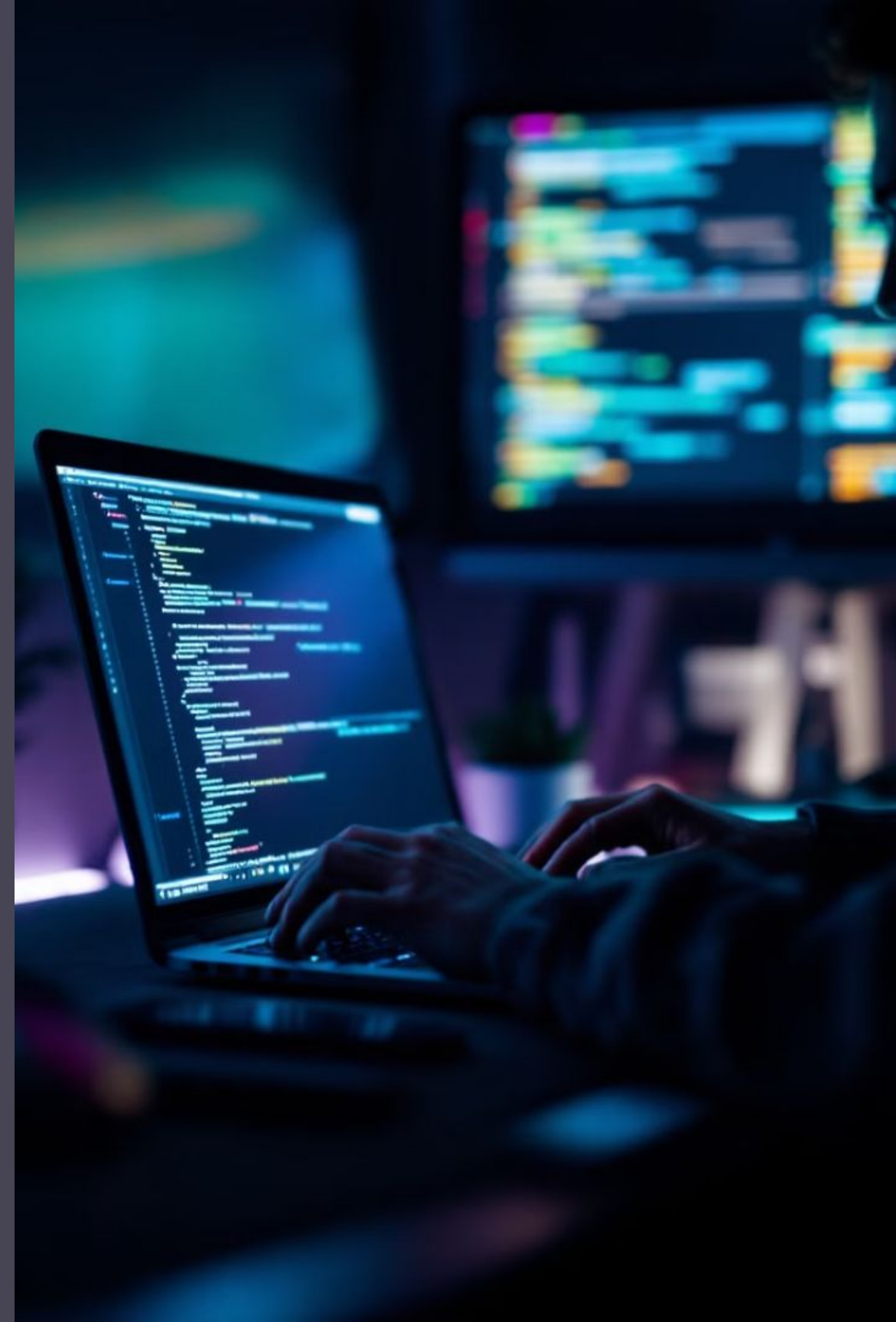
