

INSTITUT TEKNOLOGI DEL**Mata Kuliah Keamanan Jaringan****MODUL PRAKTIKUM 01****External Reconnaissance dan Pemahaman Attack Surface**

Durasi : 2 jam
Target : <https://pentest.tobasmartfarming.com>
Mode : External Web Application Security Assessment

Catatan penting. Praktikum ini dilakukan pada lingkungan yang memang disiapkan untuk pembelajaran keamanan siber. Seluruh aktivitas mahasiswa harus tetap berada pada ruang lingkup yang ditetapkan di modul ini. Mahasiswa tidak diperbolehkan menguji sistem, domain, alamat IP, atau layanan lain di luar target resmi.

Daftar Isi

1 Tujuan Praktikum	2
2 Konfigurasi Lingkungan Praktikum	2
3 Rules of Engagement	3
3.1 Authorized Scope	3
3.2 Aktivitas yang Dilarang	3
4 Petunjuk Pengerjaan	3
4.1 Tahap 1 - Pahami Scope dan Target	3
4.2 Tahap 2 - Identifikasi Target melalui DNS	4
4.3 Tahap 3 - Observasi Konektivitas	4
4.4 Tahap 4 - Analisis Respons HTTP/HTTPS	4
4.5 Tahap 5 - Analisis Redirect	5
4.6 Tahap 6 - Identifikasi Teknologi Aplikasi	5
4.7 Tahap 7 - Analisis Cookie	5
4.8 Tahap 8 - Security Header Assessment	6
4.9 Tahap 9 - Identifikasi Attack Surface Awal	6
4.10 Tahap 10 - Bedakan Observation dan Vulnerability	6
5 Flag yang Harus Ditemukan	7

6	Evidence yang Wajib Dikumpulkan	7
7	Pertanyaan Analisis	7
8	Deliverable	8
9	Rubrik Penilaian	8
10	Kriteria Keberhasilan Modul	8

1 Tujuan Praktikum

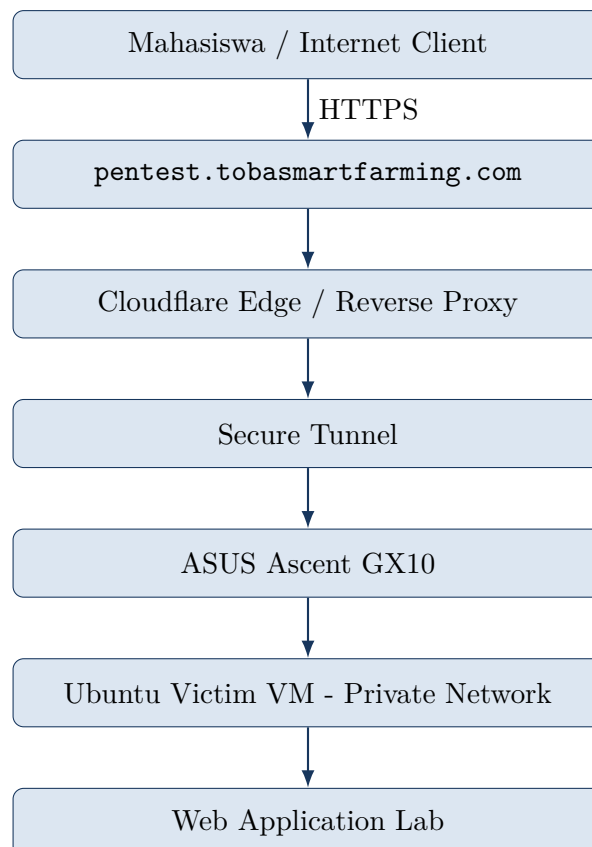
Pada modul ini mahasiswa berperan sebagai *junior penetration tester* yang melakukan tahap awal security assessment terhadap sebuah aplikasi web yang dapat diakses melalui Internet. Fokus utama bukan eksploitasi kerentanan, melainkan memahami target dari perspektif pihak luar melalui reconnaissance, observasi komunikasi HTTP/HTTPS, identifikasi teknologi, analisis mekanisme sesi, serta pemetaan awal attack surface.

