Burp Suite Starter

Bab 2 - Versi Bahasa Indonesia

Penulisan ulang sederhana untuk materi halaman buku 13-20 (mengacu ke halaman tercetak di isi buku, yang berada pada PDF halaman 24-31).

Sumber: Seitz, J. (2013). Instant Burp Suite starter. Packt Publishing.

Catatan penting: Dokumen ini bukan terjemahan kata per kata. Isinya sudah disederhanakan agar lebih mudah dipahami orang awam, tetapi urutan ide dan inti praktik tetap mengikuti sumber aslinya. Istilah seperti request, response, header, cookie, dan proxy tetap dipakai supaya mudah dicocokkan saat latihan.

1. Apa itu Burp Proxy?

Burp Proxy adalah fitur di Burp Suite yang bekerja seperti pintu pemeriksaan di tengah jalan. Semua data dari browser lewat dulu ke Burp, lalu baru diteruskan ke website. Karena itu, kita bisa melihat, menahan, mengubah, atau bahkan membatalkan permintaan sebelum sampai ke server.

Fungsi ini sangat penting untuk belajar cara kerja aplikasi web dan untuk menguji apakah server aman ketika menerima data yang dimodifikasi.

Tiga tab utama di Burp Proxy

Bagian	Penjelasan sederhana
Intercept	Tempat untuk menahan request atau response yang sedang lewat, lalu memeriksanya sebelum diteruskan.
Options	Tempat untuk mengatur perilaku proxy, misalnya aturan intersep, match and replace, dan modifikasi HTML otomatis.
History	Tempat untuk melihat daftar semua traffic yang sudah lewat, sehingga mudah dianalisis lagi kapan saja.

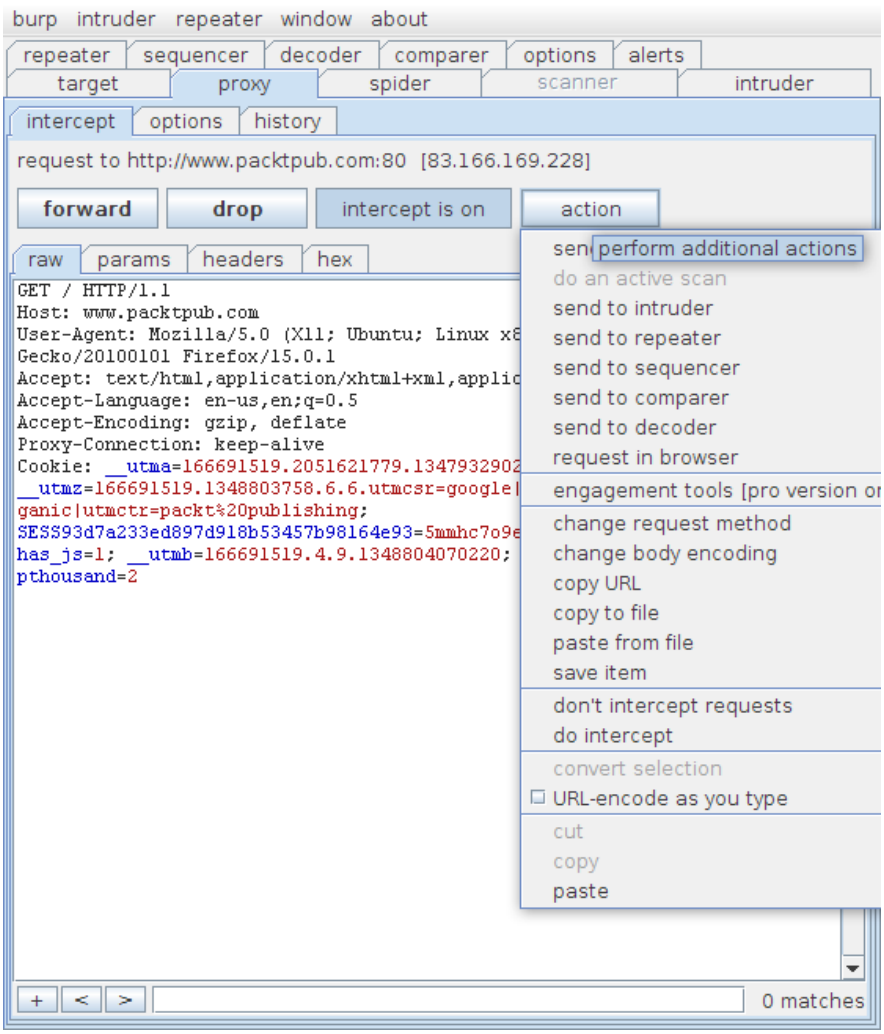
Gambaran singkat cara kerjanya

Alurnya sederhana: browser -> Burp Proxy -> server. Saat tombol *intercept is on*, Burp akan berhenti sejenak di tengah agar kita bisa memeriksa isinya. Saat tombol itu dimatikan, traffic tetap lewat melalui Burp, tetapi tidak perlu menunggu tombol *forward* dari kita.

