Security at Slack: the first 3 years
bit.ly/securityatslack
About Me
What is Slack?
Messaging for Teams
Pre-History
2012
2013
From: Leigh Honeywell <leigh@hypatia.ca>
Date: December 4, 2013 9:12:21 PM PST
To: Slack Support <feedback@slack.com>
Subject: Re: Slack Help Contact from hypatia at seattleattic

Account: leigh@hypatia.ca

Hey folks!

Just signed up for Slack to look into using it for my non-profit. I was wondering if you're planning on having non-profit plans at some point - I don't want to get everyone switched over and excited about the product if we won't be able to afford it going forwards :)

We're fiscally sponsored by a US 501c3 charity, if that helps.

Thanks!

-Leigh
THE MOST FASCINATING PROFILE YOU’LL EVER READ ABOUT A GUY AND HIS BORING STARTUP
2014 Lessons:
● Hire your first security person early, and support their work
● 2fa all the things
● Bounties are great... but don’t jump the gun
In which @SlackHQ sets a new gold standard for security incident communications. Something to aspire to.

March 2015 security incident and the launch of Two Factor ...
We were recently able to confirm that there was unauthorized access to a Slack database storing user profile information. We have since...
slackhq.com
thing today: it's my last day at Heroku.

THING: I'm joining @SlackHQ!
Slack is committed to treating our customers’ data with the utmost care. As part of this, we encourage security researchers to put our security to the test - and we offer a variety of rewards for doing so. As of December 2015, we have paid out over $110,000 to researchers, and we look forward to continuing to work with the community as we add new features and services.

This page is intended for security researchers. For general information about security at Slack, please see our main website.

Love hacking on Slack? We’re hiring security engineers!

Program Rules
2015 Lessons:

- If you’re going to get breached, earlier is better
- Don’t forget to communicate how you’re doing security-wise
2016
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.
Everyone seemed to like this representation of DevOps and Security from my talk at #devopsdays Austin
Self-Service SDL
Initial Risk Assessment
Component Survey
Instructions

Please start by selecting the preset tags button. The preset tags will select the corresponding checklist which are relevant to project that you are working on. As a sample, you can select the "iOS" preset if your project related to feature / code changes in Slack iOS mobile client. You can select as many preset tags as you want as long as it relevant to your project.

It is highly recommended to check the checklist before submitting and also select any remaining modules/submodules that are relevant to your project (language choices, etc) even it's not selected by the preset tags.

If you are completing this survey before a lot of code has been written (or any at all), and are unsure if some modules may apply to your feature down the road, please err on the side of inclusiveness. It’s totally ok to select all of the options if you’re unsure - we include a "Not Applicable" column to move unused cards to automatically if they end up not being relevant as your project progresses.

Preset Tags

- WebApp
- API
- MessageServer
- iOS
- Android
- DesktopApp

Language

- All-Language Questionnaire
  These are questions apply to any language, and should be included

- PHP Language Guidance
  PHP can be difficult to get right. Here are some trouble spots that can trip up some projects

- Python Language Guidance
  Python-specific guidance for common traps

- C/C++ Language Guidance
  C and C++ guidance for common traps
Parsing

- XML
  Does your code work with/write/read XML?

- URL Parsing
  Does your component build/parse URLs, read/write URLs, or operate with/consume URLs?
  - PHP URL Parsing Guidance
    PHP-specific advice to parsing URLs
  - Javascript URL Parsing Guidance
    Javascript-specific advice to parsing URLs

Web

- CSRF
  Implementing functionality that causes user actions to happen can sometimes be triggered remotely without the user being aware. If your functionality is exposed directly on web, please make sure that you are protected against csrf attacks

- Open-Redirection
  Do you send users to another url?

- Secure Cookies
  Do you set cookies in your component?
Our Checklists
Ongoing Feedback
2016 Lessons:

- Bring security tools to where people live and they will adopt them enthusiastically
- Less rocket science and vendor bling, more hard work
2017
Slack Security Today:

● Incident Response
● Risk & Compliance
● Security Operations
● Product Security
Key Lessons:

- Hire Security early
- Share the internal oral history of your breach
- Build or buy the tools that make sense for your culture
What’s Next?
Leigh Honeywell
leigh@slack-corp.com
bit.ly/securityatslack
@hypatiadotca