Moving Fast and Securing Things:

Scaling security to growing organizations
Introduction

**Nikki Brandt**  
Sr Product Security Engineer  
- nbrandt@slack-corp.com  
- Has run every day in 2018 (so far)  
- Expert on vegan baking

**Kelly Ann**  
Product Security Engineer  
- kellyann@slack-corp.com  
- Has battled poachers in Antarctica  
- Expert on eating vegan baked goods
Agenda

- Slack and deployment
- Our Secure Development Lifecycle (SDL) process and tooling
- Feedback and lessons learned
Slack
Slack’s Rapid Early Growth

Daily Active Users

- 2013
- 2014
- 2015
- 2016
- 2017

6M daily active users

2.25 hours of daily active user engagement

55% of users outside the US
Slack’s Rapid Early Growth

- 6M daily active users
- 2.25 hours of daily active user engagement
- 55% of users outside the US

Daily Active Users

- 2013
- 2014
- 2015
- 2016
- 2017

Slack
Slack Today

- 7 million simultaneously connected users
- 13 million weekly active users
- Users average 10 hours/weekday connected to Slack
- 2+ hours/weekday in active use
- Over half of Daily Active Users are outside of North America
  - UK, Japan, Germany, France, India
Public launch: 2014

~30 Security Engineers +
~300 Application Engineers
~700 Engineers
5 Product Security engineers supporting all those developers

1200+ employees across 7 countries worldwide
HQ in San Francisco

Diverse set of industries
including software/technology, retail, media, telecom and professional services.
Culture of Continuous Integration - Continuous Deployment

- App Developers handle Development -> PR -> Deployment
- Deploys happen several times daily
- Designed to be an easy, accessible process
At peak, deploys were happening 100-150 times daily.
Everyone seemed to like this representation of DevOps and Security from my talk at #devopsdays Austin
Welcome to the SDL!
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.
“It was simply not going to be possible for a small team to conduct sufficient design and code reviews to materially improve the security of the next Windows release.

Instead of fishing for security vulnerabilities on behalf of the product groups, the SWI team would teach them how to fish.”

Deployment Culture at Slack
Transparency
Trust our developers
Culture of Empathy

- We set engineers up for success
  - Security is a resource for devs

- We’re here to help!
  - We host weekly security office hours

- Foster mutual trust
  - Not an adversarial relationship
Culture of Trust and Collaboration

- **Transparency and availability**
  - We keep our discussions in open forum
  - We have dedicated channels for consultation and triage

- **Security as visible part of engineering**
  - Present (friendly) faces of the security team
  - Offer basic tutorials of OWASP Top Ten
  - Annual CTF for Hacktober
Self-Service SDL
First off, we need some info from you about your project

Your Slack display name: @fynaz

Project Name: Reminders

JIRA EPIC id: XTEAM-1234

Link to spec: https://

#channel: #feat-x-y-z (optional)

Link to PR / code location: https:// (optional)

Please describe the feature you're developing?

1-2 sentence summary of the purpose of this feature.

Project Security Risk: I'm not sure

Let's Go!
Initial Risk Assessment
Do you want direct security involvement throughout the project?

If you think the project is risky and want help from Security from the beginning: trust your gut. We'll be involved and help however we can.

Yes  No

Does this component make major changes or implement new authentication or security controls?

Say "yes" if this component adds new ways for people to authenticate, adds to or changes existing security controls, or otherwise explicitly implements security/privacy features.

Yes  No

Your project's Risk Ranking

Your project is **High risk!**

Next
Component Survey
Choose Your Components and Go!

**App or Custom Integration**

- [ ] App or Custom Integration
  - We are building an App or Custom Integration

**New Infrastructure**

- [ ] New Infrastructure
  - We are implementing new infrastructure or internet facing service

**Legal & Privacy**

- [ ] Legal
  - Legal needs to make sure we can continue to make good with our customers and contracts. Please reach out to #help-legal if your team has any licensing or legal concern

- [ ] Privacy
  - Please ensure that we are properly protecting our customers and data in transit.
Checklists Save Lives
(no really)
All these disciplines use checklists!!

- Medicine
- Aviation
- Construction
- Factory lines
Our Checklists
Secure Development Lifecycle (SDL)

Your JIRA ticket is created!

Now, please go visit the JIRA ticket: **PRODSEC-509** and follow the Instructions
<table>
<thead>
<tr>
<th></th>
<th>Standard</th>
<th>SDL Backend</th>
<th>SDL Legal &amp; Privacy</th>
<th>SDL App or Custom Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zendesk Count</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

**Instruction**

Please complete the above checklist in the "SDL" tabs. Mark the items to complete the checklist. Once all of the checklist is completed then move this ticket's status to "Done" and enter resolution "Done".