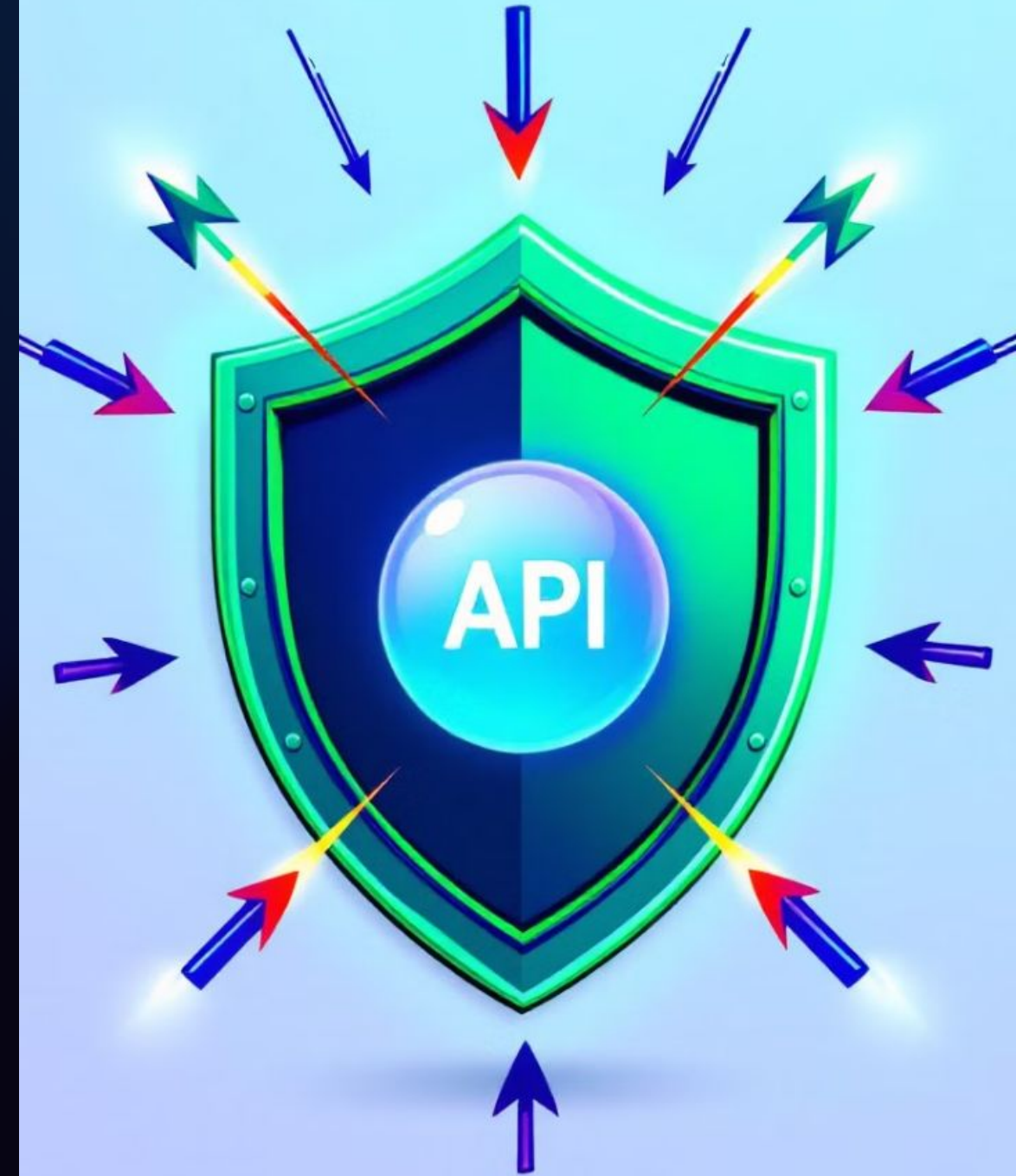


