สยามชำนาญกิจ
SIAM CHAMNAN KIT

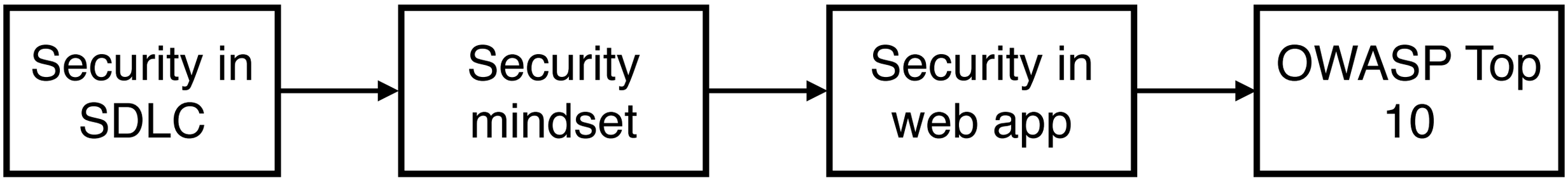
Workshop API with NodeJS

Workshop API with NodeJS

Software Delivery

Fast (Time to market)
High quality
Scalable
More secure

Learning Path



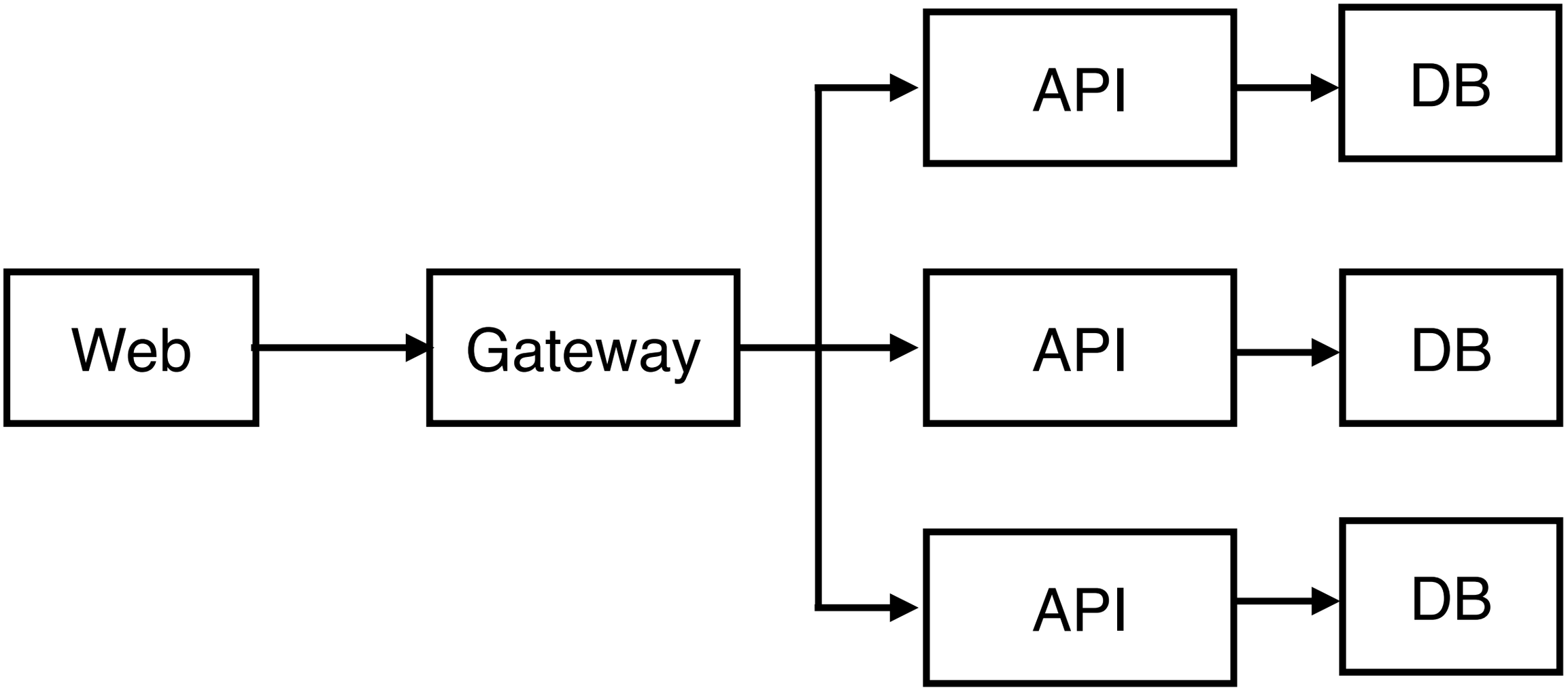
Secure Coding Standard

Avoid vulnerabilities
Focus on Web and API security

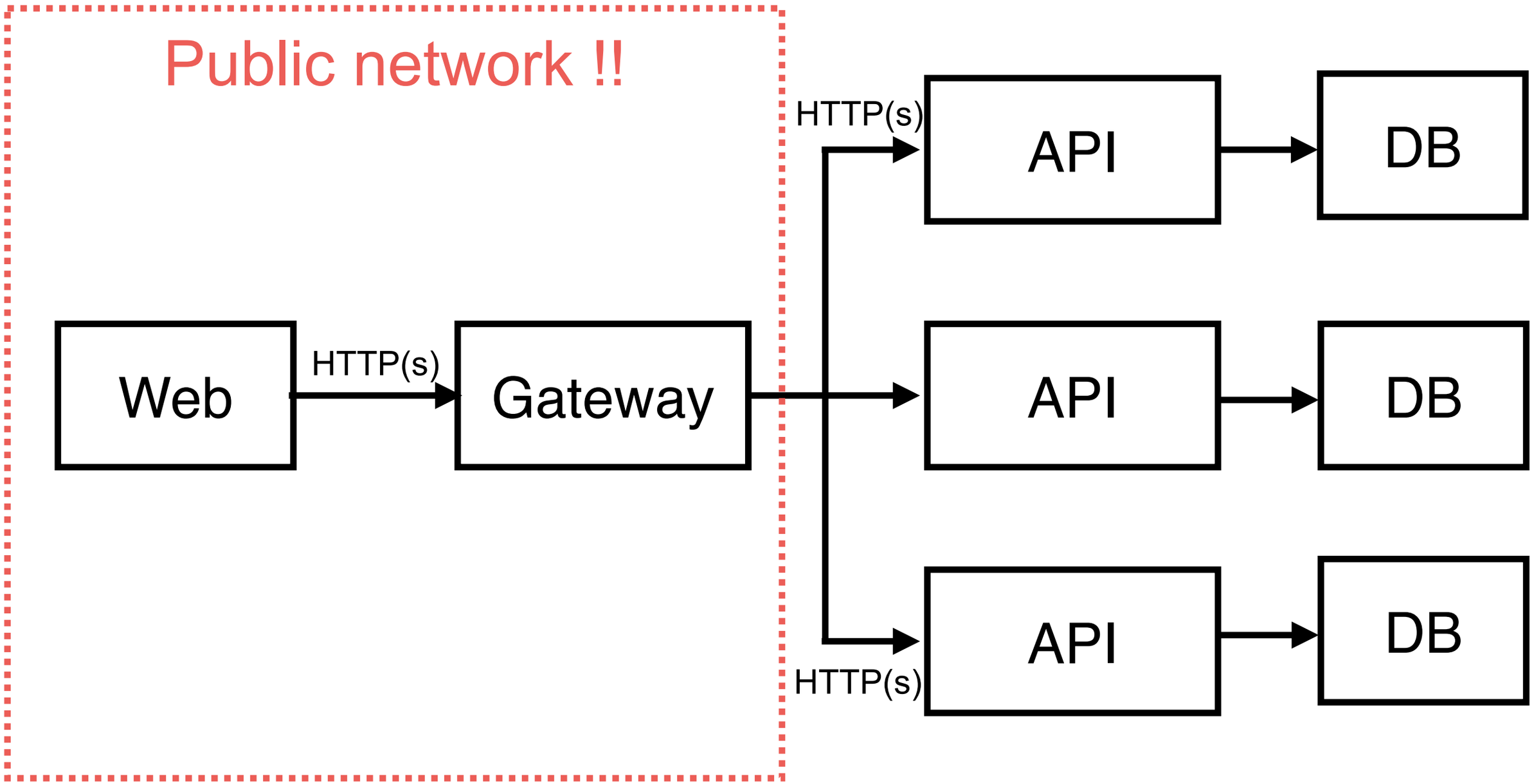
Web	**API**
OWASP Top 10	

SANS
20 software errors