If you end up over-scoping and have too many checklist, and you end up not needing it, you can mark the item as "Not Applicable" by putting the "N/A" status to the checklist items.

If you have question completing a specific checklist, feel free to reach out to #triage-security-prdct for any help or pointers.

Your initial risk assessment questionnaire came back with a rating of High.

**SDL Documentation**
### Checklist for each component

<table>
<thead>
<tr>
<th>Standard</th>
<th>SDL Backend</th>
<th>SDL Legal &amp; Privacy</th>
<th>SDL App or Custom Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDL App or Custom Integration:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **App or Custom Integration ★** - We are verifying the verification token on every slash command or Interactive Components
- **App or Custom Integration ★** - We locked down the App token usage to a known set of IP addresses when installing a custom app to Tinyspeck
- **App or Custom Integration ★** - We stored the App / bot / verification token in vault
- **App or Custom Integration ★** - Our application is running on machines supported by Ops team or using BuiltbySlack infrastructure
- **App or Custom Integration ★** - We have implement rate limit on every custom integration API endpoint
Completed!
The Security Team is here to help!
SDL submission notifications

jira APP 11:04 AM
Security API created Task PRODSEC-474

High Risk: Review: test project
Priority
Normal
Security Triage channels

#triage-security-prdct

maria created this channel today. This is the very beginning of the #triage-security-prdct channel. Purpose: Questions for Product Security Team. Group: @productsecurity

george 1:22 PM
joined #triage-security-prdct

george 1:30 PM
Hey 👋 I have a few questions about the SDL checklists for my project. I've checked off all the ones I'm sure of, and enlisted help from people who would know better in feat-awesome, but would like to meet or discuss via DM specifics around some of the unchecked SDL General checklist as a sanity check.
PRODSEC-679 SDL Checklist - Awesome Feature (Triage)
## Feature channels

### #feat-awesome

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:50 AM</td>
<td>josh</td>
<td>Hmm, regarding &quot;If the redirection must be arbitrary, and user-controlled, we are utilizing <a href="https://slack-redir.net">slack-redir.net</a> to facilitate the redirection&quot;, we can't do that since we're generating URLs outside of the app. I wonder if there's a different way to go about this one.</td>
</tr>
<tr>
<td>10:51 AM</td>
<td>kelly</td>
<td>good point @josh. Maybe @maria from the Security team can help out here?</td>
</tr>
<tr>
<td>10:51 AM</td>
<td>maria</td>
<td>joined #zebra from an invitation by @kelly</td>
</tr>
<tr>
<td>10:53 AM</td>
<td>maria</td>
<td>Hey! So I read the backscroll, and the main issue we're trying to prevent against is an open-redirect, which is primarily a social attack vector. If you can't use <a href="https://slack-redir.net">slack-redir.net</a> to generate the links, is it possible to force the user through a flow that makes it obvious that the user is going off-domain to a potentially trusted site?</td>
</tr>
<tr>
<td>10:54 AM</td>
<td>mary</td>
<td>I think we could do that. Might make the UX a tad bit difficult though. Do you have an example of what you're thinking of @maria?</td>
</tr>
<tr>
<td>10:54 AM</td>
<td>maria</td>
<td>Yea, one second</td>
</tr>
</tbody>
</table>
Here's an example of what HackerOne does to address this. We can do something similar (maybe with less-extreme text) for our implementation.

mary uploaded an image: Screenshot 2015-12-28 10.55.49.png

External link warning

You are about to visit an external link and we would like to pause for a moment out of an abundance of caution. Links to proof-of-concepts are generally benign but may often be accompanied by unintentional consequences. At a minimum, you should consider using a separate browser or virtual machine before proceeding.

External link:
http://www.microsoft.com/safelink

Proceed

mary Great, that's enough for me to go on. Thanks @maria!
maria No problem - Let me know if you have any other Security questions!
maria left #zebra
Why this matters!
Ongoing feedback
Unsolicited and Solicited Feedback

“Having my team see me complete the SDL was useful, and made me think through the things I was marking as complete.”

 “[The SDL] made me think of security things I normally don’t think about.”

“Upon going over [the SDL], we discovered there were a few things we needed to look at… Wonderful.”
Slack

All your team communication in one place, instantly searchable, and available wherever you go.

slack.com  ·  @slackhq  ·  Launched on February 28th, 2014

Rewards

<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1,500</td>
<td>$1,000</td>
<td>$500</td>
<td>$100</td>
</tr>
</tbody>
</table>

Policy

NEW: Program Update and Guide

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. 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

Response Efficiency

- 96% of reports
  - Meet response standards

Program Statistics

- $355,966
  - Total bounties paid
- $1,000 - $10,000
  - Top bounty range
- 760
  - Reports resolved
- 389
  - Hackers thanked
What’s next?
Thank You!

For more information go to: slack.com/security
Questions?