



# Three Friends from the OWASP Top 10

Things that keep me up at night

Garth Boyd  
OWASP Ottawa  
April 2023

# TL;DR

- OWASP has a few "Top 10" projects.
- Ok, there are a LOT of projects.
- This talk attempt to condense these top 10 into "3 Friends" that bother me the most.



# TOP10

---

# Who is this guy?

- Erstwhile Engineer (B.Eng. Electrical/Computer Systems 1987)
- Blue Team: MMHS, Key Management, PKI, Threat Modeling
- Red Team: Pentest
- Web/Cloud Application Security Architecture
- DevSec\*.\*
- OWASP Ottawa Chapter Leader/Volunteer



# Agenda

- Whither OWASP
- OWASP Ottawa Chapter
- Active Canadian Chapters
- Other Chapters
- Friend 1
- Friend 2
- Friend 3





# OWASP



- ~~Open Web Application Security Project~~
- Open Worldwide Application Security Project
- Since 2001, 501(c)(3) non-profit organization in the US (2004)
- Community Led
- 250+ chapters worldwide
- Tens of thousands of members
- World's largest non-profit organization focused on software security
- Conferences/ Educational Publications/ Projects





OWASP<sup>®</sup>  
OTTAWA



# OWASP Ottawa



- Created in 2007-ish by Sherif Koussa
- Monthly meetups
- Workshops
- Community collaboration
- Online, and now In-Person
- We have our own DJ





# OWASP Ottawa



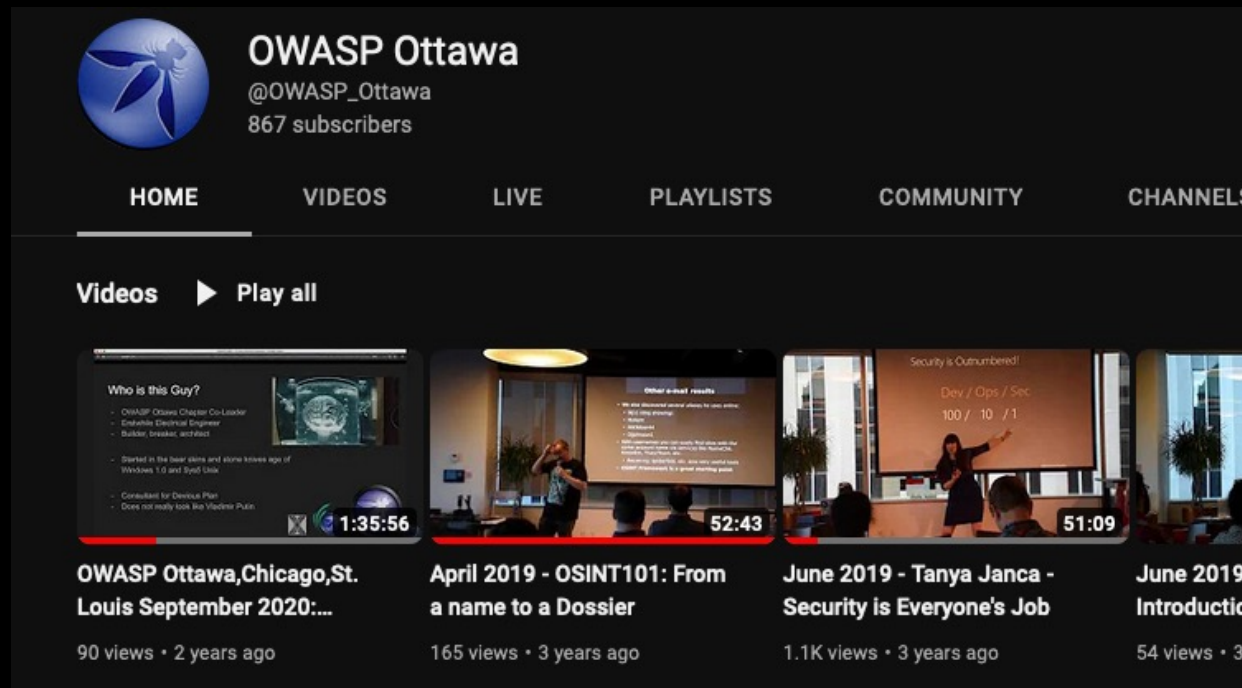
- Informal, approachable,
- Thankful for your assistance.
- We encourage and welcome beginners.
- We are an open, tolerant, and inclusive organisation that accepts all races, genders, creeds, abilities, things, and ideas with the exception of one
- Hate: Hate has no home at OWASP Ottawa.