Software Architecture



Software Architecture + Network



OWASP

TOP 10

https://owasp.org/Top10/

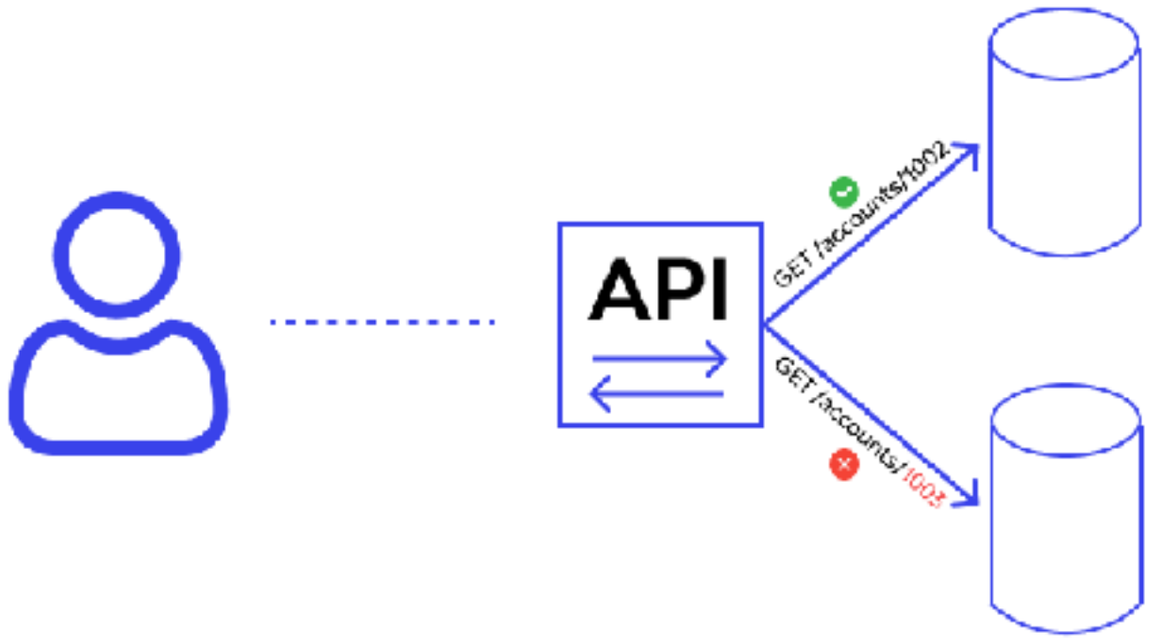
https://owasp.org/API-Security/editions/2023/en/0x11-t10/

Broken Object Level Authorization (BOLA)

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

Broken Object Level Authorization (BOLA)

Bypassing access control
Access API with mission access control



Solution ?

