Modul 3: Web Application Fundamentals

Memahami bagaimana aplikasi web bekerja dan bagaimana kerentanan biasanya muncul — fondasi teknis sebelum memulai perjalanan bug hunting.

EDY SUSANTO — FOUNDER C-SIX SECURITY

Tujuan Pembelajaran

Setelah menyelesaikan modul ini, peserta akan memiliki pemahaman mendalam tentang cara kerja aplikasi web modern serta mampu mengidentifikasi titik-titik rawan yang sering menjadi celah keamanan.

🎯 Fondasi Teknis

Memahami arsitektur dan alur kerja aplikasi web dari sisi client hingga server.

🔍 Identifikasi Kerentanan

Mengenali bagaimana celah keamanan muncul dalam siklus komunikasi web.

🛠️ Kesiapan Praktik

Menggunakan tools standar industri untuk analisis dan intercept traffic secara langsung.

Agenda Modul

Yang Akan Kita Pelajari

01

Cara Kerja Website Modern

Arsitektur client-server, DNS, dan alur request-response.

02

HTTP & HTTPS

Protokol komunikasi web dan pentingnya enkripsi TLS.

03

Cookies, Session & Authentication

Mekanisme manajemen identitas dan sesi pengguna.

04

Authorization & API

Kontrol akses dan komunikasi berbasis API modern.

05

OWASP Top 10

Pengenalan sepuluh kerentanan web paling kritis di dunia.

Cara Kerja Website Modern

Setiap kali Anda membuka browser dan mengetik sebuah URL, terjadi serangkaian proses kompleks di balik layar: DNS lookup, TCP handshake, HTTP request, pemrosesan server, hingga rendering di browser. Memahami alur ini adalah kunci untuk menemukan celah keamanan.

1

Browser

Pengguna memasukkan URL, browser melakukan DNS lookup.

2

Server

Server menerima request, memproses logika bisnis.

3

Response

Server mengirimkan HTML, CSS, JS kembali ke browser.

HTTP & HTTPS: Bahasa Aplikasi Web

HTTP Methods

- **GET** — Mengambil data dari server
- **POST** — Mengirim data ke server
- **PUT/PATCH** — Memperbarui data
- **DELETE** — Menghapus data

Status Code Penting

- **200** OK — Request berhasil
- **301** Redirect — Dialihkan
- **403** Forbidden — Akses ditolak
- **500** Server Error — Kesalahan server

Mengapa HTTPS Penting?

HTTPS mengenkripsi komunikasi antara browser dan server menggunakan TLS. Tanpa enkripsi, attacker di jaringan yang sama dapat membaca seluruh data yang dikirim — termasuk password dan token sesi.

⚠ Perhatian: Website yang masih menggunakan HTTP murni sangat rentan terhadap serangan Man-in-the-Middle (MitM).

Dalam bug hunting, perbedaan perilaku antara HTTP dan HTTPS sering menjadi titik awal investigasi.

HTTP Headers: Informasi Tersembunyi yang Berharga

HTTP headers membawa metadata penting dalam setiap request dan response. Bagi seorang security researcher, header adalah sumber informasi berharga tentang teknologi, kebijakan keamanan, dan potensi celah.

Request Headers

`User-Agent`, `Authorization`, `Cookie`, `Origin` — dikirim oleh browser ke server.

Response Headers

`Set-Cookie`, `Content-Type`, `X-Frame-Options`, `Strict-Transport-Security` — dikirim server ke browser.

Security Headers

`Content-Security-Policy`, `X-XSS-Protection` — ketidakhadiran header ini adalah temuan bug yang valid.

Cookies & Session Management

Cookies adalah mekanisme utama yang digunakan aplikasi web untuk mengingat pengguna. Karena HTTP bersifat stateless, cookies menjembatani identitas antar request. Pengelolaan cookies yang buruk adalah salah satu sumber kerentanan terbesar.

Session Cookie

Menyimpan session ID yang menghubungkan browser ke sesi server. Hilang saat browser ditutup.

Atribut HttpOnly

Mencegah JavaScript membaca cookie — melindungi dari serangan XSS yang mencuri sesi.

