Burp Suite Starter

Bab 1 – What's Burp Suite?

Terjemahan bebas Seitz, J. (2013). Instant Burp Suite starter. Packt Publishing: materi halaman buku halaman 3-12.

Catatan penting: Dokumen ini bukan terjemahan kata per kata. Isinya sudah disederhanakan agar lebih mudah dipahami pemula, tetapi urutan gagasan dan inti materi tetap mengikuti sumber aslinya. Istilah teknis seperti Proxy, Intruder, Repeater, dan Scanner tetap dipertahankan supaya mudah dicocokkan saat praktik.

1. Gambaran umum: apa itu Burp Suite?

Burp Suite adalah aplikasi untuk membantu menguji keamanan website atau aplikasi web. Cara paling mudah membayangkannya adalah seperti *pos pemeriksaan* di antara browser dan website. Semua permintaan dari browser lewat dulu ke Burp, sehingga kita bisa melihat, menahan, mengubah, lalu meneruskannya lagi.

Dengan alat ini, kita bisa:

- melihat isi request dan response HTTP/HTTPS
- mengecek parameter, cookie, header, dan halaman yang diakses
- mencoba mengubah data sebelum dikirim ke server
- mengulang request untuk pengujian manual
- membantu mencari potensi celah keamanan

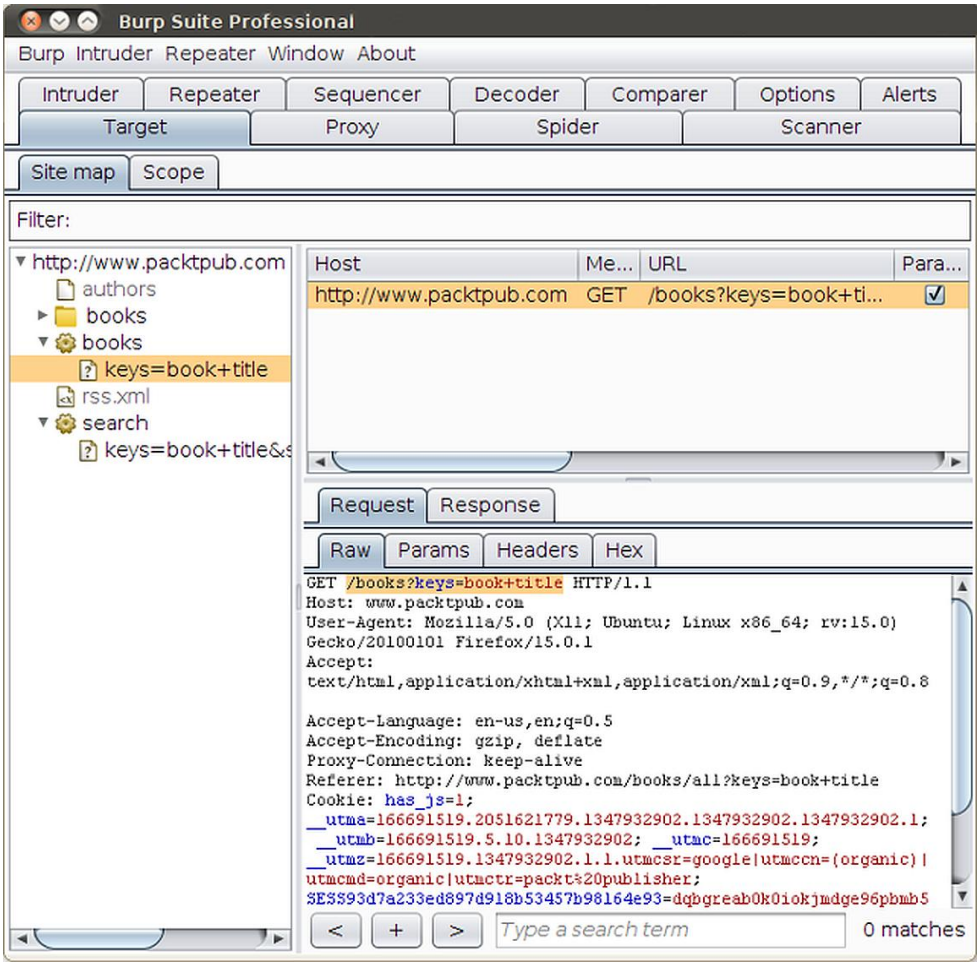
Burp Suite tersedia dalam dua edisi: Free dan Professional. Versi Professional punya fitur pemindaian otomatis yang lebih lengkap, tetapi versi Free sudah cukup untuk belajar dasar-dasarnya.