Setelah menyelesaikan modul ini, mahasiswa diharapkan mampu:

1. memahami arsitektur publikasi aplikasi melalui reverse proxy dan secure tunnel;
2. melakukan reconnaissance terhadap target yang berada di Internet;
3. membedakan informasi yang berasal dari reverse proxy dengan informasi yang berasal dari aplikasi backend;
4. menganalisis response HTTP/HTTPS, redirect, cookie, dan security header;
5. mengidentifikasi teknologi aplikasi tanpa melakukan eksploitasi;
6. menyusun attack surface awal berdasarkan evidence yang ditemukan;
7. membedakan observation, weakness, dan vulnerability;
8. mendokumentasikan hasil pengujian secara sistematis dan dapat direproduksi.

2 Konfigurasi Lingkungan Praktikum

Aplikasi target tidak berada langsung di Internet. Infrastruktur laboratorium dibangun dengan arsitektur berikut.



Mahasiswa tidak memiliki akses langsung ke jaringan privat server. Dari perspektif mahasiswa, satu-satunya target sah adalah:

`https://pentest.tobasmartfarming.com`

Konfigurasi ini mensimulasikan kondisi nyata ketika sebuah aplikasi internal dipublikasikan ke Internet melalui reverse proxy atau secure tunnel. Karena itu, alamat IP yang terlihat dari Internet belum tentu merupakan alamat IP server aplikasi sebenarnya.

3 Rules of Engagement

3.1 Authorized Scope

Target resmi: `https://pentest.tobasmartfarming.com`

Pada Modul 01 mahasiswa hanya diperbolehkan melakukan aktivitas berikut:

- pengumpulan informasi target;
- observasi konfigurasi DNS;
- pemeriksaan keterjangkauan target;
- analisis HTTP/HTTPS;
- identifikasi teknologi;
- observasi cookie dan session mechanism;
- pemeriksaan security header;
- pemetaan awal aplikasi dan attack surface.

3.2 Aktivitas yang Dilarang

Mahasiswa tidak diperbolehkan melakukan denial of service, flooding, brute-force, credential attack, pemindaian sistem lain, pencarian atau bypass origin server, pengujian domain/subdomain lain, atau aktivitas lain yang dapat mengganggu layanan.

Modul 01 secara eksplisit **belum mencakup eksploitasi vulnerability**. Jika mahasiswa menemukan indikasi kelemahan, dokumentasikan sebagai observation atau potential finding tanpa melakukan eksploitasi lanjutan.

4 Petunjuk Pengerjaan

4.1 Tahap 1 - Pahami Scope dan Target

Sebelum melakukan aktivitas teknis, tuliskan kembali target yang diotorisasi, tujuan praktikum, dan batasan pengujian pada laporan. Pastikan seluruh evidence yang dikumpulkan merujuk hanya pada target resmi.

Output yang harus dihasilkan:

- target yang diotorisasi;
- jenis pengujian yang dilakukan;
- daftar singkat aktivitas yang diperbolehkan dan dilarang.

4.2 Tahap 2 - Identifikasi Target melalui DNS

Lakukan pemeriksaan terhadap nama domain target. Temukan dan dokumentasikan setidaknya:

- alamat IP yang diperoleh dari resolusi nama;
- jenis record DNS yang relevan;
- indikasi penyedia infrastruktur yang berada di depan target;
- kemungkinan apakah alamat IP tersebut merupakan server aplikasi sebenarnya atau server perantara.

Pertanyaan analisis:

1. Alamat IP apa yang diperoleh?
2. Apakah alamat tersebut dapat dipastikan sebagai IP server aplikasi?
3. Apa indikasi bahwa target menggunakan reverse proxy atau CDN?
4. Mengapa alamat IP privat server tidak terlihat dari Internet?

4.3 Tahap 3 - Observasi Konektivitas

Lakukan pemeriksaan dasar terhadap keterjangkauan hostname target. Catat apakah hostname dapat di-resolve, apakah terdapat respons jaringan, alamat IP yang terlihat, dan apakah hasil tersebut konsisten dengan tahap sebelumnya.