Atribut Secure

Memastikan cookie hanya dikirim melalui koneksi HTTPS, mencegah intercept pada jaringan tidak aman.

Atribut SameSite

Mengontrol pengiriman cookie lintas situs — mitigasi utama terhadap serangan CSRF.

Authentication: Memverifikasi Identitas

Authentication adalah proses membuktikan "siapa Anda" kepada sistem. Ini adalah garis pertahanan pertama — dan sering kali yang paling banyak mengandung bug kritis.

Form-Based Auth

Username dan password dikirim via POST, server memvalidasi dan membuat sesi. Rentan terhadap brute force dan credential stuffing.

Token-Based Auth (JWT)

Server menerbitkan token yang ditandatangani secara kriptografis. Klien menyimpan dan mengirim token di setiap request melalui header Authorization.

Multi-Factor Authentication

Kombinasi sesuatu yang Anda tahu, miliki, dan biometrik. Mengurangi risiko credential compromise secara signifikan.

Authorization: Siapa Boleh Mengakses Apa?

Authentication vs Authorization

Authentication memverifikasi identitas ("Apakah ini benar-benar kamu?"), sedangkan **Authorization** menentukan hak akses ("Apa yang boleh kamu lakukan?"). Keduanya sering dikacaukan, namun kerentanannya sangat berbeda.

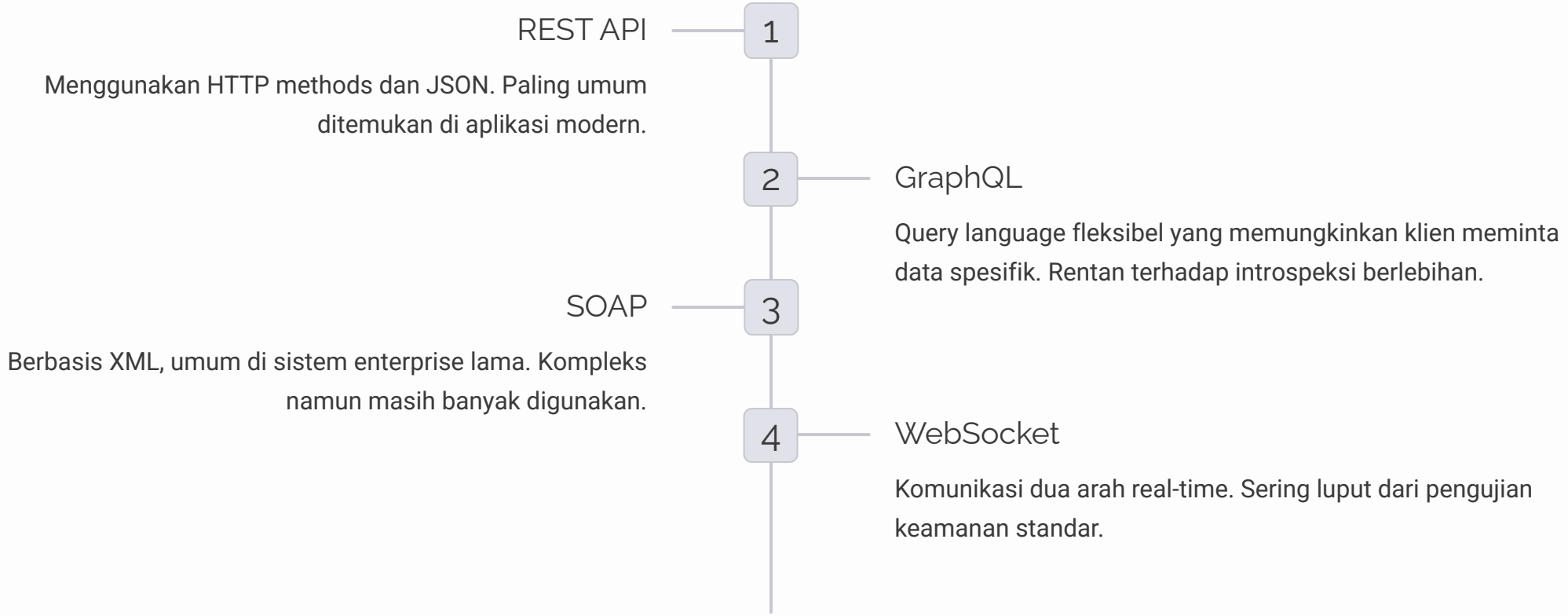
Broken Access Control masuk dalam posisi #1 OWASP Top 10 2021 — menjadikannya kerentanan paling umum ditemukan di aplikasi web nyata.