Menu utama yang paling sering dipakai

Menu	Fungsi singkat
Target	Mencatat halaman, folder, parameter, dan struktur target yang sedang diuji.

Proxy	Inti dari Burp. Dipakai untuk menyadap, menahan, dan mengubah lalu lintas web.
Spider	Perayap otomatis untuk menemukan halaman atau parameter baru.
Scanner	Pemindai celah keamanan otomatis. Umumnya tersedia di versi Professional.
Intruder	Mengirim banyak variasi request untuk pengujian otomatis atau semi-otomatis.
Repeater	Mengulang request manual berkali-kali sambil mengubah isinya.
Sequencer	Menganalisis apakah token atau cookie cukup acak atau mudah ditebak.
Decoder	Mengubah data ke format lain atau membalikkan hasil encoding.
Comparer	Membandingkan dua request, response, atau site map untuk melihat perbedaannya.

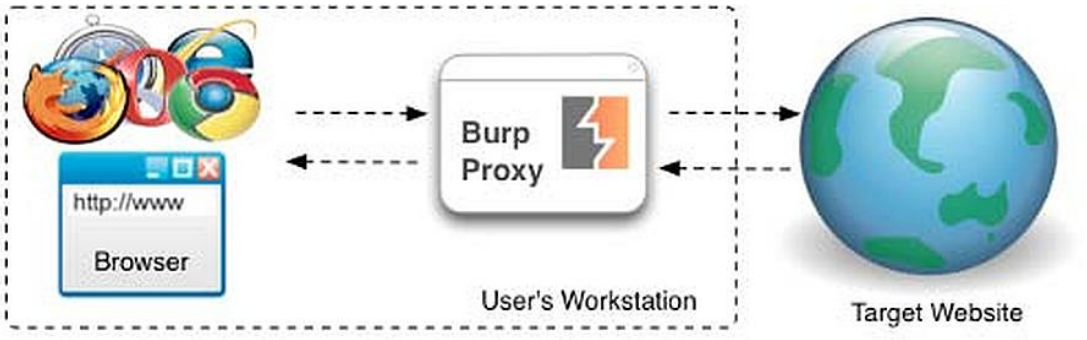
Seitz, J. (2013). *Instant Burp Suite starter*. Packt Publishing.2



Gambar 1. Tampilan utama Burp Suite.

Cara kerja sederhananya

Saat browser diarahkan ke Burp Proxy, permintaan tidak langsung menuju website. Burp menerima dulu traffic tersebut, lalu kita bisa memilih apakah request mau diteruskan, dibuang, atau diedit. Karena itu, Burp sangat berguna untuk belajar memahami cara kerja aplikasi web.



Gambar 2. Burp Proxy berada di tengah antara browser dan website target.

2. Instalasi dan persiapan awal

Yang perlu disiapkan

- Ruang penyimpanan kosong minimal sekitar 100 MB.
- RAM minimal 2 GB; jika aplikasi yang diuji besar, kebutuhan bisa lebih tinggi.
- Sistem operasi Windows, Linux, atau Mac OS X.
- Java Runtime Environment (minimal versi 1.6 pada sumber asli).
- Satu browser modern; penulis buku menyarankan Mozilla Firefox.

Langkah 1 - Unduh Burp Suite

Burp Suite diunduh dalam bentuk paket terkompresi. Setelah file dibuka, biasanya kita akan mendapatkan file utama berbentuk JAR. Versi gratis cocok untuk mulai belajar, lalu nanti bisa naik ke versi Professional kalau memang butuh fitur otomatis yang lebih lengkap.

