Modul 3 – Website Footprinting & Security Assessment

Mengevaluasi eksposur keamanan website menggunakan layanan online dan teknik footprinting profesional. Modul ini dirancang untuk membekali peserta dengan kemampuan praktis dalam mengidentifikasi kelemahan konfigurasi umum pada infrastruktur web.

Edy Susanto – Founder C-SIX Security

Gambaran Modul

Tujuan Pembelajaran

Setelah menyelesaikan modul ini, peserta mampu melakukan evaluasi menyeluruh terhadap eksposur keamanan sebuah website menggunakan berbagai layanan online dan metodologi assessment yang terstandar.

🔍 Analisis Teknologi

Mengidentifikasi stack teknologi dan framework yang digunakan sebuah website

🔐 Evaluasi SSL/TLS

Menilai kekuatan konfigurasi enkripsi dan sertifikat digital

🛡️ Review Header

Memeriksa implementasi security headers dan konfigurasi HTTP

📋 Temuan Awal

Mendokumentasikan kelemahan konfigurasi dan risiko eksposur publik

Edy Susanto – Founder C-SIX Security

Tools & Sumber Daya

Toolkit Website Footprinting

Empat layanan online utama yang digunakan dalam modul ini — semuanya gratis dan dapat diakses tanpa instalasi. Kombinasi tool ini memberikan gambaran komprehensif tentang postur keamanan sebuah website.

BuiltWith

Menganalisis teknologi, framework, CMS, dan layanan pihak ketiga yang digunakan sebuah website. Berguna untuk mendeteksi potensi kerentanan berbasis versi software.

SSL Labs Server Test

Memberikan penilaian mendalam terhadap konfigurasi SSL/TLS server, termasuk grading dari A+ hingga F berdasarkan standar industri.

Security Headers

Memeriksa kehadiran dan konfigurasi HTTP security headers yang krusial seperti HSTS, CSP, X-Frame-Options, dan lainnya.

Mozilla Observatory

Platform assessment komprehensif dari Mozilla yang menguji berbagai aspek keamanan website sekaligus dan memberikan rekomendasi perbaikan.

Edy Susanto – Founder C-SIX Security

Materi 1

Web Technology Analysis

Web technology analysis adalah proses mengidentifikasi komponen teknis sebuah website — mulai dari server web, bahasa pemrograman, CMS, hingga CDN dan library JavaScript. Informasi ini sangat berharga dalam security assessment karena setiap komponen berpotensi memiliki kerentanan yang diketahui publik (CVE).

Apa yang Bisa Diidentifikasi?

- CMS (WordPress, Joomla, Drupal)
- Web server (Apache, Nginx, IIS)
- Framework frontend & backend
- Versi software & plugin
- Layanan analitik & tracking

Mengapa Ini Penting?

Versi software yang usang sering kali memiliki kerentanan yang terdokumentasi. Penyerang dapat memanfaatkan database seperti **CVE Details** atau **Exploit-DB** untuk mencari eksploit yang sesuai dengan versi yang ditemukan.

