Hitchhiker's Guide to Security Vulnerabilities

DON'T PANIC

Here's how all this stuff works!

Who are these clowns?

Combined, your presenters have more than X years of Development, Enterprise Operations, Support, and Security experience most major industries: Retail, Legal, Medical, Financial, Insurance, Manufacturing, & Technology.

CRob

Cat Herder

Red Hat Inc.

~~President~~,

(ISC)2 CLE Chapter

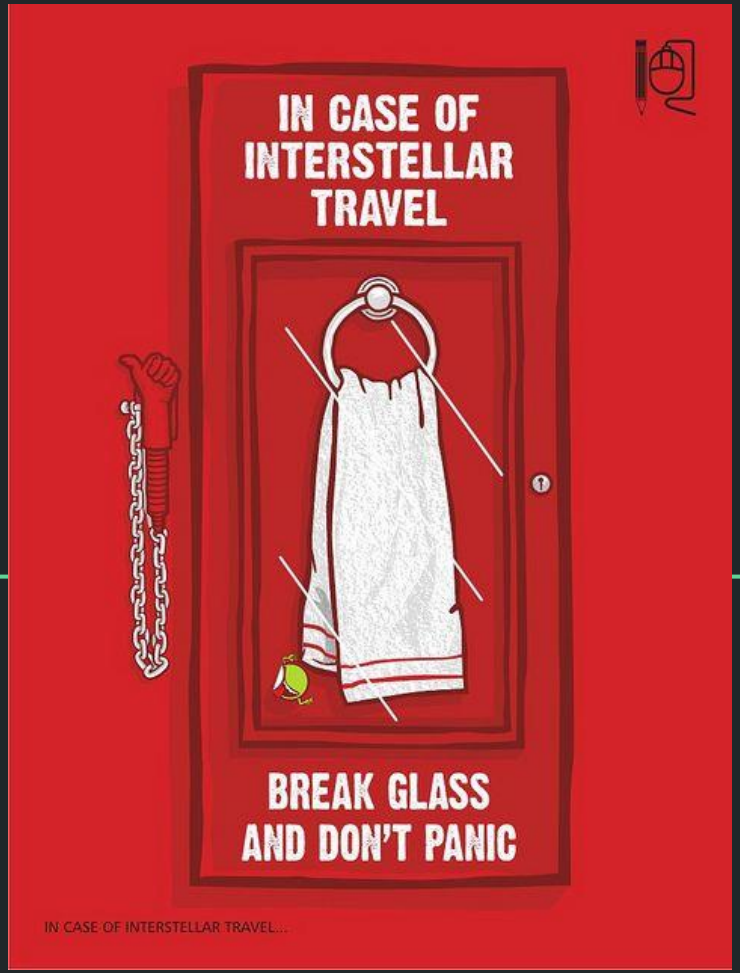

DON'T
PANIC

Why Are We Here?

- The practice of “The Security” can be complex and jargon-filled.
- There are many critical aspects that have similar-sounding names/acronyms.
- Computers are hard.

- We’d like to explain the concepts around CVE, CWE, CVSS, DWF and other practices around security vulnerability management
- We’ll also show how a small little bug grows into a big, nasty Threat to you!

So grab a towel and put your sunglasses on.....



View from up here....

A simple workflow illustrates what we'll be diving into

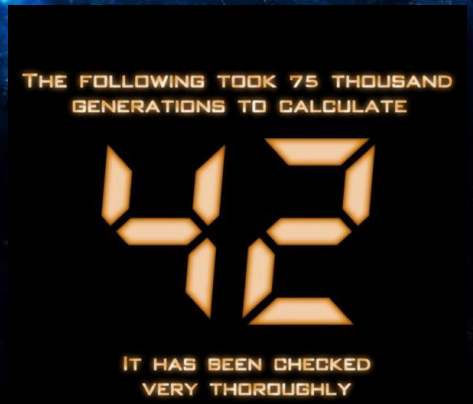
How does this stuff get found?

People

- Security Researchers
- Security Companies (Talos, etc.)
- Students
- Organizations
- Developers
- Community Maintainers
- Users
- 3V33L H@x0rs

How?

- Patching/Maintenance
- Development Lifecycle
- Pentesting/Fuzzing/Scanning
- By Accident




THIS WILL ALL
END IN TEARS

Flaw Analysis

The reports are reviewed by analysts that seek to understand what the problem is.

They seek to understand if the report Is valid or not.

