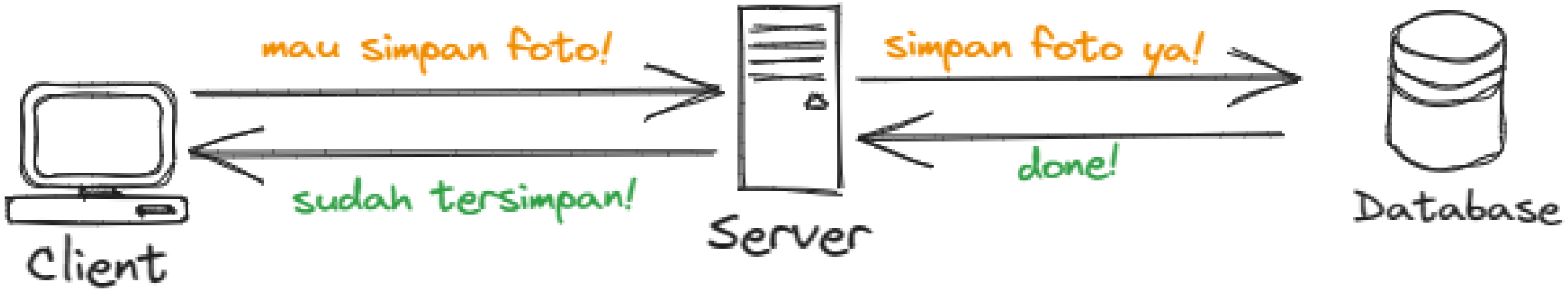
Web Security: JWT Injection with Burp Suite

What is the Web?

- *A Software*
- HTML,
- JavaScript,
- CSS.
- Diakses dengan *browser*
- Digunakan belanja dan perbankan streaming media dan mengelola keuangan.

Web Architecture? Wait There's a Web Architect?

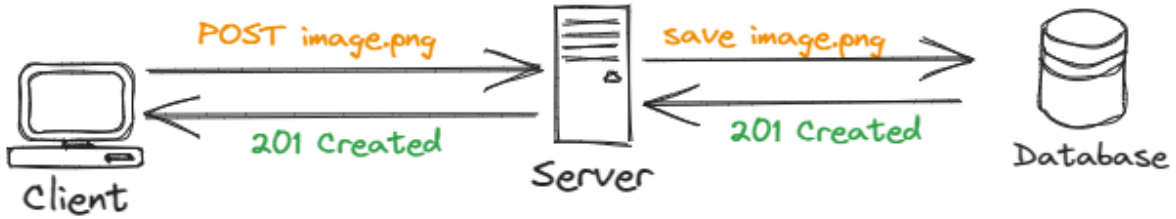

mau simpan foto!
sudah tersimpan!
simpan foto ya!
done!
Client
Server
Database

Presentation Layer

Application Layer

Data Layer

HTTP Protocol? Huh?


POST image.png
201 Created
save image.png
201 Created
Client
Server
Database

The Hypertext Transfer Protocol (HTTP)

Protokol utama yang digunakan untuk komunikasi antara sebuah *client* dan *server*

HTTP mendefinisikan bagaimana sebuah pesan diformat dan dikirimkan dan juga bagaimana sebuah *server* dan *client* harus membalas sebuah *request*.

1. Bekerja diatas Protocol TCP (*Transmission Control Protocol*) merupakan sebuah protokol yang digunakan dalam *reliable data transmission* (pengiriman data antar internet)
2. Mendefinisikan bagaimana sebuah pesan atau data diformat dan di transmit antara *client* dan *server*.
3. Dieksekusi ketika sebuah *client* melakukan *request* kepada *server*, serta *server* melakukan *response* kepada *client*.
4. Terdapat beberapa metode HTTP yang paling penting untuk melakukan CRUD (*Create Replicate Update Delete*) untuk diingat adalah

HTTP *Method*

GET

POST

PUT

DELETE

Client Side Code vs Server Side Code

Web applications melakukan eksekusi kode program dengan menjalankan kode pada *client-side* (Web browser pengguna) dan juga *server-side* (Web Server atau komputer penyedia layanan).

1. **PHP** dengan Laravel (Client Side, Server Side)
2. **Python** dengan PyReact (Client Side), Flask (Server Side)
3. **Javascript** dengan ReactJS (Client Side), Express (Server Side), Hapi (Server Side)
4. **Go** dengan Gin (Server Side)
5. **Java**dengan Spring (Server Side)

Then What is Web Security?

Solusi keamanan yang luas yang melindungi pengguna, perangkat, dan jaringan Anda yang lebih luas dari di internet.

Why is it Important?

Pelanggaran data

Unauthorized Access

Data Manipulation

System Compromise

Application Disruption

Kerugian Finansial

Privacy Violation

Malware distribution

What Cause of Web Insecurities?

Input Validation

Unsecure Code Practices

Failed Software Update

Weak Access Control

Less Encryption

Unsecure Network

Bad Logging and Monitoring

Vulnerabilities on Packages/Library

Social Engineering

What are the list attacks on Web?

Cross Site Scripting (XSS)

SQL Injection

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

API Security Issues

XML Injection

Server-Side Request Forgery (SSRF)

Session Hijacking

Brute Force Attack

File Upload Vulnerability

OS Injection

Before Continuing to JWT Injection Let’s Dive in on What Is JWT

JSON Web Tokens (JWT)

JWT (dibaca “jot”)

- Sebuah standar format secara kriptografi yang digunakan sesuai standard RFC 7519
- Digunakan untuk pertukaran data secara aman dari satu pihak ke pihak lainnya.