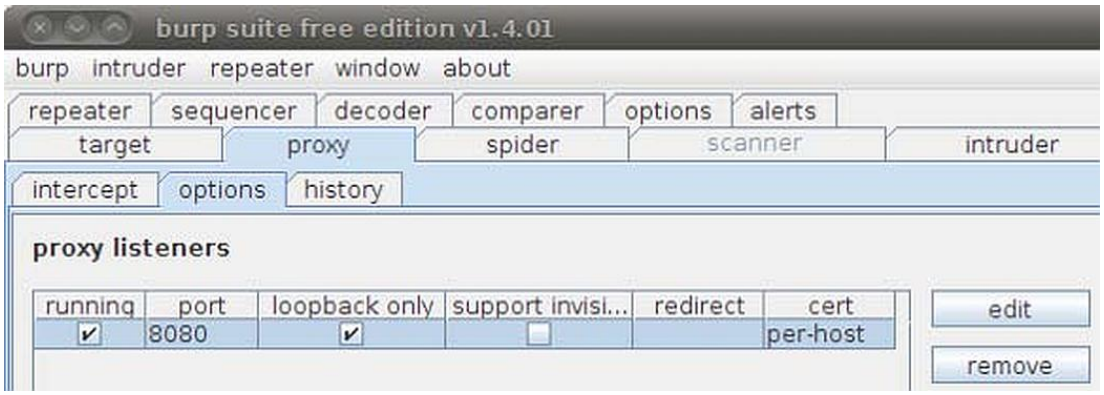
Langkah 2 - Jalankan Burp Suite

Di Windows, Linux, atau Mac, prinsipnya sama: buka terminal/command prompt, pindah ke folder tempat file JAR disimpan, lalu jalankan Burp memakai Java. Contoh yang dipakai di buku adalah perintah *java -Xmx2g -jar burpsuite_v1.4.01.jar*. Opsi *-Xmx2g* berarti Java boleh memakai memori sampai 2 GB.

> **Tip:** Pada beberapa komputer, file JAR memang bisa dibuka dengan klik ganda. Namun cara itu biasanya tidak memberi kendali atas batas memori yang dipakai. Untuk pengujian yang lebih stabil, menjalankannya dari terminal sering lebih aman.

Langkah 3 - Pastikan Burp Proxy aktif

Secara bawaan, Burp Proxy mendengarkan traffic di port 8080. Buka tab *Proxy* > *Options* dan cek apakah listener dalam keadaan berjalan. Kalau ada aplikasi lain yang memakai port itu, Burp bisa gagal menerima koneksi. Solusinya: ganti port, lalu aktifkan ulang listener.



Gambar 3. Contoh listener Burp Proxy pada port 8080.

Opsi penting yang perlu dipahami:

- Running: menandakan listener sedang aktif atau tidak.
- Loopback only: kalau aktif, hanya komputer sendiri yang boleh terhubung ke Burp.
- Port: nomor pintu tempat browser mengirim traffic ke Burp.
- Invisible proxying: dipakai pada situasi khusus, misalnya klien non-standar atau aplikasi mobile tertentu.