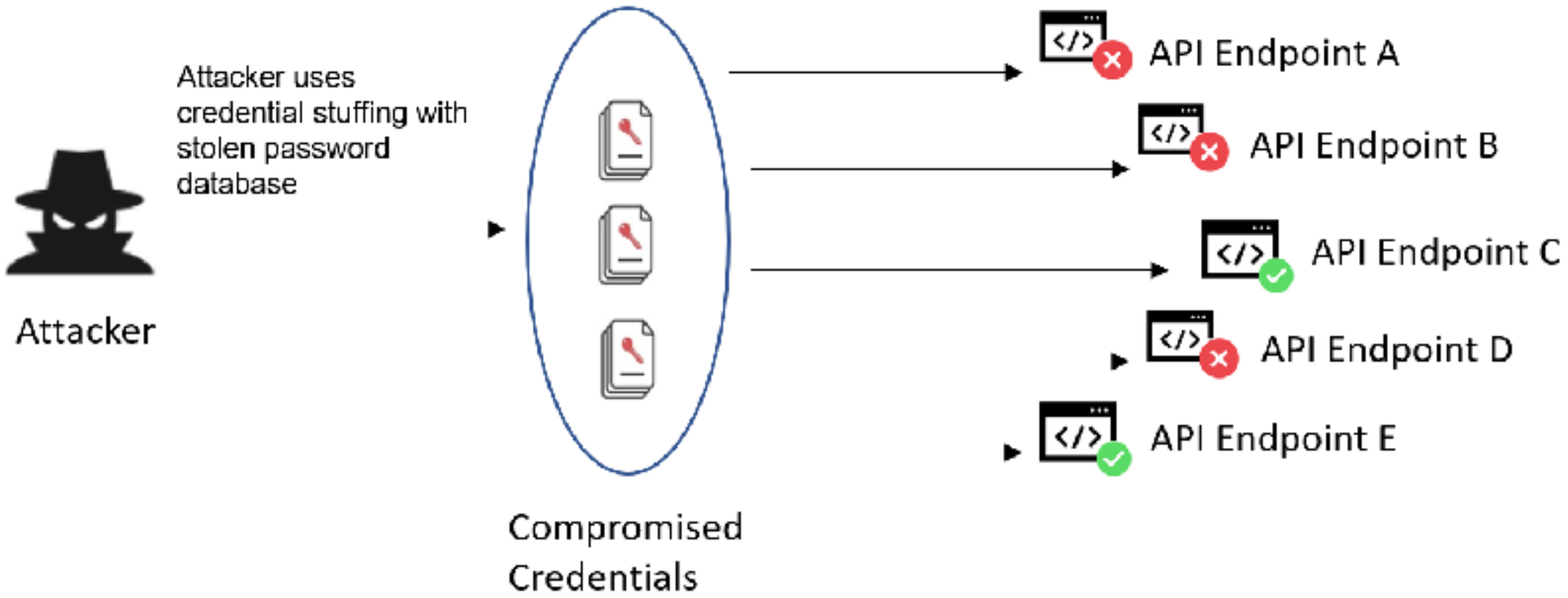
Use random number or UUID
Always check permission before access
Use strong authorization process

Broken Authentication

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

Broken Authentication

Authentication is process to validate a person
Lack authentication process



Broken Object Property Level Authorization

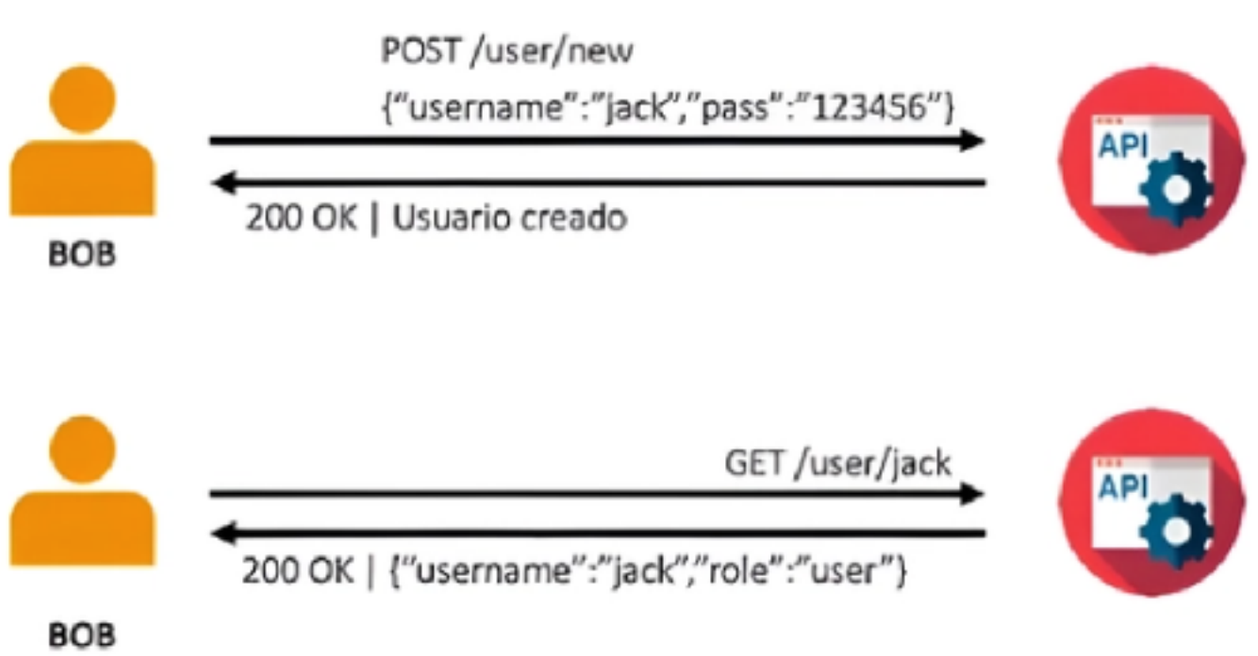
https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/