Jenis Kontrol Akses

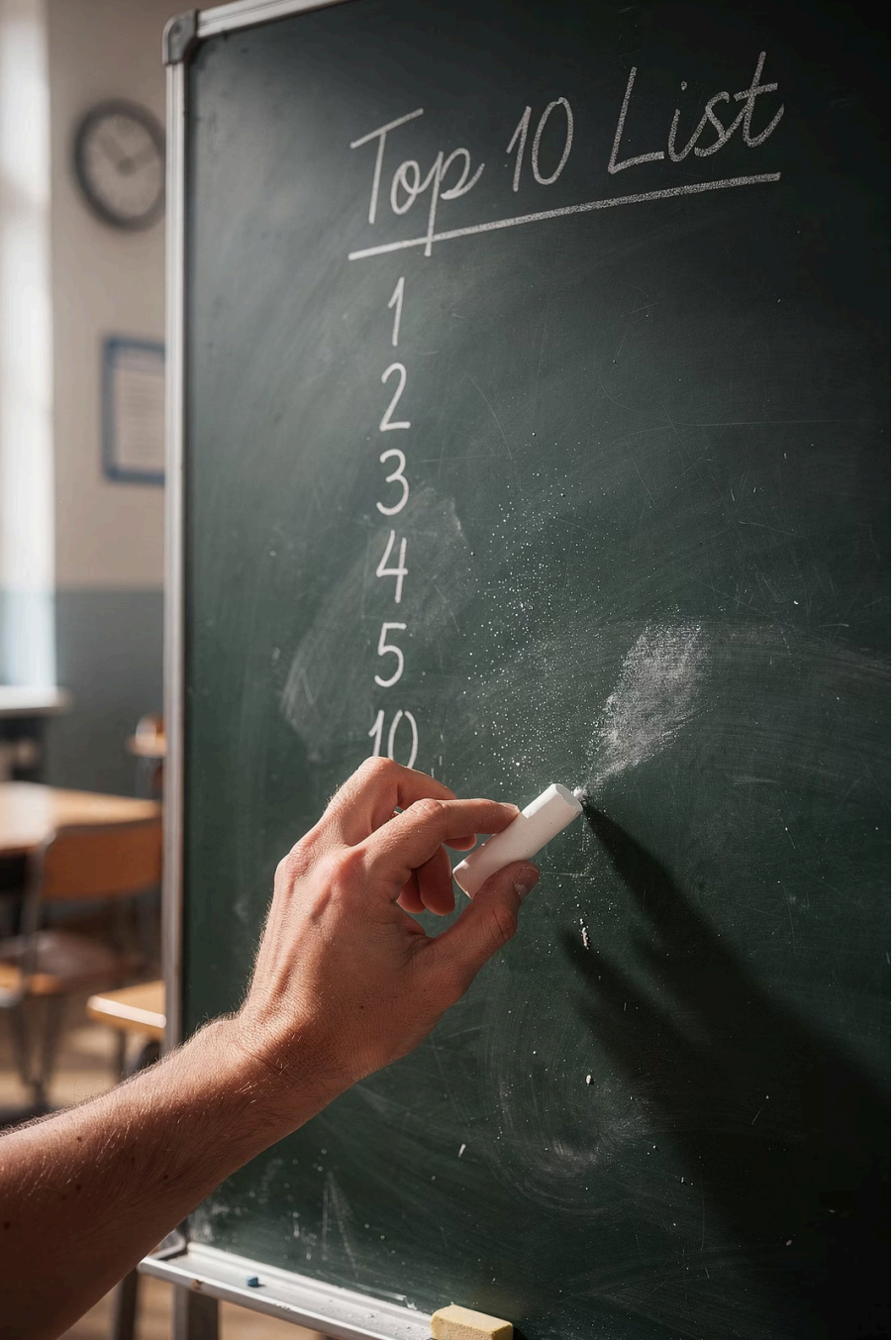
- **RBAC** — Role-Based: akses berdasarkan peran pengguna (admin, user, guest).
- **ABAC** — Attribute-Based: akses berdasarkan atribut konteks dan sumber daya.
- **Horizontal Privilege** — User A mengakses data User B dengan ID yang sama levelnya.
- **Vertical Privilege** — User biasa mengakses fungsi admin.

