tool to automatically moderate and prioritize the reports. We also got a $1,000 reward from our sponsor Lob. Our median payout is $500 and our average payout is $665. We used a third-party tool to automatically moderate and prioritize the reports. We also got a $1,000 reward from our sponsor Lob.

Hackerone also keeps track of our response efficiency statistics:

<table>
<thead>
<tr>
<th>Response Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 hrs</td>
</tr>
<tr>
<td>Average time to first response</td>
</tr>
<tr>
<td>about 1 day</td>
</tr>
<tr>
<td>Average time to triage</td>
</tr>
<tr>
<td>3 days</td>
</tr>
<tr>
<td>Average time to bounty</td>
</tr>
<tr>
<td>9 days</td>
</tr>
<tr>
<td>Average time to resolution</td>
</tr>
<tr>
<td>99% of reports</td>
</tr>
<tr>
<td>Meet response standards</td>
</tr>
<tr>
<td>Based on last 90 days</td>
</tr>
</tbody>
</table>
3) SEND OUT CURRENT HAPPENINGS

- writeup current security events & explain their significance
- know your audience
4) HACKING 101

<table>
<thead>
<tr>
<th>Image</th>
<th>Product</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Apple Juice" /></td>
<td>Apple Juice (1000ml)</td>
<td>The all-time classic.</td>
<td>1.99</td>
</tr>
<tr>
<td><img src="image" alt="Apple Pomace" /></td>
<td>Apple Pomace</td>
<td>Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.</td>
<td>0.89</td>
</tr>
<tr>
<td><img src="image" alt="Banana Juice" /></td>
<td>Banana Juice (1000ml)</td>
<td>Monkeys love it the most.</td>
<td>1.99</td>
</tr>
</tbody>
</table>
4) HACKING 101

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

Their plans for tomorrow depend on SECURITY TODAY!