API Security

– Komal
Chowdhar
y



**Are You Sure Your API'S are
Secure ?**



Explosive Growth

83% of all internet traffic is from APIs

Akamai


Major Attack Target

2022: APIs “most frequent attack vector”

Gartner

High Profile Breaches

High-profile API breaches announced weekly

 PELOTON  coinbase

Regulatory Compliance

Regulations mandate privacy, vulnerability detection, testing

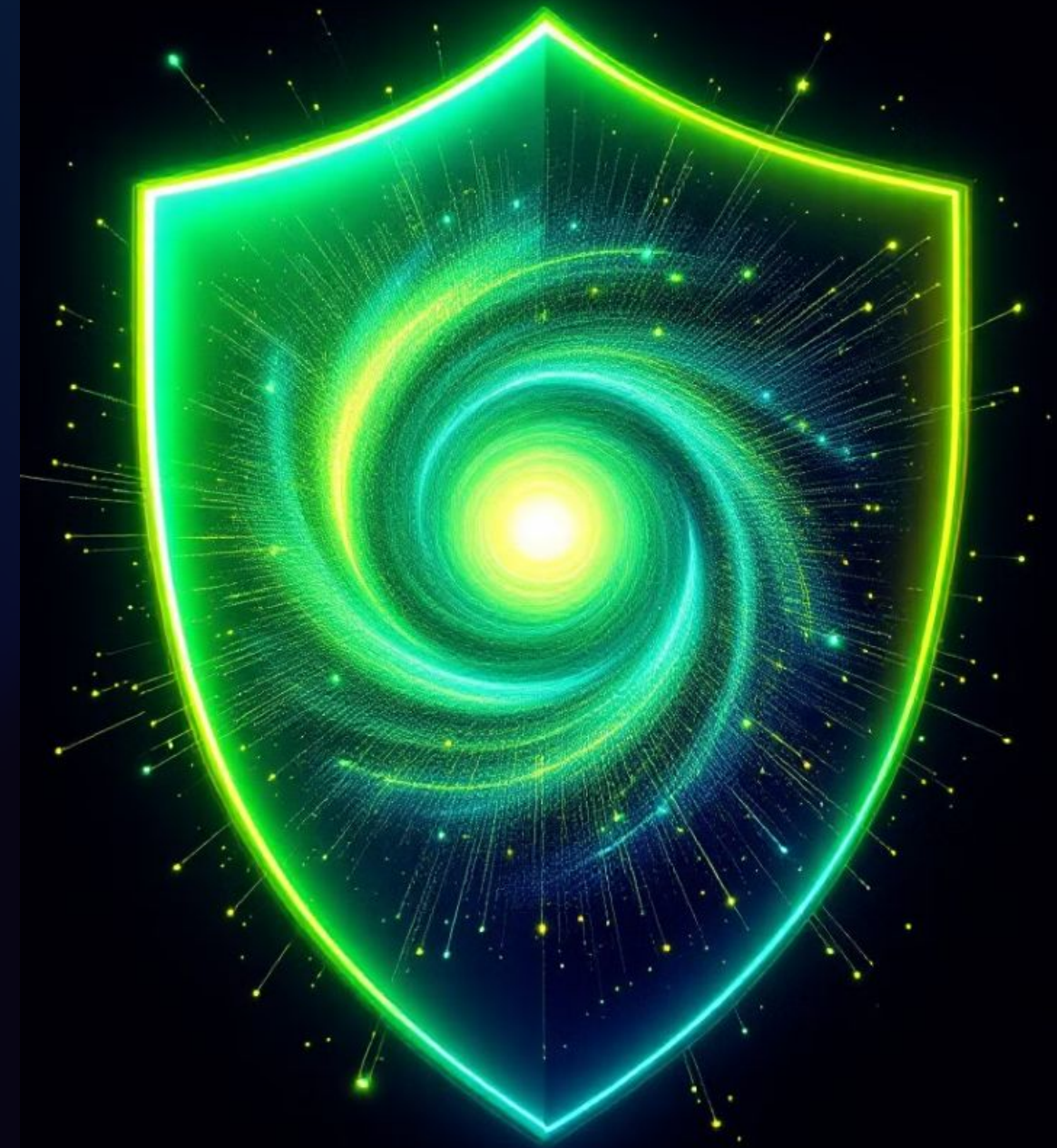
 

Why API Security Testing

**But isn't API Security testing
something best left to the expert**



**You can do a lot with some basic
tools and healthy dose of
curiosity and creativity**



Let's Look at some examples



Vulnerability : Injection



eBay

In late 2015 and early 2016, eBay had a severe XSS vulnerability. The website used a "url" parameter that redirected users to different pages on the platform, but the value of the parameter was not validated. This allowed attackers to inject malicious code into a page.