Pertanyaan analisis:

Apakah keberhasilan memperoleh respons jaringan membuktikan bahwa mahasiswa telah mencapai server aplikasi sebenarnya? Jelaskan alasan teknisnya.

4.4 Tahap 4 - Analisis Respons HTTP/HTTPS

Lakukan permintaan HTTP/HTTPS terhadap halaman utama target. Identifikasi dan dokumentasikan:

- HTTP status code;
- protocol version;
- redirect dan target redirect;
- response headers;
- cookie yang diberikan;
- informasi teknologi yang terlihat.

Perhatikan informasi seperti **Location**, **Server**, **Set-Cookie**, **Content-Type**, **X-Powered-By**, dan **Cache-Control**. Jangan hanya menyalin output; setiap informasi harus diberi interpretasi.

4.5 Tahap 5 - Analisis Redirect

Perhatikan apakah akses ke halaman utama diarahkan ke halaman lain. Identifikasi status code redirect, halaman tujuan, serta kemungkinan fungsi halaman tersebut.

Pertanyaan analisis:

1. Apa arti HTTP 302 Found?
2. Mengapa sebuah aplikasi dapat mengarahkan pengguna ke halaman lain?
3. Apakah redirect itu sendiri merupakan vulnerability?

4.6 Tahap 6 - Identifikasi Teknologi Aplikasi

Gunakan metode fingerprinting yang sesuai untuk mengetahui teknologi yang mungkin digunakan aplikasi. Cari informasi seperti:

- server-side language;
- reverse proxy atau web server yang terlihat dari sisi Internet;
- jenis aplikasi atau pola aplikasi;
- cookie framework/session;
- teknologi lain yang dapat diidentifikasi secara wajar.

Mahasiswa harus membedakan antara informasi yang berasal dari reverse proxy dengan informasi yang berasal dari backend application.

Pertanyaan analisis: Mengapa identifikasi teknologi penting bagi penetration tester?

4.7 Tahap 7 - Analisis Cookie

Identifikasi seluruh cookie yang diberikan oleh aplikasi. Untuk setiap cookie, analisis atribut keamanan yang relevan seperti **HttpOnly**, **Secure**, **SameSite**, **Path**, **Domain**, dan masa berlaku.

Cookie	Attribute	Nilai/Status	Analisis Keamanan
	HttpOnly		
	Secure		
	SameSite		

Pertanyaan analisis:

1. Apa fungsi session cookie?
2. Apa fungsi **HttpOnly**?
3. Apa fungsi **Secure**?
4. Apa fungsi **SameSite**?
5. Apakah sebuah cookie tanpa atribut tertentu selalu berarti aplikasi langsung dapat dieksploitasi?

4.8 Tahap 8 - Security Header Assessment

Periksa security header yang dikirim aplikasi. Perhatikan keberadaan atau ketidakberadaan header berikut:

- Content-Security-Policy;
- Strict-Transport-Security;
- X-Content-Type-Options;
- X-Frame-Options;
- Referrer-Policy;
- Permissions-Policy.

Security Header	Ada/Tidak	Fungsi	Risiko Potensial
Content-Security-Policy			
Strict-Transport-Security			
X-Content-Type-Options			
X-Frame-Options			
Referrer-Policy			
Permissions-Policy			

Jangan langsung mengklasifikasikan header yang tidak tersedia sebagai vulnerability kritis. Mahasiswa harus mempertimbangkan konteks dan fungsi kontrol tersebut.

4.9 Tahap 9 - Identifikasi Attack Surface Awal

Berdasarkan seluruh informasi yang ditemukan, buat gambaran attack surface awal. Gunakan evidence yang benar-benar ditemukan selama praktikum.

Contoh struktur konseptual:

```

Target Web Application
|
+-- Public hostname
+-- Reverse proxy / CDN
+-- HTTPS
+-- Authentication endpoint
+-- Session mechanism
+-- Server-side technology
+-- Application endpoints

```

4.10 Tahap 10 - Bedakan Observation dan Vulnerability

Kelompokkan temuan ke dalam kategori berikut:

Observation: fakta teknis yang ditemukan, tetapi belum tentu merupakan kelemahan. Contoh: aplikasi menggunakan teknologi server-side tertentu atau berada di belakang reverse proxy.

