INTRODUCTION TO WEB APPLICATION SECURITY WITH OWASP TOP 10

Tekna 2023

Johan Paramanathan
Security Lead

whoami

root

- Education: MSc in Cyber Security from UiO
- Experience: Security Analyst/Engineer/🥔/🏆/Architect
- Certifications: CCSP, Microsoft, Google, Splunk, ISO27k ++
- **Blog: Diary of Security Engineer - johanpara.substack.com**

whoRu???

- Developers
- Designers
- Advisors/Architects
- SysAdmins?
- Security People
- Other??

bouvet

THIS IS BOUVET

- We are a Norwegian consulting company that assists other companies in developing efficient and user-oriented solutions within technology, consulting, design and communication.
- Contented employees, who feel they can make the best of their talents, will deliver the best work.
- We are a team of over 1, 800 dedicated employees spread across 15 offices in Norway and Sweden. We are also listed on the Oslo Stock Exchange

bouvet

bouvet

OUR VISION

We lead the way and build tomorrow’s society.

bouvet

AGENDA

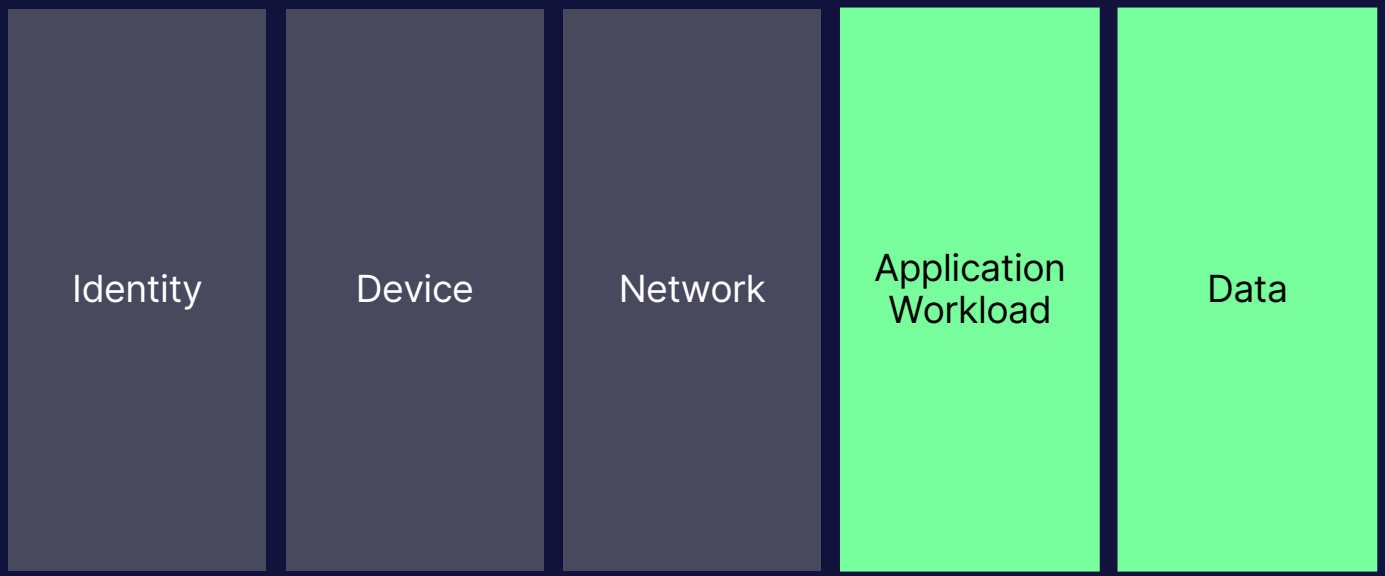
Agenda

Basics of Web Applications + Cyber Security	10 min
Top 10 risks from OWASP	30 min
Q&A	5 min
Conclusion	1 min 337Seconds

Disclaimer

🌊

- I'll try to cover the basics, but there is more..
- There are some bad movie examples; on purpose ☺