The vulnerability enabled attackers to gain full access to eBay seller accounts, sell products at a discount, and steal payment details. It was actively used by attackers to manipulate eBay listings of high value products such as vehicles. eBay eventually remediated the vulnerability, but follow-on attacks continued until 2017.

The OWASP API Security Top 10

<https://owasp.org/API-Security/editions/2023/en/0x11-t10/>

OWASP Top 10 API Security Risks

OWASP Top 10 API Security Risks are the most critical security risks for APIs. They are ranked based on their prevalence and the potential impact on the system. The risks are: 1. Injection flaws, 2. Broken access authentication, 3. Sensitive data exposure, 4. Sensitive data exposure, 5. XML external control (XXE), 6. Insufficient components with known vulnerabilities, 7. Cross-site deserialization, 8. Insufficient logging & monitoring, 9. Cross-site configuration, 10. Insufficient logging & monitoring.



1. Injection flaws



2. Broken access authentication



3. Sensitive data exposure



4. Sensitive data exposure



XML external control (XXE)



3. Security misconfiguration



5. Cross-site deserialization



6. Insufficient components with known vulnerabilities



4. Cross-site configuration



10. Insufficient logging & monitoring



10. Insufficient logging & monitoring

**Let's Look at the list one by one with
examples (Postman Demo)**



Vulnerability : Broken Object Level Authorization (BOLA)

Weakness in API Access Controls for Individual data objects (Ex: Records, Files)

2023 OWASP API Security top 10 : #1



Broken Object Level Authorization (BOLA)

LOOK OUT for ...

Predictable or findable resource ID's

Insufficient or lack of rate limiting

[https://owasp.org/API-Security/editions/
2023/en/0xa1-broken-object-level-authorization/](https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/)

