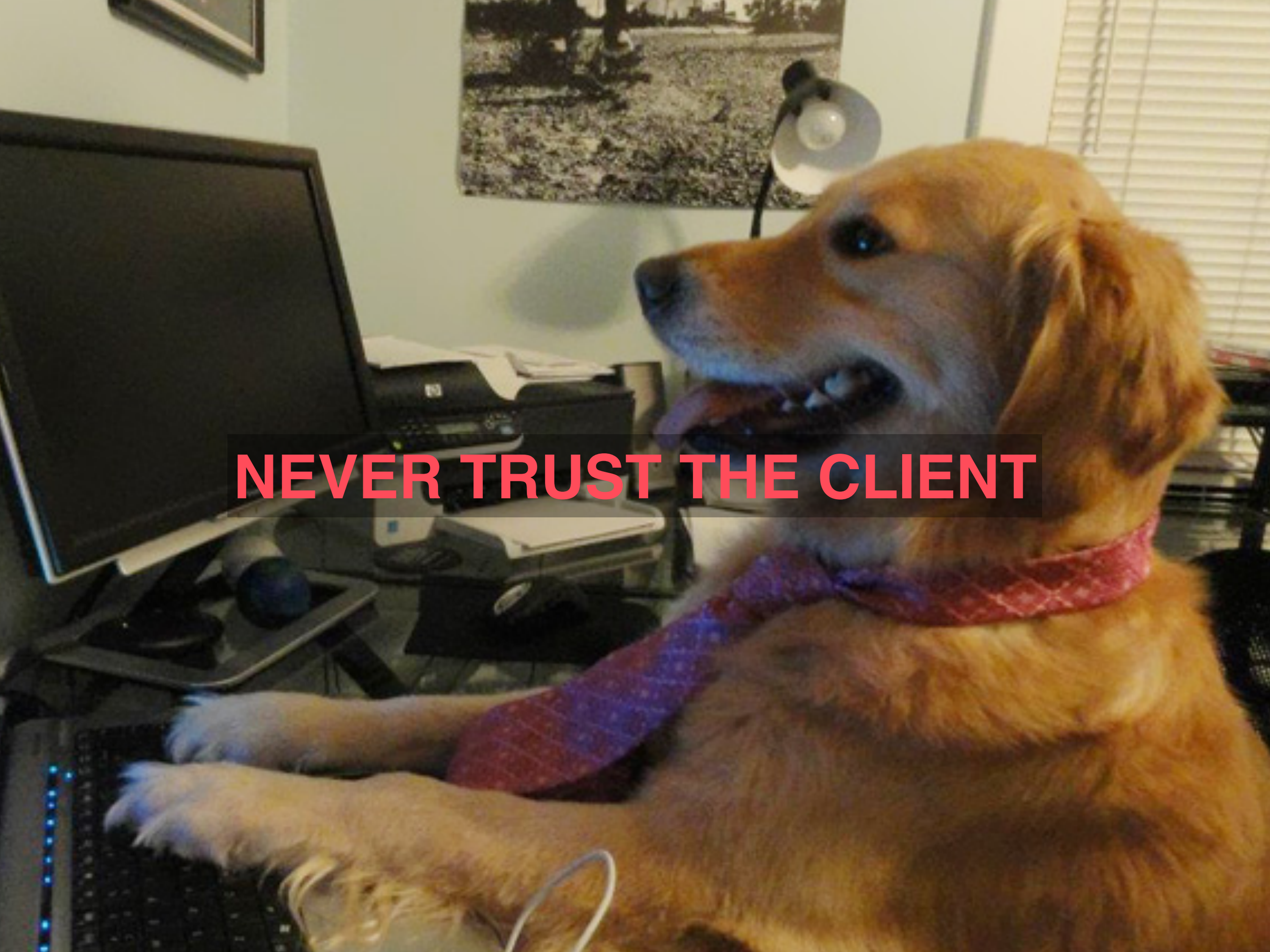
SECURING YOUR WEBSERVICE

@garrybodsworth
https://www.yagro.com


NEVER TRUST THE CLIENT

server.com

x.x.x.x

Server

Your code

Database

Storage

server.com

x.x.x.x

Server

Your code

Database

Storage


© Bob Elsdale