Broken Object Property Level Authorization

Unauthorized data access
Data tempering
Elevation of privilege
Compliance violations

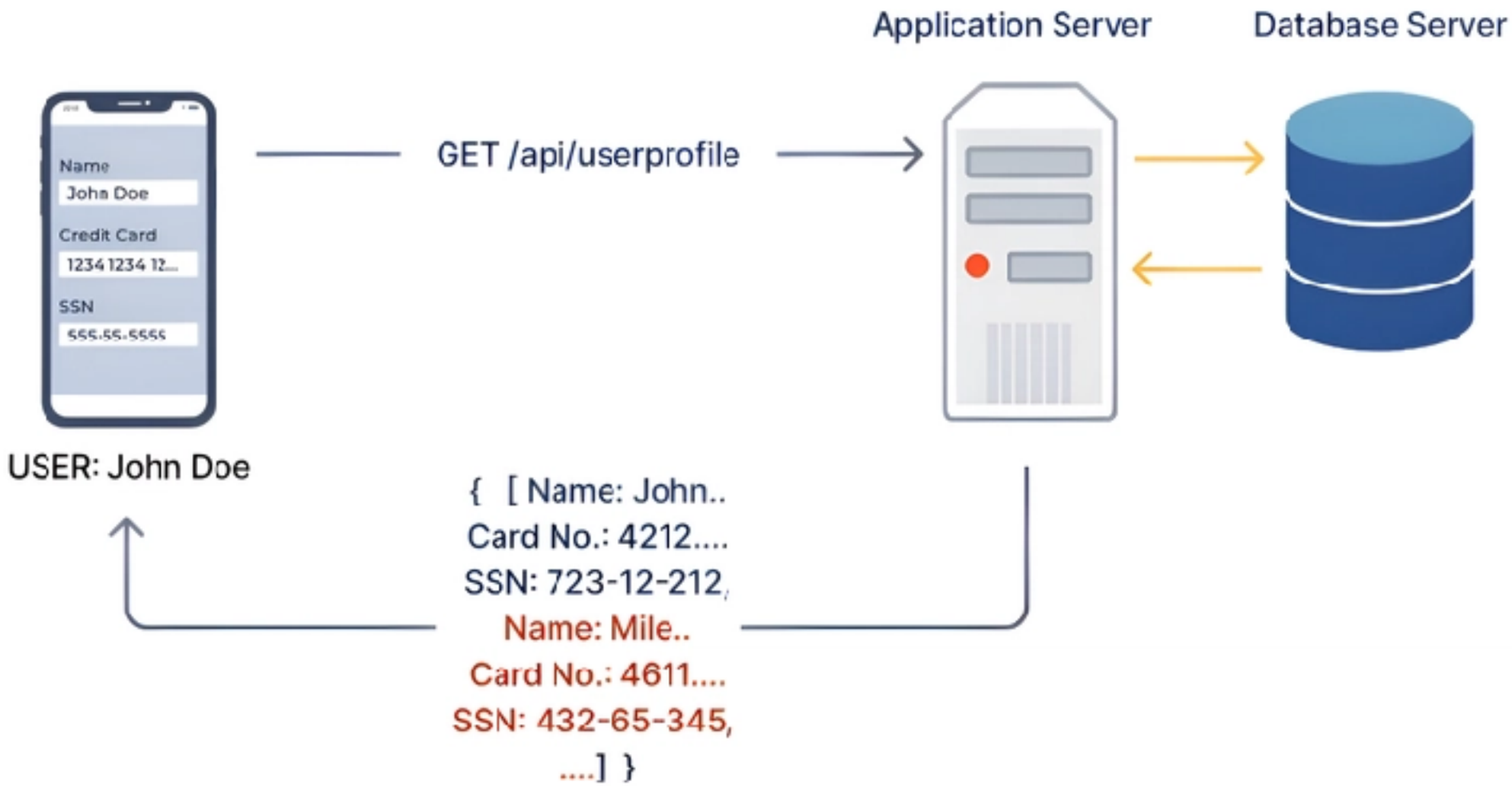
Broken Object Property Level Authorization

