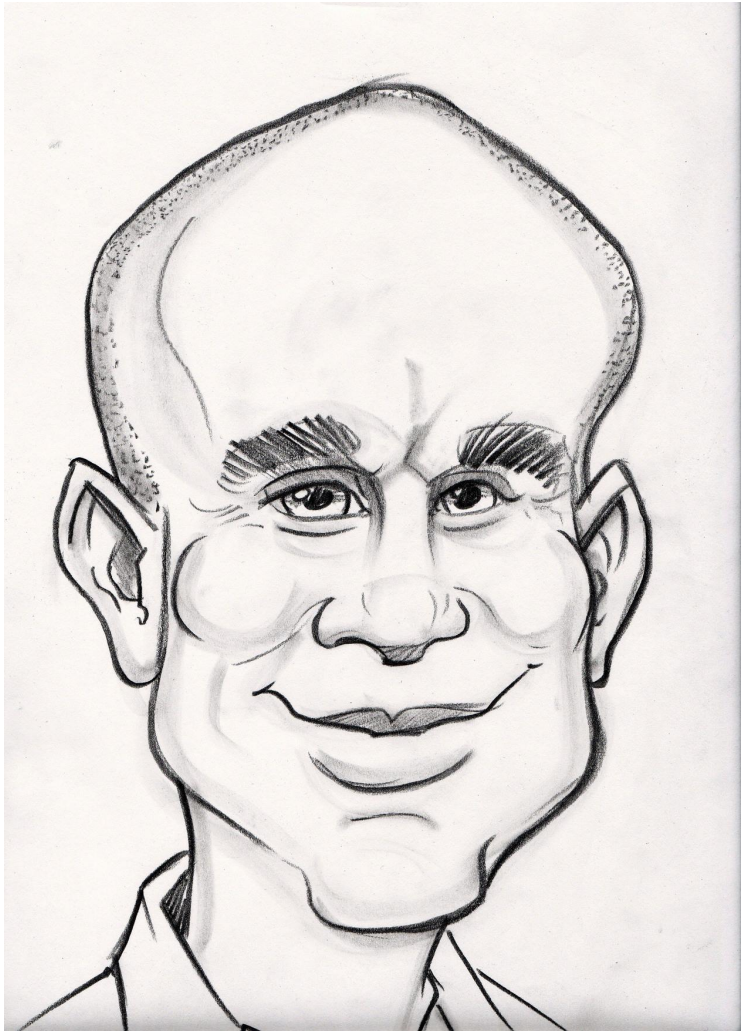
Writing Secure

Code

Miki Tebeka



CEO, CTO, UFO ...

353solutions

First rule of computer security: **don't buy a computer**.
Second rule: if you buy one, **don't turn it on**.

- Dark Avenger

The Security Mindset

Bruce Schneier

Culture > Process

Go Security Policy

OWASP Top Ten

Input

A03:2021-Injection

A10:2021-Server-Side Request Forgery

Output

A02:2021-Cryptographic Failures

A05:2021-Security Misconfiguration

Authentication

A01:2021-Broken Access Control

A07:2021-Identification and Authentication Failures

A05:2021-Security Misconfiguration

Infrastructure

A04:2021-Insecure Design

A06:2021-Vulnerable and Outdated Components

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

Code

Input

A03:2021-Injection

database/sql

A08:2021-Software and Data Integrity Failures

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

Billion laughs attack

Java Hangs When Converting 2.2250738585072012e-308

[Exploring Binary]

io.LimitReader

Output

A03:2021-Injection

html/template

A02:2021-Cryptographic Failures

//grep.app

AWS_SECRET_ACCESS_KEY=".{40}"

Case sensitive | Regular expression | Whole words

Repository

Filter repos

- kanisterio/kanister
- mongodb/mongo-ruby-driver
- ParabolInc/parabol
- aws/aws-health-tools
- schireson/pytest-mock-resources
- vwal/awscli-mfa
- restic/restic
- SUSE/skuba

Path

Filter paths

- .evergreen
- docs
- tests

Showing **1 - 10** out of **33** results

Default | Extended

This is a partial result set. The search was stopped early because it would take too long to check every file for this regular expression. If you're looking for files within a particular repository, try typing it into the repo filter box.

JuliaWeb/HTTP.jl

test/aws4.jl — 3 matches

```
23              aws_access_key_id="AKIDEXAMPLE",
24              aws_secret_access_key="wJalrXUtnFEMI/K7MDENG+bPxRfiCYEXAMPLEKEY",
25              include_md5=false,

157              aws_access_key_id="AKIAIOSFODNN7EXAMPLE",
158              aws_secret_access_key="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
159              include_md5=false)
```

returntocorp/semgrep-rules

python/boto3/security/hardcoded-token.py — 2 matches

```
4  # ruleid:hardcoded-token
5  client("s3", aws_secret_access_key="jWnyxxxxxxxxxxxxxxxX7ZQxxxxxxxxxxxxxxx")
6
7  # ruleid:hardcoded-token
```

Authentication

A07:2021-Identification and Authentication Failures

- Basic
- Oauth2
- JWT
- OICD
- ...

A01:2021-Broken Access Control

- ACL
- RBAC
- ...

Infrastructure

A05:2021-Security Misconfiguration

http.ListenAndServeTLS

x/crypto/acme/autocert

A06:2021-Vulnerable and Outdated Components

- Go CVE List
- Synk Vulnerability DB
- golang-announce
- golang/x/vuln

go.mod
go.sum

dependatbot

A09:2021-Security Logging and Monitoring Failures

- log
- go.uber.org/zap
- ...

- expvar
- prometheus
- ...

Questions?

Thank You!

@tebeka

miki@353solutions.com

yoni@ariga.io