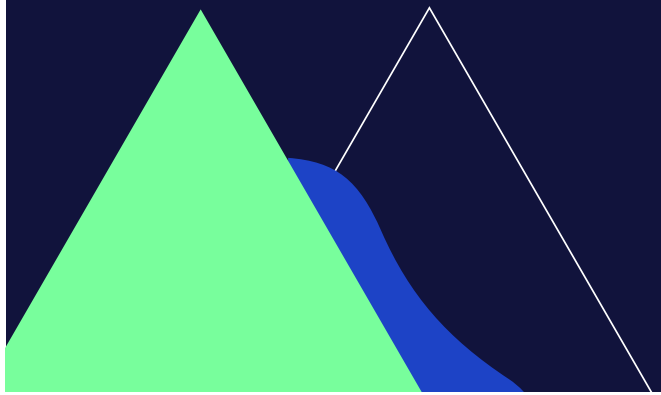


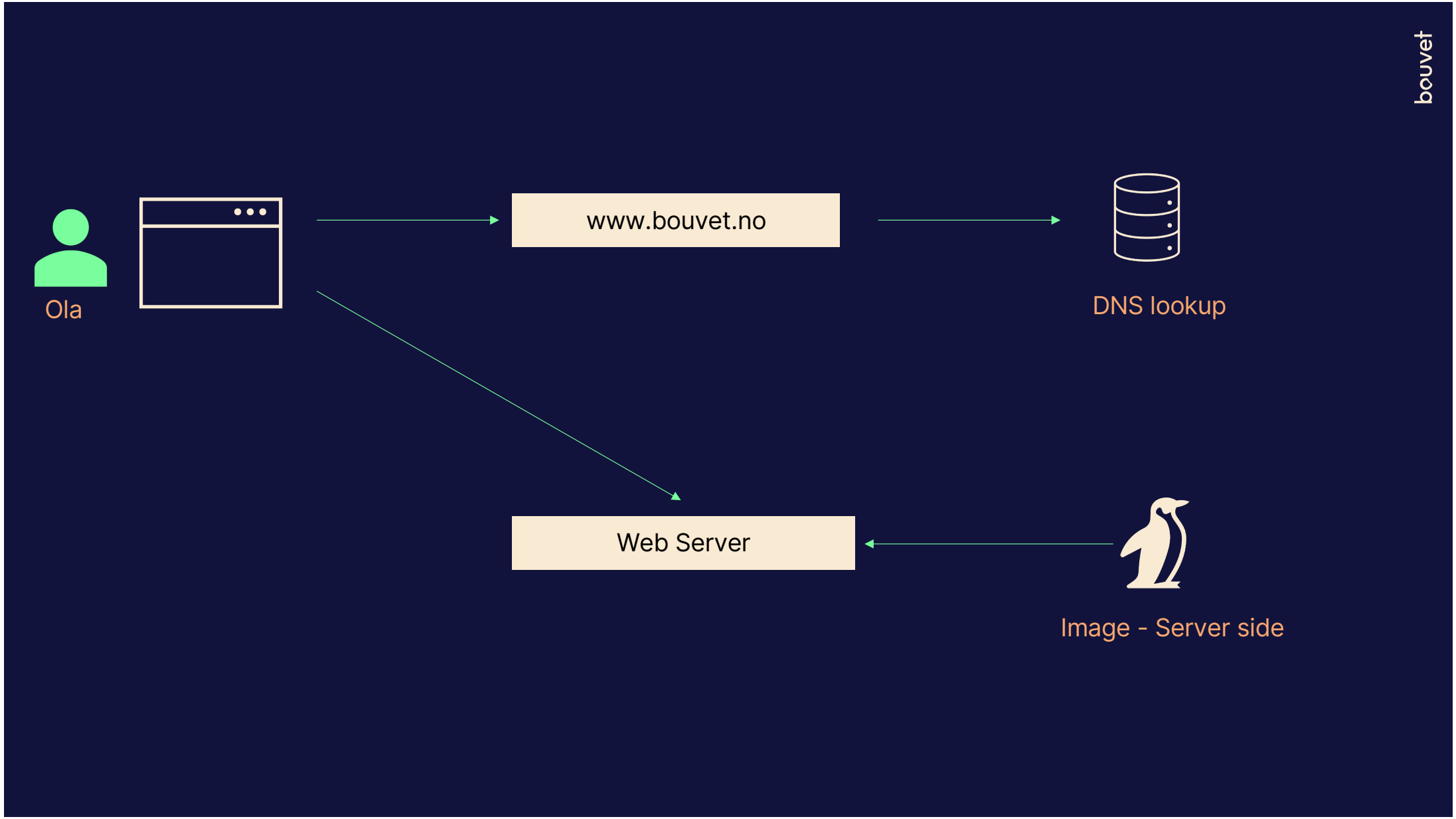
Source: Zero-Trust Pillars, CISA

bouvet

THE BASICS

Like the super duper simple version




bouvet
Ola
www.bouvet.no
DNS lookup
Web Server
Image - Server side

We use - HTTP HEADERS

POST/PUT/GET

- General Headers
- Request Headers
- Response Headers
- Entity Headers
- Security Headers

.

.

.

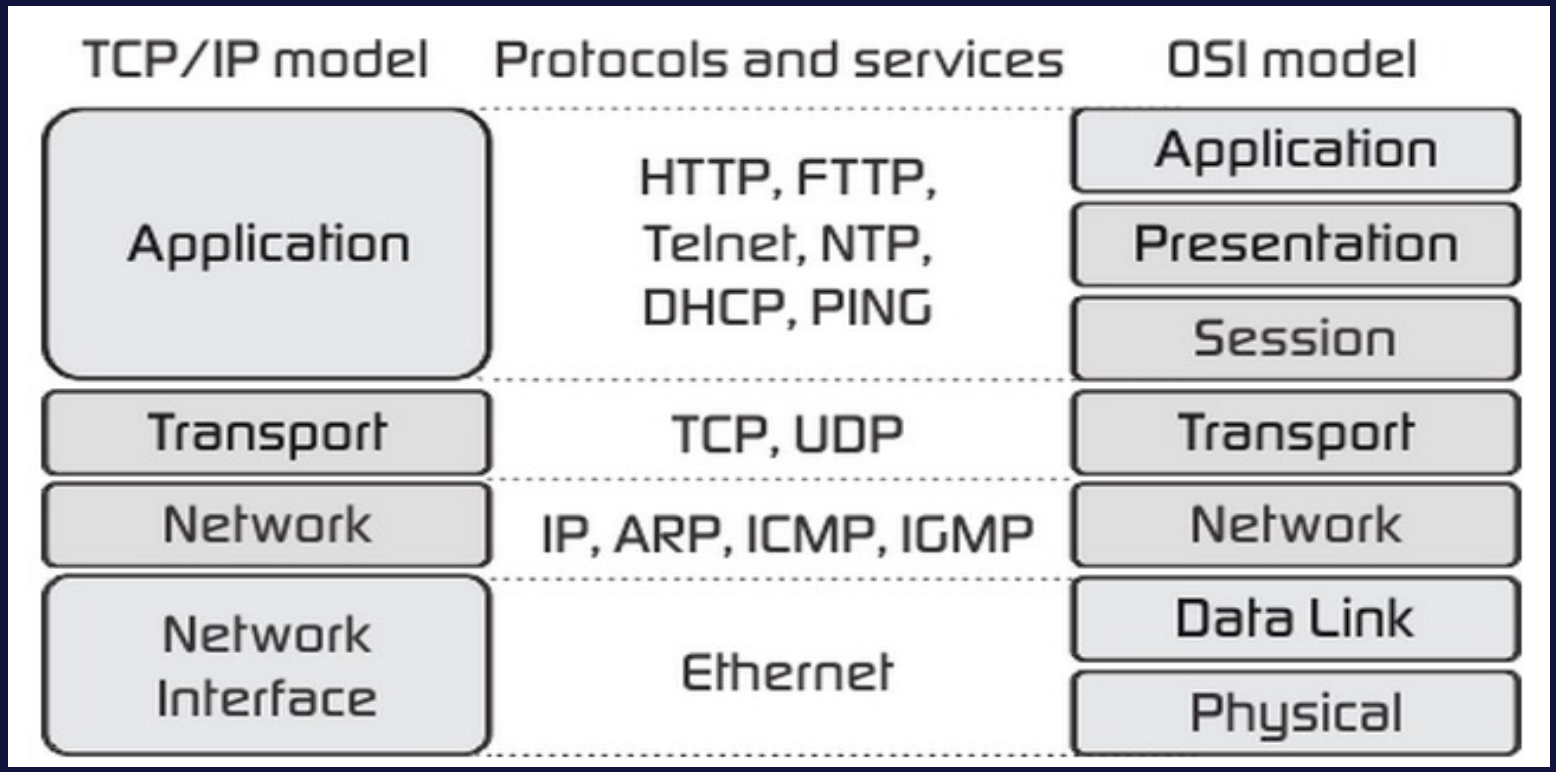
.

Internet Engineering Task Force (IETF) RFC 9110

We often talk about layers

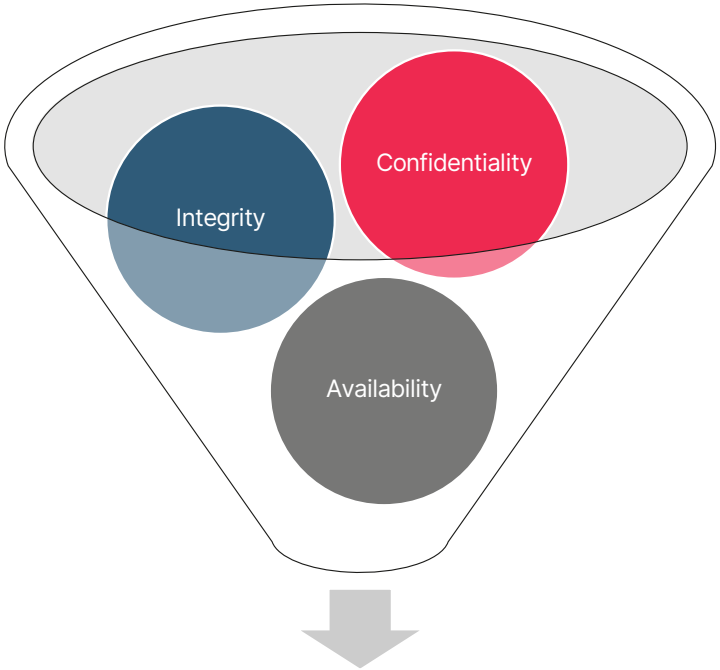
Layer 7
Our focus!