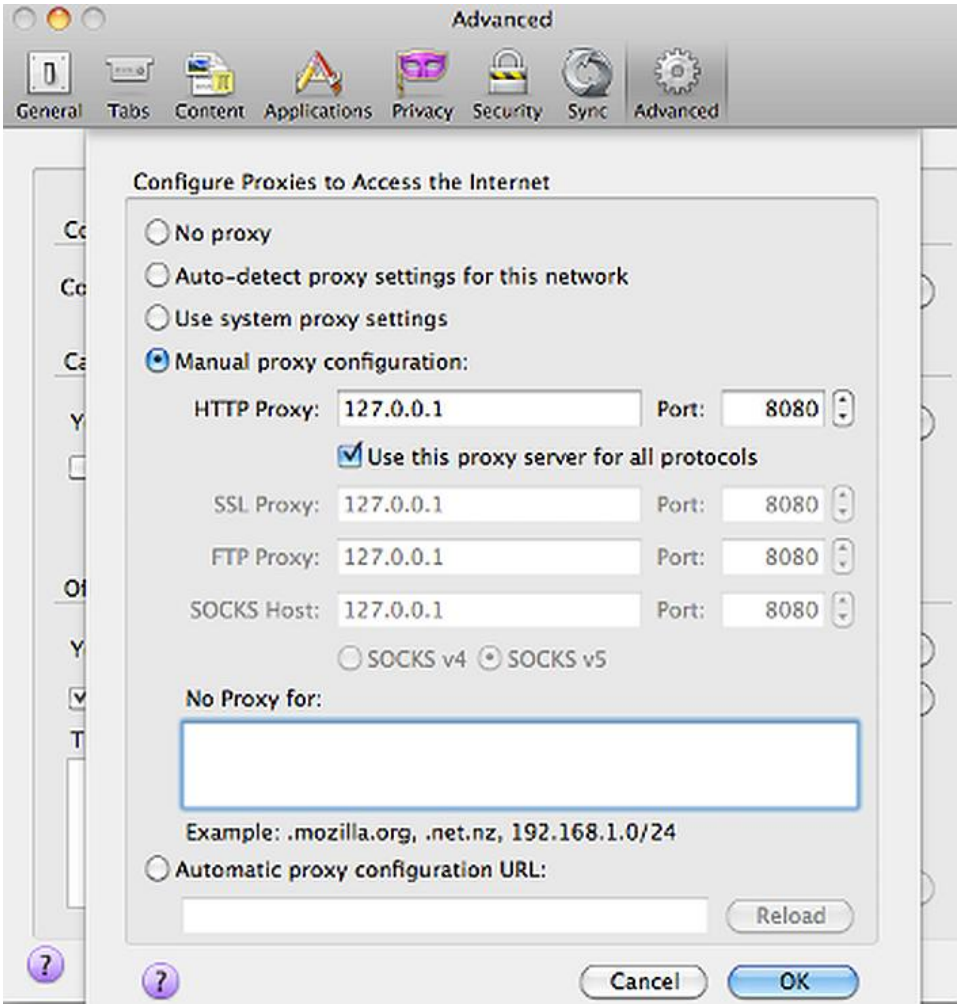
> **Peringatan:** Membuka listener Burp agar bisa diakses komputer lain sebaiknya dihindari, kecuali benar-benar paham risikonya. Semakin terbuka listener, semakin besar potensi penyalahgunaan.

Langkah 4 - Atur browser agar lewat Burp

Setelah Burp aktif, browser juga harus diarahkan ke Burp. Kalau masih memakai pengaturan bawaan, biasanya host proxy diisi *127.0.0.1* dan port *8080* untuk HTTP maupun HTTPS.

