BAB 3
Fitur-Fitur Penting Burp Suite untuk Pengujian Aplikasi Web

Ditulis ulang dalam bahasa Indonesia yang lebih mudah dipahami berdasarkan halaman 21-54 dari ebook sumber.

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

Catatan etika: Gunakan Burp Suite hanya pada sistem atau situs yang memang memberi izin untuk diuji. Uji keamanan tanpa izin bisa melanggar hukum dan merugikan pihak lain.

Gambaran umum bab ini

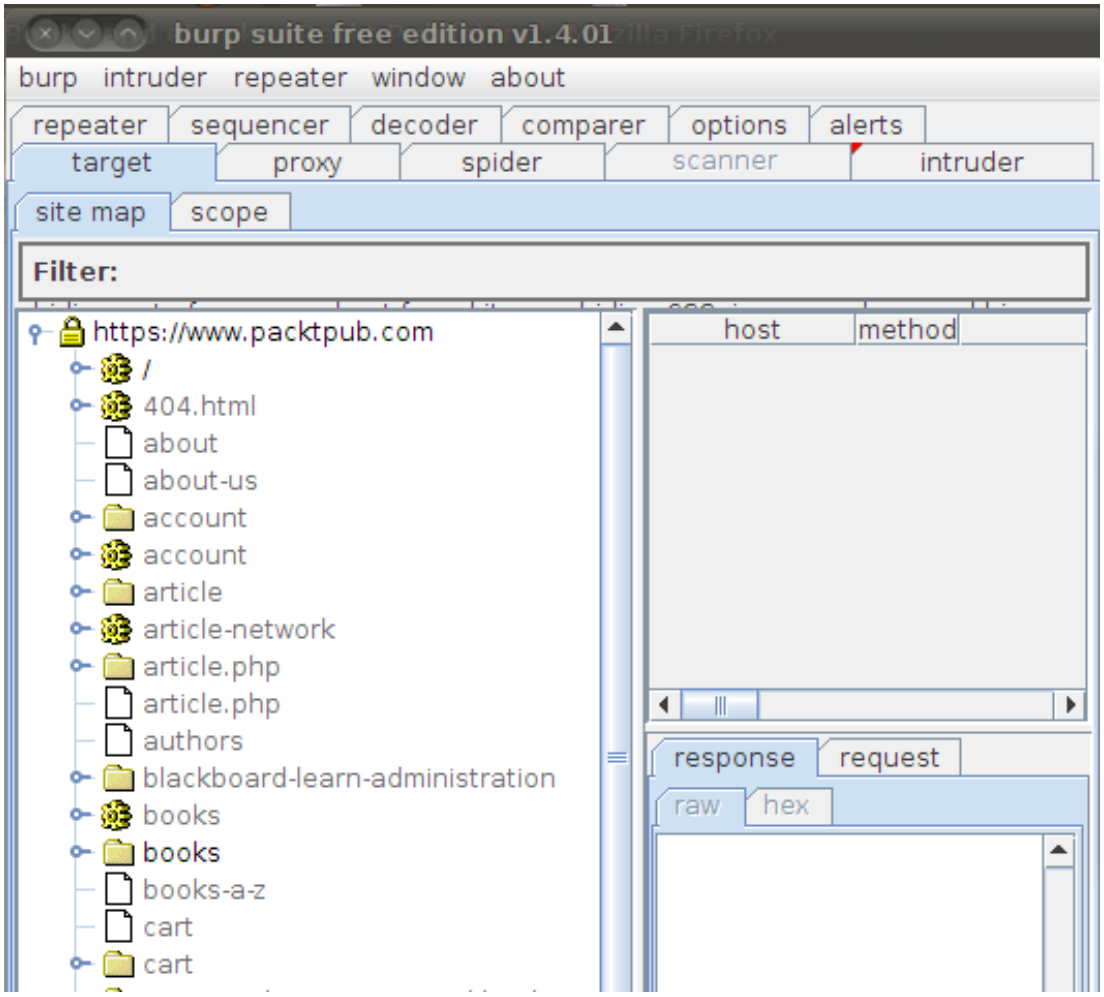
Bab ini membahas delapan fitur penting Burp Suite yang paling sering dipakai saat menguji aplikasi web. Penjelasan di sini tidak dibuat terlalu teknis agar pembaca pemula tetap bisa mengikuti alurnya. Fokusnya adalah memahami fungsi setiap fitur, kapan dipakai, cara dasar mengoperasikannya, dan hal-hal penting yang harus diperhatikan.