Layer 4



Principles: Information Security

CIA TRIAD – (Not Central Intelligence Agency 😂)



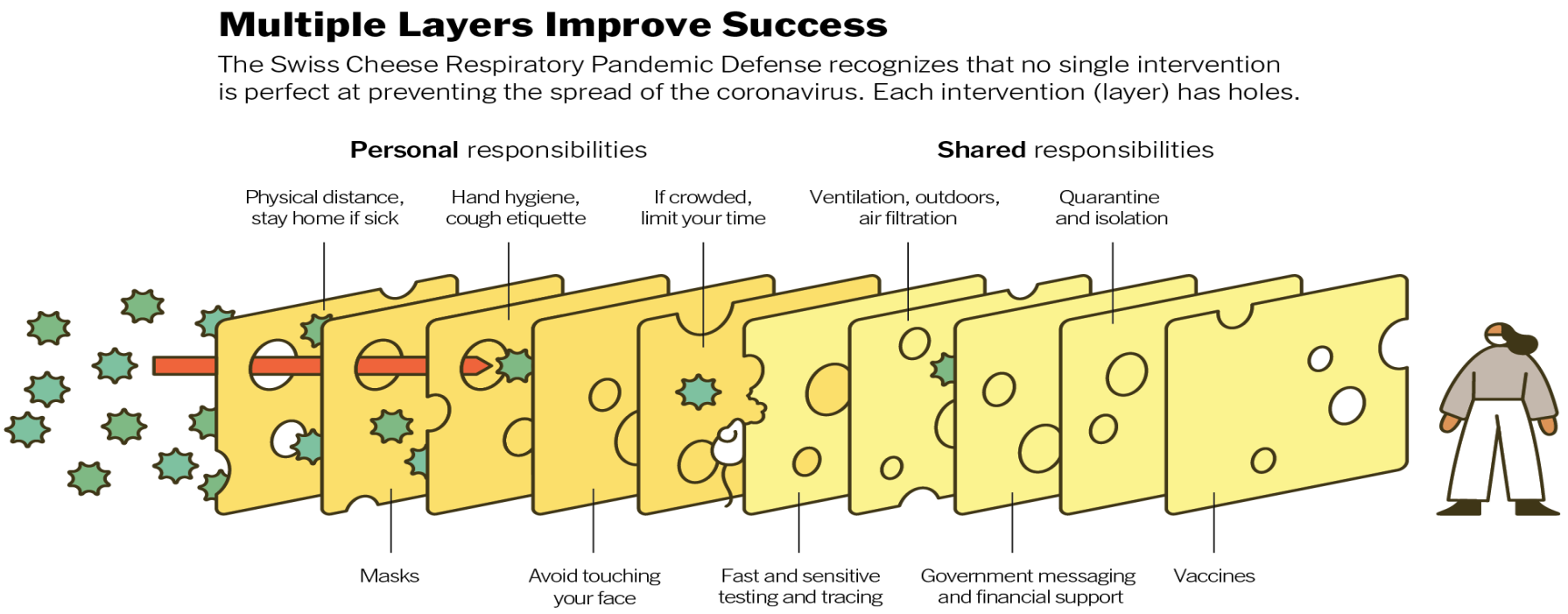
Information Security

Source: ISO27001

bouvet

Principles: Information Security

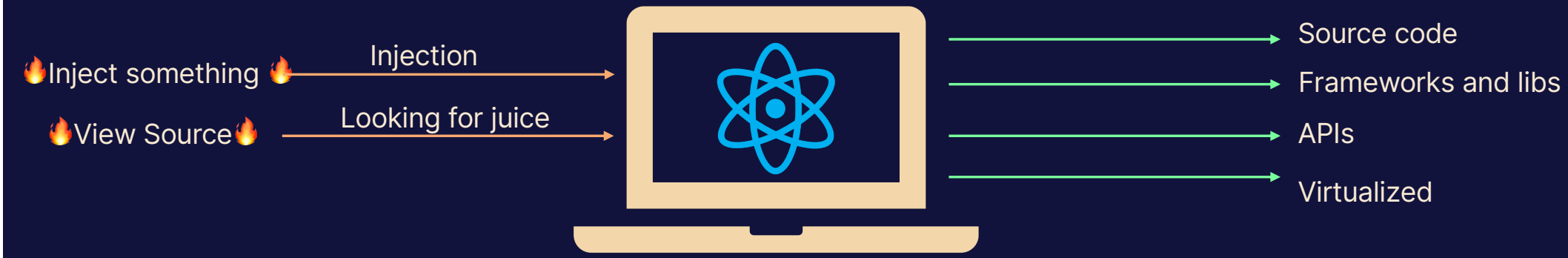
Defence in depth (Swiss Cheese model)



Source: Adapted from Ian M. Mackay (virologydownunder.com) and James T. Reason. Illustration by Rose Wong