Excessive Data Exposure
Mass assignment



Excessive Data Exposure

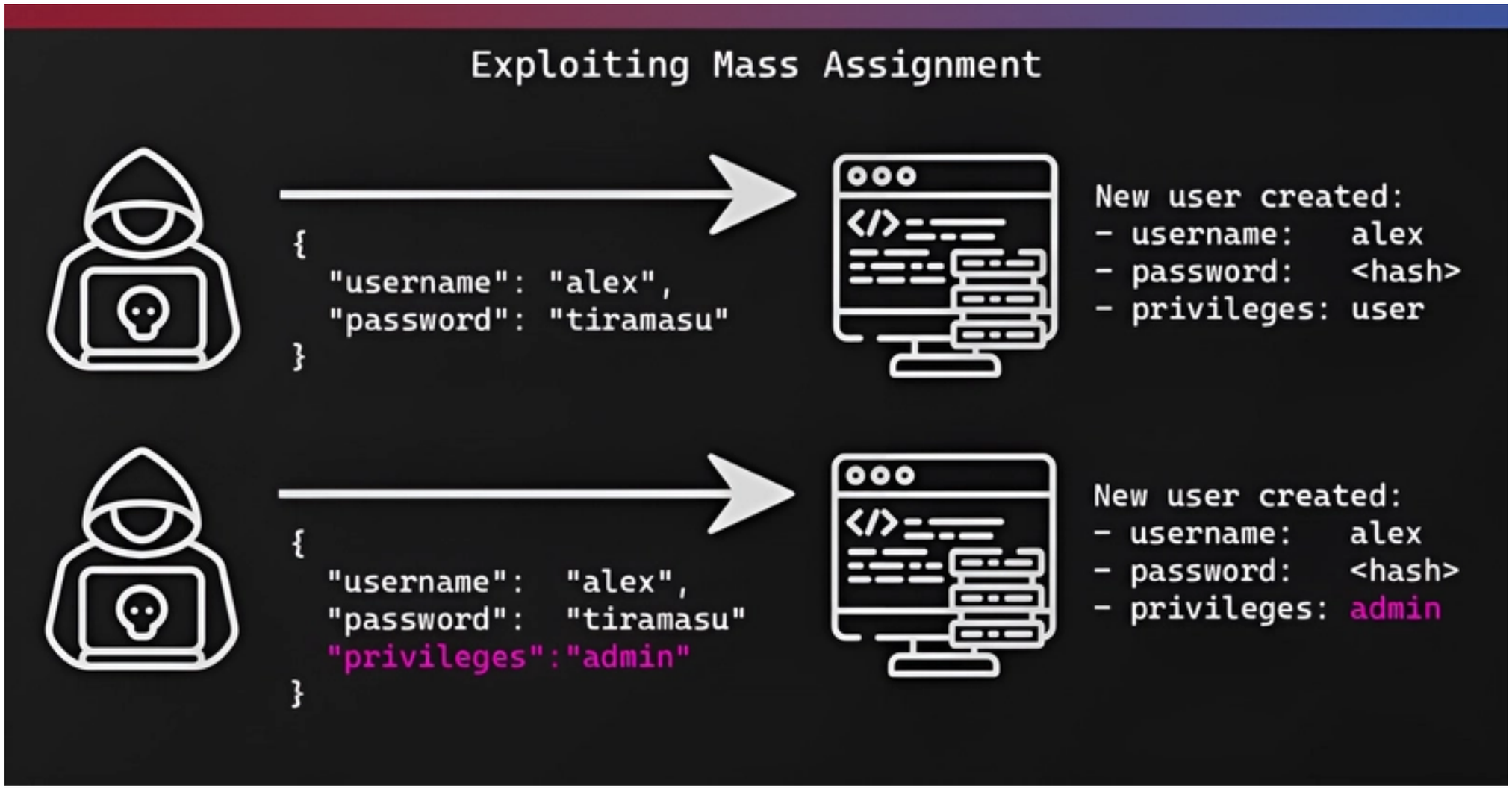
API return more details, expose sensitive data



https://dev.to/sre_panchanan/broken-object-property-level-authorization-bk8

Mass Assignment

API return more details, expose sensitive data



https://dev.to/sre_panchanan/broken-object-property-level-authorization-bk8

Unrestricted Resource Consumption

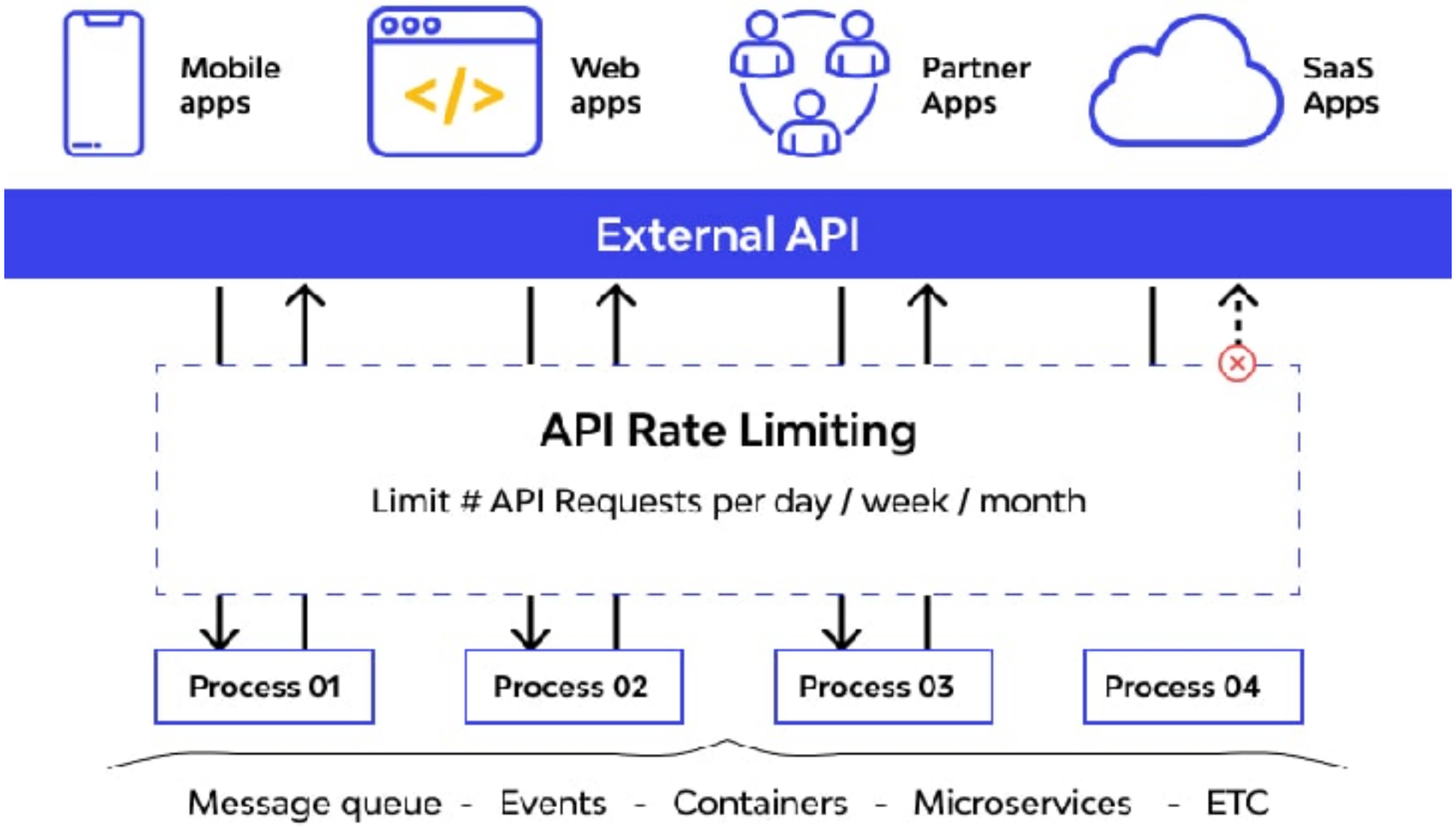
https://owasp.org/API-Security/editions/2023/en/0xa4-unrestricted-resource-consumption/