# Other Active Canadian Chapters

- Victoria
- Vancouver
- Toronto
- Edmonton

# Other Chapters

- Wealth of information from other chapters
- YouTube channels of past meetups



The screenshot shows the YouTube channel page for OWASP Ottawa. The channel name is "OWASP Ottawa" with the handle "@OWASP\_Ottawa" and 867 subscribers. The navigation bar includes links for HOME, VIDEOS, LIVE, PLAYLISTS, COMMUNITY, and CHANNELS. The "Videos" section is active, showing a list of four videos:

Video Title	Duration	Views	Age
OWASP Ottawa, Chicago, St. Louis September 2020:...	1:35:56	90 views	2 years ago
April 2019 - OSINT101: From a name to a Dossier	52:43	165 views	3 years ago
June 2019 - Tanya Janca - Security is Everyone's Job	51:09	1.1K views	3 years ago
June 2019 - Introduction	-	54 views	3 years ago

# Three Friends that Keep me up at Night

A hand holding a lit matchstick in front of a dark city skyline at night. The matchstick is lit, with a bright yellow flame. The city skyline is visible in the background, with various buildings and spires. The text "Are You Afraid of the Dark?" is overlaid on the image in a stylized, arched font. The words "Are You Afraid" are in a light blue color, "of the" is in a darker blue, and "Dark?" is in a large, bold, light blue font.

Are You Afraid  
of the  
Dark?