bouvet

Typical Modern Application



bouvet

Cyber Security 101 – Risk Management

Threat Actor

LOG4SHELL

Uses Vulnerability

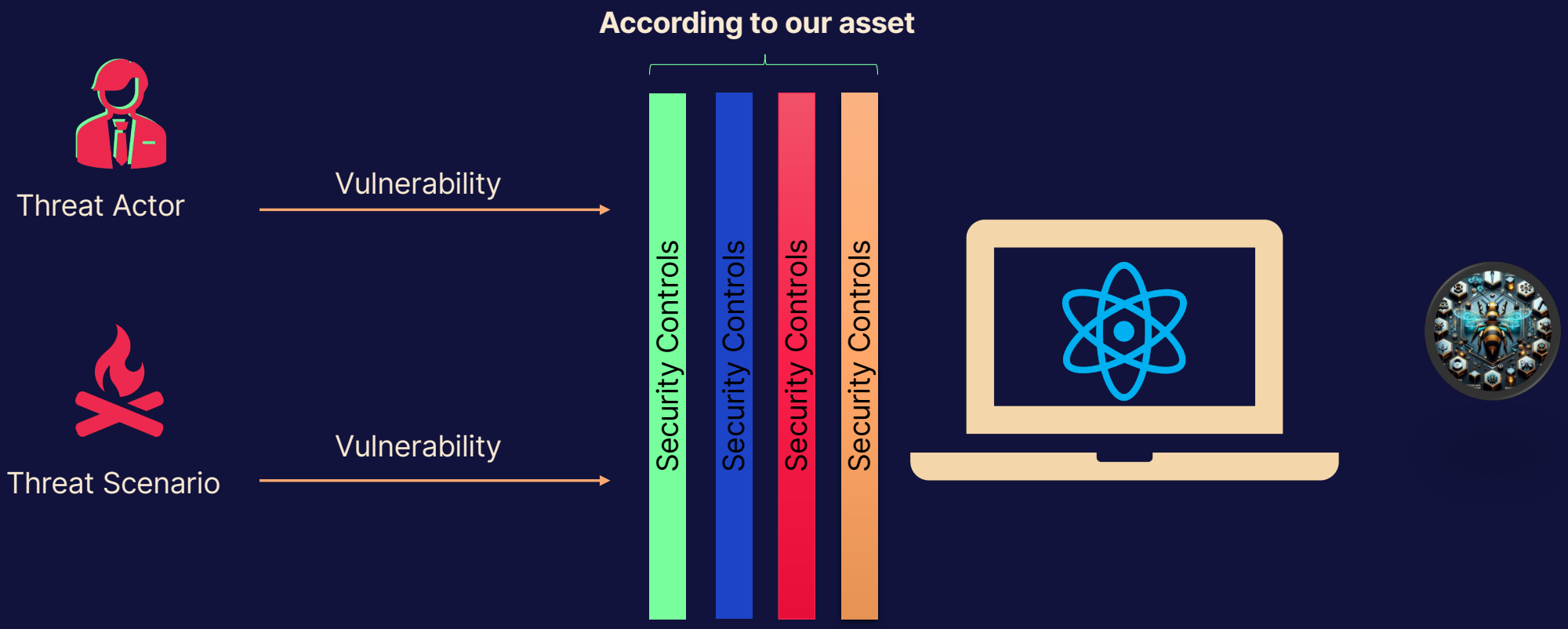
Threat Scenario

Outage

Vulnerability

Source: ISO27001

Cyber Security 101 – Risk Management



Source: ISO27001

bouvet

OWASP TOP 10

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

Fun fact 😂

O + WASP = OWASP

bouvet

Introduction to OWASP

Much ❤ to the OWASP Community!

Who is OWASP?

An international nonprofit organization
Dedicated to improving software security

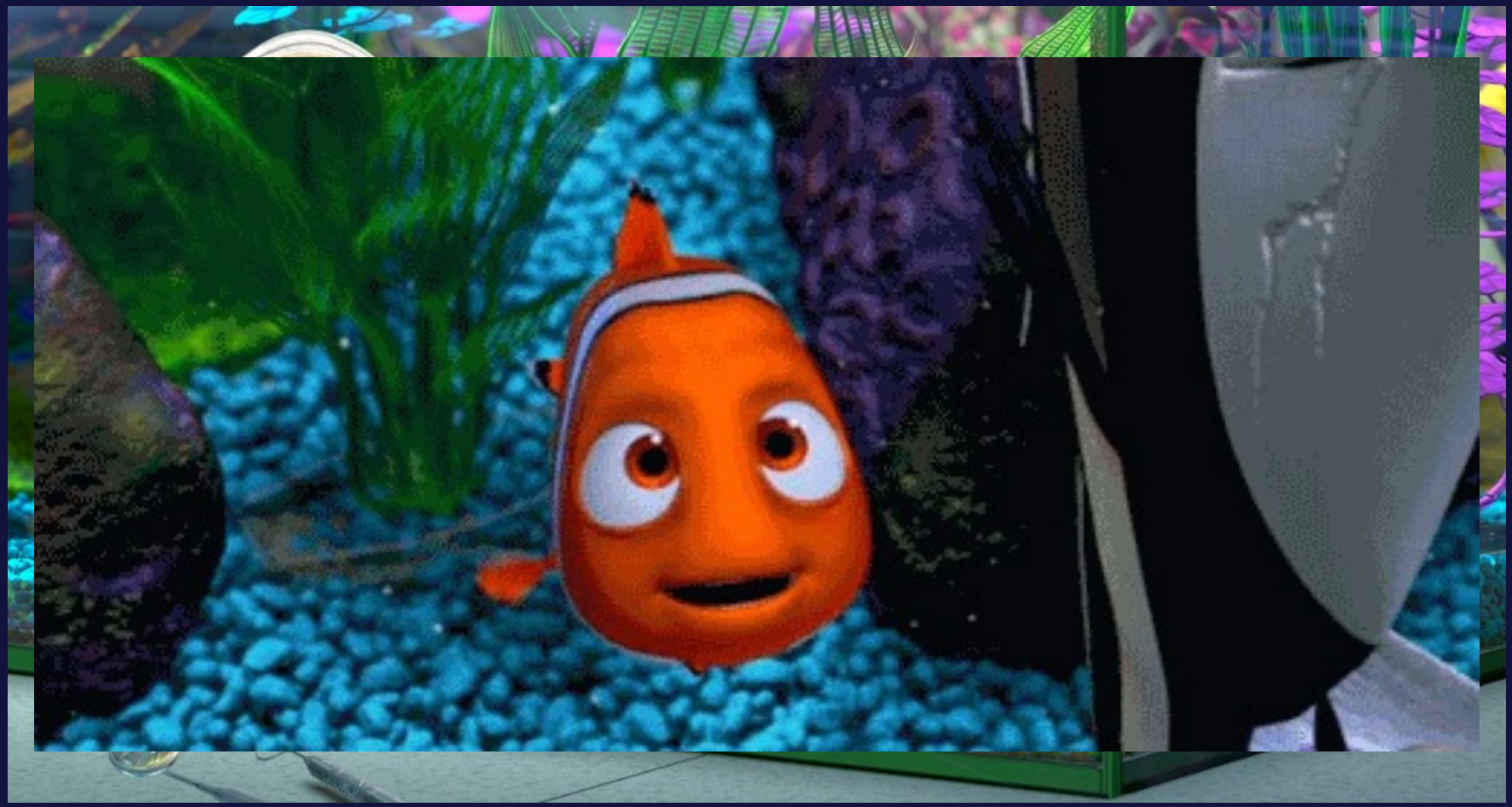
Activities and Offerings

Publishes the OWASP Top 10 list of the most critical security risks to web applications
Provides free, openly available documentation and tools
Hosts local chapters, conferences, and training sessions

A01:2021

BROKEN ACCESS CONTROL

To break or not to break



Movie: Finding Nemo

bouvet

Broken Access Control

94% of applications were tested for some form of broken access control

OWASP Perspective

- Users can access and perform actions beyond their permissions.
- Modification or destruction of data.
- Execution of business functions beyond user's authorized limits.

Practicioners perspective

- Increase of cloud services, most use IAM as their primary security architechture.
- *Agree or disagree that this is the most prominent risk?*

Broken Access Control

Attack/Defense

Bypass Access Control checks

🔥**Insecure direct object references**🔥

Missing Access controls for PUT/POST and Delete

Elevation of privilege

Server-Side Access Control

Deny by Default

CORS
Controls when content can be shared between different domains.