API Fundamentals: Komunikasi Aplikasi Modern

Hampir semua aplikasi web modern berkomunikasi melalui API. Memahami struktur API adalah keahlian wajib dalam web security testing karena sebagian besar logika bisnis dan data sensitif mengalir melalui endpoint API.



Dalam bug hunting, endpoint API yang tidak terdokumentasi (*shadow API*) sering menjadi tambang emas temuan kerentanan.

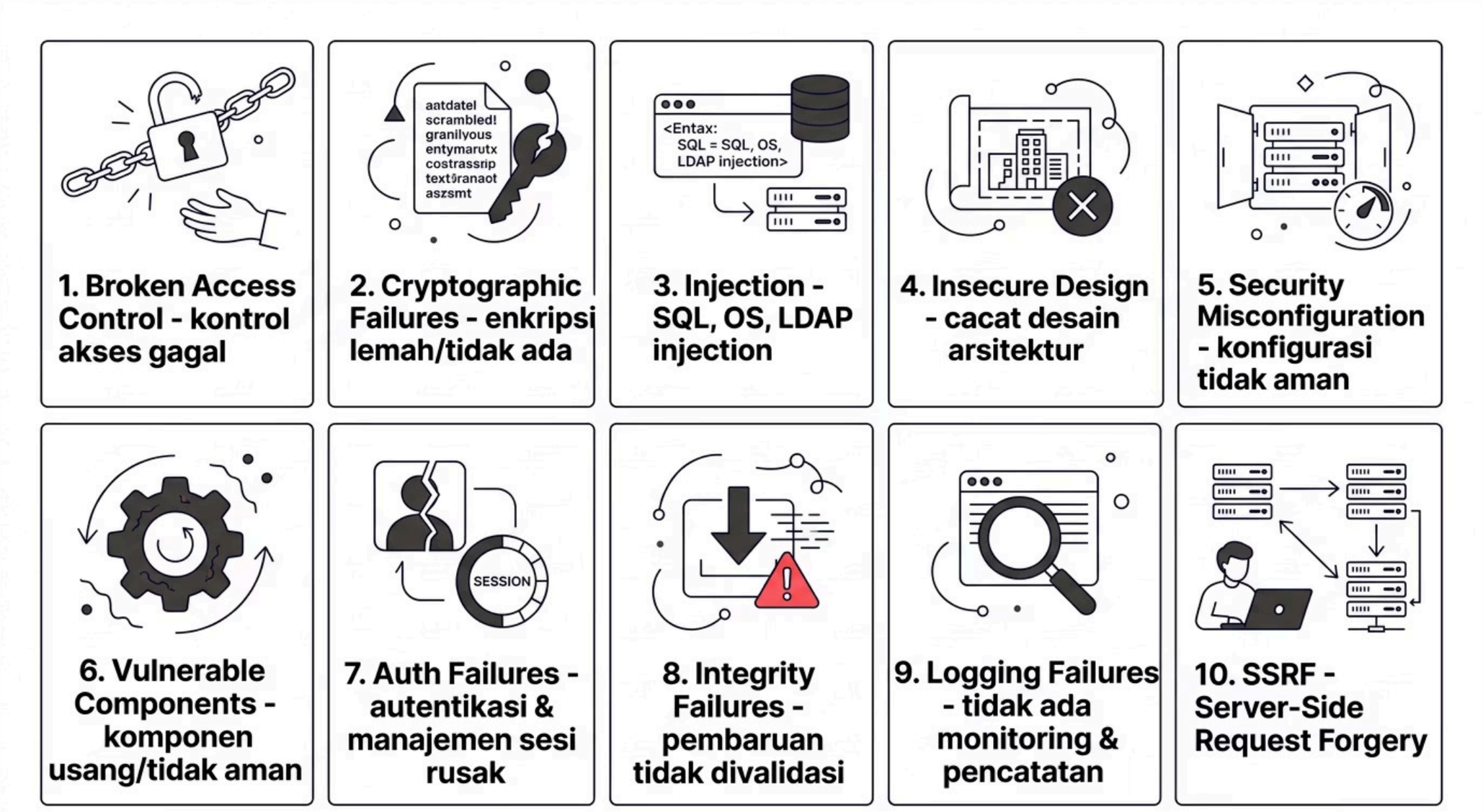


Pengenalan

OWASP Top 10: Kerentanan Paling Kritis

OWASP (Open Web Application Security Project) menerbitkan daftar sepuluh kerentanan web paling berbahaya yang diperbarui secara berkala berdasarkan data industri nyata. Daftar ini menjadi standar referensi global dalam keamanan aplikasi web.

OWASP Top 10 — 2021



Setiap kategori mewakili kelas kerentanan yang ditemukan di ribuan aplikasi nyata. Modul-modul berikutnya akan membahas masing-masing secara mendalam.

Tools: Burp Suite Community Edition

Apa itu Burp Suite?

Burp Suite adalah platform pengujian keamanan aplikasi web terkemuka di industri. Versi Community (gratis) sudah mencakup fitur-fitur esensial yang dibutuhkan untuk analisis mendalam.

Komponen Utama

- **Proxy** — Intercept dan modifikasi HTTP request/response secara real-time.
- **Repeater** — Ulangi dan modifikasi request untuk pengujian manual.
- **Intruder** — Automated fuzzing untuk parameter testing.
- **Decoder** — Encode/decode data (Base64, URL, HTML, dll).

Firefox Developer Tools

Browser built-in tool yang powerful untuk analisis awal sebelum menggunakan Burp Suite.

- **Network Tab** — Melihat semua request/response secara langsung.
- **Storage Inspector** — Inspeksi cookies, localStorage, sessionStorage.