They'll look to see if the issue has or needs a CVE assigned to it.

What is a CVE?

Term - CVE

- Stands for Common Vulnerability & Exposures
- It is a unique identifier for a specific problem.
- All CVEs are centrally coordinated by MITRE & their delegates (CNAs - CVE Numbering Authority).
- It allows researchers and maintainers the ability to have a common language used to describe vulnerabilities no matter what the platform.

https://cve.mitre.org/about/

CVE in-depth

CVE's all contain a unique identifier

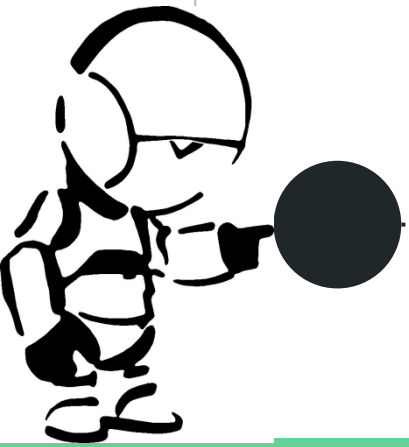
CVE-2017-42

CVE's all contain a brief description

A flaw in the memory manager of the Babel Fish could allow a malicious attacker to change output from the Babel Fish's translation

CVE's all include relevant references

Megadodo Industries Bug Tracker: 42
www.md.org.net.com/bz=42.htm



I guess I'll go read more about this.

NVD - the big vulnerability dictionary in the cloud....

- NVD is the National Vulnerability Database and is maintained by the National Institute of Standards and Technology (NIST) [part of the US Department of Commerce]
- It is a database of enhanced CVE content.
- NVD is great, but can be incomplete or out of synch.
- THE best source for information on a CVE is the vendor or team that supports that technology.

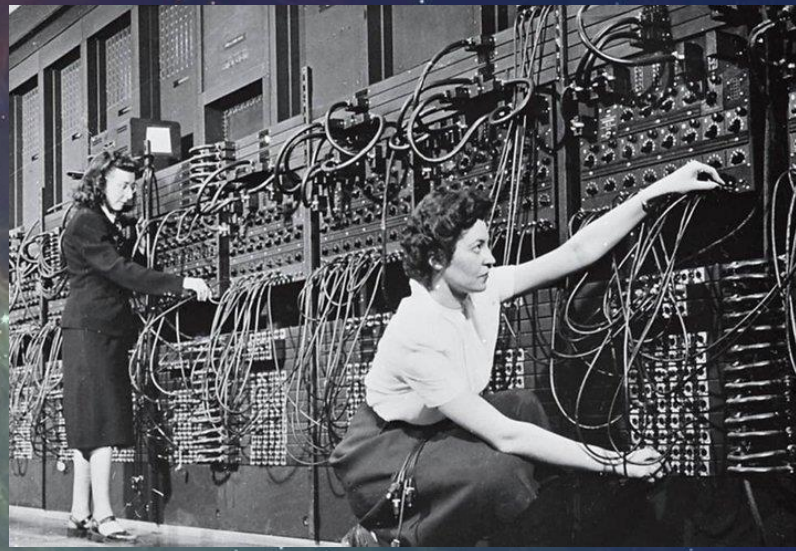
https://nvd.nist.gov/

Flaw Analysis, continued

The vulnerability gets a CVE identifier (or already has one).

Next the analyst will look to see what the reasons are for the flaw and assign a CWE.

What is a CWE?



Term - CWE

- Stands for Common Weakness Enumeration
- It is a unique identifier for a specific coding flaw.
- It allows developers and security practitioners to have a common language used to describe the weakness.
- Provides a baseline standard for weakness identification, mitigation, and prevention efforts.

https://cwe.mitre.org/about/index.html

CWE in-depth

What is a “software weakness”?

