DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK TWO / LESSON TWO

Code ”Sharing”

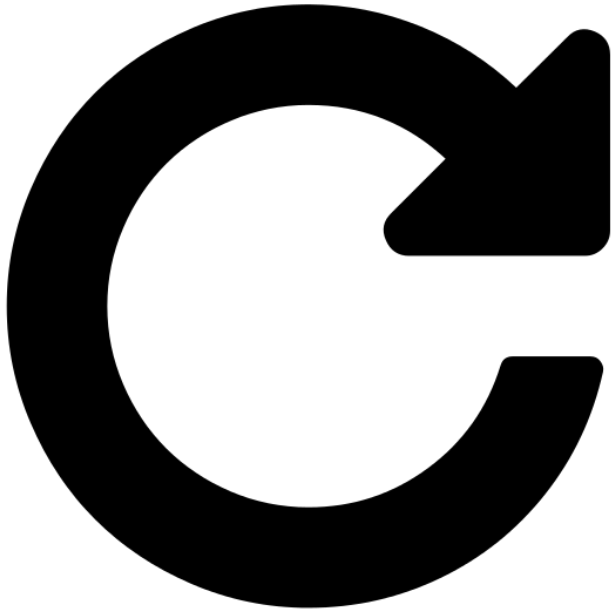
- Github makes copy paste easy
- It also makes it easy to paste in vulnerabilities
- Have you ever included a library without looking at it?
- https://github.com/rubysec/ruby-advisory-db

Bad Coding Practices

- Trusting the User
- Not Validating Input
- Hardcoding Secrets
- Trusting code without validating it
- Adding secrets to SCM (gitrob)
- What's your favorite?

Intersection with DevOps

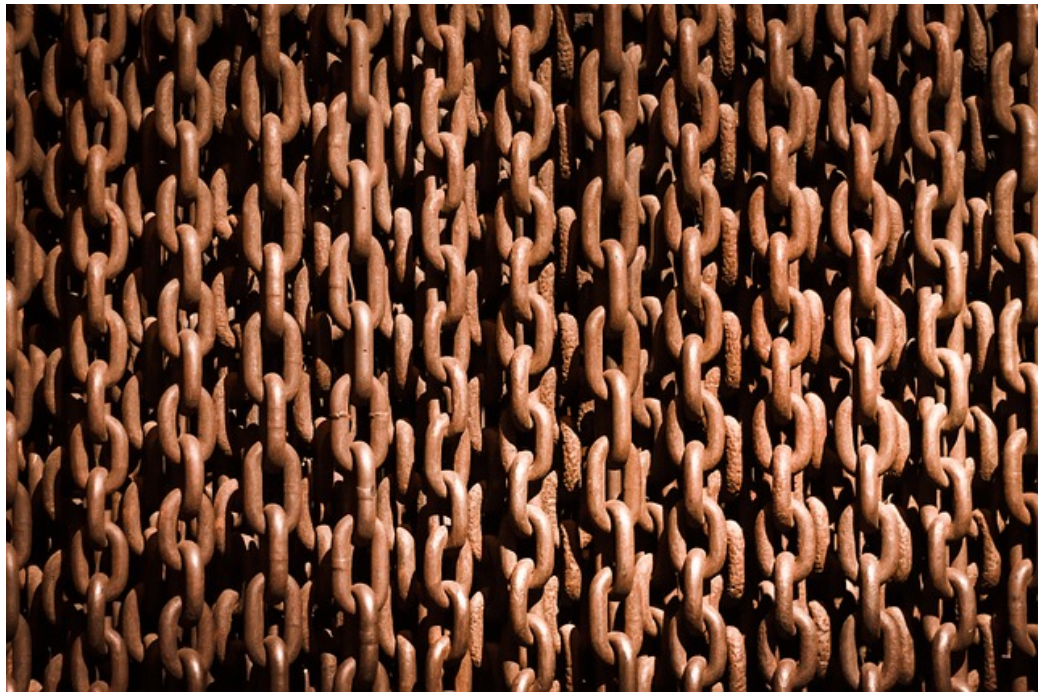
- Faster iterations can mean faster introduction of defects.
- Deployments now include infrastructure.
- Deployments now include application configurations.
- Anyone ever use Jenkins?
- BUT -> Faster iterations can mean faster fixes.



Font Awesome by Dave Gandy - http://fortawesome.github.com/Font-Awesome [CC BY-SA 3.0], via Wikimedia Commons

Software Supply Chain

- Better fewer suppliers
- Humans can’t move fast enough
- Automation is a must
- Be careful about selecting your dependencies
- The new hotness is not necessarily the most secure option



Top 10

- Code Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Lab 2 - Rails App from the Ground Up

Lab 3 - Deploying Vulnerable App

- You will be deploying the web app that you wrote this week to an AWS free tier account.
- There are vulnerabilities in this application so be Careful!
- Do not deploy this application to a cloud provider unless you know how to lock down access to only your remote IP!