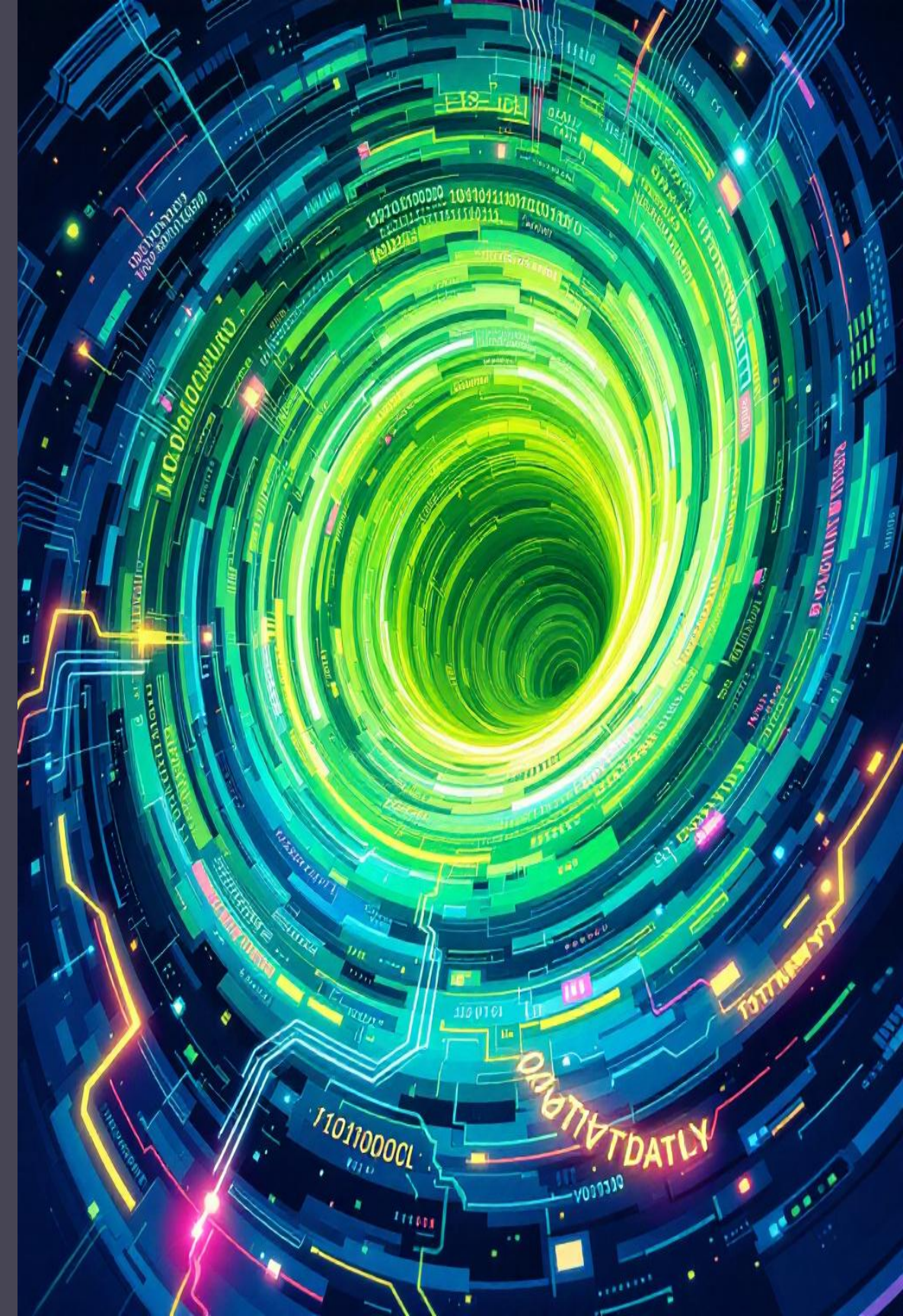
Type	Valid request	BOLA test
Predictable ID	GET /api/v1/account/ 2222 Token: UserA_token	GET /api/v1/account/ 3333 Token: UserA_token
ID combo	GET /api/v1/ UserA /data/2222 Token: UserA_token	GET /api/v1/ UserB /data/ 3333 Token: UserA_token
Integer as ID	POST /api/v1/account/ Token: UserA token { "Account": 2222 }	POST /api/v1/account/ Token: UserA token { "Account": [3333] }
Email as user ID	POST /api/v1/user/account Token: UserA_token { "email": " UserA@email.com" }	POST /api/v1/user/account Token: UserA_token { "email": " UserB@email.com" }
Group ID	GET /api/v1/group/ CompanyA Token: UserA_token	GET /api/v1/group/ CompanyB Token: UserA_token
Group and user combo	POST /api/v1/group/ CompanyA Token: UserA token { "email": " userA@CompanyA .com" }	POST /api/v1/group/ CompanyB Token: UserA token { "email": " userB@CompanyB .com" }
Nested object	POST /api/v1/user/checking Token: UserA token { "Account": 2222 }	POST /api/v1/user/checking Token: UserA token { "Account": { "Account" :3333} }
Multiple objects	POST /api/v1/user/checking Token: UserA token { "Account": 2222 }	POST /api/v1/user/checking Token: UserA token { "Account": 2222, "Account": 3333, "Account": 5555 }
Predictable token	POST /api/v1/user/account Token: UserA token { "data": "DfIK1df7jSdfa1acaa" }	POST /api/v1/user/account Token: UserA token { "data": "DfIK1df7jSdfa2dfaa" }

Also Covered

Vulnerability : Unrestricted Resource Consumption

APIs that do not limit client interactions or resource consumption

2023 OWASP API Security top 10 : #4





Unrestricted Resource Consumption



LOOK OUT if one of them below has no limit on

- Execution timeouts
- Maximum allocable memory
- Maximum number of file descriptors
- Maximum upload file size
- Number of records per page to return in a single request-response



USPS Site Exposed Data on 60 Million Users

November 21, 2018

54 Comments

U.S. Postal Service just fixed a security weakness that allowed anyone who has an account at **usps.com** to view account details for some 60 million other users, and in some cases to modify account details on their behalf.