Rate Limit API and Controller Access

Invalidate Session Identifiers After Logout (Oauth)

bouvet

Broken Access Control - IDOR

```
pstmt.setString(1, request.getParameter("acct"));

ResultSet results = pstmt.executeQuery( );
```

Voldemort1337

→ https://example.com/app/accountInfo?acct=~~Dobby93~~

bouvet

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph: Strava Heatmap

Real World: Strava 2018

- 2018 Strava fitness app tried to show anonymized data
- *Disclosed "Secret" US army base*

bouvet

A02:2021

CRYPTOGRAPHIC FAILURES

Better to encrypt, than to be sorry

bouvet

Due to bad encryption, Jafar gets access to the lamp

Cryptographic Failures

46% of applications were tested for some form of cryptographic failures

OWASP Perspective

- Weak algorithms or poor key management.
- The shift in naming from Sensitive Data Exposure to Cryptographic Failures

Practitioner Perspective

- AWS buckets
- Quantum Computing
- Confidential Computing
- *Compliance engineering? Anyone?*

Cryptographic Failures

Attack/Defense

Default passwords

Downgrade Attacks

Exploiting Cryptographic Errors

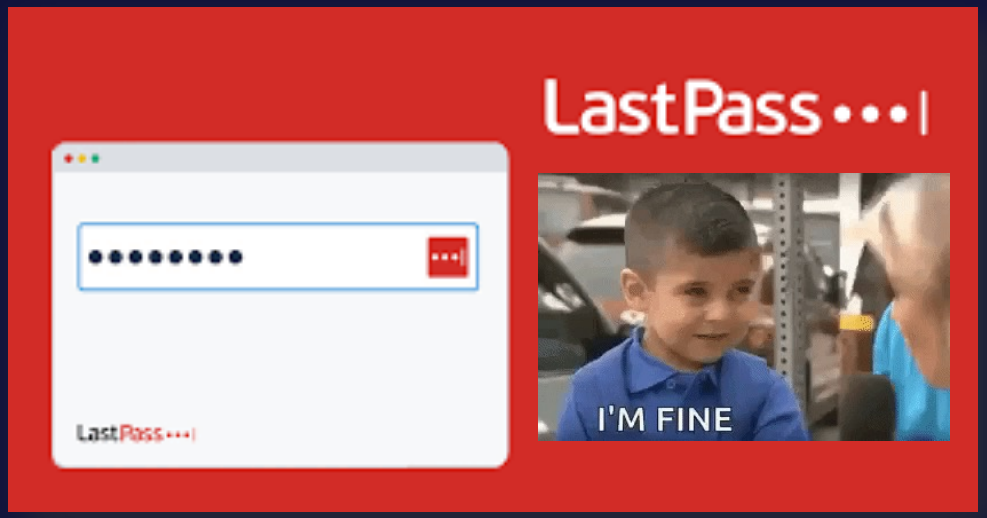
Secret managers

Proper Implementation

Data Classification and Protection

Secure Data Transit: TLS 1.3

bouvet



bouvet

Real World: Last Pass

- **Threat actor exfiltrated encrypted backups and an encryption key from the same storage vault it shares with LastPass.** 🔥
- Older users older configs – Users from 2018 has 1000 iterations? They have 100k today ☺

A03:2021

INJECTION

Injections are just like vacines, we need to validate them

bouvet

vet

A03:2021 – Injection

From 1 → 3

OWASP Perspective

- Malicious data is executed by an application, leading to unauthorized access.
- User-supplied data is not validated, filtered, or sanitized by the application.

Practitioner Perspective

- It's gotten a lot better over the years. Probably because of the awareness the OWASP Top 10 brings.
- *Who has implemented input/output validation in their application?*

Injection

Attack/Defense

SQL Injection	Executing unintended commands or accessing unauthorized data.
Command Injection	An attacker injects malicious commands into an applications (LDAP, XML, Xpath, HTML, OS etc)
Cross-Site Script (XSS)	Malicious scripts from running on the user's browser
CSRF	User browser → Request to unwanted site(Authenticated)

Parameterized Querries

- Don't take *user input* for good fish 🐟

Input Validation

- OWASP ASVS Chapter 5.1

🔥Web application Firewall🔥

Error Handling

- 👀A lot of juicy information is given here!👀 500?

🔥Content Security Policy🔥

Limited database access

bouvet

Not related at all

Real World:

- In 2011, Sony Pictures suffered a breach by a hacker group LulzSec, who used a SQL injection vulnerability to access the personal information of over 1 million customers.
  (This had nothing to do with the PSN outage in 2011, that made me not able to play Fifa 12 and COD)

Security – the necessary breaks for Software Development?

Does a formula 1 driver complain about not having breaks?

bouvet

A04:2021

INSECURE DESIGN

bouvet

bouvet

Insecure Design

New category in 2021

OWASP Perspective

- Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.”
- Lack of security controls and security architecture in design phase

Practitioner Perspective

- I hope more cross-functional teams get a security engineer.
- The category that tries to address all «other issues» that is not covered by OWASP Top 10.

Insecure Design

Attack/Defense

Lack of security controls

Abuse business logic

Threat modelleling

- ❤(I LOVE THIS)❤

DevSecOps

- what does this even mean?

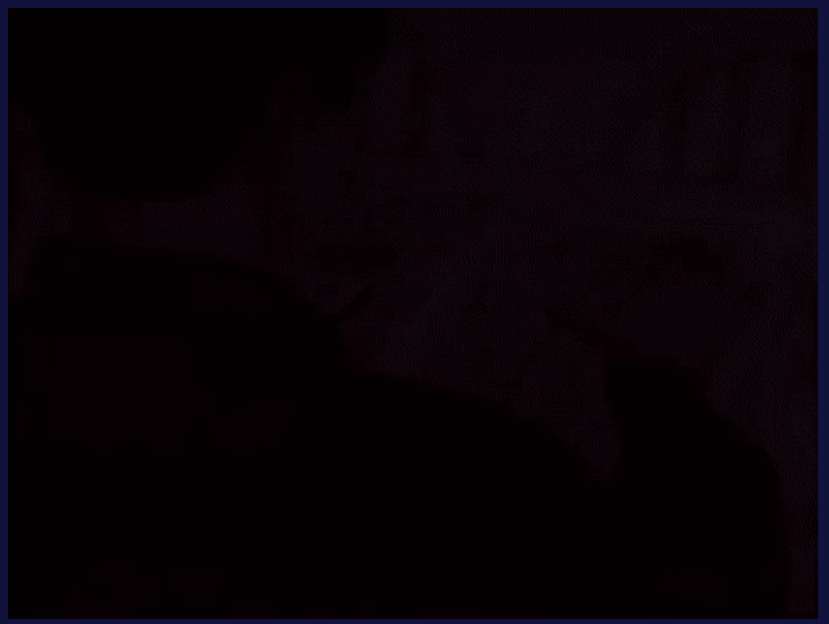
OWASP SAMM

- A road map for Tech Leads, AppSec and CISOs

bouvet

Real World: VIPPS

- Vipps ☺
- The new yellow pages



S/O to Cecilie Wian

Let’s take a little break! ☕

For those interested – Scan your website

SECURITYHEADERS.COM
(S/O Kenneth Fossen)

OBSERVATORY.MOZILLA.ORG/

Follow up: Now you have something to show after the presentation!

A05:2021

SECURITY MISCONFIGURATION

To fix or not to fix

bouvet

Security Misconfiguration

bouvet

OWASP Perspective

- Security Misconfiguration occurs when a app is set up without appropriate security settings, leaving it vulnerable to potential threats.

Practitioner Perspective

- Very similar to the previous one
- Increase in «Developer Platforms»
  - Pre configured plattforms to increase security and standardization of tooling.
  - NAV NAIS
- *Anyone feels like this is hard to master? Constant chase*

(S/O SC Norway!)❤

Security Misconfigurations

Attack/Defense

🔥Lack of security hardening in application stack or cloud services permissions. 🔥

🔥Enabled unnecessary features (e.g., ports, services, pages, accounts)🔥

Unchanged default accounts and passwords.

Disabled or insecurely configured security features in upgraded systems.