2. Langkah 1 - Menangkap request dari browser

1. Buka tab Intercept, lalu pastikan tombolnya menunjukkan tulisan intercept is on.
2. Di browser, ketik http://www.packtpub.com/ lalu tekan Enter.
3. Kembali ke Burp. Request dari browser akan muncul dan berhenti sementara di jendela Intercept.
4. Klik forward jika Anda ingin request diteruskan ke server. Halaman website akan terbuka seperti biasa di browser.
5. Ulangi lagi, tetapi klik drop. Kali ini request dibatalkan, sehingga browser menampilkan pesan kesalahan dari Burp.
6. Jika request sudah tertangkap, tombol action akan aktif. Dari sini, request yang sama bisa dikirim ke alat lain seperti Decoder, Repeater, atau Intruder.

Makna dua tombol yang paling penting: forward berarti lanjutkan request, sedangkan drop berarti batalkan request. Dengan dua tombol ini saja, kita sudah bisa mulai memahami bagaimana browser berkomunikasi dengan server.



Gambar 1. Request yang tertangkap di Burp Proxy dapat diteruskan, dibatalkan, atau dikirim ke tool lain.

Mencegat response dari server

Burp tidak hanya bisa menahan request, tetapi juga response dari server. Di tab Options, kita bisa mengatur kapan response harus dihentikan. Ini berguna saat kita ingin membandingkan hasil sebelum dan sesudah request dimodifikasi, atau saat ingin fokus pada response dengan status tertentu seperti 200 OK.

3. Langkah 2 - Memeriksa isi request dan response

Setelah request tertangkap, Burp menyediakan beberapa tampilan untuk membantu kita membaca isi data dari sudut yang berbeda.

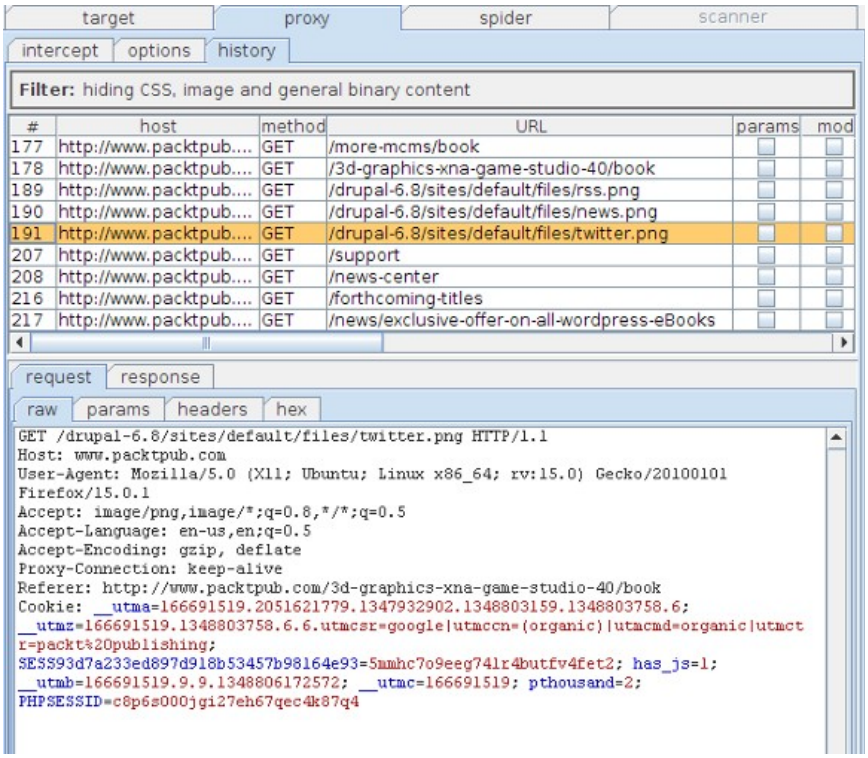
Empat tampilan analisis pesan

Bagian	Penjelasan sederhana
Raw	Menampilkan isi request dalam bentuk mentah. Tampilan ini paling fleksibel jika Anda ingin mengedit teks secara langsung.

Bagian	Penjelasan sederhana
Params	Menyorot parameter yang dikirim pengguna, seperti GET, POST, dan cookie. Cocok untuk mencari titik input yang berpotensi bermasalah.
Headers	Menampilkan nama dan nilai header HTTP dalam bentuk daftar yang lebih rapi dan cepat dibaca.
Hex	Dipakai untuk melihat data biner dalam format heksadesimal, misalnya saat konten tidak nyaman dibaca sebagai teks biasa.

Menggunakan tab History

- Tab History menyimpan semua request yang pernah lewat melalui proxy.
- Bagian atas berisi daftar traffic; bagian bawah menampilkan detail request dan response dari item yang dipilih.
- Setiap item biasanya menampilkan metode request, URL, kode status response, dan ukuran data.
- Jika sebuah request pernah diubah sebelum diteruskan, versi hasil ubahannya juga bisa terlihat di sini.
- Anda dapat memberi warna pada item tertentu agar request penting mudah ditemukan kembali.
- Fitur filter membantu menyembunyikan traffic yang tidak relevan, misalnya hanya menampilkan request yang punya parameter atau status code tertentu.