The Facebook logo, consisting of the word "facebook" in its characteristic blue, lowercase, sans-serif font.

Facebook Data Breach:

- Incident: 2018 Facebook data breach.
- Vulnerability: BOLA exploit in Facebook's API allowing unauthorized access to private photos.
- Consequences: Exposure of millions of users' private photos, causing significant privacy concerns and damage to Facebook's reputation.

**Let's Look at another example
about altering the data**



Vulnerability : Broken Function Level Authorization (BFLA)

2023 OWASP API Security top 10 : #5



Vulnerability : Broken Function Level Authorization (BFLA)

LOOK OUT for ...

Access to admin endpoints by regular users

<https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/>



Where BOLA is about accessing data

...BFLA is about the ability to alter or delete data

BFLA is related to BOLA

So, if you happen upon a BOLA vulnerability

... it might be a good idea to check for BFLA , too



Checklist for Controlling Access to your APIs

- ✓ Using UUID's (Universally Unique Identifiers)
- ✓ Robust Authorization Mechanisms (RBAC)
- ✓ Implement Zero-Trust Security Model
- ✓ Implement Two-factor/Multi Factor Authentication
- ✓ Enforce Transport Layer Security
- ✓ Implement Rate Limiting



Another example



Vulnerability : Broken Object Property Level Authorization (BOPLA)

Broken Object Property Level Authorization (BOPLA) is a combination of
Mass Assignment and Excessive Data Exposure

2023 OWASP API Security top 10 : #6



Vulnerability : Broken Object Property Level

Authorization (BOPLA)

Mitigation/Measures

- Implement Access Controls
- Minimize Data Exposure
- Schema Based Validations
- Avoid Client-Side Filtering

Last second example



Vulnerability : Server-Side Request Forgery

Application retrieves remote resources without validating user input

2023 OWASP API Security top 10 : #7



Vulnerability : Server-Side Request Forgery

Mitigation/Measures

- Use URL parser to avoid issues caused by URL parsing inconsistencies
- Validating URL Schemas and port

Last example



Vulnerability : Improper Inventory Management

Improper Inventory Management represents the risks involved with exposing non-production and unsupported API versions

2023 OWASP API Security top 10 : #9



OWASP Top 10: API Security

OWASP API Security Top-10 2019
API1 Broken Object Level Authorization
API2 Broken User Authentication
API3 Excessive Data Exposure
API4 Lack of Resources & Rate Limiting
API5 Broken Function Level Authorization
API6 Mass Assignment
API7 Security Misconfiguration
API8 Injection
API9 Improper Assets Management
API10 Insufficient Logging & Monitoring

OWASP API Security Top-10 2023	
API1 Broken Object Level Authorization	Same
API2 Broken Authentication	Updated
API3 Broken Object Property Level Authorization	Updated
API4 Unrestricted Resource Consumption	Updated
API5 Broken Function Level Authorization	Same
API6 Unrestricted Access to Sensitive Business Flows	New
API7 Server-Side Request Forgery (SSRF)	New
API8 Security Misconfiguration	Same
API9 Improper Inventory Management	Updated
API10 Unsafe Consumption of APIs	New

OWASP Top 10 2023: API Security



1. Broken Object Level Authorization
2. Broken Authentication
3. Broken Object Property Level Authorization
4. Unrestricted Resource Consumption
5. Broken Function Level Authorization
6. Unrestricted Access to Sensitive Business Flows
7. Server-Side Request Forgery
8. Security Misconfiguration
9. Improper Inventory Management
10. Unsafe Consumption of APIs

Resources to learn from

<https://www.apisecuniversity.com/#courses>

Our Courses

APIsec University courses provide actionable, hands-on training to help you keep APIs secure.



API Penetration Testing

Learn how to hack APIs like a professional penetration tester and find vulnerabilities.

Advanced

Free



API Security Fundamentals

If you're new to API security, this is the place to start. Learn about the OWASP API Top 10, real-world API breaches and more.