Fitur	Kegunaan singkat
Target Site Map	Memetakan halaman, parameter, dan endpoint aplikasi yang sudah ditemukan.
Spider	Merayapi aplikasi secara otomatis untuk mencari resource yang terlihat maupun tersembunyi.
Scanner	Membantu mendeteksi celah keamanan umum secara otomatis.
Intruder	Mengirim banyak variasi request untuk menguji parameter tertentu.
Repeater	Mengulang request yang sama sambil mengubah isinya secara manual.
Sequencer	Menilai apakah token sesi atau token anti-CSRF cukup acak.
Decoder	Mengubah data ke bentuk encode/decode seperti URL, Base64, atau hex.
Compare Site Maps	Membandingkan dua tampilan aplikasi untuk melihat perbedaan akses atau respons.

1. Menggunakan Target Site Map

Saat mulai menguji sebuah aplikasi web, langkah pertama yang sangat penting adalah mengenali isi aplikasinya. Kita perlu tahu halaman apa saja yang ada, URL apa yang dipakai, parameter apa yang muncul, dan bagaimana hubungan antarbagian aplikasi. Di Burp Suite, fungsi ini ditangani oleh Target Site Map.

Site map menampilkan daftar resource dalam bentuk pohon atau struktur bertingkat. Dengan tampilan ini, kita bisa melihat domain utama, folder, file, endpoint, sampai parameter yang sudah pernah lewat di Burp. Bagi pemula, bayangkan fitur ini seperti peta jalan yang menunjukkan area mana saja dari aplikasi yang sudah dikunjungi.



Gambar 1. Contoh tampilan Burp Target Site Map.

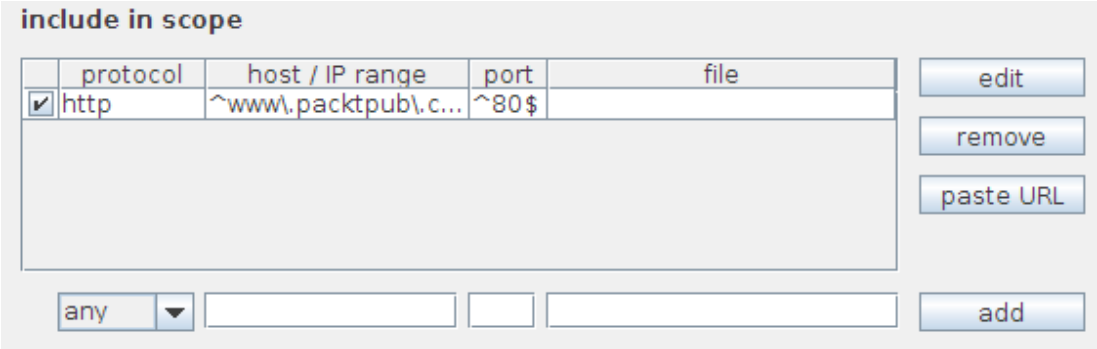
Kenapa site map penting?

- Membantu melihat gambaran besar aplikasi yang sedang diuji.
- Memudahkan menentukan area yang masuk ruang lingkup pengujian.
- Menjadi titik awal untuk mengirim request ke tool lain seperti Spider, Scanner, Intruder, Repeater, atau Comparer.
- Membantu memastikan tidak ada endpoint penting yang terlewat.

Mengatur scope agar pengujian tetap fokus

Burp memungkinkan kita membatasi target hanya pada domain atau resource tertentu. Ini disebut in scope. Fitur ini penting karena saat pengujian berlangsung, request yang keluar sebaiknya benar-benar hanya menuju aplikasi yang diizinkan untuk diuji.