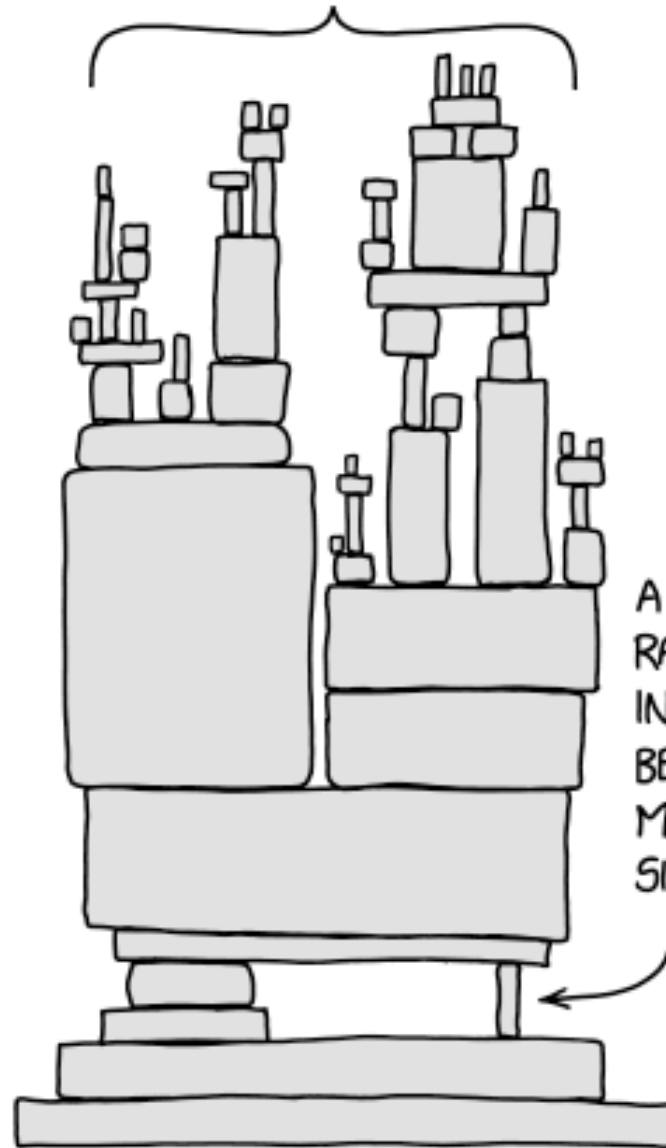




# Friend 1

A06:2021 Vulnerable Components

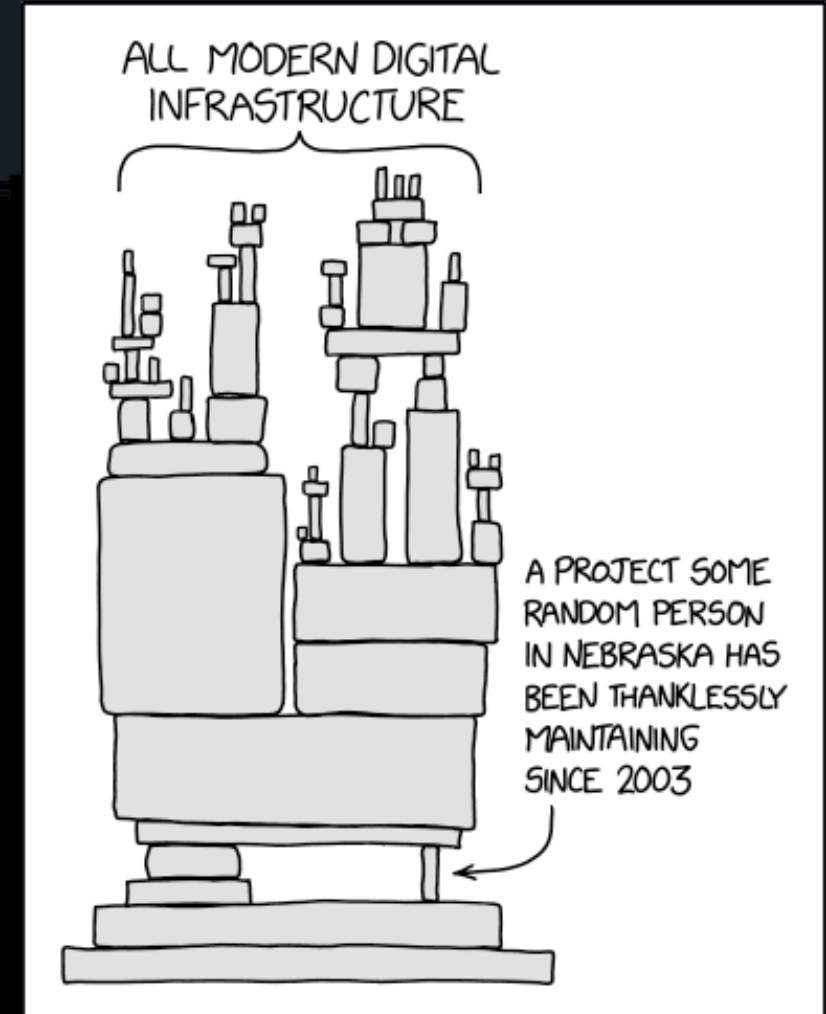
# ALL MODERN DIGITAL INFRASTRUCTURE



A PROJECT SOME  
RANDOM PERSON  
IN NEBRASKA HAS  
BEEN THANKLESSLY  
MAINTAINING  
SINCE 2003

# Friend 1 – A06:2021 Vulnerable Components

- CWE-1104: Use of Unmaintained Third-Party Components
- CVE-2021-44228, Log4J, “Log4jShell”
- CVE-2017-5638, Struts 2 remote code execution vulnerability
- Malicious Clones
- Valid libraries with malicious content
- Valid libraries with Flaws



# Friend 1 – A06:2021 Vulnerable Components

- CVE-2021-44228, Log4J, “Log4jShell” experience
- “Log4J Party”
- Fortune 75 – International reach
- Thousands of Applications
  - Internal builds
  - External
- Had no idea if log4J was in their infrastructure
- Spent millions of \$ and delayed projects to determine if log4J was in their environment



# Friend 1 - Defences

## 1. Provenance

When deciding upon a component to use what do we check?

