

How To Fix The Most Critical API Security Risks

Niloufer Tamboly, CISSP, CPA

Disclaimer

The views expressed in this presentation and during the session are my personal opinions and do not reflect the official policy or position of my employers.

- MBA in Security Assurance

- Certifications

- CPA - Accountancy
- CISSP - Information Security
- CISA - IT Audit
- CFE - Fraud Prevention
- CIA - Internal Audit
- CDPSE - Privacy
- Open FAIR - Risk Quantification

- Work

- Verizon - IT Audit, Fraud Operations & Risk
- Samsung (Harman) - IT Audit

- Patents

- Establishing An Alternate Call Path Using Short-Range Wireless Technology
 - Patent Issued Jul 12, 2016 Patent issuer and number 9,392,523
- System For And Method of Generating Visual Passwords
 - Patent Issued Oct 27, 2015 Patent issuer and number US 9,171,143 B2

- Volunteer

- Cofounder - Step Up Skill and (ISC)2 New Jersey Chapter
- Organizer - Largest CISSP & CCSP Exam Meetup Group

- Part-time lecturer

- Rutgers University

Evolution and decoupling of tech infrastructure

Client server → Web applications → Web services/SOAP → APIs



Why is API usage so popular?

API Management Market to Hit Sales of \$8.36 Billion by 2028 | Pay as you Go Pricing is Becoming Popular in API Management Market

Top Players in Global API Management Market

Google (US)

IBM (US)

Microsoft (US)

Axway Software (US)

Broadcom Inc. (US)

MuleSoft (US)

Oracle Corporation (US)

Software AG (Germany)

Kong Inc. (US)

Red Hat (US)

SAP SE (Germany)

TIBCO Software (US)

Amazon Web Services (US)



API design

New York City Metropolitan ...