CENTRAL BUREAUCRACY

Est. 2159 A.D., License Pending

server.com
HTTPS
x.x.x.x

HTTP

Bastion/
NAT

SSH

Server
Your code
Database

Database

Database

TCP

Storage

TCP 3306

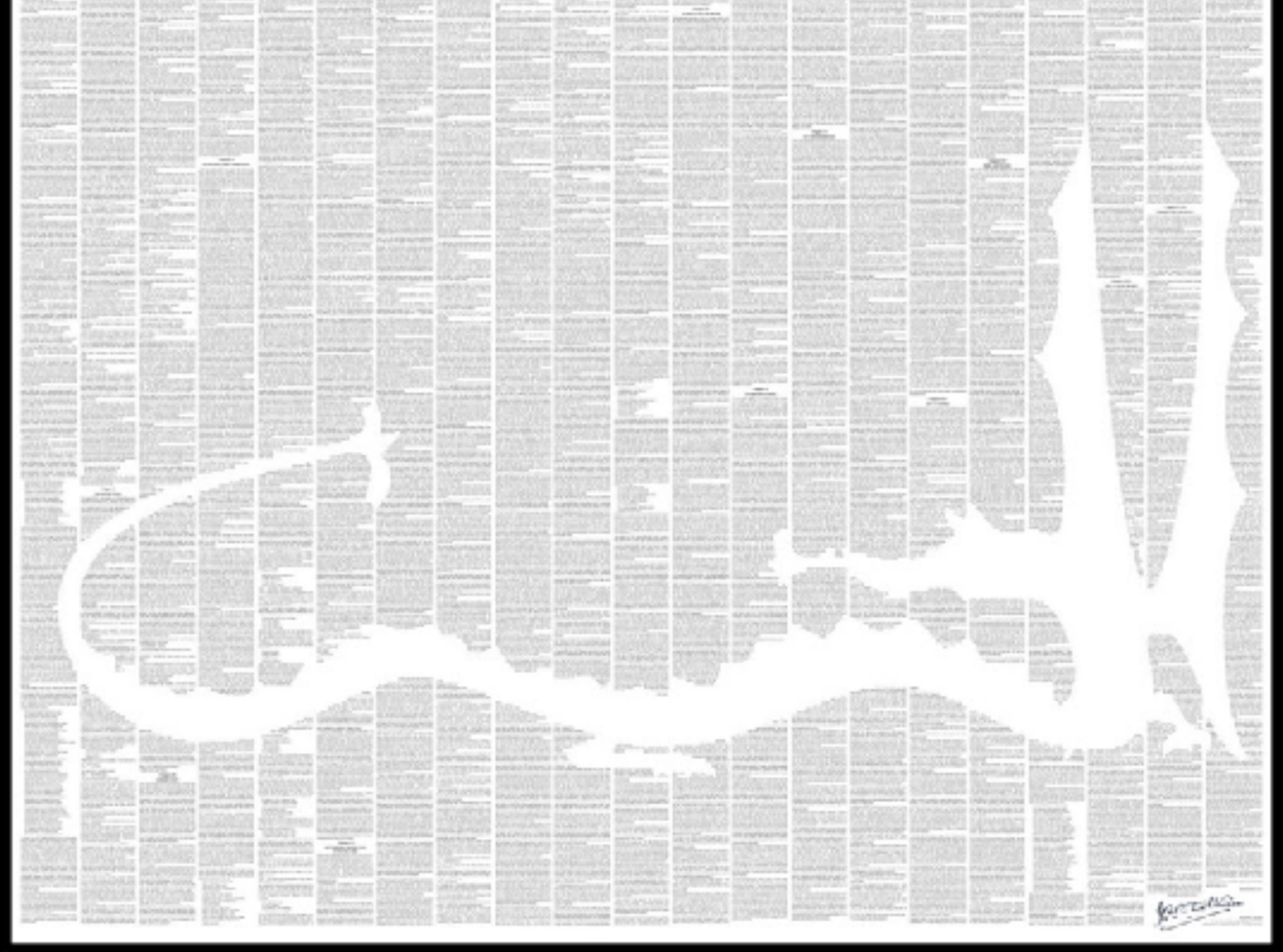
Database


gifbin.com

Gear Up!


DELETE COOKIES?!

