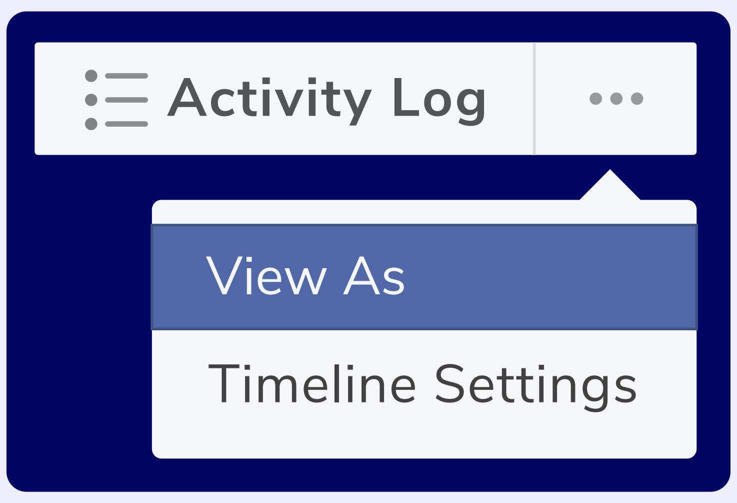
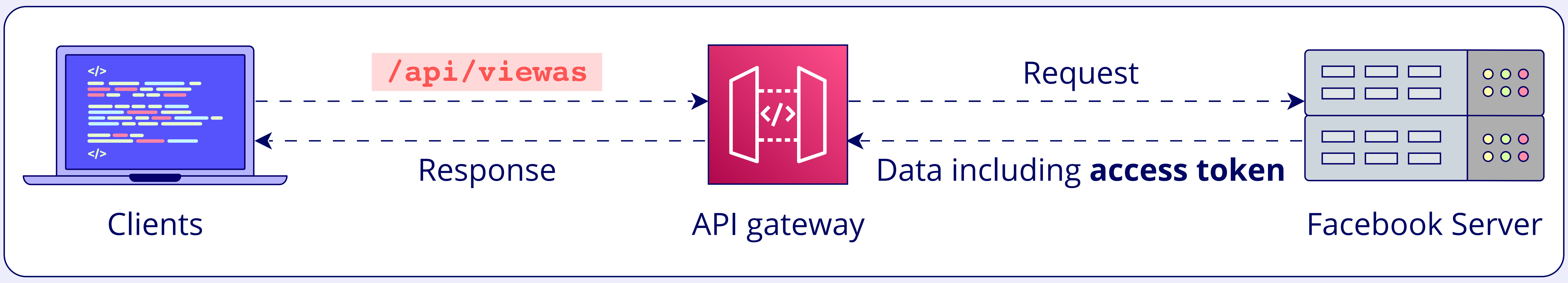
API Security

educative

Data Breach at Facebook

In 2018, Facebook's "View As" feature accidentally generated access tokens, allowing hackers to access private user information.





What Is API Security?

It is a set of practices and measures to protect APIs from unauthorized access, misuse, and attacks.

Why is it important?

- Safeguards digital assets.
- Prevents data breaches.
- Blocks unauthorized access.
- Mitigates cyber threats.
- Maintains data integrity.
- Protects API services.

API Security Risks/Vulnerability, Attack Types, and Mitigations

Risk/Vulnerability	Attack	Mitigation
Broken object-level auth	Breaching data	Validate user access per object
Broken user-level auth	Phishing and Credential stuffing	Strong authentication
Excessive data exposure	Information harvesting	Data minimization
Service outage	DDoS and brute-force attacks	Rate limiting
Broken function-level auth	Privilege escalation	ACLs and Role-based access
Mass assignment	Unauthorized data changes	Allowlisting and specified parameterized queries
Security misconfiguration	Various exploits	Secure config. management, Regular audits, auto scan
Injection	SQL/NoSQL, command injections, and XSS	Input validation, parameterized queries
Improper asset management	Unpatched vulnerabilities	Asset inventory and review
Insufficient logging and monitoring	Delayed response and undetected attacks	Detailed logging and reviewing, and alerts

Key Tips

- Strong authentication and authorization.
- Secure data transmission (SSL/TLS).
- Rate limiting.
- Security audits and monitoring.
- Access control.
- Minimize data exposure.

Scenario

Suppose you are a lead security engineer and an ethical hacker reported the following issues in your system:

- Misconfigured security setting.
- Weak authentication.
- Sensitive data leakage.

What mitigation techniques would you acquire to overcome these vulnerabilities?

Drop your answers below!

Learn More!

Grokking the API Design Interview

Grokking Modern System Design Interview for Engineers & Managers