1. Di tab Target, pilih node domain utama aplikasi yang ingin diuji.
2. Klik kanan lalu pilih add item to scope.
3. Aktifkan filter show only in-scope items agar daftar resource lebih bersih dan fokus.
4. Periksa lagi di tab Scope untuk memastikan domain yang benar sudah masuk ke daftar include in scope.

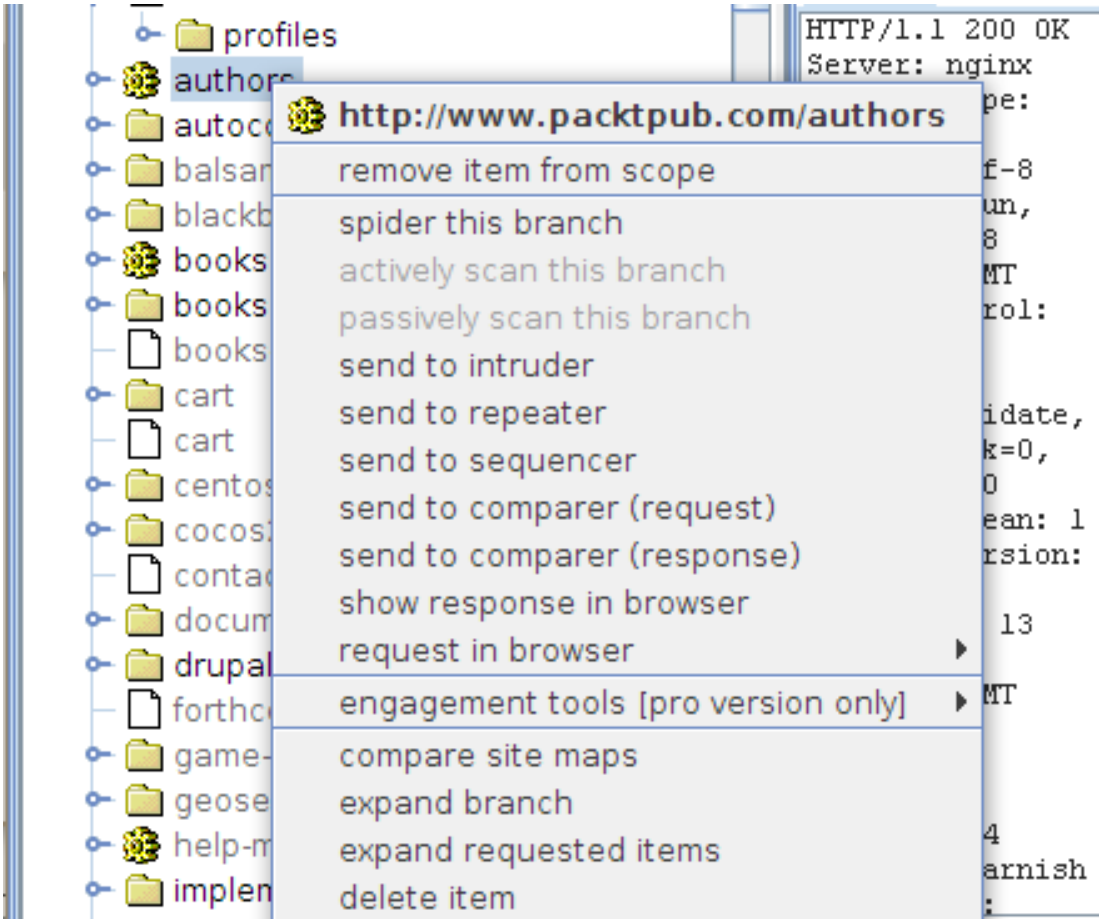


Gambar 2. Contoh pengaturan item yang dimasukkan ke dalam scope.

Selain memasukkan resource ke scope, kita juga bisa mengecualikan resource tertentu. Ini berguna untuk menghindari halaman logout, tombol reset, atau fungsi yang bisa merusak data. Jadi, bukan hanya fokus pengujian yang lebih rapi, risikonya juga lebih kecil.