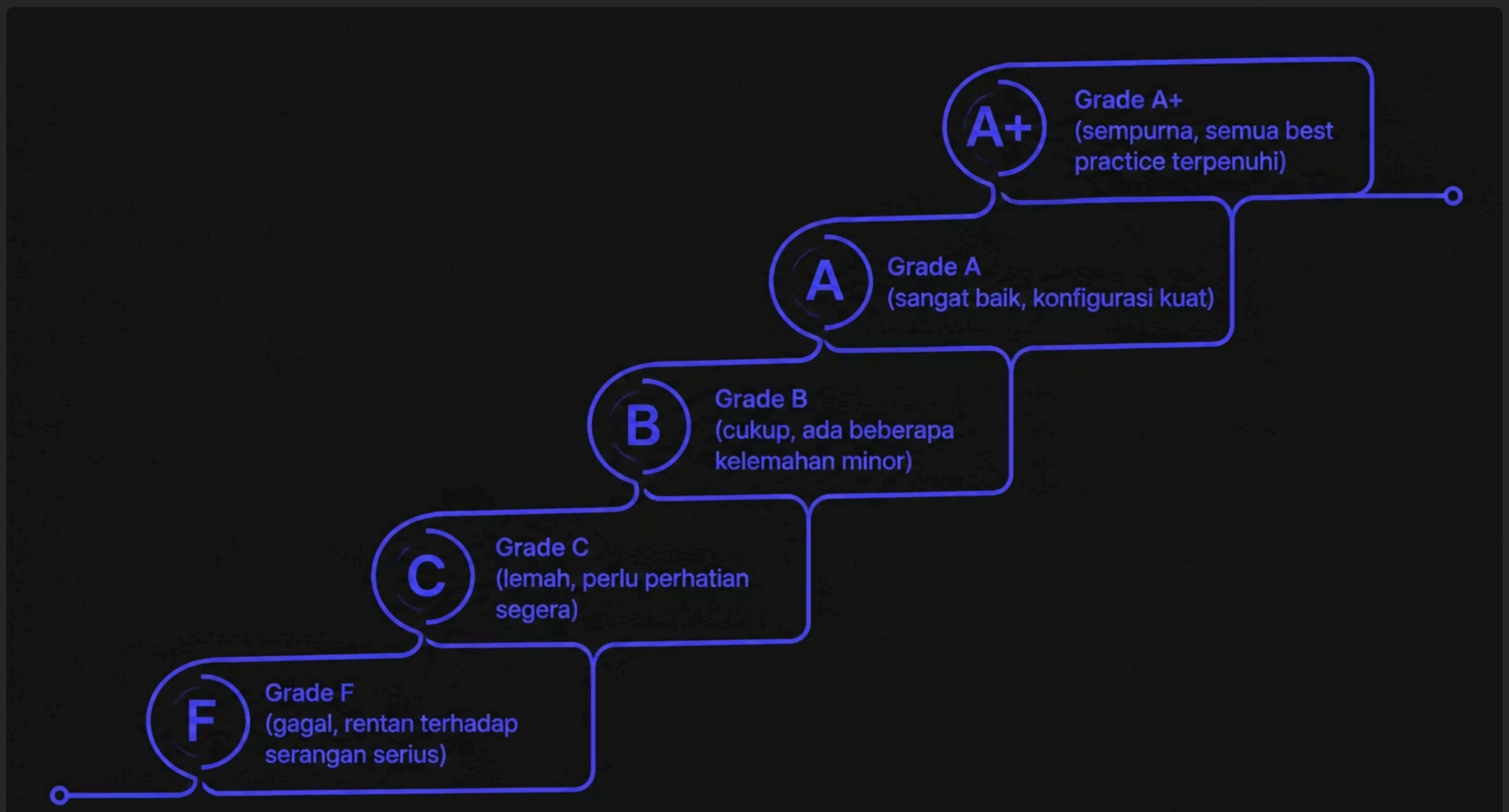
⚠ Versi CMS atau plugin yang tidak diperbarui adalah vektor serangan paling umum pada website publik.

Edy Susanto – Founder C-SIX Security

Materi 2

SSL/TLS Assessment

SSL/TLS adalah tulang punggung keamanan komunikasi web. Namun konfigurasi yang lemah atau usang dapat membuka celah bagi serangan seperti POODLE, BEAST, dan MITM. SSL Labs memberikan grading standar industri yang memudahkan evaluasi.



Aspek yang Dievaluasi

- Validitas dan rantai sertifikat
- Protokol yang didukung (TLS 1.2, 1.3)
- Cipher suite dan kekuatan enkripsi
- Forward Secrecy & HSTS preloading

Red Flags Umum

- Masih mendukung TLS 1.0 / SSL 3.0
- Sertifikat kadaluarsa atau self-signed
- Cipher suite lemah (RC4, DES, 3DES)
- Tidak ada HSTS header

Edy Susanto – Founder C-SIX Security

Materi 3

Security Headers Review

HTTP Security Headers adalah lapisan pertahanan tambahan yang dikonfigurasi di sisi server. Ketiadaan header-header ini tidak selalu menyebabkan kerentanan langsung, namun meningkatkan permukaan serangan secara signifikan dan mencerminkan maturitas keamanan sebuah website.

Content-Security-Policy (CSP)

Mencegah serangan Cross-Site Scripting (XSS) dengan membatasi sumber konten yang boleh dimuat oleh browser. Salah satu header paling kritis dan kompleks untuk dikonfigurasi.

Strict-Transport-Security (HSTS)

Memaksa browser untuk selalu menggunakan HTTPS, mencegah downgrade attack dan cookie hijacking melalui koneksi HTTP yang tidak terenkripsi.

X-Frame-Options

Melindungi dari serangan Clickjacking dengan mencegah website dimuat dalam iframe dari domain lain tanpa izin eksplisit.

X-Content-Type-Options

Mencegah browser melakukan MIME sniffing yang dapat dieksploitasi untuk menjalankan konten berbahaya dengan tipe MIME yang salah.

Edy Susanto – Founder C-SIX Security

Materi 4 & 5

Configuration Review & Public Exposure Analysis

Configuration Review

Memeriksa konfigurasi server yang dapat mengekspos informasi sensitif atau membuka celah keamanan:

- Directory listing yang aktif
- File sensitif yang dapat diakses (`robots.txt`, `.env`, `backup.zip`)
- Error messages yang verbose
- HTTP methods berbahaya (PUT, DELETE, TRACE)
- Default credentials tidak diubah

Public Exposure Analysis

Menganalisis informasi yang terekspos secara publik melalui berbagai sumber:

- WHOIS & DNS records
- Subdomain enumeration
- Shodan & Censys fingerprinting
- Google dorking untuk file sensitif
- Certificate Transparency logs