- **Console** — Eksekusi JavaScript dan debug error.
- **Inspector** — Analisis struktur DOM dan hidden fields.

Kombinasi kedua tools ini memberi visibilitas penuh terhadap komunikasi aplikasi web.

Praktik: Analisis Request & Response

Pemahaman teoritis harus diperkuat dengan praktik langsung. Sesi praktik akan memandu peserta melalui dua latihan utama yang menggunakan tools nyata.

1	2
Analisis Request & Response Menggunakan Firefox Developer Tools, peserta mengamati setiap request yang dikirim browser: memeriksa headers, payload body, cookies yang dikirim, dan response yang diterima. Fokus pada pola autentikasi dan pengelolaan sesi.	**Intercept Traffic dengan Proxy** Mengkonfigurasi Burp Suite sebagai proxy, mengaktifkan intercept, dan memodifikasi request sebelum sampai ke server. Peserta akan mencoba mengubah parameter, memanipulasi cookies, dan mengamati respons server terhadap perubahan tersebut.

ⓘ Lab environment telah disiapkan. Pastikan Burp Suite sudah terinstall dan Firefox sudah dikonfigurasi menggunakan proxy 127.0.0.1:8080.

Outcome Modul 3

Siap Memulai Bug Hunting

Dengan memahami fondasi teknis ini, peserta kini memiliki bekal yang diperlukan untuk mulai mengidentifikasi dan mengeksploitasi kerentanan secara sistematis pada modul-modul berikutnya.

✅ Fondasi Dikuasai

HTTP, cookies, auth, authorization, dan API sudah dipahami secara mendalam.

🔧 Tools Siap Pakai

Burp Suite dan Firefox DevTools terkonfigurasi dan siap digunakan untuk pengujian.

🚀 Modul Selanjutnya

Eksploitasi mendalam setiap kategori OWASP Top 10 dengan lab praktis interaktif.

Edy Susanto — Founder C-SIX Security