Menu klik kanan yang sangat berguna

Dari site map, hampir semua item bisa diklik kanan untuk dikirim ke tool lain. Inilah yang membuat Target menjadi pusat navigasi utama di Burp Suite.



Gambar 3. Menu konteks pada Target yang dapat mengirim data ke tool lain.

- Spider this branch: merayapi cabang resource yang dipilih.
- Actively/Passively scan this branch: memindai area tertentu dengan Scanner.
- Send to Intruder: menyiapkan serangan otomatis dengan banyak payload.
- Send to Repeater: mengirim request untuk diuji manual berulang-ulang.
- Send to Sequencer: menganalisis tingkat keacakan token.
- Send to Comparer atau Compare Site Maps: membandingkan request atau hasil pemetaan.

Inti penting: Sebelum melakukan pengujian lebih jauh, biasakan memeriksa site map terlebih dahulu. Dari sana, Anda bisa melihat area mana yang sudah terekam dan area mana yang masih perlu dijelajahi.

2. Merayapi Aplikasi dengan Burp Spider

Burp Spider dipakai untuk menjelajahi aplikasi web secara otomatis. Tool ini mencari halaman, link, form, dan resource lain yang bisa diakses dari aplikasi. Hasil penelusuran Spider akan menambah isi site map, sehingga peta aplikasi menjadi lebih lengkap.

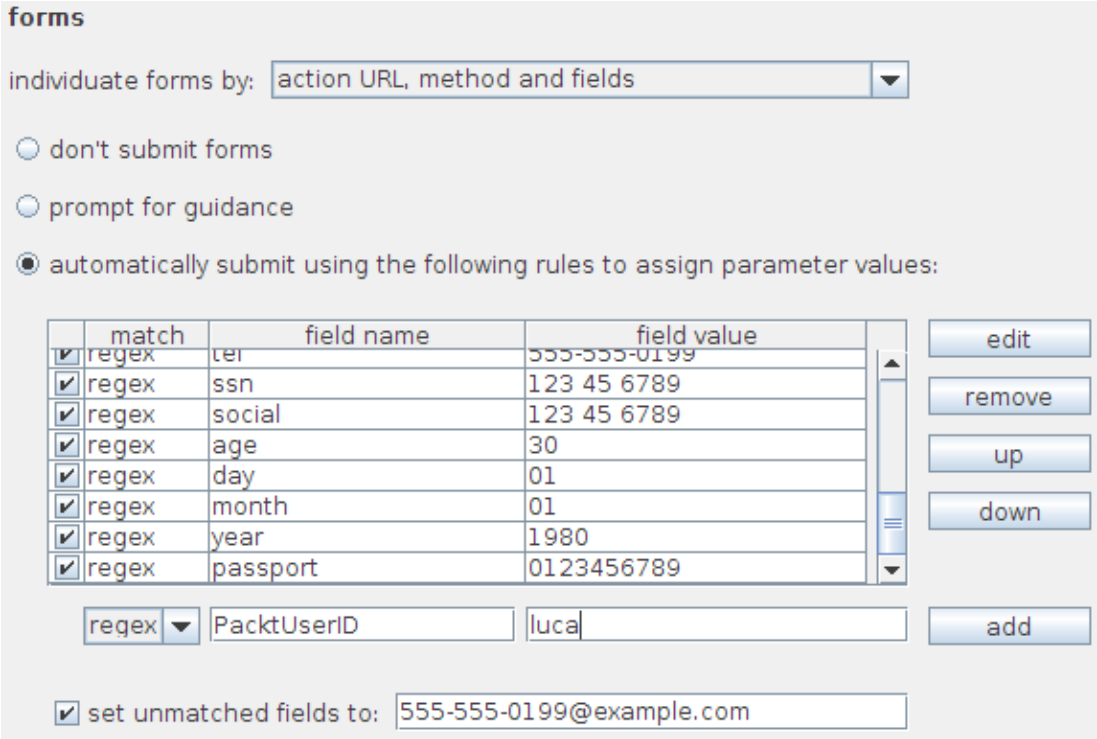
Spider sangat berguna saat aplikasi cukup besar atau saat Anda khawatir ada halaman yang tidak sempat ditemukan secara manual. Meski begitu, penjelajahan manual tetap penting karena ada area aplikasi yang kadang hanya muncul setelah interaksi tertentu.