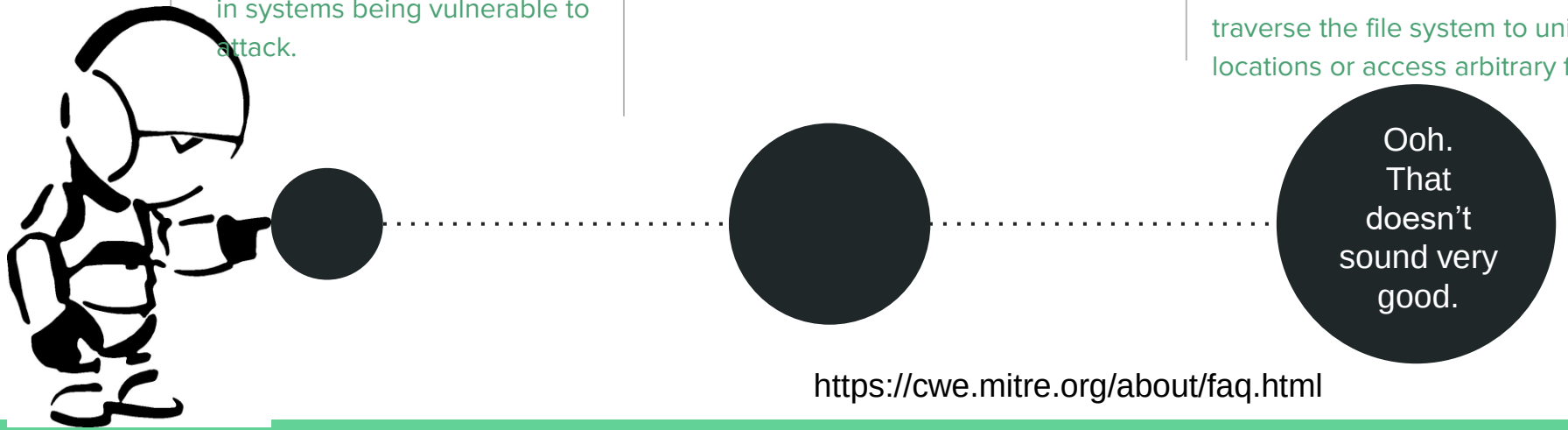
This is a problem within a software’s architecture, design, code, or implementation that if left unaddressed could result in systems being vulnerable to attack.

What does it look like?

CWE-42 - Path Equivalence: ‘filename.’ (Trailing Dot)

What does that mean?

A software system that accepts path input in the form of trailing dot ('filedir.') without appropriate validation can lead to ambiguous path resolution and allow an attacker to traverse the file system to unintended locations or access arbitrary files.



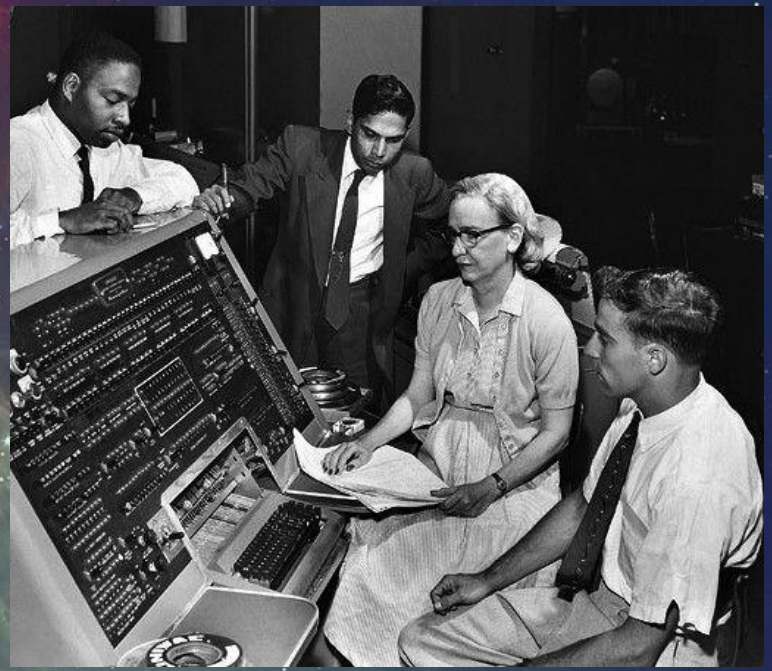
https://cwe.mitre.org/about/faq.html

Flaw Analysis, continuing to be continued

At this point we know how to talk about the problem (CVE) and what the fundamental coding problem is (CWE).

Next the analyst will work to understand how bad this thing is. The most common method of scoring flaws is CVSS.

What is a CVSS?