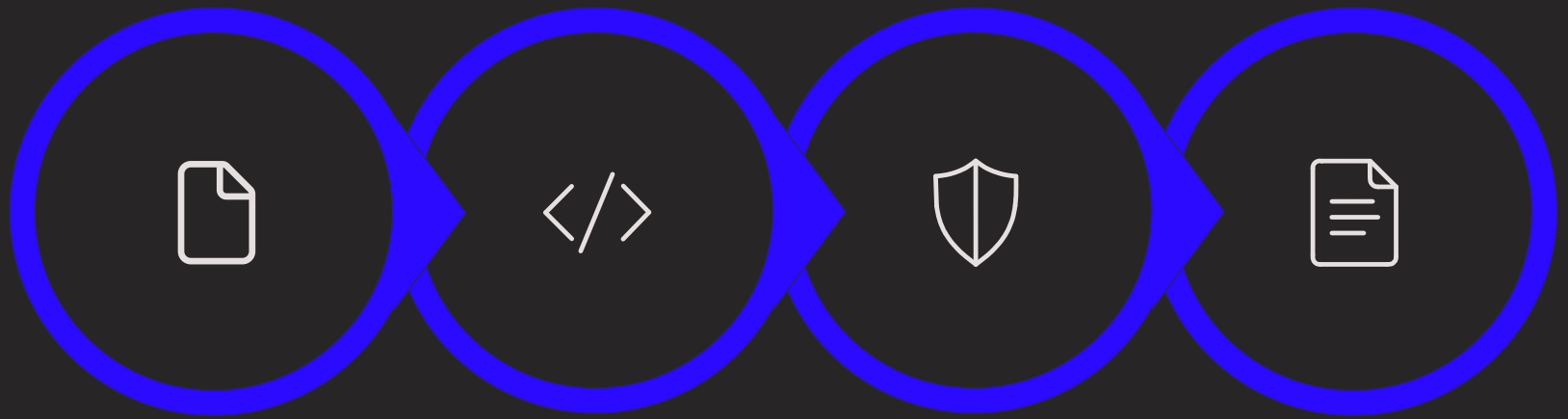
ⓘ Kombinasi analisis konfigurasi dan eksposur publik memberikan gambaran lengkap tentang attack surface sebuah website.

Edy Susanto – Founder C-SIX Security

Sesi Praktik

Audit Keamanan Website Lab

Peserta akan melakukan security assessment terhadap website lab yang telah disiapkan. Gunakan keempat tool yang telah dipelajari secara berurutan untuk membangun gambaran komprehensif tentang postur keamanan target.



Reconnaissance

SSL Assessment

Header Analysis

Dokumentasi

Setiap langkah menghasilkan temuan yang saling melengkapi. Catat semua hasil — termasuk konfigurasi yang sudah baik — karena laporan keamanan yang baik mencakup kondisi positif maupun area yang perlu diperbaiki.

Edy Susanto – Founder C-SIX Security

Output Praktik

Membuat Daftar Temuan Awal

Dokumentasi yang terstruktur adalah keterampilan krusial dalam security assessment profesional. Setiap temuan harus dicatat dengan format yang konsisten agar dapat dipahami oleh stakeholder teknis maupun non-teknis.

1

Identitas Temuan

Nama temuan, kategori (SSL/Header/Config/Exposure), URL atau komponen yang terpengaruh, dan tanggal ditemukan.

2

Tingkat Risiko

Klasifikasikan setiap temuan: **Kritis**, **Tinggi**, **Sedang**, atau **Rendah** berdasarkan dampak potensial dan kemudahan eksploitasi.

3

Deskripsi & Bukti

Jelaskan temuan secara teknis, sertakan screenshot atau output tool sebagai bukti, dan jelaskan dampak jika dibiarkan.

4

Rekomendasi

Berikan langkah perbaikan yang konkret dan dapat ditindaklanjuti, termasuk referensi ke best practice atau dokumentasi resmi.

Edy Susanto – Founder C-SIX Security

Outcome Modul 3

Apa yang Telah Anda Kuasai?

Setelah menyelesaikan Modul 3, peserta memiliki kemampuan praktis untuk melakukan evaluasi eksposur website secara mandiri menggunakan tools industri standar.

Identifikasi Teknologi

Mampu memetakan stack teknologi website dan menghubungkannya dengan potensi kerentanan yang diketahui

Evaluasi SSL/TLS

Mampu menilai kualitas konfigurasi enkripsi dan mengidentifikasi protokol atau cipher yang usang

Analisis Header

Mampu mengidentifikasi security headers yang hilang dan memahami dampak keamanan dari setiap header

Dokumentasi Profesional

Mampu menyusun laporan temuan awal yang terstruktur, lengkap dengan tingkat risiko dan rekomendasi perbaikan

Keterampilan ini adalah fondasi dari security assessment profesional. Lanjutkan ke Modul 4 untuk teknik yang lebih mendalam!

Edy Susanto – Founder C-SIX Security