Unrestricted Resource Consumption

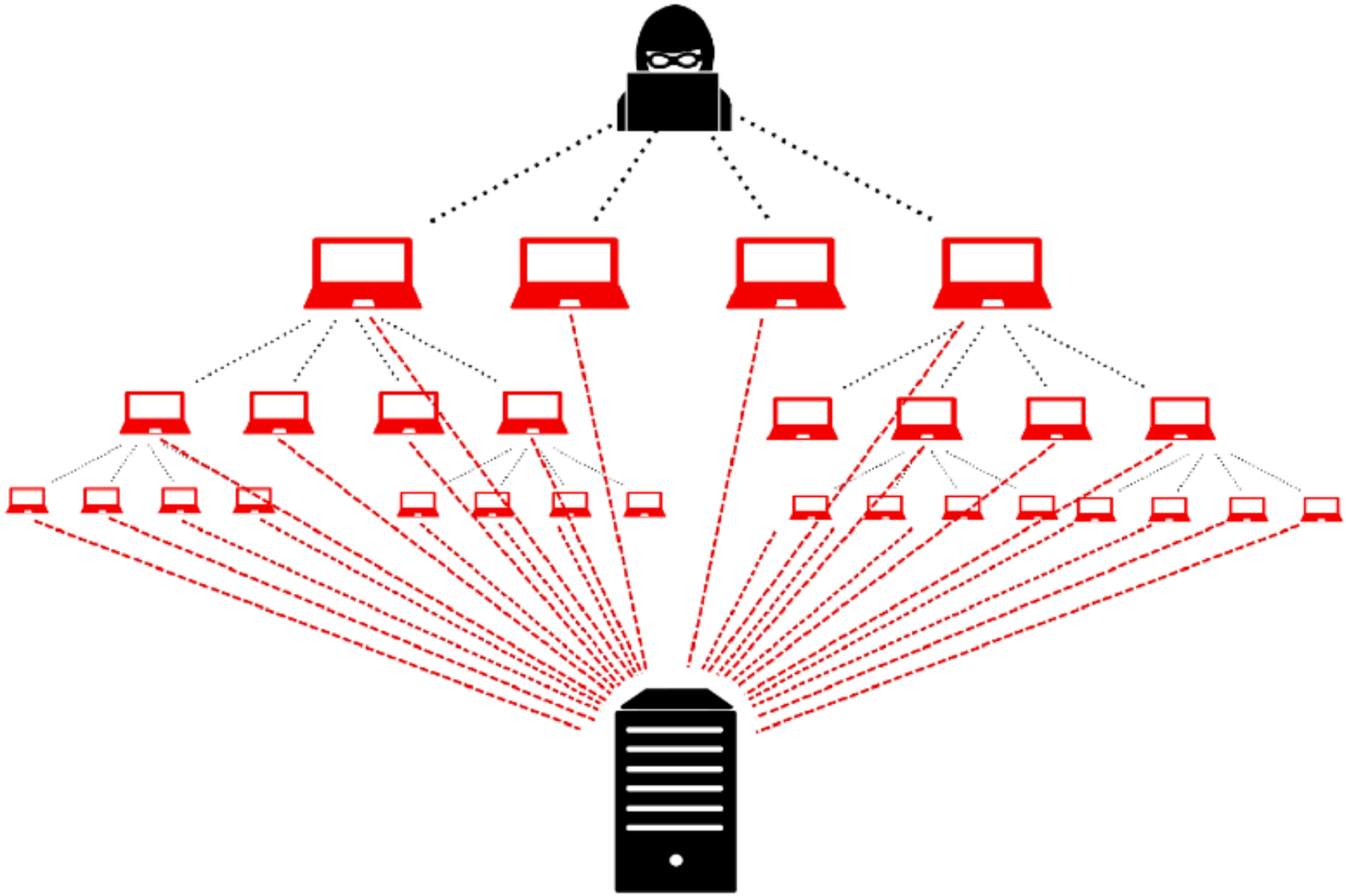
Lack of resource and rate limit
Request size
Response size