Jobs ▾

Date Posted ▾

Experience Level ▾

Company ▾

API design in New York City Metropolitan Area

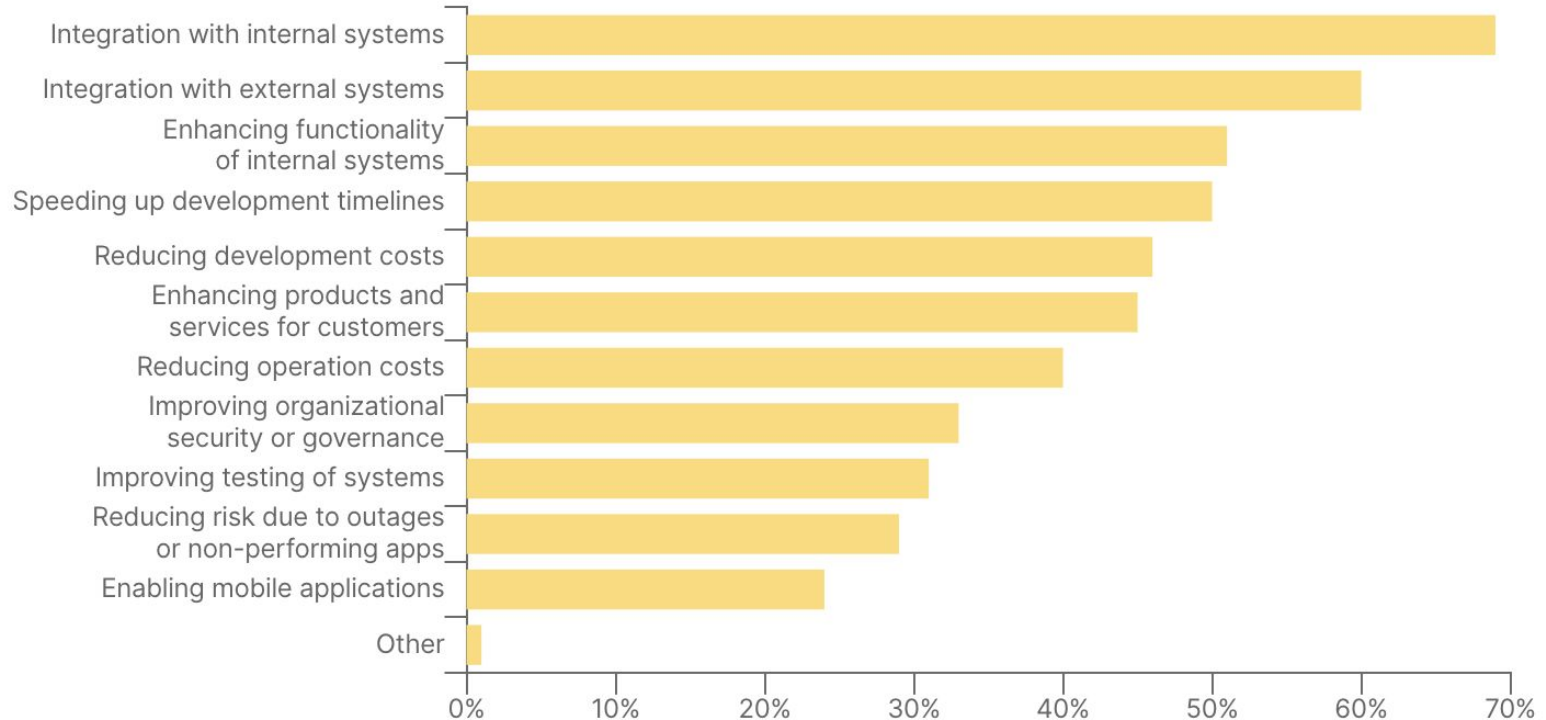
25,833 results

Set alert

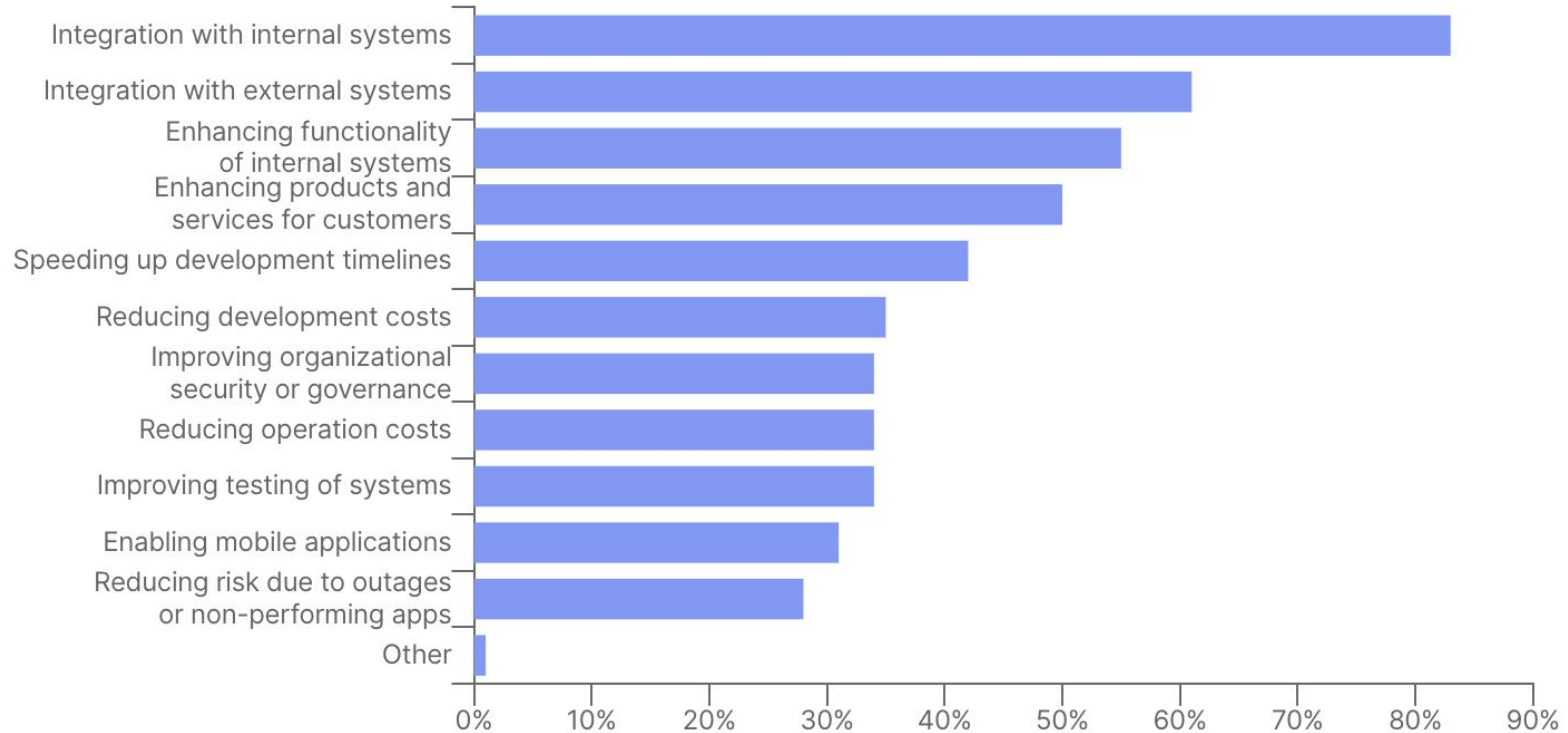


Change in approach - configure not code security

Top reasons for consuming APIs



Top reasons for producing APIs



Top factors to consider before integrating with an API

Performance

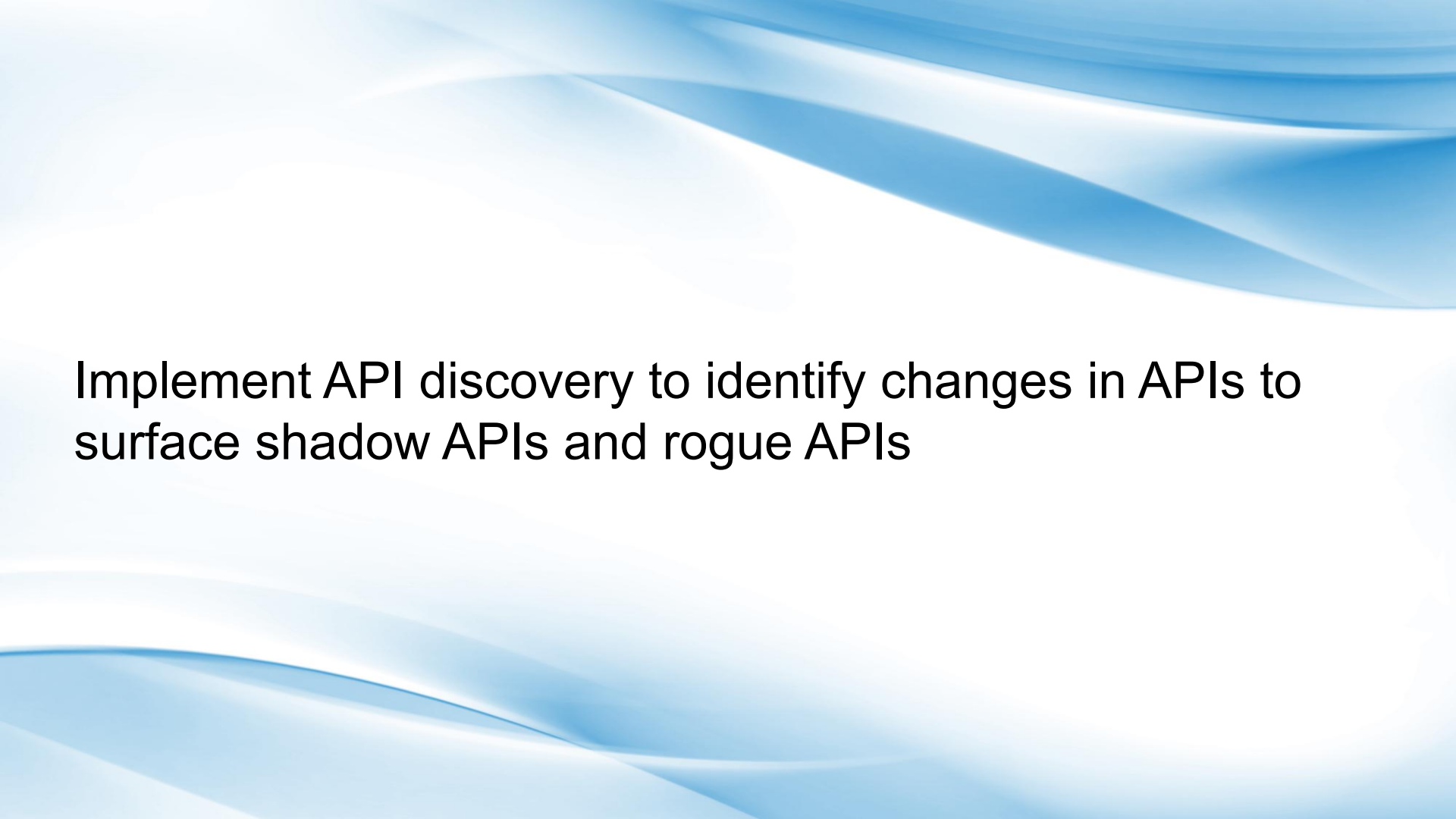
Security

Reliability

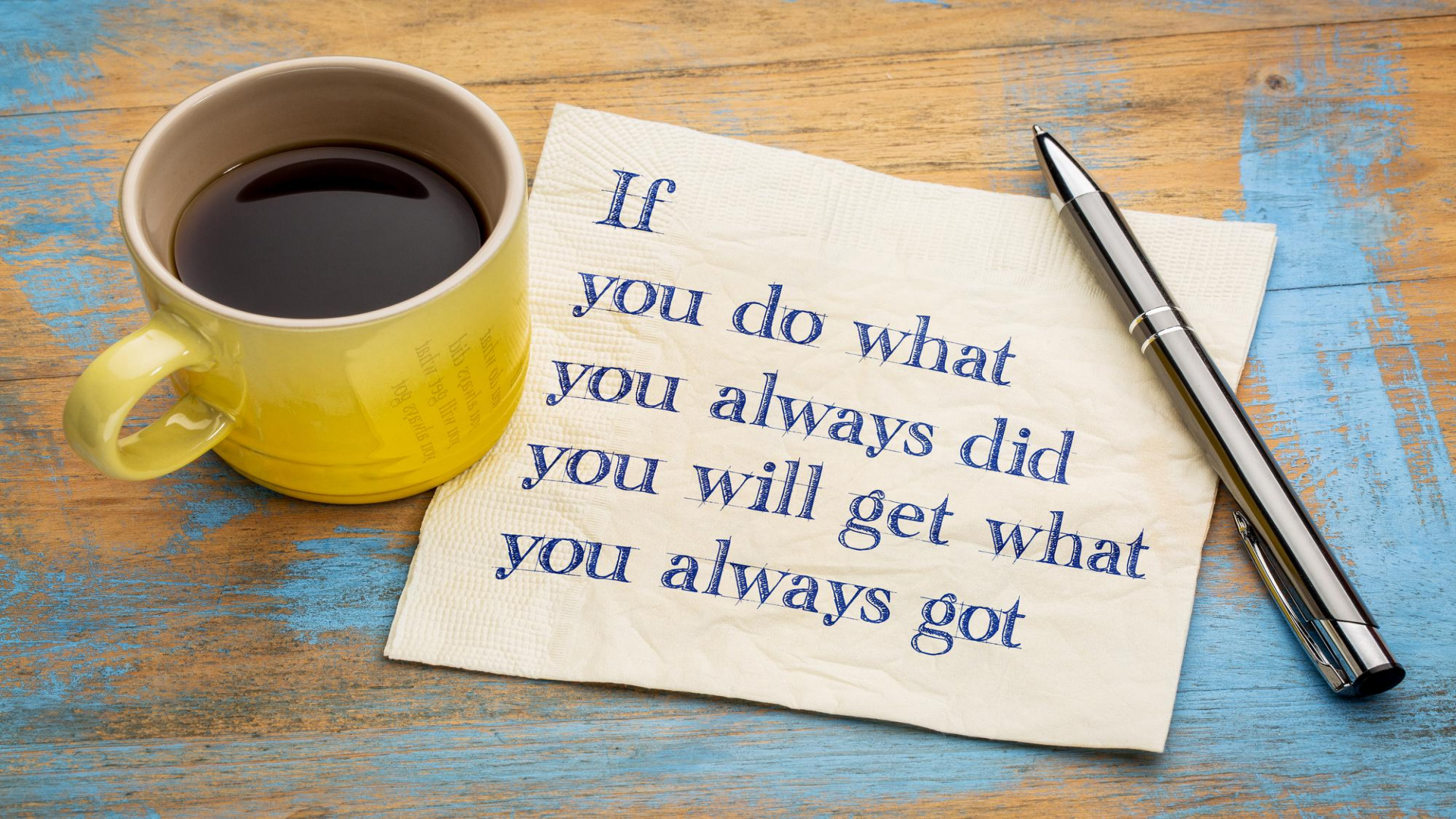
Documentation

The background of the slide features a series of flowing, wavy bands in various shades of light blue and white, creating a sense of motion and depth. The waves are more pronounced in the upper and lower portions of the frame, leaving a clear white space in the center for the text.

Understand the technical capabilities of your APIs

The background of the slide features a light blue and white color palette with soft, flowing, wavy patterns that create a sense of movement and depth. The waves are more pronounced in the upper and lower portions of the frame, while the center is relatively clear, providing a space for the text.

Implement API discovery to identify changes in APIs to surface shadow APIs and rogue APIs

A photograph of a yellow ceramic mug filled with dark coffee, a silver pen, and a white paper napkin with a blue-inked quote. The items are arranged on a rustic wooden surface with blue-painted accents. The quote is written in a classic serif font and reads: "If you do what you always did you will get what you always got".

If
you do what
you always did
you will get what
you always got

The background of the slide features a series of flowing, wavy bands in various shades of light blue and white, creating a sense of movement and depth. The waves are layered, with some appearing more prominent than others, and they curve across the frame from top to bottom.