THE HOBBIT



SSL CERTIFICATES

ENCRYPTION

- Transport
- Data at rest

- Cryptographic hash (one-way)
- Reversible (two-way)

- Symmetric
- Asymmetric

MANAGING SECRETS

- Updating certificates
- Rolling keys
- Service passwords
- Who knows all your secrets?
- Are your secrets safe?
- “Secret Server”, Vault, KMS

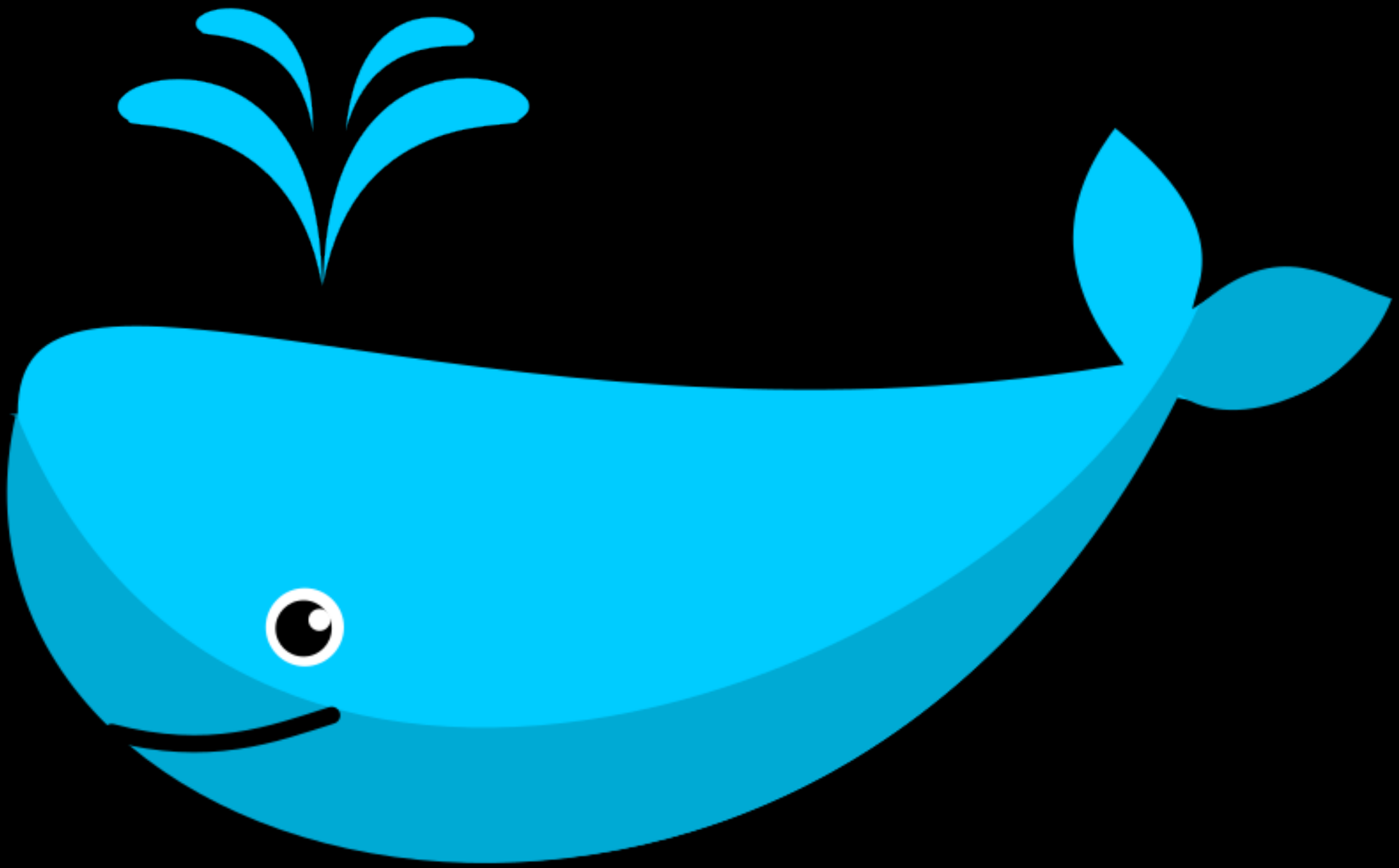
SQL INJECTION

CODE QUALITY

- Static analysis
- Language specific tools
- Don’t repeat yourself (D.R.Y)
- Code coverage