https://dev.to/sre_panchanan/broken-object-property-level-authorization-bk8

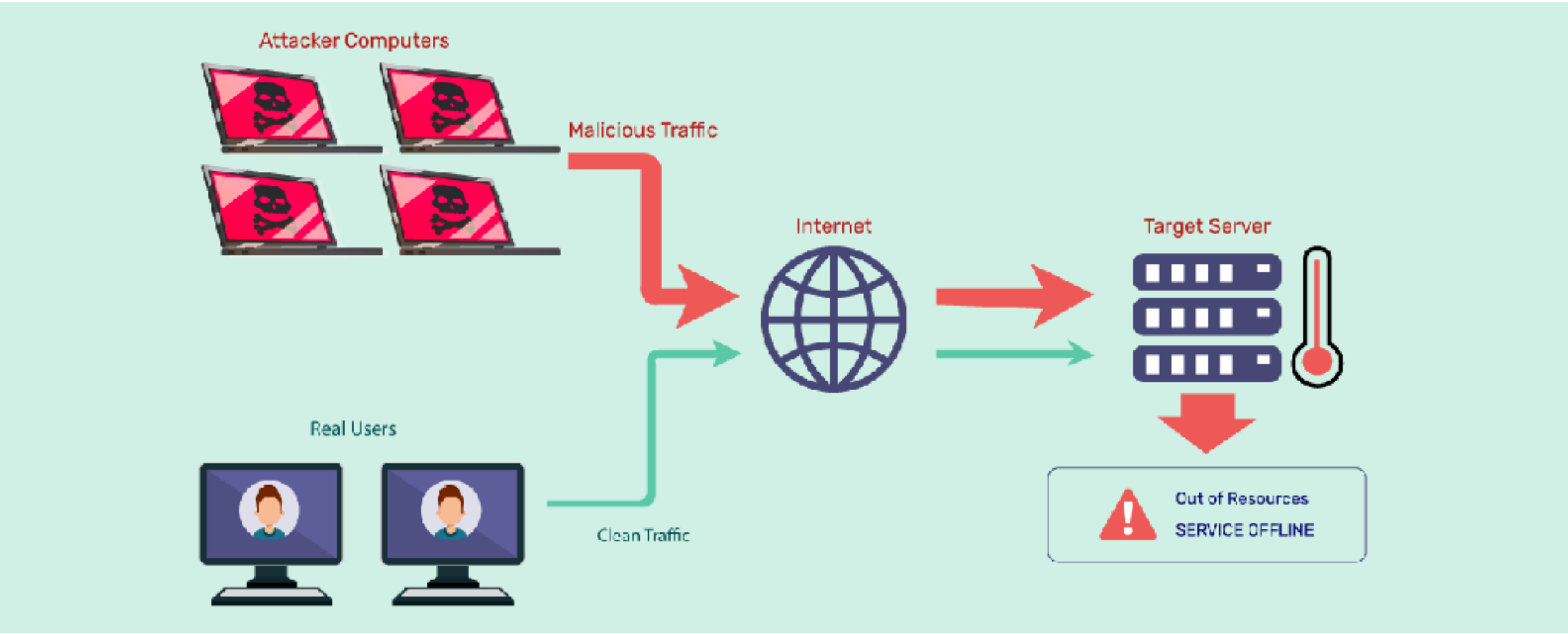
Rate Limit



DDOS (Distributed Denial-of-Service)



DDOS (Distributed Denial-of-Service)