- History
- Number of users
- Contributors
- Reviews
- Typo-squatting

# Friend 1 - Defences

## 2. Vulnerability Checks

In the build pipeline:

- OWASP Dependency Check
- Commercial dependency checkers

# Friend 1 - Defences

## 3. Code Scanning

In the build pipeline:

- Static Applicate Security Testing (SAST)
- Manual review
- Golden image in container registry
- Scanning containers in pipeline



When potato salad goes bad



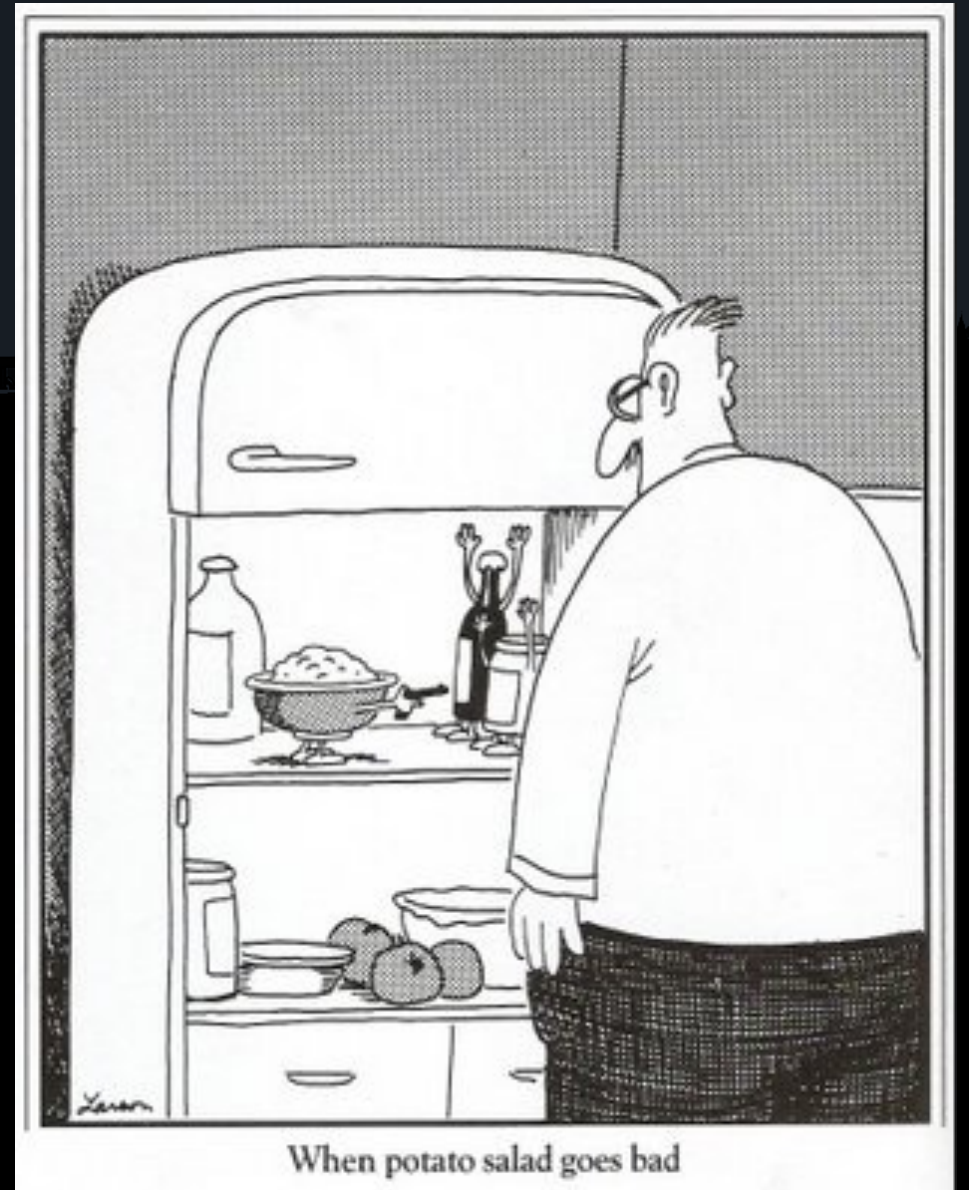
# Friend 1 - Defences

## 4. Software Bill of Materials

How do you know that your production code does not have a new vulnerability?