Foundation

Free



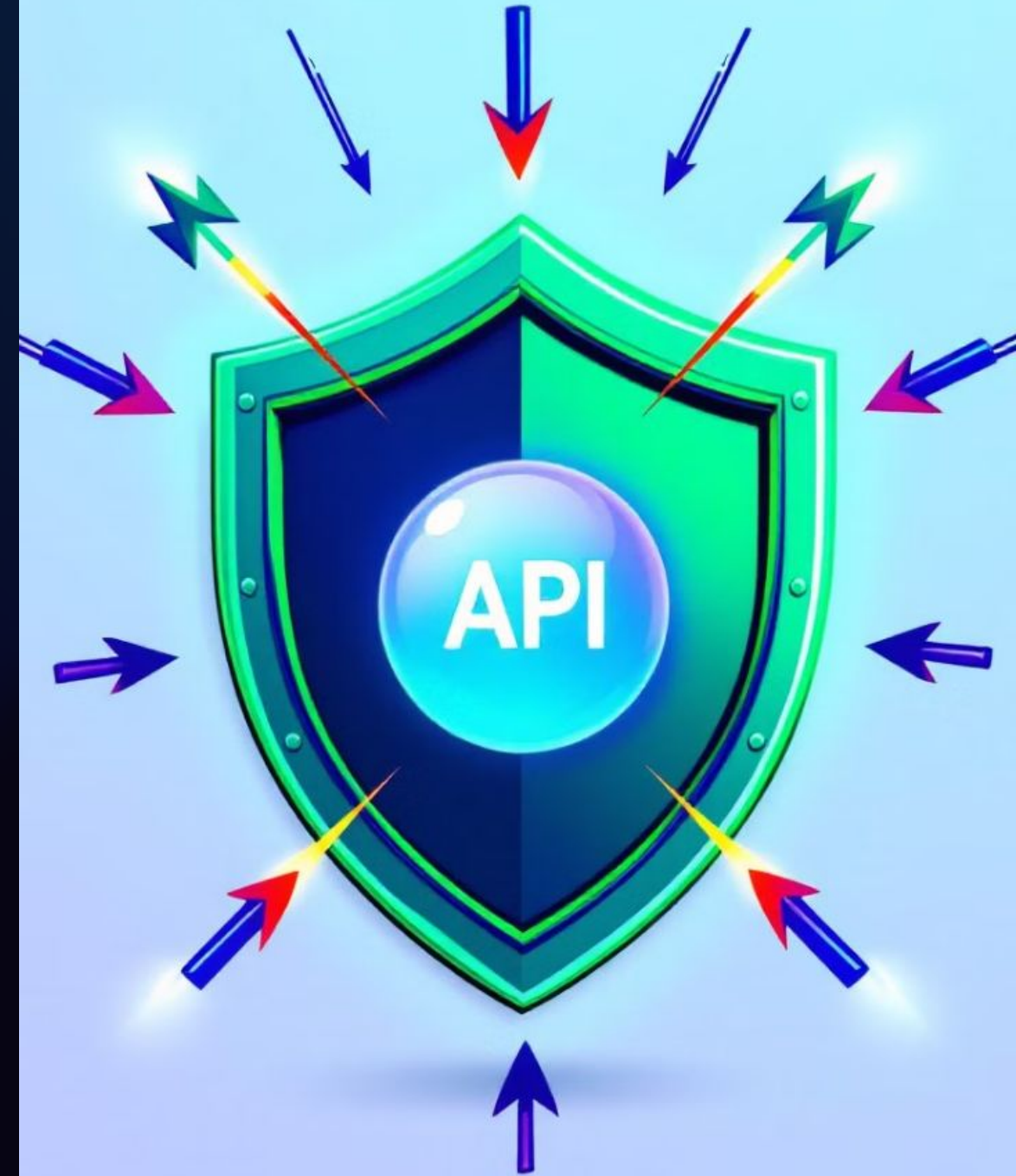
OWASP API Top 10 & Beyond!

Build your API security foundation with a strong understanding of the OWASP API Top 10.

Foundation

Free

**Will you make Sure Your API'S
are Secure ?**



Thank You....



Komal Chowdhary

Quality Assurance Manager | Creative
problem solver | Growth mindset