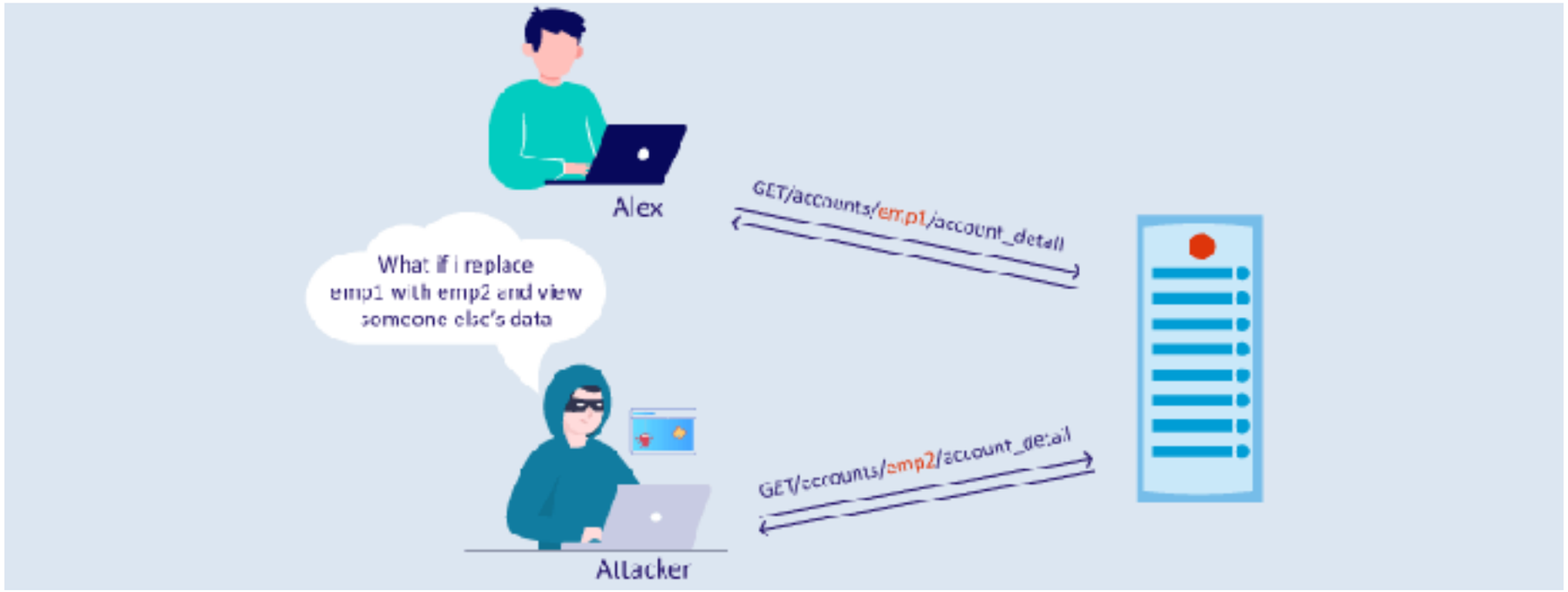


Broken Function Level Authorization

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

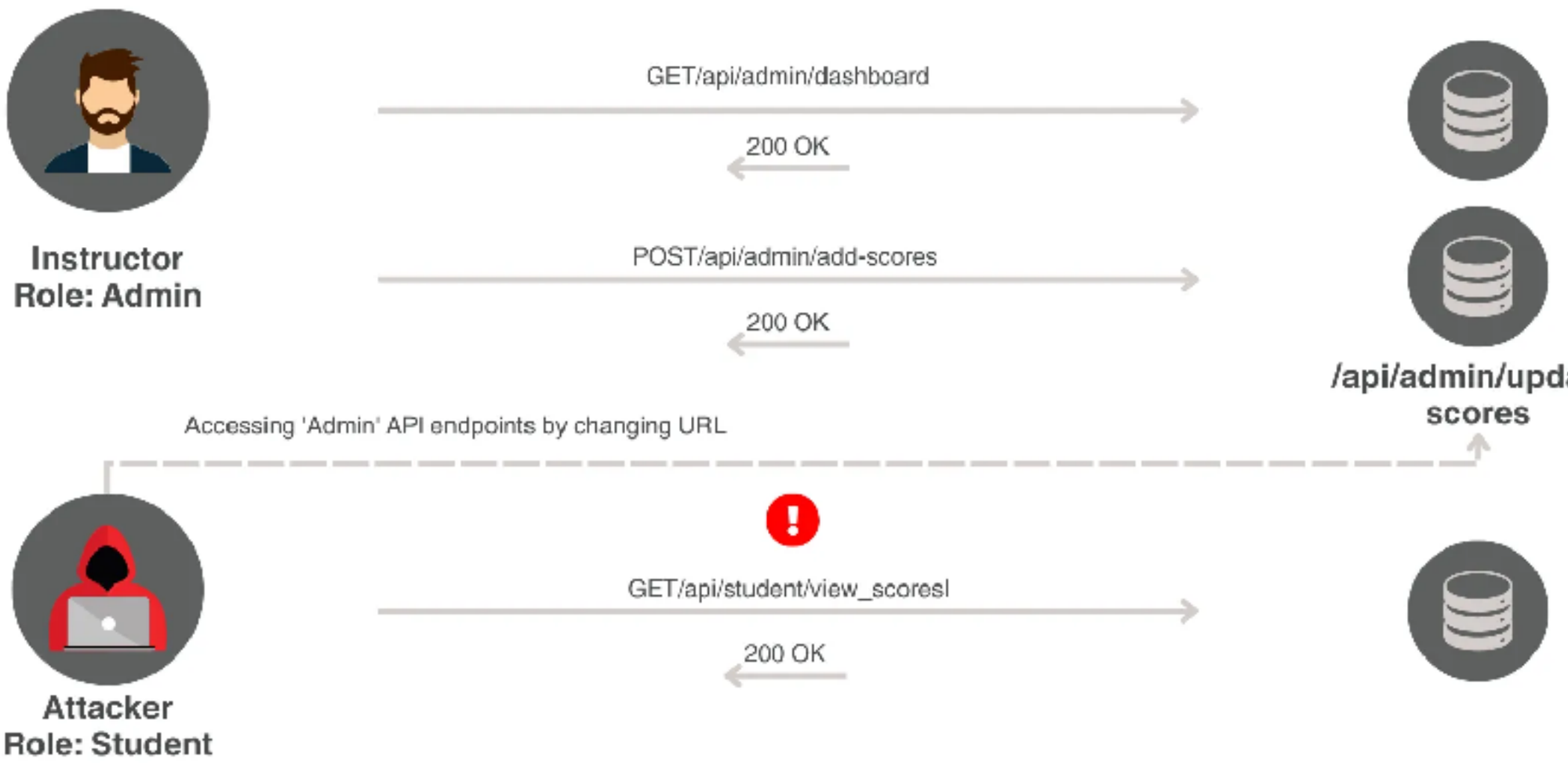
Broken Function Level Authorization

Practice to controlling access to functions/operation



https://www.indusface.com/blog/broken-function-level-authorization/

BROKEN FUNCTION LEVEL AUTHORIZATION



https://api7.ai/blog/protect-top-10-owasp-api-security-threats

Unrestricted Access to Sensitive Business Flow

https://owasp.org/API-Security/editions/2023/en/0xa6-unrestricted-access-to-sensitive-business-flows/

Unrestricted Access to Sensitive Business Flow

Sensitive business flows are exposed
Without risk evaluation
Insufficiency logging and monitoring
Rate limiting not enough

UNRESTRICTED ACCESS TO SENSITIVE BUSINESS FLOWS

https://api7.ai/blog/protect-top-10-owasp-api-security-threats

Server Side Request Forgery

https://owasp.org/API-Security/editions/2023/en/0xa7-server-side-request-forgery/

Security Misconfiguration

https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/

Improper Inventory Management

https://owasp.org/API-Security/editions/2023/en/0xa9-improper-inventory-management/

Unsafe Consumption of APIs

https://owasp.org/API-Security/editions/2023/en/0xaa-unsafe-consumption-of-apis/

Q/A