Insecure settings in servers, frameworks (e.g., Spring, ASP.NET), libraries, or databases.

Absence of or insecure server security headers/directives.

Implement a hardening process

- Check out: CIS hardened images

Automate the setup process to reduce the effort required in configuring a new secure environment.

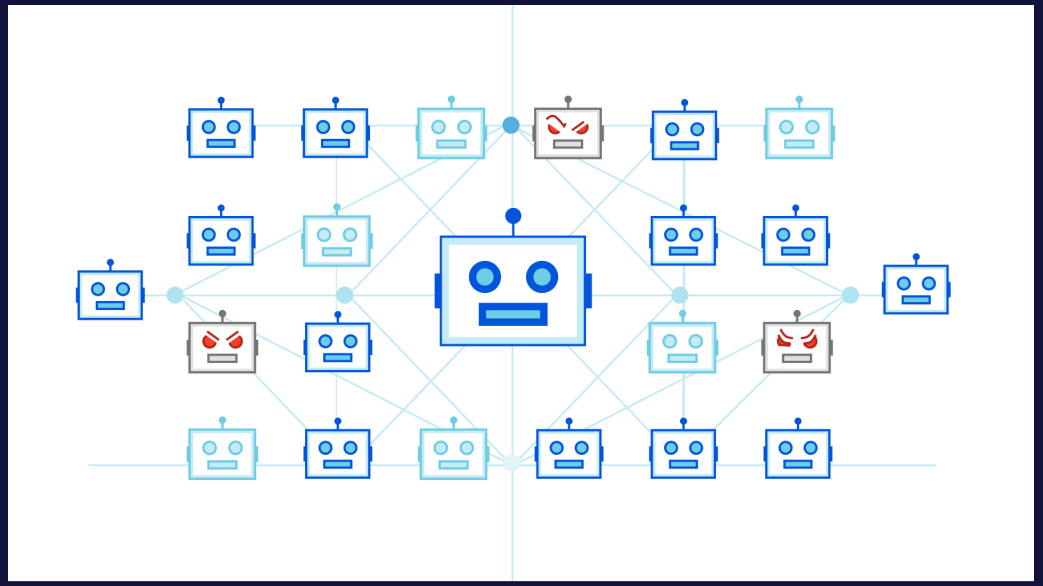
- Dev Plattform?

Patch management and CMDB

Review cloud storage permissions

Security Headers!

bouvet



Real World: IoT
Internet of Threats

- Mirai botnet
- Scan for public IoT devices with default username and password
  - Shodan.io?
- Redirect traffic towards victim

A06:2021

VULNERABLE AND OUTDATED COMPONENTS

All cool projects have abillities, sometimes they are vulnerabilities
- NPM, Audit

Tv-Shows: Mr. Robot

bouvet

Vulnerable and Outdated Components

It was #2 from the Top 10 community survey

OWASP Perspective

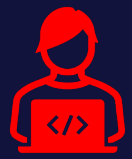
- A Software Bug → Security Implications → Vulnerabillity
- Involves using components with known vulnerabilities in an application

Practitioner Perspective

- The hardest thing to manage because:
  - Time
  - React: npm audit – release hell
  - Continuous monitoring
- How many of you struggle with this?

Vulnerable and Outdated Components

Attack/Defense



Vulnerable Third party Component, Library, files etc.

Monitor:

- CVE, NVD, CISA, WWE exploited

Tools:

- Snyk, OWASP dependency check, Dependabot

Process:

- There should be dedicated time to maintain an application.

bouvet

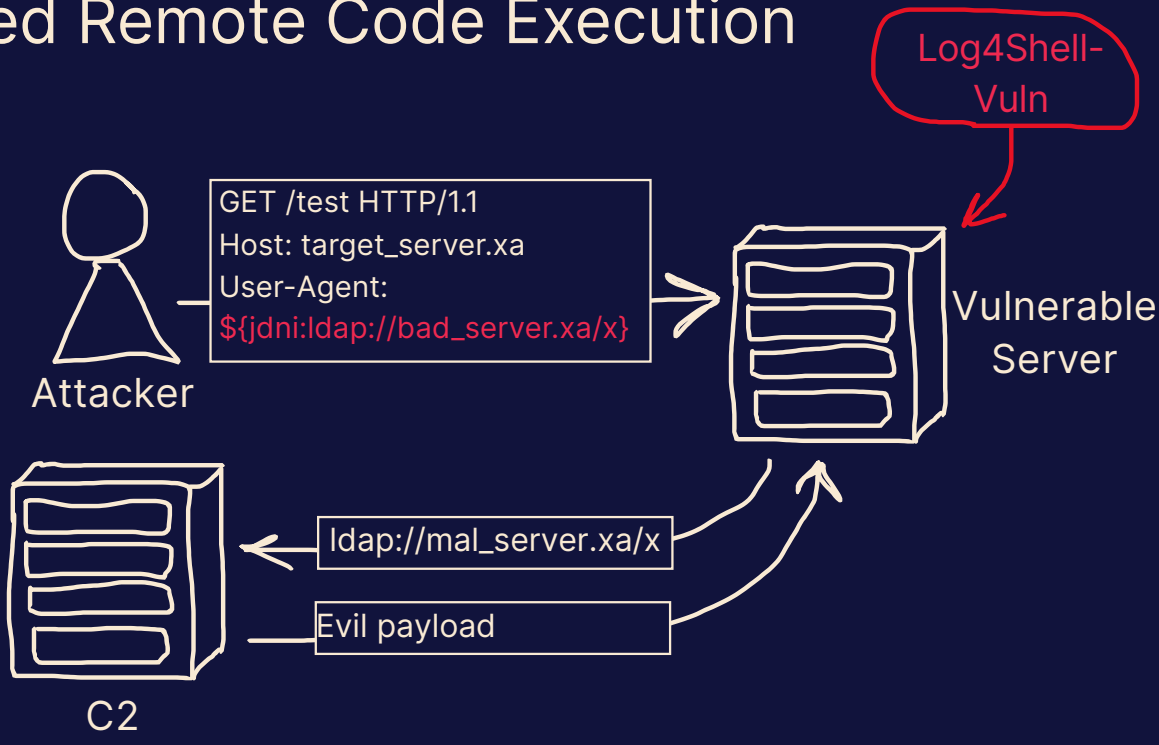
Real World:

- **Panama Papers Leak (2016)**:
- Hackers exploited outdated, unpatched versions of Drupal CMS and WordPress used by Mossack Fonseca, a Panamanian law firm and corporate service provider.
- Over 11 million confidential documents were leaked, disclosing sensitive information of high-ranking politicians and public figures from more than 50 countries.

Bonus: Log4J ☺

Log4Shell - Unauthenticated Remote Code Execution

- Log4J
  - Java Logging Library
  - Open source
  - Used in millions of applications
  - Communicating with the system
- Log4shell
  - 10.0 CVSS score
  - Thousands of attacks/second



Check this out: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

What’s new vs. What’s still there

- *We often prioritize what’s new and shiny, over what’s actually needed.*

- *CIS Benchmark or OWASP Application Security Verification Standard > new vulnerability*

bouvet

A07:2021

IDENTIFICATION AND AUTHENTICATION FAILURES

Sometimes I forget who I am

Identification and Authentication Failures

What is it?