Pengaturan dasar Spider

- Kedalaman link: menentukan seberapa jauh Spider mengikuti tautan berantai.
- Jumlah thread: mengatur seberapa banyak request dikirim bersamaan.
- Retry dan jeda: berguna jika server lambat atau tidak stabil.
- Login aplikasi: bisa diatur agar Spider mengirim username dan password secara otomatis bila dibutuhkan.

Spider juga bisa membantu mengisi form HTML secara otomatis. Ini berguna untuk form pendaftaran, login, pencarian, dan form sederhana lain yang perlu diisi sebelum halaman berikutnya muncul.

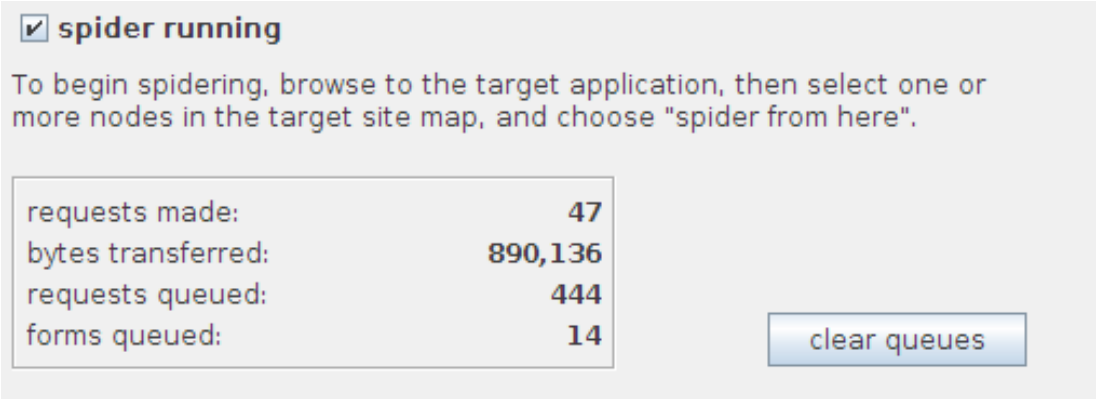
5. Buka Burp Spider lalu masuk ke bagian Options > Forms.
6. Aktifkan opsi agar Spider mengisi form secara otomatis berdasarkan aturan yang ditentukan.
7. Tambahkan aturan nama field dan nilai yang ingin digunakan. Misalnya, jika field berisi user ID tertentu, Anda bisa menentukan nilai tetap untuk field itu.



Gambar 4. Pengaturan pengisian form otomatis pada Burp Spider.

Cara menjalankan Spider

8. Pilih resource awal dari site map pada tab Target.
9. Klik kanan lalu pilih spider from here agar perayapan dimulai dari cabang tersebut.
10. Pantau proses di tab Control untuk melihat berapa request yang sudah dikirim dan berapa resource yang masih menunggu.



Gambar 5. Burp Spider saat sedang berjalan.

Secara umum, Spider akan mengikuti scope yang sudah ditetapkan di tab Target. Ini membantu mencegah tool menjelajah ke domain lain yang sebenarnya tidak sedang diuji.

Tips praktis: Gabungkan perayapan otomatis dengan penelusuran manual. Spider bagus untuk mempercepat penemuan resource, tetapi penjelajahan manual sering kali tetap dibutuhkan untuk melihat alur bisnis aplikasi secara utuh.

3. Menjalankan Pemindaian Otomatis dengan Burp Scanner

Burp Scanner adalah fitur yang membantu mendeteksi kelemahan keamanan umum secara otomatis. Tool ini tersedia di edisi Professional. Contoh masalah yang bisa dicari antara lain SQL Injection, Cross-Site Scripting, XML Injection, dan konfigurasi cookie yang tidak aman.