Legacy threats are now API threats

More Than 30% of All Malicious Attacks Target Shadow APIs

Peloton's Leaky API Spilled Riders' Private Data



Hacker breaches Fast Company systems to send offensive Apple News notifications

infiltrate the publication. The message claims that Fast Company had a "ridiculously easy" default password that was used across a number of accounts, including an administrator. This enabled the attacker to access a bunch of sensitive information, including authentication tokens, Apple News API keys and Amazon Simple Email Service (SES) tokens, allowing the hacker to send emails using any @fastcompany.com email.

Optus Hack Exposes Data of Nearly 2.1 Million Australian Telecom Customers



Breach of 9.8 million customer records includes driver's licenses, passports, and Medicare ID numbers, in addition to names, phone numbers, and email addresses.

The incident reportedly started with the attacker accessing an API server that was not protected with any type of authentication. In other words, the attacker didn't even have to log in.

Common Threat Vectors

Authorization

Authentication

MisConfiguration

Business logic

Improper logging and monitoring

Use API Management Tools

Discovery

Rate limiting

Workflow automation

Security

The background of the slide features abstract, flowing blue and white patterns that resemble waves or liquid motion, creating a sense of fluidity and depth. The colors range from light, airy blues to deeper, more saturated tones, with soft gradients and highlights that give the impression of light reflecting off a moving surface.

Broken object level authorization

Implement an authorization mechanism to checks if logged in user has permission to perform an action;

Use this authorization mechanism in all functions that accesses sensitive data;

Use randomly generated GUIDs (UUIDs) as object identifiers for user requests.

Use standards like OAuth and JWT for the authentication process

Identify all paths that can be used to authenticate with your API

Do not return passwords, keys, or tokens directly in API responses;

Protect all login, password recovery, and registration paths (use rate limiting),
brute force protection

Add lockout measures for abusive traffic sources;

Implement multi factor authentication (MFA)

Use revocable tokens where implementing MFA is not feasible.



Excessive data exposure

Return only the data the client requests from your API functions

Define object properties to be returned in your API functions

Do not return entire objects

Limit the number of records that can be queried in API functions to prevent mass updating or disclosure of records

Validate API responses and filter object properties that should not be visible to the user.

The background of the slide features abstract, flowing blue and white patterns that resemble liquid or smoke, creating a sense of movement and depth. The colors range from light, airy blues to deeper, more saturated tones, with soft gradients and highlights that give the impression of light reflecting off a fluid surface.

Broken function level authorization

The background of the slide features a light blue and white color palette with soft, flowing, wavy patterns that create a sense of movement and depth. The waves are more pronounced in the upper right and lower left corners, while the center is relatively clear, providing space for the text.

Grant access explicitly to individual resources.

Set default permission for all users for all resources to deny access.

Centralize your authorization code, review and vet it to cover authorization wherever it is used in your API.

Mass assignment

Validate input

Do not directly assign user input to objects in your API functions

Do not create or update objects by directly assigning user input

Explicitly define the object properties a user can update in API code

Enforce validation and data schemas to only approved object properties that can be used by API functions.

The background of the slide is an abstract composition of flowing, wavy lines in various shades of blue, ranging from light sky blue to a deeper cerulean. These lines create a sense of movement and depth, set against a clean white background.

Security misconfiguration

The background of the slide features a light blue gradient with several flowing, wavy bands of a slightly darker blue, creating a sense of movement and depth.

Secure your API endpoints

Harden and document deployment process to create a secure hosting environment

Review configurations and software dependencies used in your API and the security of your cloud infrastructure

Limit all client interactions with your API and other resources to authorized channels

Only allow API access using necessary HTTP verbs to reduce attack surfaces

Set CORS policies for APIs that are publicly accessible from browser-based clients

The background of the slide features a series of flowing, wavy bands in various shades of light blue and white, creating a sense of movement and depth. The waves are layered, with some appearing more prominent than others, and they curve across the frame from top to bottom.

Insufficient logging & monitoring

Log all authentication and authorization failures

Use API security management tool to identify the source of attack

Properly format logs

Treat logs as sensitive data, because they have both user and API vulnerabilities

Continuously monitor infrastructure

Source:

<https://www.globenewswire.com/news-release/2022/10/04/2528080/0/en/API-Management-Market-to-Hit-Sales-of-8-36-Billion-by-2028-Pay-as-you-Go-Pricing-is-Becoming-Popular-in-API-Management-Market.html>

<https://owasp.org/www-project-api-security/>