**How Secrets Leak?**

Passwords, API keys and secret tokens must not be left lying around your environment unprotected. Their purpose is to provide controlled access to sensitive resources such as a database that holds customer information, or your billing system, or the provider that you send usage data to for calculating customers’ bills each month. They could even provide controlled access to other systems in your own environment.

**The following lists some of the ways that secrets might leak and who they might be leaked to:**

* Code repository exposure:
  + Secrets exposed to internal employees (depending on the secret, this might or might not be an issue).
  + Secrets exposed to external people (for example, a misconfigured public GitHub repo might expose your secrets).
* Laptop loss/equipment theft:
  + A developer's laptop might be lost and accessed by a third party.
* Application reverse engineering/code reading:
  + Not all code is private. Front-end web application code is sent to the user to be rendered.
  + Some software stacks will reveal code and/or a stack trace back to the user on failure, potentially revealing secrets.
  + Some deploy methods use *git pull* but don’t restrict access to the .git directory.

**Workplace Scenario:**

The configuration management code base has some secrets listed in it, but none of them relate to the product services. For example, you have found a database username and password, and that user is being setup for database access through configuration management.

However, you can’t figure out how a developer’s application might know how to talk to that database using those credentials. You check for S3 buckets that might contain credentials but find none. Finally, you ask a developer how their application connects to the database, and they point you to a line of code on GitHub. There you see a username and password stored in plain text. As you look at their code and the code from other services, you realize the passwords and API tokens are regularly stored directly in code.