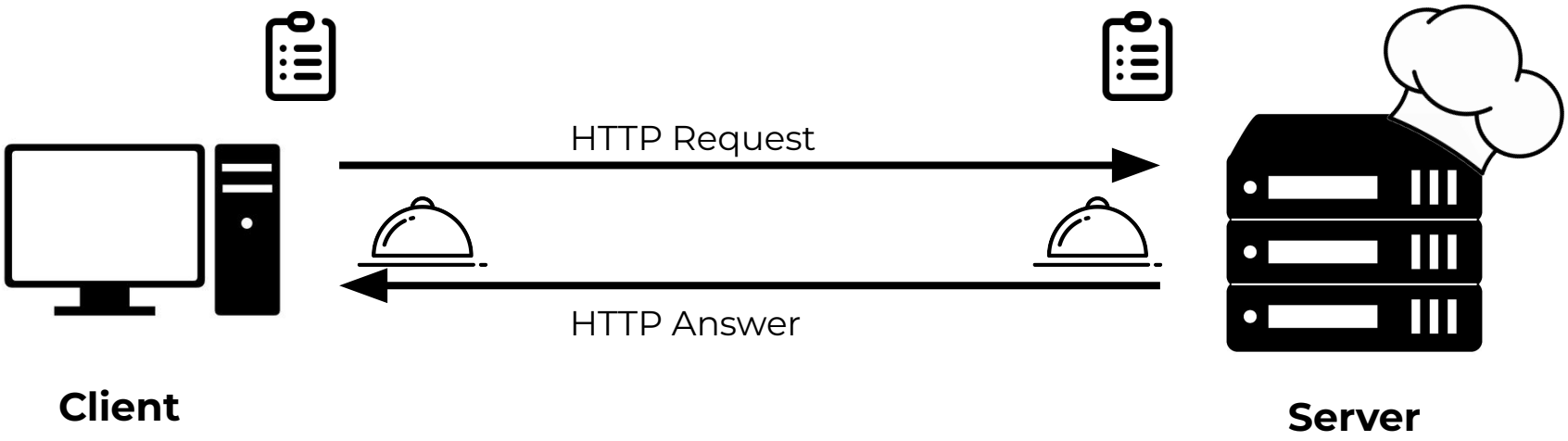
We cannot **REST** on **API** security

RESTAPI

REST API

Representational State Transfer

Application Programming Interfaces


HTTP Request
HTTP Answer
Client
Server

OWASP: Open Web Application Security Project

OWASP™

What is OWASP?

A global non-profit organization dedicated to improving web and API security through:

- Best practices & guidelines.
- Open-source security tools Industry-leading research.

Why does it matter?

- Helps developers and businesses identify and mitigate security risks.
- Used as a standard in cybersecurity frameworks and compliance.

OWASP Top 10 API Security Risks – 2023

API1:2023 - Broken Object Level Authorization

POST /api/order

```
{
  "tableNumber": 12,
  "dish": "Truffle Pasta",
  "quantity": 1,
  "priority": "high"
}
```

HTTP/1.1 **401 Unauthorized**

API1:2023 - Broken Object Level Authorization

POST /api/order

```
{
  "tableNumber": 12,
  "dish": "Truffle Pasta",
  "quantity": 1,
  "priority": "high"
}
```

HTTP/1.1 **200 OK**

API2:2023 - Broken Authentication

POST /api/order

```
{
  "tableNumber": 12,
  "dish": "Red wine bottle",
  "quantity": 1,
  "order_age": 17,
  "priority": "high"
}
```

HTTP/1.1 **200 OK**

API3:2023 - Broken Object Property Level Authorization

POST /api/order

```
{
  "tableNumber": 12,
  "dish": "Red wine bottle",
  "quantity": 1,
  "order_age": 18,
  "price": 2
}
```

HTTP/1.1 **200 OK**

```
{
  "order_id": 9999,
  "items": [
    {
      "dish": "Red wine bottle",
      "price": 2.00,
      "quantity": 1,
      "legal_age": True
    }
  ],
  "total_price": 2.00
}
```

API4:2023 - Unrestricted Resource Consumption

POST /api/order/free-bread

```
{
  "tableNumber": 12,
  "quantity": 1000
}
```

HTTP/1.1 **418 I’m a Teapot**

API4:2023 - Unrestricted Resource Consumption

POST /api/order/free-bread

```
{
  "tableNumber": 12,
  "quantity": 1000
}
```

API5:2023 - Broken Function Level Authorization

POST /api/admin/add-dish

```
{
  "name": "Hawaii Pizza",
  "price": 10000.00
}
```

HTTP/1.1 **401 Unauthorized**

API6:2023 - Unrestricted Access to Sensitive Business Flows

GET /api/recipes/

```
{
  "dish": "Federico's Tiramisu'"
}
```

HTTP/1.1 **200 OK**

API7:2023 - Server Side Request Forgery

GET /api/menu

```
{
 "language": "it",
 "category": "main_course",
 "source_url":"localhost:/database"
}
```

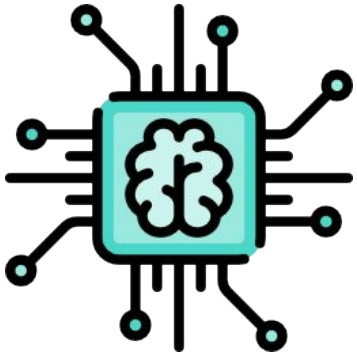
HTTP/1.1 **200 OK**

API8:2023 -
Security Misconfiguration

API9:2023 -
Improper Inventory Management

API10:2023 -
Unsafe Consumption of APIs

API Security **2025 Trends**:



Thank you for your attention!