Contoh pengaturan di Mozilla Firefox

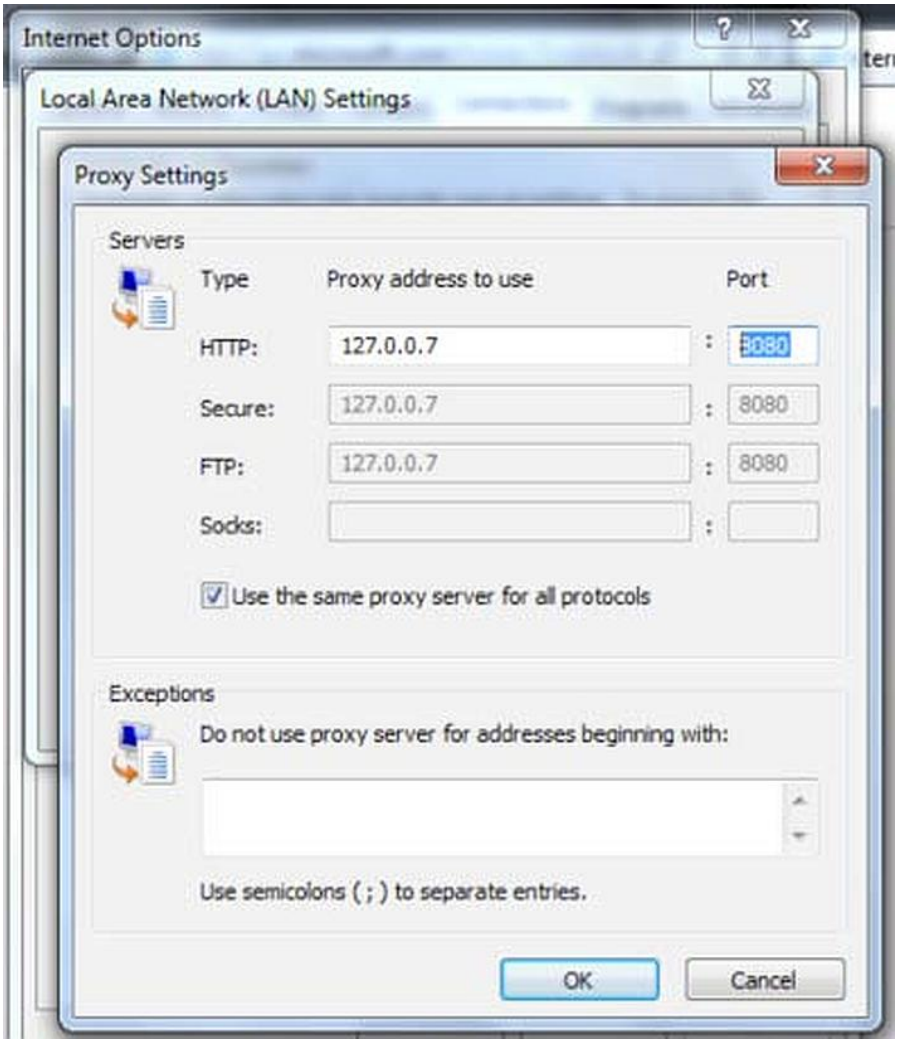
1. Buka menu Preferences.
2. Masuk ke Advanced > Network > Connection Settings.
3. Pilih Manual proxy configuration.
4. Isi host proxy dengan 127.0.0.1 dan port 8080.
5. Aktifkan Use this proxy server for all protocols.
6. Hapus semua pengecualian pada kolom No Proxy for.
7. Simpan perubahan.



Gambar 4. Contoh pengaturan proxy manual di Mozilla Firefox.

Contoh pengaturan di Internet Explorer

8. Buka Tools > Internet Options.
9. Masuk ke tab Connections lalu pilih LAN Settings.
10. Aktifkan Use a proxy server for your LAN.
11. Masuk ke Advanced.
12. Isi host dan port proxy seperti di Burp, misalnya 127.0.0.1:8080.
13. Gunakan proxy yang sama untuk semua protokol.
14. Hapus pengecualian yang bisa membuat traffic tidak lewat Burp.



Gambar 5. Contoh pengaturan proxy di Internet Explorer.

Saran kerja: Saat menguji aplikasi, sebaiknya nonaktifkan add-on atau fitur browser yang dapat mengubah perilaku halaman, misalnya filter keamanan tambahan atau ekstensi proxy lain. Lebih baik lagi jika memakai profil browser khusus untuk testing.

