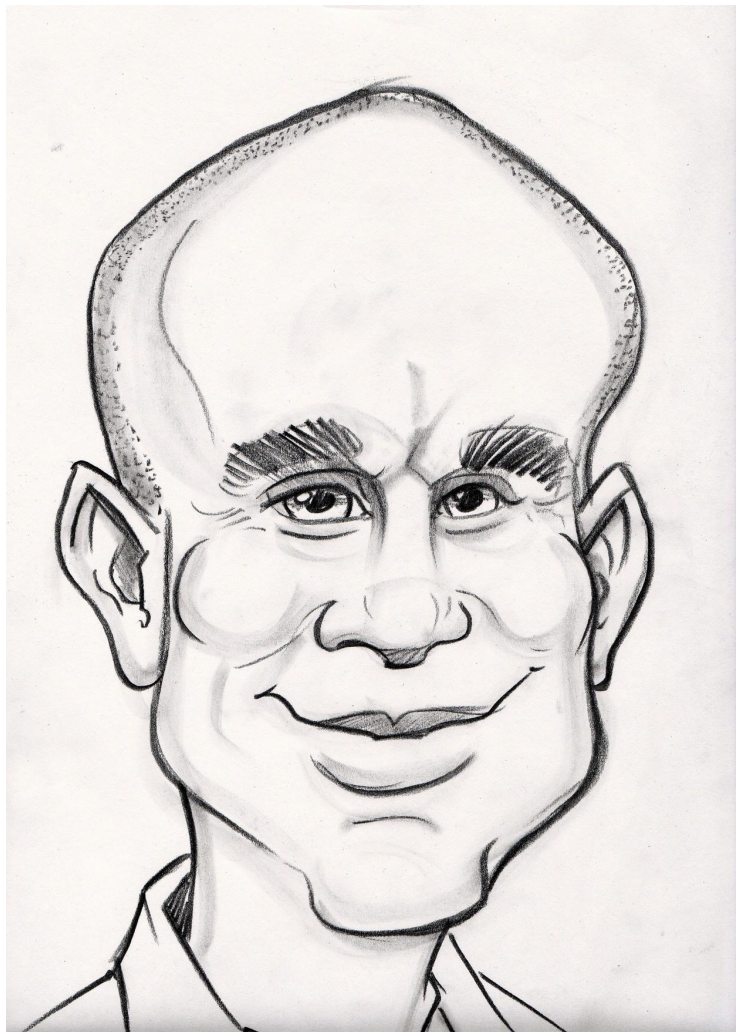


Writing Secure



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

The image features the word "GO" in a bold, sans-serif font. The letters are a vibrant magenta color. To the left of the letter "G", there are three horizontal, parallel lines of the same color, which are slightly slanted and appear to be trailing behind the letter, suggesting speed or motion. The entire graphic is centered horizontally on a plain white background.

Go Security Policy

Where?

- Go CVE List
- Synk Vulnerability DB
- golang-announce

OWASP Top Ten

A1: Injection

A2: Broken Authentication

A3: Sensitive Data Exposure

A4: XML External Entities (XXE)

A5: Broken Access Control

A6: Security Misconfiguration

A7: Cross-Site Scripting (XSS)

A8: Insecure Deserialization

A9: Using Components with Known Vulnerabilities

A10: Insufficient Logging & Monitoring

Input	A1: Injection A4: XML External Entities (XXE) A8: Insecure Deserialization
Output	A7: Cross-Site Scripting (XSS) A3: Sensitive Data Exposure
Authentication	A2: Broken Authentication A5: Broken Access Control
Infrastructure	A6: Security Misconfiguration A9: Using Components with Known Vulnerabilities A10: Insufficient Logging & Monitoring

Code

Input

A1: Injection

database / sql

A8: Insecure Deserialization


```
<?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

A7: Cross-Site Scripting (XSS)









html/template

A3: Sensitive Data Exposure

Case sensitive Regular expression Whole words





Repository

Filter repos

-  kanisterio/kanister
-  mongodb/mongo-ruby-driver
-  ParabollInc/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

i 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+bPxrRf1CYEXAMPLEKEY",
25     include_md5=false,
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58     aws_access_key_id="AKIAIOSFODNN7EXAMPLE",
59     aws_secret_access_key="wJalrXUtnFEMI/K7MDENG/bPxrRf1CYEXAMPLEKEY",
60     include_md5=false)
61
```

 returntoCorp/semgrep-rules

python/boto3/security/hardcoded-token.py

2 matches

```
4 # ruleid:hardcoded-token
5 client("s3", aws_secret_access_key="jWnyxxxxxxxxxxxxxxxxX7ZQxxxxxxxxxxxxxxxx")
6
7 # ruleid:hardcoded-token
```


Authentication

A2: Broken Authentication

- Basic
- OAuth2
- JWT
- OIDC
- ...

A5: Broken Access Control

- ACL
- RBAC
- ...

Infrastructure

A6: Security Misconfiguration

http.ListenAndServeTLS

x/crypto/acme/autocert

A9: Using Components with Known Vulnerabilities

go . mod

go . sum

dependatbot

A10: Insufficient Logging & Monitoring

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

- `expvar`

- `prometheus`

- `...`

Questions?

Thank You!

@tebeka

miki@353solutions.com