OWASP Perspective

- Flaws in user verification processes allow attackers to impersonate users.
- Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application:

Practitioner Perspective

- Most customers use a hybrid Active Directory with Azure AD(Entra ID)
- *Who has not fully outsourced Authentication and Authorization?*

Identification and Authentication Failures

Attack/Defense

Credential Stuffing: known passord lists - rockyou.txt

Brute Force Attacks

Use of Default, Weak, or Well-known Passwords

Ineffective Credential Recovery Processes

Exposure of Session Identifier in URL

Reuse of Session Identifier after Login

Incorrect Invalidation of Session IDs

Multi Factor:

Rate limit

Don’t use default credentials

API Keys management

Session ID: Don’t expose, enumerate random and invalidate

Fun fact about NIST security questions

bouvet

A08:2021

SOFTWARE AND DATA INTEGRITY FAILURES

Sometimes I wish a bug could be smacked, instead of fixed

Real World: CD project Behind Cyber Punk

- In 2021, a software bug in a popular video game allowed attackers to execute malicious code on players' computers. The attackers used the bug to steal personal information, such as names, addresses, and credit card numbers, from over 100 million players.

Software and Data Integrity Failures

What is it?

OWASP Perspective:

- Missing or weak integrity checks make software/data manipulation possible.

Practitioner Perspective

- Software Bill of Materials (SBOM)is becoming a regulatory aspect that's affecting SWD.
  - CycloneDX

Software and Data Integrity Failures

Attack/Defense

Untrusted Sources:

Insecure CI/CD Pipeline:

Auto-Update Functionality:

Insecure Deserialization:

🔥 CI/CD is the new holy grail for cloud environments.

Due Dilligence around untrusted and trusted data.

- Snyk open source

Digital Signatures to verify software integrity – SHA256

Software supply chain tool:

- Dependency check, dependabot, OWASP cycloneDX

🔥 Integrity Check for Serialized Data:

- Avoid sending unsigned or serialized data to untrusted clients without integrity checks/digital signatures to detect tampering

bouvet

A09:2021

SECURITY LOGGING AND MONITORING FAILURES

We don’t see anything, and that is why we are secure

Movie: Monster INC (AGAIN)

Security Logging and Monitoring Failures

What is it?

OWASP Perspective

- Hard to traditionally «check»
- Inadequate logging and monitoring delay or prevent detection of security breaches.
- Warnings and errors generate no, inadequate, or unclear log messages.

Practitioner Perspective

- Often a forgotten aspect
- Sensitive data in logs
- Logs are typically «one level» above in confidentiality.
- Logs are only stored locally or in silo system