Gambar 2. Tab History memudahkan kita meninjau ulang request dan response yang sudah lewat.

4. Langkah 3 - Mengubah request (tampering)

Dalam pengujian keamanan, kita sering perlu mengubah data yang dikirim ke server, lalu melihat reaksi aplikasi. Cara ini dipakai untuk mengecek validasi input, penanganan parameter, atau potensi celah seperti SQL injection dan masalah logika aplikasi.

Contoh sederhana dari buku: buka alamat pencarian buku berikut di browser: *http://www.packtpub.com/books/all?keys=ASP*. Saat request tertangkap di Burp, ubah nilai parameter **keys** dari *ASP* menjadi *PHP*, lalu klik *forward*. Hasil pencarian di browser akan berubah mengikuti nilai parameter baru tersebut.

```
GET /books/all?keys=PHP HTTP/1.1
Host: www.packtpub.com
```

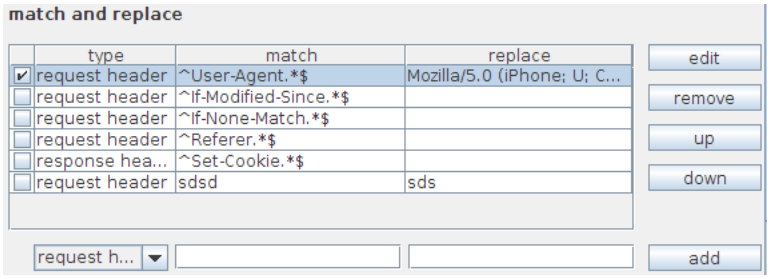
Burp juga tidak membatasi kita pada tampilan Raw saja. Di tab Params, kita bisa menambah parameter baru dengan menekan tombol New, memilih jenis parameter (URL untuk GET, Body untuk POST, atau Cookie), lalu mengisi nama dan nilainya.

5. Fitur lanjutan yang berguna

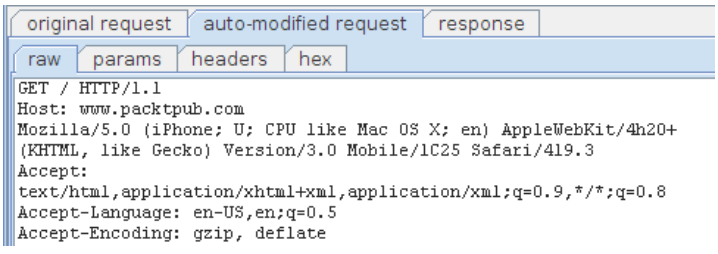
Match and Replace

Fitur ini dipakai untuk mengganti isi request atau response secara otomatis. Contoh yang dibahas di sumber asli adalah mengganti header **User-Agent** agar server mengira kita sedang memakai browser di iPhone. Ini berguna ketika website menampilkan versi berbeda untuk perangkat mobile.

1. Buka Burp Proxy -> Options, lalu cari bagian Match and Replace.
2. Pilih request header sebagai target aturan.
3. Isi kolom match dengan pola ^User-Agent.*$ untuk mencari baris header User-Agent.
4. Isi kolom replace dengan User-Agent palsu yang ingin dipakai.
5. Klik Add. Setelah itu, request yang lewat bisa berubah otomatis sesuai aturan tersebut.



Gambar 3. Daftar aturan Match and Replace di Burp Proxy.



Gambar 4. Contoh header request yang sudah diubah otomatis.

HTML Modification

Burp Proxy juga dapat mengubah HTML yang diterima browser secara otomatis. Fitur ini sangat membantu saat aplikasi memakai validasi di sisi klien, misalnya field yang disembunyikan, form yang dinonaktifkan, batas panjang input, atau pemeriksaan JavaScript sebelum form dikirim.

- menampilkan field form yang semula tersembunyi
- mengaktifkan field yang tadinya disabled
- menghapus batas panjang input
- menghapus validasi form berbasis JavaScript
- menghapus semua JavaScript
- menghapus object tags tertentu dari halaman

Tujuan utamanya adalah melihat apakah server benar-benar memeriksa data yang masuk. Kalau setelah validasi di browser dimatikan aplikasi masih menerima data sembarangan, berarti ada kemungkinan validasi di sisi server lemah atau tidak ada.

6. Inti yang perlu diingat

- Burp Proxy berada di antara browser dan server, sehingga semua traffic bisa diperiksa dari tengah.
- Intercept dipakai untuk menahan data yang sedang lewat; History dipakai untuk meninjau ulang semua traffic yang sudah lewat.
- Request bisa diubah secara manual di tampilan Raw atau Params untuk menguji perilaku aplikasi.
- Match and Replace berguna untuk otomatisasi perubahan tertentu, misalnya mengganti User-Agent.
- HTML Modification membantu mematikan hambatan di sisi browser agar kita bisa fokus menguji validasi di sisi server.

Sumber

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