3. Cara mengecek apakah instalasi berhasil

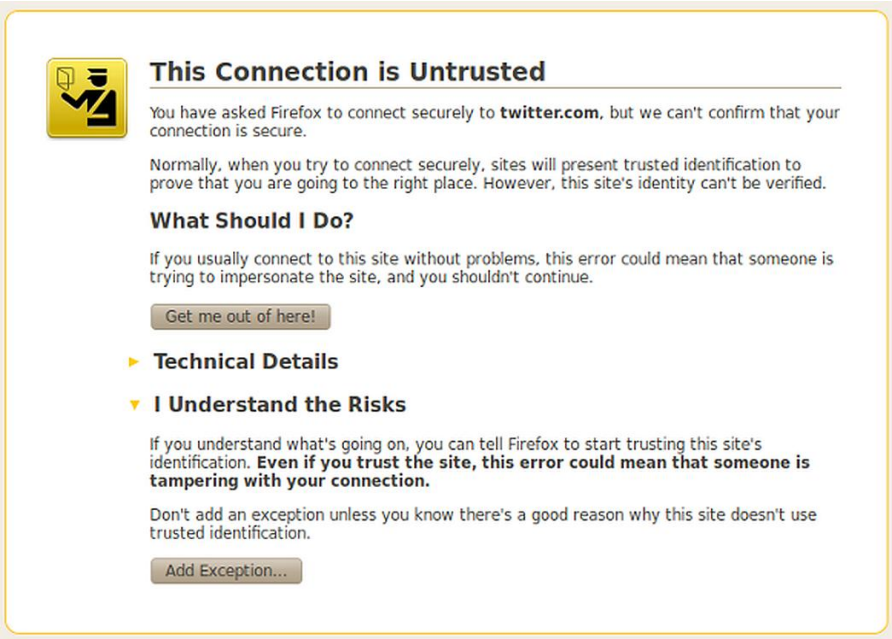
Uji cepatnya sederhana: buka sebuah website dari browser. Jika konfigurasi sudah benar, request akan tertahan di *Proxy* > *Intercept* dan menunggu persetujuan kita.

- Jika tombol Intercept aktif, request akan berhenti dulu di Burp.
- Jika kita klik Forward, request diteruskan ke website dan halaman akan terbuka.
- Jika browser berhenti lama atau halaman tidak kunjung terbuka, biasanya request atau response masih tertahan di Burp.

4. Hal penting saat membuka situs HTTPS

Burp tidak hanya bekerja untuk HTTP, tetapi juga HTTPS. Di sinilah sering muncul kebingungan pemula: browser bisa menampilkan peringatan sertifikat. Itu terjadi karena Burp memang bertindak sebagai perantara *(man-in-the-middle)* agar traffic terenkripsi tetap bisa diperiksa.

Artinya, peringatan sertifikat itu bukan otomatis tanda malware. Dalam konteks pengujian, hal itu muncul karena browser melihat sertifikat dari Burp/PortSwigger, bukan sertifikat asli website tujuan.



Gambar 6. Contoh peringatan sertifikat saat HTTPS diarahkan lewat Burp.

Apa yang biasanya dilakukan?

- Di Firefox, pengguna biasanya perlu membuka penjelasan risiko, menambahkan exception, lalu mengonfirmasi sertifikat.
- Di browser lain, prinsipnya sama: ada langkah untuk tetap melanjutkan koneksi.
- Sebelum menyetujui, pastikan memang Burp yang menyebabkan peringatan tersebut.

> **Awas:** Saat browser sedang disetel untuk melewati Burp, jangan gunakan browser itu untuk belanja online, membuka email utama, atau mengakses internet banking. Pakailah browser atau profil khusus testing agar aktivitas sensitif tetap aman.

5. Ringkasan yang mudah diingat

- Burp Suite adalah alat untuk melihat dan mengubah komunikasi antara browser dan website.
- Langkah paling penting untuk pemula adalah: instal Java, jalankan file JAR, aktifkan Proxy listener, lalu arahkan browser ke 127.0.0.1:8080.
- Kalau request tertahan di tab Intercept, berarti Burp sudah bekerja.

- Untuk situs HTTPS, peringatan sertifikat adalah hal yang normal saat Burp dipakai sebagai perantara.
- Selalu gunakan lingkungan uji dan browser khusus testing.
  Bab berikutnya biasanya sudah mulai masuk ke penggunaan Burp Proxy untuk menyadap, melihat, dan mengubah request. Kalau Anda setuju, saya bisa lanjutkan ke bagian halaman buku 13-56 dengan gaya penjelasan yang sama.