Approved for Release by NSA on 04-17-2018, FDIA Case # 83661
LET SECURITY LIGHT UP YOUR LIFE
5) NSA POSTCARDS
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
<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Length</th>
<th>Link</th>
<th>Date Watched</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>6) SECURITY CONFERENCE WATCH PARTY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Blue Team Fundamentals</td>
<td>27m</td>
<td><a href="https://www.youtube.com/watch?v=4Di34iv388A">https://www.youtube.com/watch?v=4Di34iv388A</a></td>
<td>5/17/2018</td>
</tr>
<tr>
<td>5</td>
<td>A New Era of SSRF - Exploiting URL Parsers</td>
<td>50m</td>
<td><a href="https://www.youtube.com/watch?v=D1S_G8rJrEk">https://www.youtube.com/watch?v=D1S_G8rJrEk</a></td>
<td>5/31/2018</td>
</tr>
<tr>
<td>6</td>
<td>The Security of Class Game Consoles</td>
<td>35m</td>
<td><a href="https://www.youtube.com/watch?v=s0XmiRs8iRw">https://www.youtube.com/watch?v=s0XmiRs8iRw</a></td>
<td>6/14/2018</td>
</tr>
<tr>
<td>7</td>
<td>Remote Exploitation of an Unaltered Passenger Vehicle</td>
<td>46m</td>
<td><a href="https://www.youtube.com/watch?v=OobLb1Mcxnl">https://www.youtube.com/watch?v=OobLb1Mcxnl</a></td>
<td>6/28/2018</td>
</tr>
<tr>
<td>8</td>
<td>NSA TAO Chief on Disrupting Nation State Hackers</td>
<td>34m</td>
<td><a href="https://www.youtube.com/watch?v=bDjB8WOJyDA">https://www.youtube.com/watch?v=bDjB8WOJyDA</a></td>
<td>7/11/2018</td>
</tr>
<tr>
<td>9</td>
<td>The Web Tracking Arms Race: Past, Present, and Future</td>
<td>21m</td>
<td><a href="https://www.youtube.com/watch?v=UhSya5J_cxw">https://www.youtube.com/watch?v=UhSya5J_cxw</a></td>
<td>7/26/2018</td>
</tr>
<tr>
<td>10</td>
<td>Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits</td>
<td>45m</td>
<td><a href="https://www60.zippyshare.com/d/DkJUT5Bw/30891">https://www60.zippyshare.com/d/DkJUT5Bw/30891</a></td>
<td>8/22/2018</td>
</tr>
<tr>
<td>11</td>
<td>Gig Work and the Digital Security Divide</td>
<td>19m</td>
<td><a href="https://www.youtube.com/watch?v=RMQx69ZdEwQ">https://www.youtube.com/watch?v=RMQx69ZdEwQ</a></td>
<td>9/5/2018</td>
</tr>
<tr>
<td>12</td>
<td>An Open Letter The White Hat's Dilemma</td>
<td>49m</td>
<td><a href="https://www.youtube.com/watch?v=eEeHTQHTSgE">https://www.youtube.com/watch?v=eEeHTQHTSgE</a></td>
<td>9/19/2018</td>
</tr>
<tr>
<td>13</td>
<td>How WhatsApp Reduced Spam while Launching End-to-End Encryption</td>
<td>18m</td>
<td><a href="https://www.youtube.com/watch?v=LBTOKlrKXk">https://www.youtube.com/watch?v=LBTOKlrKXk</a></td>
<td>10/3/2018</td>
</tr>
<tr>
<td>14</td>
<td>American Spies</td>
<td>15m</td>
<td><a href="https://www.youtube.com/watch?v=nbJy210s8II">https://www.youtube.com/watch?v=nbJy210s8II</a></td>
<td>10/17/2018</td>
</tr>
<tr>
<td>15</td>
<td>The Price of Cyber-Warfare</td>
<td>4m</td>
<td><a href="https://www.youtube.com/watch?v=XYsGhYNfEw0">https://www.youtube.com/watch?v=XYsGhYNfEw0</a></td>
<td>11/1/2018</td>
</tr>
<tr>
<td>16</td>
<td>Running With Scissors</td>
<td>18m</td>
<td><a href="https://www.youtube.com/watch?v=itrV-Qmh3oY">https://www.youtube.com/watch?v=itrV-Qmh3oY</a></td>
<td>11/4/2018</td>
</tr>
<tr>
<td>17</td>
<td>Become an IAM Policy Master in 60 Minutes or Less</td>
<td>55m</td>
<td><a href="https://www.youtube.com/watch?v=YQsK4MtsELU">https://www.youtube.com/watch?v=YQsK4MtsELU</a></td>
<td>11/29/2018</td>
</tr>
<tr>
<td>18</td>
<td>From Bounties to Bureaucracy</td>
<td>36m</td>
<td><a href="https://www.youtube.com/watch?v=6KZGmpPwUvL1">https://www.youtube.com/watch?v=6KZGmpPwUvL1</a></td>
<td>12/14/2018</td>
</tr>
<tr>
<td>19</td>
<td>This Was Not an Intended Use of the Internet</td>
<td>24m</td>
<td><a href="https://www.youtube.com/watch?v=laQ-Q6pCSE">https://www.youtube.com/watch?v=laQ-Q6pCSE</a></td>
<td>1/10/2019</td>
</tr>
<tr>
<td>20</td>
<td>Inside Cloudbleed</td>
<td>39m</td>
<td><a href="https://www.youtube.com/watch?v=hojAgTsTeCA">https://www.youtube.com/watch?v=hojAgTsTeCA</a></td>
<td>2/7/2019</td>
</tr>
<tr>
<td>21</td>
<td>Don't Talk To the Police</td>
<td>46m</td>
<td><a href="https://www.youtube.com/watch?v=d-7o9xYp7eE">https://www.youtube.com/watch?v=d-7o9xYp7eE</a></td>
<td>2/21/2019</td>
</tr>
</tbody>
</table>
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

Hey all,

Here are some little security wins we had in January:

- Successfully upgraded lob-api to node to fix a known vulnerability. Previous attempts failed due to a memory leak - kudos to [user] for figuring out the root cause (ENG-9456)
- Removed lob api keys from [redacted] (ENG-9560, ENG-9577, ENG-9579)
- Removed lob api keys from [redacted] (ENG-9581)
- Removed lob api keys from [redacted] (ENG-9578)
- Made script to codify the blacklisted database columns that [redacted] should not get access to (ENG-9569)
- Upgraded a known vulnerable dependency in the lob-java client (ENG-9635)
- Rotated our team account api key (email)
- Limited lob-api asset downloads to 256MB (lob-api)
- Deleted unused s3 bucket (ENG-9540)
- Removed unused github credentials from CircleCI for several repos (metrics-go, mock, assets-proxy, sentry-echo)
- Updated our versions of golang to [redacted] in several repos to resolve a known vulnerability (mock, flashpaper, assets-proxy)
- Dropped unused 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
- Added a regression test for [redacted] (ENG-9380)
- Removed an unused SPF DNS record, which previously allowed the company [redacted] to send email as if it were from lob.com (ENG-9814)
- 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've suspicious outbound network connections.
- 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:

- 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
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.
Questions

Twitter: @arkadiyt

I’m hiring: bit.ly/lobsecurity