

Building Secure Cultures

Leigh Honeywell
@hypatiadotca

about me

Canadian

ex-Symantec, Microsoft

Rebooted your Windows machines a few times
in 2012


Now at Heroku, a Salesforce.com company

**move fast and break
things....**

→ ↻ 🏠 <https://www.facebook.com/zuck>

f Mark Zuckerberg 🔍

👤 💬 1 🌐 21 Home 20+ Khalil 🔒 ⚙️




Mark Zuckerberg ✓

Follow Message ⚙️

Timeline About Photos Friends More ▾

Follow Mark to get his public posts in your news feed.

 18,821,144 Followers [Follow](#)

About


👤 **Founder and CEO at Facebook**
February 4, 2004 to present

🎓 **Studied Computer Science at Harvard University**
Past: Phillips Exeter Academy and Ardsley High School

🏠 **Lives in Palo Alto, California**

📍 **From Dobbs Ferry, New York**

📊 **Followed by 18,821,144 people**

 **Khalil** shared a link.
about a minute ago 🌐

Dear Mark Zuckerberg,

First sorry for breaking your privacy and post to your wall , i has no other choice to make after all the reports i sent to Facebook team .

My name is KHALIL, from Palestine .
... See More

Hi Khalil, I am sorry this is not a bug. Thanks, Emrakul Securit - Pastebin.com
pastebin.com

Recent

2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2002
2000
1998
Born

until this happens

red flags

- “blameful” interactions between security + engineering
- disconnect between severity of security findings and what gets fixed
- long lag between engineering changes and policy changes

green flags

Some signs you have a healthy security culture:

- devs reach out to the security team when stuck or unsure
- devs find security bugs in eachothers' code
- people self-report security issues (cred leaks etc.)

how do you get to green?

**transparency +
accountability
=
trust**

transparency



accountability



trust



“impacting and influencing”

in a breach situation it's rarely the CEO who gets fired

feigned surprise

“The first rule means you shouldn't act surprised when people say they don't know something. This applies to both technical things ("What?! I can't believe you don't know what the stack is!") and non-technical things ("You don't know who RMS is?!"). Feigning surprise has absolutely no social or educational benefit: When people feign surprise, it's usually to make them feel better about themselves and others feel worse. And even when that's not the intention, it's almost always the effect. As you've probably already guessed, this rule is tightly coupled to our belief in the importance of people feeling comfortable saying "I don't know" and "I don't understand."”

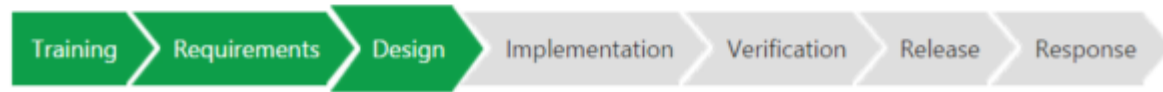
<https://www.hackerschool.com/manual#sub-sec-social-rules>

secure development

What is the Security Development Lifecycle ?



The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.



microsoft.com/sdl

minimum viable SDL

- self-assessment to determine if a project needs security team review or not
- up-front threat modeling that is kept up to date as things evolve
- security review checklist
 - stay tuned on this one

extra credit

- security tooling in your CI process
 - codeclimate
 - ??? others
 - there is a huge gap in the market here

bug bounty



Heroku

Cloud computing for developers

\$100 - \$1,500 Per Bug.



Report Bug

bug bounty problems

- lots of work in progress with external inputs and dependencies
- emotional labour involved in negotiating severity and reproducibility of bugs
- initially, a lot of low-hanging fruit - which tapers off as you fix stuff

pre-bug-bounty checklist

- communicate the importance of prioritizing bounty bugs
- establish a weekly time bounty work session:
 - ping bounty work items
 - communicate with external researchers
 - review bugs for things that need adding to your SDL

CAPTURE



ALL THE FLAGS

memegenerator.net

security through play

ctftime.org

all you need is a google doc and an irc/hipchat/
slack room

<https://speakerdeck.com/hypatia/ctf-for-mortals>

thanks and links

Thanks to Jacob Kaplan-Moss and Owen Jacobson for reviewing this deck, and to everyone who's listened to me babble about security and emotional labour over the past few weeks.

<http://hypatia.ca> will have this deck later today
leigh@hypatia.ca / [@hypatiadotca](https://twitter.com/hypatiadotca)