1. **Ukurannya yang kecil** membuat sebuah token JWT dapat dikirim melalui URL
2. JWT memberikan **informasi dengan enkripsi** yang sudah di *sign* .
3. JWT membawa **informasi digital seperti user ID, nama User** dan lain-lainnya sesuai dengan kebutuhan sistem.
4. *Sign* JWT dilakukan dengan meggunakan algoritma **HMAC** atau dapat dengan menggunakan public/private key seperti **RSA.**

Why Use JWT?

Statelessness

Tidak seperti *session tokens*, yang menggunakan server-side storage to untuk menyimpan *state* dari user, JWT tidak diperlukan .

Scalability

Karena JWTs *stateless*, JWT mudah untuk digunakan dalam layanan-layanan they can be easily scaled across multiple servers or services

Flexibility

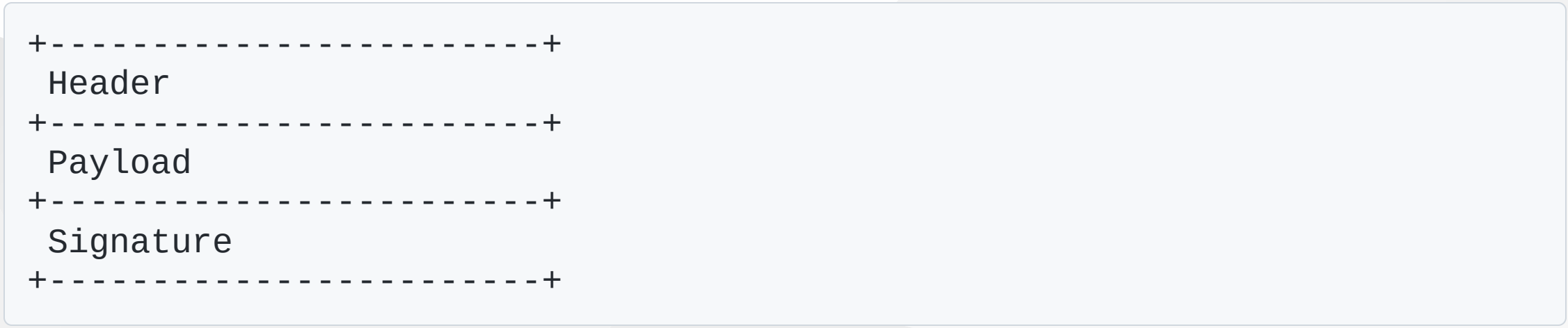
JWTs can be used for various purposes, such as authentication, authorization, or data exchange.

Security

JWTs use digital signatures to ensure that the token has not been tampered with and that the claims contained within it are valid.


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

JWT Structure



Header

- Algoritma Sign
- Jenis Token

```
{
        "alg": "HS256",
        "typ": "JWT"
}
```

Kemudian, JSON ini dikodekan dengan Base64Url untuk membentuk bagian pertama dari JWT.

Payload

- Data
- Klaim Pendaftar
- Klaim Publik
- Klaim Pribadi

Signature

- Decoded in Base64Url
- Dipisah oleh titik
- sebagai Kunci

Contoh sebuah token JWT beserta dengan Komponennya dapat dilihat pada link berikut JWT.io

But is It Secure Enough?

JWT Injection

- Perusakan JWT
- Manipulasi JWT
- Akses yang tidak sah

Penyerangan-penyerangan ini memberikan banyak dampak yang buruk terhadap situs web yang tidak aman seperti malicious code kedalam aplikasi web. Serangan injeksi peretasan web, seperti injeksi JWT, injeksi perintah OS, dan injeksi SQL, dapat menyebabkan berbagai konsekuensi dan risiko keamanan.

Referensi

1. How the web works - Learn web development | MDN
2. An overview of HTTP - HTTP | MDN (mozilla.org)
3. HTTP - Wikipedia
4. Web Application Architecture [Complete Guide & Diagrams] | by SoftKraft | Medium
5. Client-Side vs. Server-Side Code: What's the Difference? (seguetech.com)

6. Client-Server Architecture - Design Your Software Architecture Using Industry-Standard Patterns - OpenClassrooms
7. What Are Injection Attacks and How Can You Prevent Them? (makeuseof.com)
8. Working with JWTs in Burp Suite - PortSwigger
9. JSON Web Tokens (auth0.com)
10. JSON Web Token Introduction - jwt.io

11. JWT attacks | Web Security Academy (portswigger.net)
12. Cross Site Scripting (XSS) | OWASP Foundation
13. What is SQL Injection? Tutorial & Examples | Web Security Academy
14. What is a denial-of-service (DoS) attack? | Cloudflare
15. Denial-of-service attack - Wikipedia

16. What is a distributed denial-of-service (DDoS) attack? | Cloudflare
17. What is a Cross-Site Scripting (XSS) attack: Definition & Examples
18. Web Server and its Types of Attacks - GeeksforGeeks
19. What is a Denial-of-Service (DoS) Attack? | Rapid7
20. How Hackers Take Over Web Sites with SQL Injection and DDoS

21. SQL Injection | OWASP Foundation
22. What is a SQL Injection Attack? - CrowdStrike
23. What Is a Cross-Site Scripting (XSS) Attack? - CrowdStrike
24. What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy
25. What is a denial of service attack (DoS) ? - Palo Alto Networks

26. Denial-of-Service (DoS) Attack: Examples and Common Targets
27. What is a Denial of Service (DoS) Attack? | Webopedia
28. What Is a DDoS Attack? Distributed Denial of Service - Cisco
29. DDoS attacks: Definition, examples, and techniques | CSO Online