Term - CVSS

- Stands for Common Vulnerability Scoring System
- It is a methodology to capture characteristics of a vulnerability and produce a numeric score to reflect its severity.
- Again, this allows researchers and maintainers the ability to have a common language used to describe vulnerabilities and how severe the issue is.

https://www.first.org/cvss/

How to score using CVSS

Determine the base score

There are 8 dimensions of the flaw to review:

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope
- Confidentiality
- Integrity
- Availability

Each is rated (mostly) on a High-Low-None scale

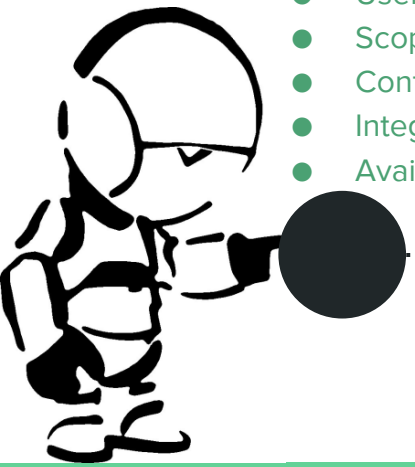
Those playing on the “Expert Level” could also look at these aspects of the issue

Temporal

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental

- CIA Requirement
- Modified base score dimension

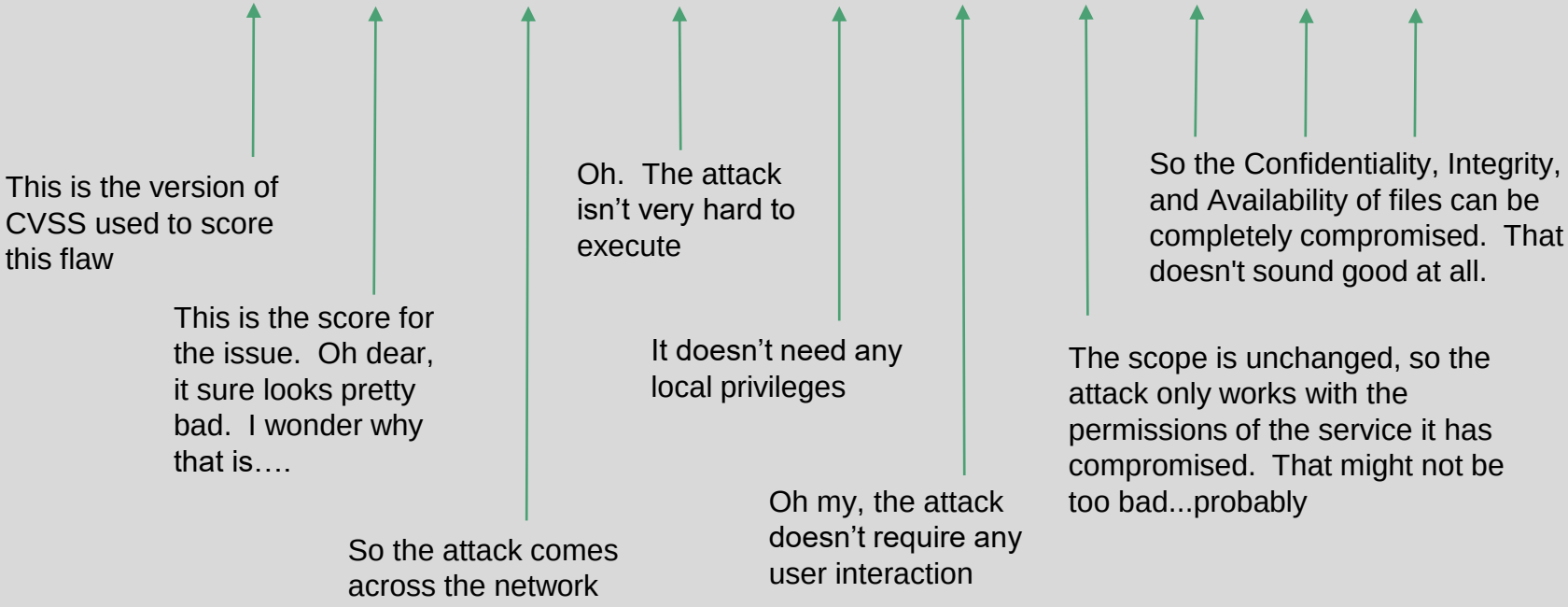


So I can modify the severity based off of *MY* environment. I guess that could be useful.

https://www.first.org/cvss/calculator/3.0

What does a CVSS Score look like?