Potential Security Finding: kondisi yang mungkin memperbesar attack surface atau memberikan informasi yang tidak perlu kepada pihak luar.

Mahasiswa harus menjelaskan mengapa suatu observation dapat atau tidak dapat dianggap sebagai security finding.

5 Flag yang Harus Ditemukan

Setiap flag wajib disertai evidence. Menuliskan jawaban tanpa evidence tidak memperoleh nilai penuh.

Flag	Informasi yang Harus Ditemukan
M01-F1	Identitas reverse proxy/CDN yang digunakan target
M01-F2	Halaman yang menjadi tujuan redirect dari halaman utama
M01-F3	Server-side technology yang terlihat dari sisi Internet
M01-F4	Nama cookie yang digunakan untuk session management

6 Evidence yang Wajib Dikumpulkan

Untuk setiap tahap, mahasiswa harus menyimpan hasil observasi, tangkapan layar atau output relevan, waktu pengujian, target yang diuji, serta interpretasi hasil.

Gunakan format berikut:

Evidence ID : E-01
Target : <https://pentest.tobasmartfarming.com>
Activity : DNS reconnaissance
Observation : ...
Interpretation : ...

Evidence harus cukup jelas sehingga dosen dapat memahami bagaimana kesimpulan diperoleh.

7 Pertanyaan Analisis

Jawab pertanyaan berikut pada laporan:

1. Jelaskan arsitektur jaringan praktikum dari mahasiswa sampai ke aplikasi target.
2. Mengapa IP yang terlihat dari Internet belum tentu merupakan IP origin server?
3. Apa fungsi reverse proxy dalam arsitektur ini?
4. Apa perbedaan DNS reconnaissance dan HTTP reconnaissance?
5. Apa arti HTTP 302 Found?
6. Apa manfaat fingerprinting bagi penetration tester?
7. Mengapa version disclosure dapat berguna bagi attacker?
8. Apa fungsi session cookie?
9. Apa perbedaan antara HttpOnly, Secure, dan SameSite?

10. Mengapa tidak adanya security header tidak selalu berarti vulnerability dengan severity tinggi?
11. Apa perbedaan observation, weakness, dan vulnerability?
12. Mengapa penetration tester harus mematuhi scope?

8 Deliverable

Mahasiswa mengumpulkan satu laporan PDF maksimal 4 halaman di luar halaman sampul. Struktur minimal laporan:

1. Scope dan Rules of Engagement;
2. Arsitektur Target;
3. DNS dan Network Observation;
4. HTTP/HTTPS Analysis;
5. Technology Fingerprinting;
6. Cookie Analysis;
7. Security Header Analysis;
8. Initial Attack Surface;
9. Flag Summary;
10. Kesimpulan.

Nama file disarankan:

NIM_Nama_Modul01.pdf

9 Rubrik Penilaian

Komponen	Bobot
Pemahaman scope dan arsitektur laboratorium	15
DNS dan network reconnaissance	15
Analisis HTTP/HTTPS dan redirect	20
Technology fingerprinting	15
Cookie dan session analysis	15
Security header assessment	10
Evidence dan kualitas interpretasi	10
Total	100

10 Kriteria Keberhasilan Modul

Modul 01 dianggap berhasil apabila mahasiswa mampu menjelaskan:

- apa target yang sedang diamati;

- bagaimana target dipublikasikan ke Internet;
- informasi apa yang dapat diperoleh tanpa autentikasi;
- perbedaan informasi reverse proxy dan backend application;
- mekanisme dasar HTTP, redirect, cookie, dan security header;
- attack surface awal berdasarkan evidence yang ditemukan.

Mahasiswa belum dituntut menemukan atau mengeksploitasi SQL Injection, Cross-Site Scripting, Command Injection, atau vulnerability lain pada modul ini. Fokus Modul 01 adalah membangun metodologi reconnaissance yang tertib, terukur, dan sesuai scope.

Gunakan lingkungan praktikum hanya untuk tujuan pembelajaran dan sesuai dengan Rules of Engagement yang telah ditetapkan.