How do you (or your clients) know what 3<sup>rd</sup> party components you have in place and what versions?

# SBOM



# Friend 1 – Defences – What is SBOM?

- Software Bill of Materials
  - A standard schema identifying 3<sup>rd</sup> party components and their versions
  - Variety of free and commercial products can generate SBOMs in your CI/CD pipeline
  - So what?
  - SBOM can be real-time monitored
  - Alerting upon news of a new vulnerability

# Friend 1 – Defences – OWASP Dependency Track





# Friend 2

## A04:2021 Insecure Design



## Friend 2 – A04:2021 Insecure Design

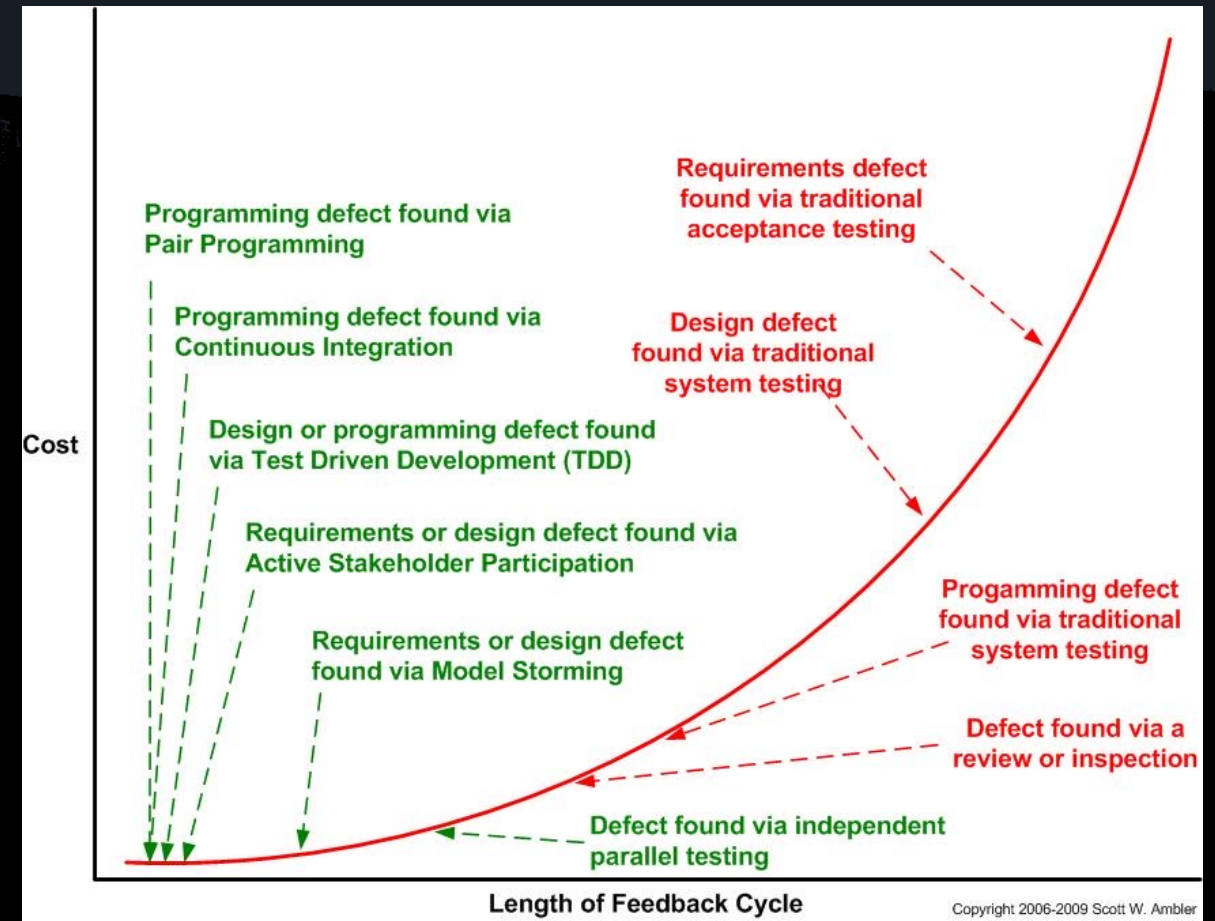
- Different from insecure *implementation*
- Secure design can still have an insecure implementation
- Insecure design *cannot* be fixed by perfect implementation

## Friend 2 – A04:2021 Insecure Design

- Design mis-step that required removing the feature. (\$\$\$\$\$\$) 🤯
- Extreme cost to the business
- Lack of consideration for malicious use cases

# Friend 2 – A04:2021 Insecure Design

- Cost of defect remediation v. time in dev cycle



<http://www.agilemodeling.com/essays/costOfChange.htm>

## Friend 2 – Defences

- Secure development lifecycle
- Security language in user stories
- Risk Analysis – Risk Register
- Threat Modeling
  - Data Flow Diagrams
  - Threat Analysis Table



# Friend 3

A10:2021 Server Side Request Forgery

## Friend 3 – A10:2021 SSRF

- 20 year old new sensation
- First noted name suggestion from Deral Heiland in 2008 Shmooscon presentation:
  - Web Portals: Gateway To Information, Or A Hole In Our Perimeter Defenses
  - <https://www.youtube.com/watch?v=KFgY5M7B5iI>





# Friend 3 – A10:2021 Server Side Request Forgery

- Unique in that it has its own category
- Several Major breaches
  - Capital One

(Customer Zero)

# Friend 3 – A10:2021 Server Side Request Forgery

- It's an attack
- Against an Application
- Tricks application into making HTTP requests
- Hijacks the trust relationship between application and backend components

# Friend 3 – A10:2021 Server Side Request Forgery

- Also Known as (AKA):
  - XSPA – Cross Site Port Attack
  - Out-of-Band Resource Load

# Friend 3 – A10:2021 Server Side Request Forgery

- Know associates :
- XXE – XML eXternal Entities
- Improper Restriction of Rendered UI Layers of Frames (CWE-1021)

# Friend 3 – A10:2021 Server Side Request Forgery

- Family Affiliations:
  - Confused Deputy (CWE-441)
  - App receives content from upstream component
  - App does preserve original source
  - Forwards content downstream making the App appear as the source of the content

# Friend 3 – A10:2021 SSRF

- Potential Impacts
  - Access data within the server or network
  - Enumeration
  - Command execution
  - Attacks against other servers, internal/external
  - Access services not directly exposed to the internet
  - Not limited to the HyperText Transfer Protocol
  - Metadata APIs in cloud environments



# Friend 3 – SSRF Known Exploits

- Capital One (Customer: Zero)
  - Personal data on over 100 million Americans and 6 million Canadians exposed
  - names, addresses, phone numbers, self-reported income, credit scores, and payment histories, SSNs, SINS
  - Misconfigured WAF
  - Enabled comms to AWS metadata service
  - Over privileged
  - Requests to metadata service enabled temporary creds to access a great many things



# Friend 3 – A10:2021 SSRF

- The species in its Natural Habitat, The road to hades is paved with 3 Conditions
  1. The Injection
    - Systems with a weakness to injection attacks (OWASP Top 10-2017,A1)
  2. The Fumble
    - Server re-issues input from the context of that process
    - Attacking the URL Parser (Orange Tsai - BH USA 2017)
  3. The Response
    - A return path for the attacker to view the response
    - Blind SSRF - no response to the initial request

# Friend 3 – Defences

- “The code documents itself”
- Input Validation
- Domain Name validation
- Stateful firewall
  - Valid routes
- Network Segmentation
- IMDSv2 for AWS in the case of metadata
- Monitoring
- Static code analysis
- IMDSv2 Sidebar
- Uses session-oriented requests
- Limited session time



Thank You



# Q&A