CVSS:3.0- 9.8/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

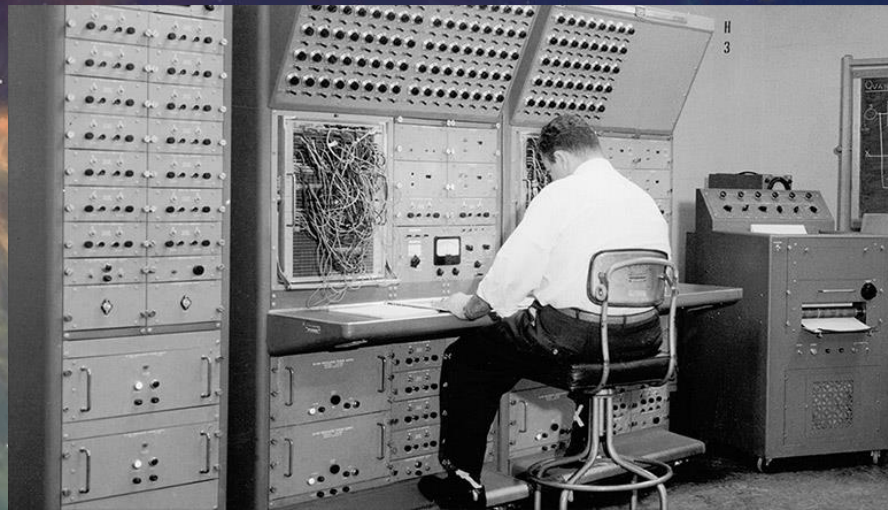


Flaw Analysis, further continued

The flaw has been scored, and the organization understands the details about the flaw.

Next the analyst will determine the exposure for any of their organization's products and assign a Severity Rating.

What is a Severity Rating?



Term - Severity Rating

- The impact of security issues found in an organization's products, typically using a scale of some sort along with Common Vulnerability Scoring System (CVSS) base scores.
- Used to help customers understand their risk of exposure.
- For example, Red Hat, Microsoft and others use a four-point scale: Critical, Important, Moderate and Low

Create and Test Fixes (finally)

The organization will begin working on resolving the flaw with a combination of knowledge articles, mitigations and code fixes.

However, sometimes the decision is made to embargo a flaw and not immediately publish any information about it.

What is an Embargo?

Term - Embargo

- A time period where vendors have access to details concerning the vulnerability, with an understanding not to publish these details or the fixes they have prepared.
- The reporter sets a date and time to lift the embargo, after which the information is considered public.
- The embargo ends with a Coordinated Release Date ("CRD").
- Sometimes embargos are broken. This is generally considered a Bad Thing...

Notifications & Advisories (yay!)

If a flaw is not under embargo, organizations will usually release an official statement about the vulnerability and if / how it affects their products, as well as any mitigations that do not require a patch.

Once fixes have been created and tested, the organization will release an advisory, containing a patch for one or more products. Typically these are published to organizational knowledge bases and mailing lists, and might also be sent to targeted groups of users.

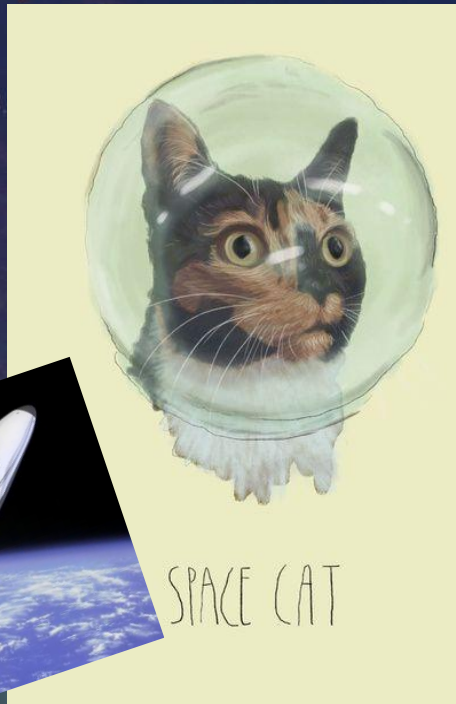
Advisories are usually digitally signed by the organization to verify their legitimacy.

A few last things...

Support Life Cycles
Open Source Tracking

Why do they call it a lifecycle if nothing ever dies?

- Nothing is supported forever. (sorry)
- Be sure to understand how your vendor/community of choice supports components/applications you use.
- Most providers will provide “all” fixes for a set period of time, then gradually start to only fix the most severe things as the product ages. READ THE FINE PRINT to understand what support you are entitled to!



Who fixes Open Source?

- There is no “The Open Source”. Each package/project/product can be managed by different types of people.
- We’ll take a moment to talk about a few types and something to help you out.