CONTINUOUS DEPLOYMENT

Bundling



AWS

- Cloudformation
- Troposphere
- EC2 Container Service
- Credentials/Secrets

* https://github.com/cloudtools/troposphere

CI/CD

GitLab

Updates

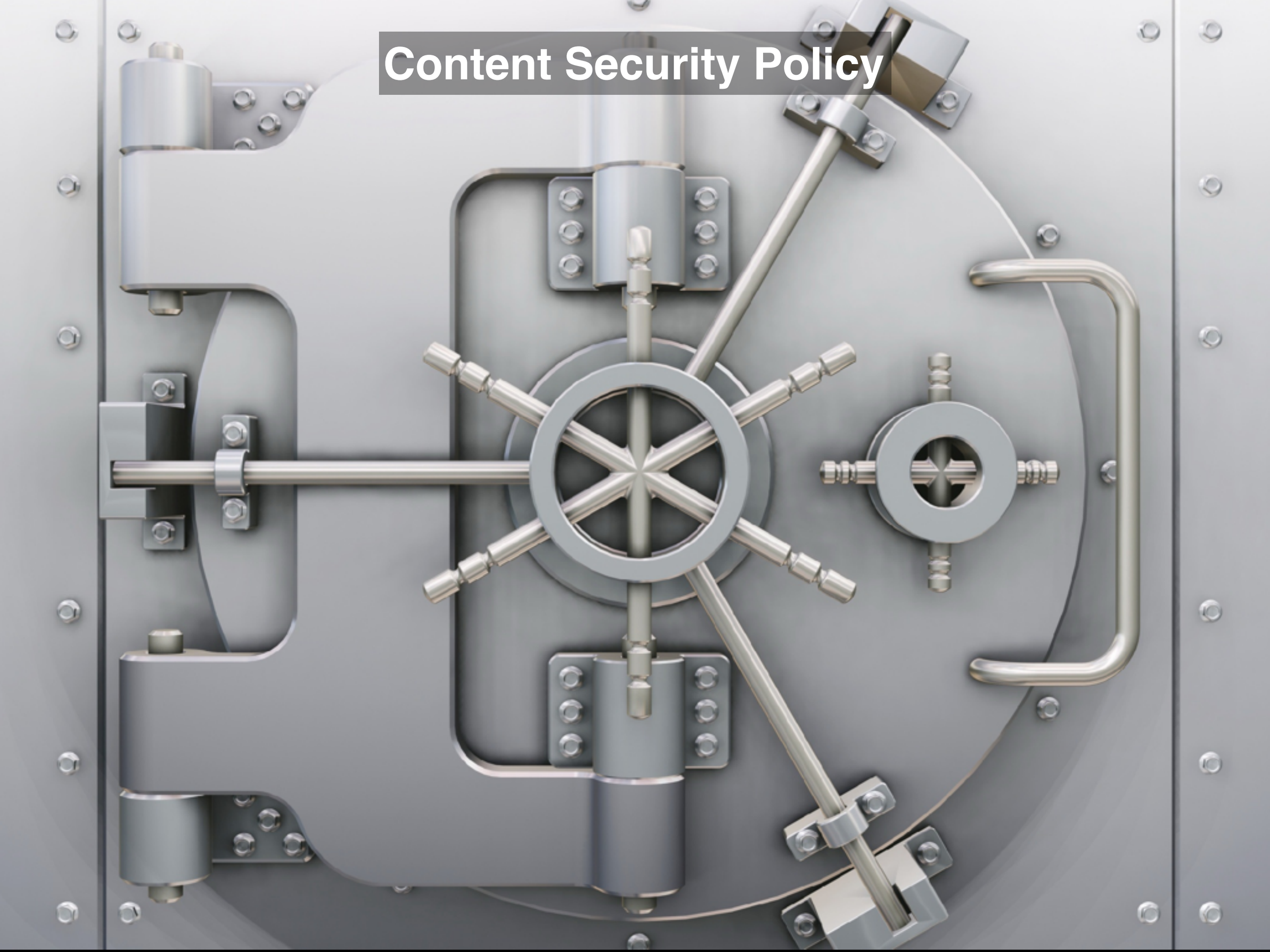
- X-CSRF
- Forms
- Referer
- Origin

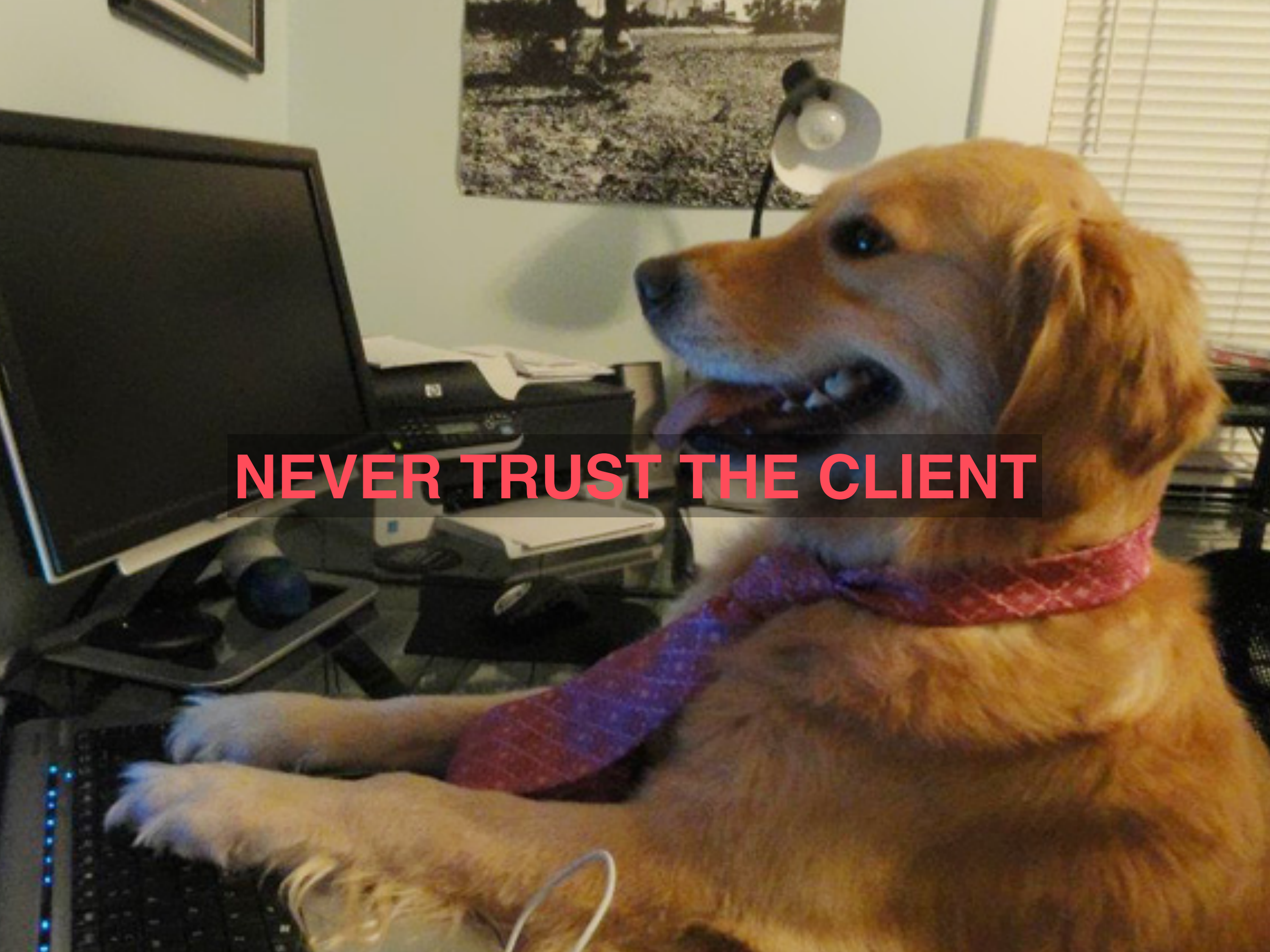
MIXED CONTENT

IFRAMES


XSS
Reflected
Persistent
UXSS

Content Security Policy




NEVER TRUST THE CLIENT

LOOK OVER THERE!

Fooled You, Didn't We?

server.com
HTTPS
x.x.x.x

HTTP

Bastion/
NAT

SSH

Server
Your code
Database

Database

Database

TCP

Storage

TCP 3306

Database

https://observatory.mozilla.org

What have I missed?

- Multiple headers
- DoS - head of line blocking
- Brute force
- Hashing is not encryption!
- SSL ciphers
- Certificate pinning
- PCI compliance
- PII
- CVEs and vulnerability disclosures
- File format parsing
- Pen tests
- Physical pen tests
- Reproducible builds
- Guessable URLs
- Examples of exploits!

- SChannel
- Enterprise networks
- CORS
- MitM
- RSA4
- goto fail;
- Malicious actors
- Physical intrusion
- More passwords stolen
- Incident response
- Physical security solutions
- Fuzz testing
- Session hijacking
- Misconfiguration
- And sooooooooooo much more

And finally….. get a password manager!

BUT DON’T USE THE BROWSER PLUGIN!!!

- **OWASP** https://www.owasp.org/ (see Reference section on left)
- **Mozilla Security Blog** https://blog.mozilla.org/security/
- **Content Security Policy** https://scotthelme.co.uk/content-security-policy-an-introduction/
- **CVEs** https://cve.mitre.org
- **SPA Security** http://www.slideshare.net/carlo.bonamico/angularjs-security-defend-your-single-page-application
- **HTML5 Security Cheatsheet** https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet