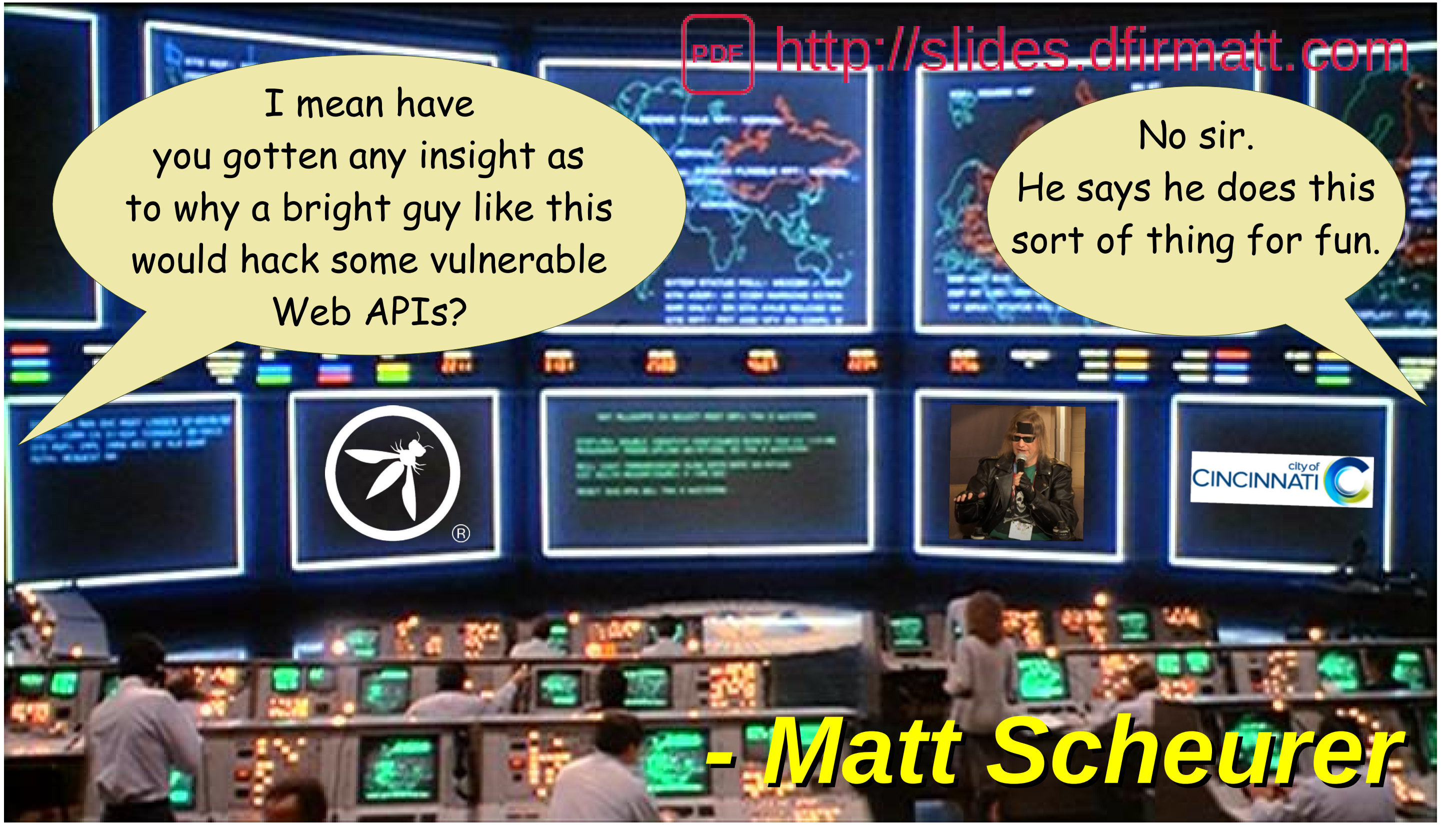
Hacking Web APIs (v1.1)

Cincinnati OWASP Chapter



I mean have you gotten any insight as to why a bright guy like this would hack some vulnerable Web APIs?
No sir. He says he does this sort of thing for fun.
PDF
city of CINCINNATI

http://slides.dfirmatt.com

- Matt Scheurer

Wednesday May, 08 2024

About Me

I work for a big well-known organization...

As Vice President (VP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Connect / Contact / Follow Matt:

https://www.linkedin.com/in/mattscheurer

https://twitter.com/c3rkah

Where I volunteer...

I am an Official

HACKING
IS NOT A CRIME

Advocate
https://www.hackingisnotacrime.org

WARREN COUNTY
CAREER
CENTER

Advisory Board: Information Technology and Cybersecurity
https://www.mywccc.org/

WOMSA
Empowering Women in Cybersecurity

Women's Security Alliance (WomSA) Technical Mentor
https://www.womsa.org

Disclaimer!

Yes, I have a day job.
However…

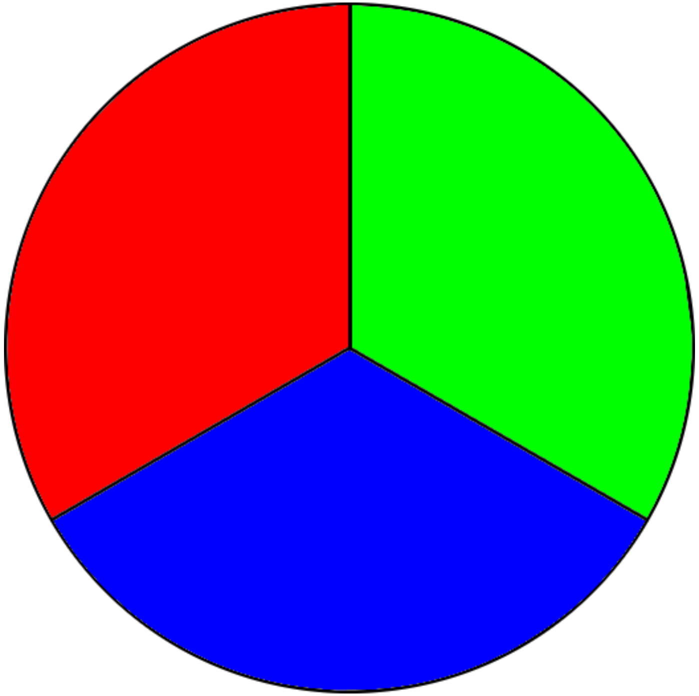
Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.

Other Disclaimers

The informational material presented is for educational purposes only. The presenter is **not responsible** for its use or misuse. No warranties or guarantees implied or otherwise are in effect. Use of these tools, techniques and technologies are at **your own risk!**

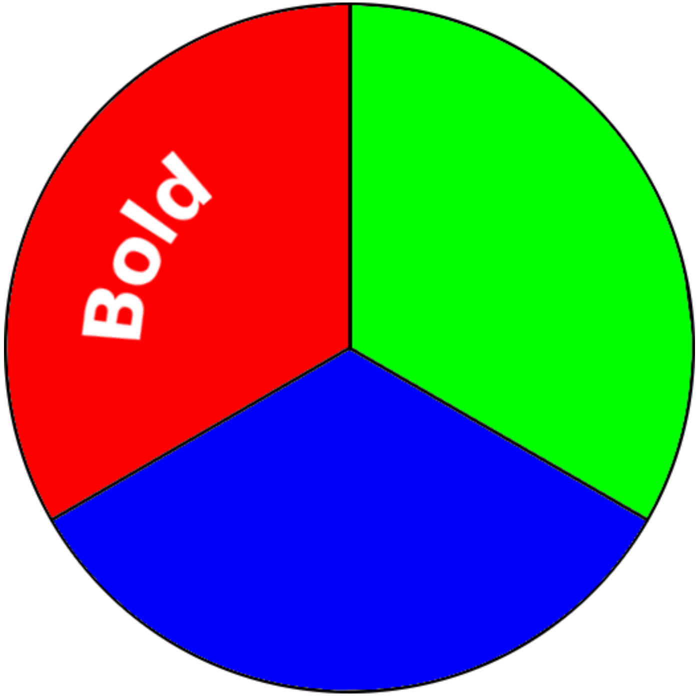
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



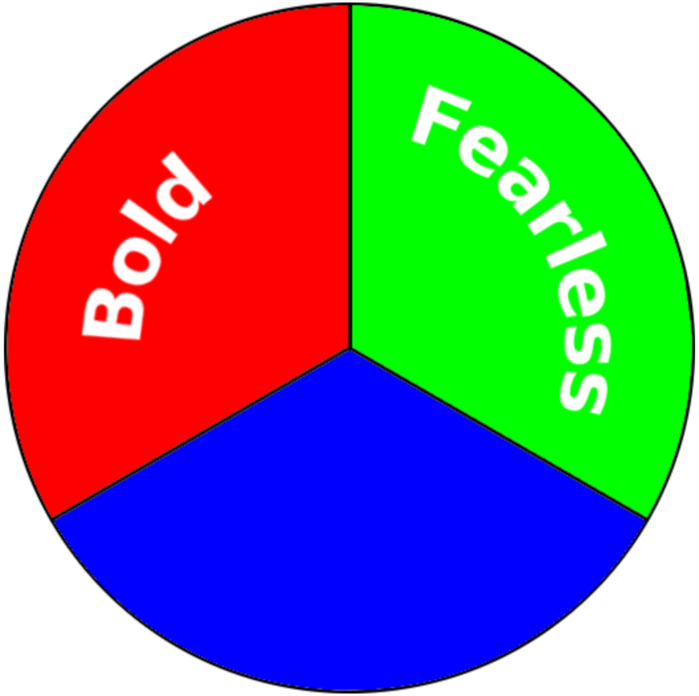
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



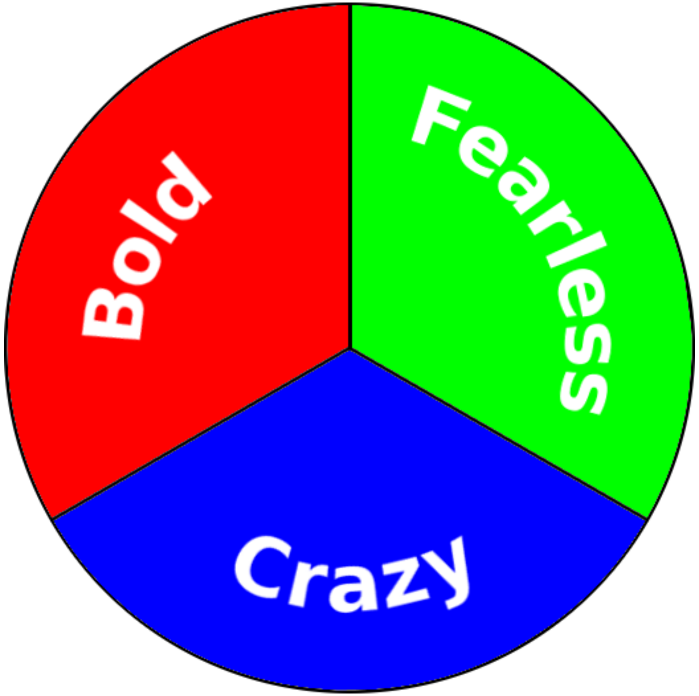
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



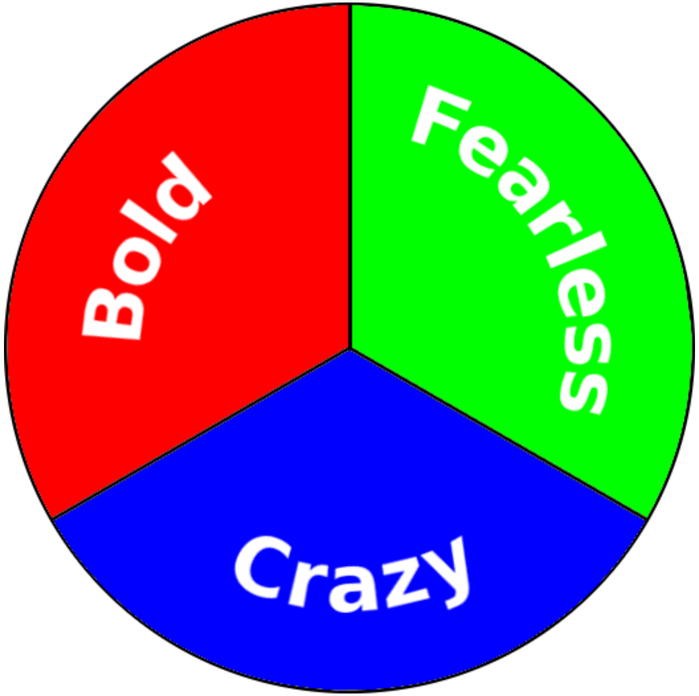
*** Live Demo Alert ***

This presentation features “Live Demos”, because the speaker is...



*** Live Demo Alert ***

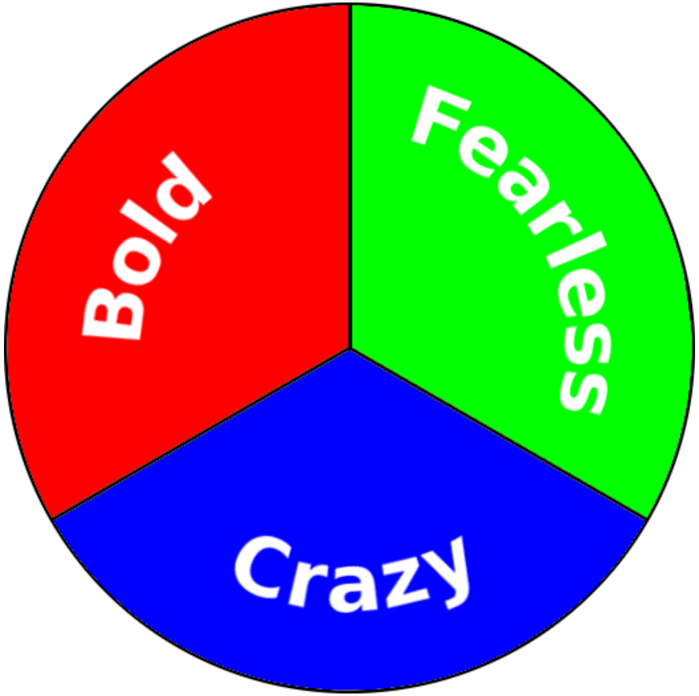
Please pick 2…



*** Live Demo Alert ***

Please pick 2…

So I am not just **Crazy**!



What is an API?

An API is an “Application Programming Interface”. API’s allow access or interaction between systems. They often provide developers and power users with a means to access or leverage data and services on external or cloud-based systems and services. API’s may grant read, write, or modify privileges depending on design, configuration, implementation, and applied permissions.

What is an API?

- Matt’s **K.I.S.S.** Definition

What is an API?

- Matt’s **K.I.S.S.** Definition
- No, not that KISS…

What is an API?

- Matt’s **K.I.S.S.** Definition
- No, not that KISS…
  - Though, admittedly, I do like their music!

What is an API?

An API is an “Application Programming Interface” which allows external interaction with data.

What is REST?

- **REST** is an acronym for **RE**presentational **S**tate **T**ransfer.
- Web Services that conform to the **REST** architectural style, called **REST**ful Web Services, provide interoperability between computer systems on the Internet.

What is the Tiredful API?

The **Tiredful API** is an intentionally broken web app by design. The purpose of the application is to teach developers, QA testers, or security professionals about flaws present in Web Services (REST API) due to insecure coding practices.

Tiredful API Vulnerabilities

- Information Disclosure
- Insecure Direct Object Reference (IDOR)
- Access Control
- Throttling
- SQL Injection (SQLi)
- Cross Site Scripting (XSS)

House Keeping

- For demo purposes, I am using a web browser with the REST Client extension
- Some challenges require authentication under an account with appropriate access
  - Exercises involving access to protected data require an access key

Authentication Control

- OAuth 2.0 Access
  - The token credentials consist of an access token and token secret used in lieu of a username and password
  - The required “token_type” typically uses the string “**Bearer**” under most implementations

Stolen Access Tokens

- MITRE ATT&CK, Tactic: **TA0006**
  - Credential Access
  - https://attack.mitre.org/tactics/TA0006/

Getting Started

1) Browse to the local Tiredful API home page
   - By default, http://127.0.0.1:8000/
2) Click on “**User Token**”
3) Login to obtain a user token (i.e., ‘batman’)
4) Note the returned “access_token” value

Information Disclosure

- Sensitive data examples
  - Financial data (i.e., PCI, account data, credit cards)
  - Personally Identifiable Information (PII)
  - System / Stacktrace Information
    - Reconnaissance

OWASP Mappings

- OWASP Top 10
  - **A02:2021** - Cryptographic Failures
- OWASP API Top 10
  - **API3:2023** - Broken Object Property Level Authorization

OWASP®

Demo 1 / 6

Scenario: *Information Disclosure*

Objective: Try to get stacktrace information.

Insecure Direct Object Reference

- **IDOR** Risks
  - Failure to restrict access appropriately
  - Threat actors exploiting flaws to gain unauthorized access to data or traversing other parts of a system

OWASP Mappings

- OWASP Top 10
  - **A01:2021** - Broken Access Control
- OWASP API Top 10
  - **API1:2023** - Broken Object Level Authorization

Demo 2 / 6

Scenario: *Insecure Direct Object Reference (IDOR)*

Objective: Try to access exam results of another user.

Access Control

- Risks
  - Allowing unintended access from the way a system or application was designed
  - Failure to restrict protected or administrative actions to authorized users

OWASP Mappings

- OWASP Top 10
  - **A01:2021** - Broken Access Control
- OWASP API Top 10
  - **API5:2023** - Broken Function Level Authorization

Demo 3 / 6

Scenario: *Access Control*

Objective: Try to execute an operation which should be only allowed to admin users.

Throttling

- Risks
  - Denial of Service (DoS)
    - A way to flood system resources which effectively makes a system unavailable
    - Prevents legitimate users from access to a system

MITRE ATT&CK Mappings

- MITRE ATT&CK
  - **T1499**: Endpoint Denial of Service
    - **T1499.003**: Application Exhaustion Flood

Demo 4 / 6

Scenario: *Throttling (a.k.a. Rate Limit Implementation)*

Objective: Force server to respond with HTTP response code 429 to abuse system resources by launching a DoS attack.

NOTE: A HTTP 429 response code means "Too Many Requests".

SQL Injection

- SQLi Risks
  - Vulnerabilities which allow unauthorized access to a back-end database
  - Abuses
    - Data exfiltration, destruction, or manipulation

OWASP Mappings

- OWASP Top 10
  - **A03:2021** - Injection

Demo 5 / 6

Scenario: *SQL Injection (a.k.a. "SQLi")*

Objective: Find table names of the SQLite database.

Cross Site Scripting

- Cross Site Scripting (XSS) Risks
  - Performs automatic code execution in client browsers upon access
  - Stolen credentials or form data
  - Execution of exploit kit payloads

OWASP Mappings

- OWASP Top 10
  - **A03:2021** - Injection

Demo 6 / 6

Scenario: *Cross Site Scripting (XSS)*

Objective: Find parameters accepting cross site scripting meta-characters.

Trending API Risks

- **Accidentally/Publicly exposed APIs**
  - Allows for direct API access
  - Circumvents front-end web & web app security
- **Shadow APIs**
  - Deployed outside of standards and controls

Reducing these risks

- Recommendations
  - Adopting a secure development life cycle
    - Having a security champion on each dev team
    - Testing as early in the **SDLC** process as possible
  - Adhering to the Principle of Least Privilege
  - **OWASP** resources
    - https://owasp.org/

Questions

Who?

What?

When?

Where?

Why?

How?

Hacking Web APIs (v1.1)

Cincinnati OWASP Chapter

PDF http://slides.dfirmatt.com
I mean have you gotten any insight as to why a bright guy like this would hack some vulnerable Web APIs?
No sir. He says he does this sort of thing for fun.
®
city of CINCINNATI
Thank you for attending!

Wednesday May, 08 2024