Who is “the Open Source”?

The Good

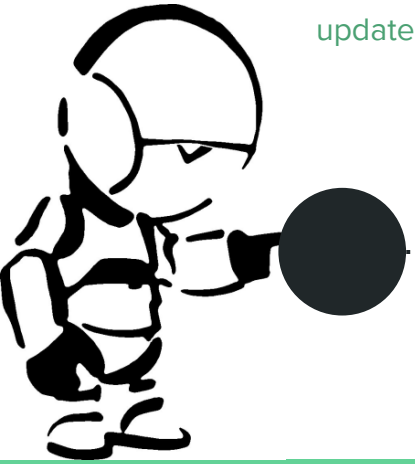
- OSS Upstream has a security contact (even better a dedicated security team/function!)
- Has the ability and track record to coordinate updates

The Bad

- Dead projects or “For Fun” projects
- No ability to secure the project or coordinate fixes for it.
- Project abandoned, has no one to correct it.

The Ugly

- Security fixes issued silently, no public notice or documentation.
- Projects that have no interest to secure or correct the packages



I guess you should know what it is I’m using, and how it will get updated when it breaks.

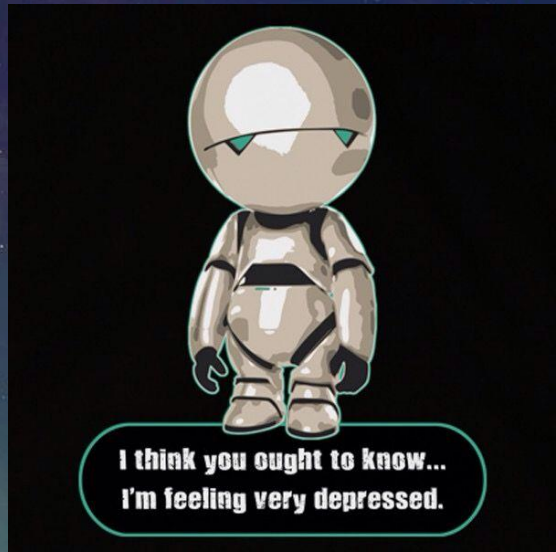
Term - DWF

- Stands for Distributed Weakness Filing
- An OSS project that acts as a CNA (CVE Numbering Authority) for Open Source
- Uses a specified format that allows both reads and writes
- Intended to facilitate better scaling of CVE
- Multiple projects working in concert with MITRE
- Helps provide a more global perspective to CVE - additional languages and countries

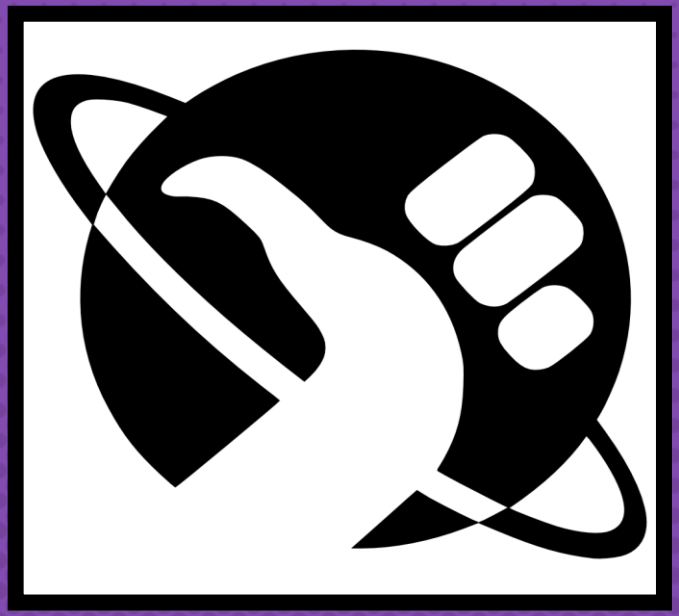
https://www.redhat.com/en/blog/introducing-dwf-project-vulnerability-reporting-done-open-source-way

Summary - ZOMG so many letters and words!!!

- Security is not easy, but it is important.
- There are existing systems and processes in place to assist securing your applications.
- Knowing IS half the battle, the other half is using the available information to identify and mitigate vulnerabilities and potential threats.
- Leverage the offerings of your communities and vendors.



DON'T PANIC AND CARRY A TOWEL



Any questions?

CRob@RedHat.com
@RedHatCRob