We have really good control on 10% on what we have

Security Logging and Monitoring Failures

Attack/Defense

Turn off logging and monitoring

DoS: Overflood logs

Alert Fatigue

Ensure all login, access control, and server-side input validation failures

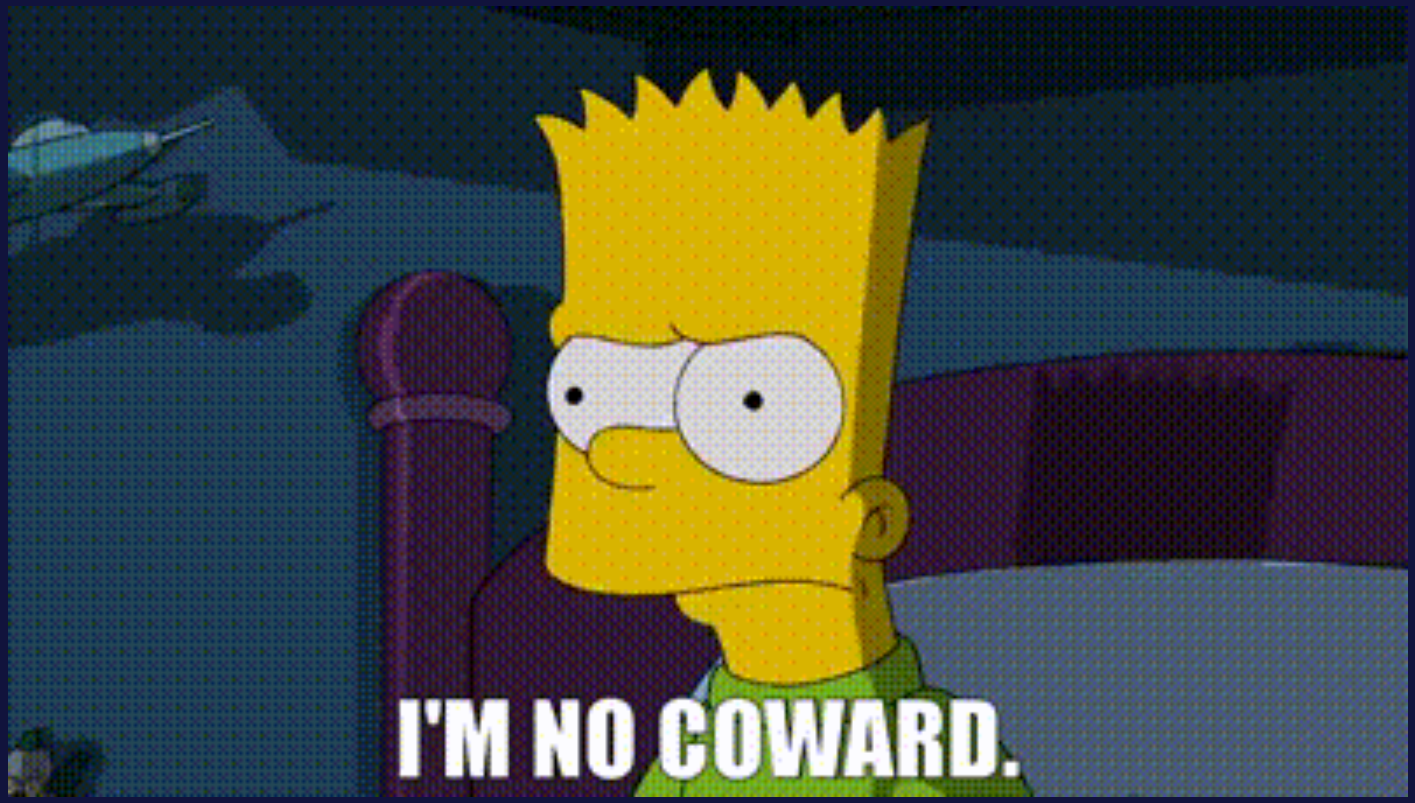
Formating

Correct encoding

High value targets, assets and transactions

Source: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

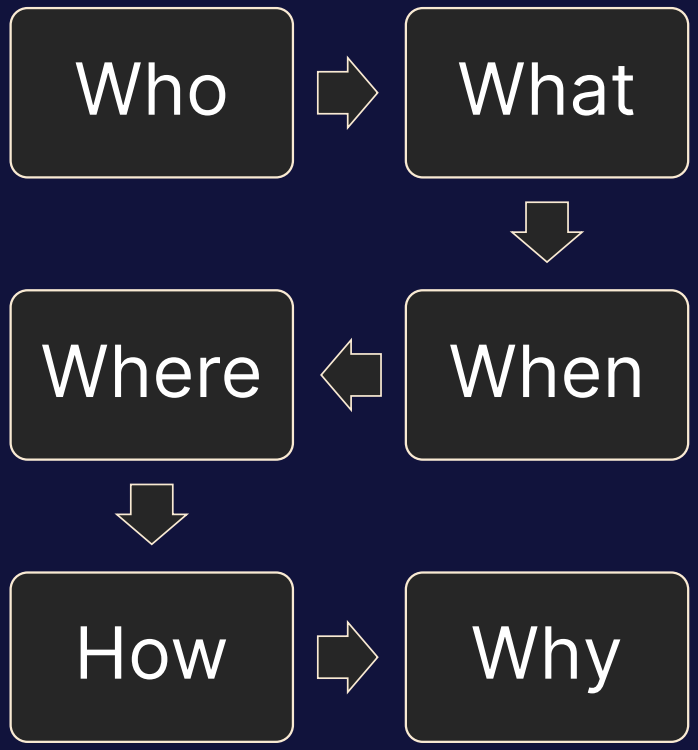
WHAT EVENTS SHOULD I LOG???????



bouvet

What should we collect?

Ask the nearest defender



- Access control logs
- Application logs:
- Network logs
- Security events
- DNS logs
- AD/AAD logs
- CDN logs

  +++

bouvet

A10:2021

SERVER-SIDE REQUEST FORGERY (SSRF):

When i doubt, make the server do it for you

Neo send a request to the Matrix → Controls the robots

Movie: Matrix

bouvet

Server-Side Request Forgery (SSRF):

What is it?

OWASP Perspective

- Attackers can trick an application into making unwanted requests to other systems.
- SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL.

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://192.168.0.68/admin
```

https://portswigger.net/web-security/ssrf#common-ssrf-attacks

Server-Side Request Forgery (SSRF):

Attack/Defense

SSRF Attacks Against the Server

- 127.0.0.1 or localhost

SSRF attacks against back-end

- **https://192.168.0.68/admin**

Whitelisting > blacklisting

Network layer:

- Remote resource in seperate network
- Deny by default
- Logging and firewall

Application layer:

- Sanitize and validate data
- Disable HTTP redirections

bouvet

bouvet

QUESTIONS

I’m also on linkedin and substack hehe

bouvet

Resources

I'm gonna be the very best like no one ever was

Resources

Flagship projects from OWASP

AppSec

- 🔥 OWASP Cheat Sheet 🔥
- Checklist: 🔥 OWASP ASVS 🔥
- OWASP ZAP

Security Analysis

- MITRE ATTACK/MITRE DEFEND
- CIS BENCHMARKS

Roadmap

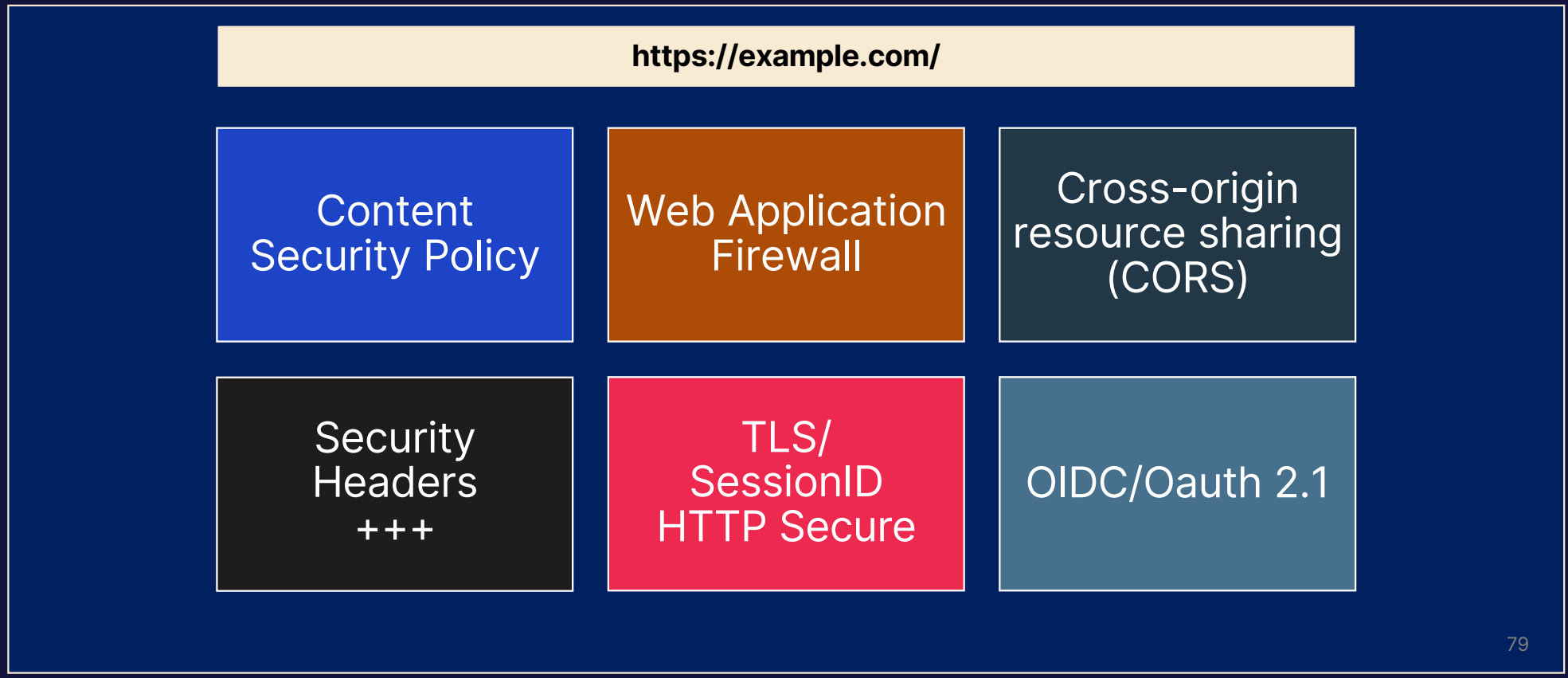
- OWASP SAMM – Maturity model

Other Top 10

- OWASP Top 10 API
- OWASP top 10 Kubernetes
- OWASP top 10 PowerBI

Security Controls mentioned today!

Web Applications



More Advanced topics

☺

- ❤Threat Modeling ❤
- CI/CD Security
- DevSecOps practices
- Advanced Explotation Techniques
- Threat Landscapes and APT
- Cloud Native Security Architecture
- Secure Coding Practices
- SAST/DAST
- Privacy/Compliance Engineering
- Security Operation - Tools tactics and procedures

Next steps

Mini Roadmap ☺

- **1 Week: Immediate Actions**
  - Identify Critical Assets
  - Set Up Basic Security logging and monitoring
- **3 Months: Building Foundations**
  - **Implement Security Headers**
  - Secure User Authentication and Authorization
- **1 Year: Maturing Your Security Posture**
  - Web Application Firewall (WAF)
  - Implement Content Security Policy (CSP)
  - Incident Response Plan: ´

bouvet

bouvet

Good luck on your journey Security Champions!

Security Blog

Johan Paramanathan
Linkedin ☺

Johanpara.substack.com