Dua mode utama Scanner

- Passive scanning: menganalisis request dan response yang sudah ada tanpa mengirim serangan tambahan. Mode ini lebih aman dan minim gangguan.
- Active scanning: mengirim variasi request yang mengandung pola uji tertentu untuk melihat apakah server rentan. Mode ini lebih kuat, tetapi juga lebih berisiko memicu masalah pada aplikasi.

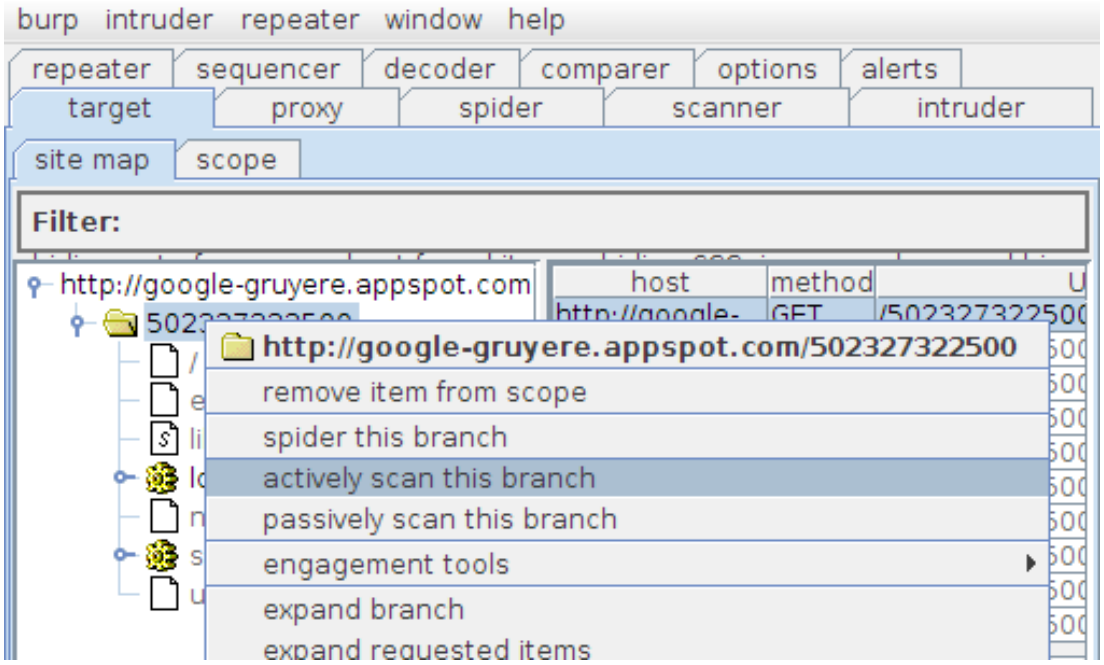
Untuk latihan, buku sumber memberi contoh memakai aplikasi uji bernama Google Gruyere. Intinya, Anda memerlukan target yang memang aman untuk diuji, bukan situs acak di internet.

Gambar 6. Contoh aplikasi uji Google Gruyere yang dipakai untuk latihan.

Menjalankan scan

Burp Scanner bisa berjalan otomatis saat Anda sedang browsing melalui Burp, atau dijalankan dari site map pada resource tertentu.

11. Buka tab Scanner lalu atur live scanning sesuai kebutuhan.
12. Untuk pengujian otomatis saat browsing, gunakan suite scope agar hanya resource dalam scope yang dipindai.
13. Atau, dari Target Site Map, klik kanan host atau cabang tertentu lalu pilih active scan atau passive scan.



Gambar 7. Menjalankan Burp Scanner dari Target Site Map.

Saat memulai active scan, Burp akan menampilkan wizard konfigurasi. Di sini Anda bisa mengecualikan resource seperti gambar, JavaScript, atau stylesheet bila memang tidak relevan. Anda juga dapat meninjau daftar endpoint yang akan diuji dan menghapus item yang dirasa sensitif atau berbahaya, misalnya fungsi hapus pengguna atau reset data.

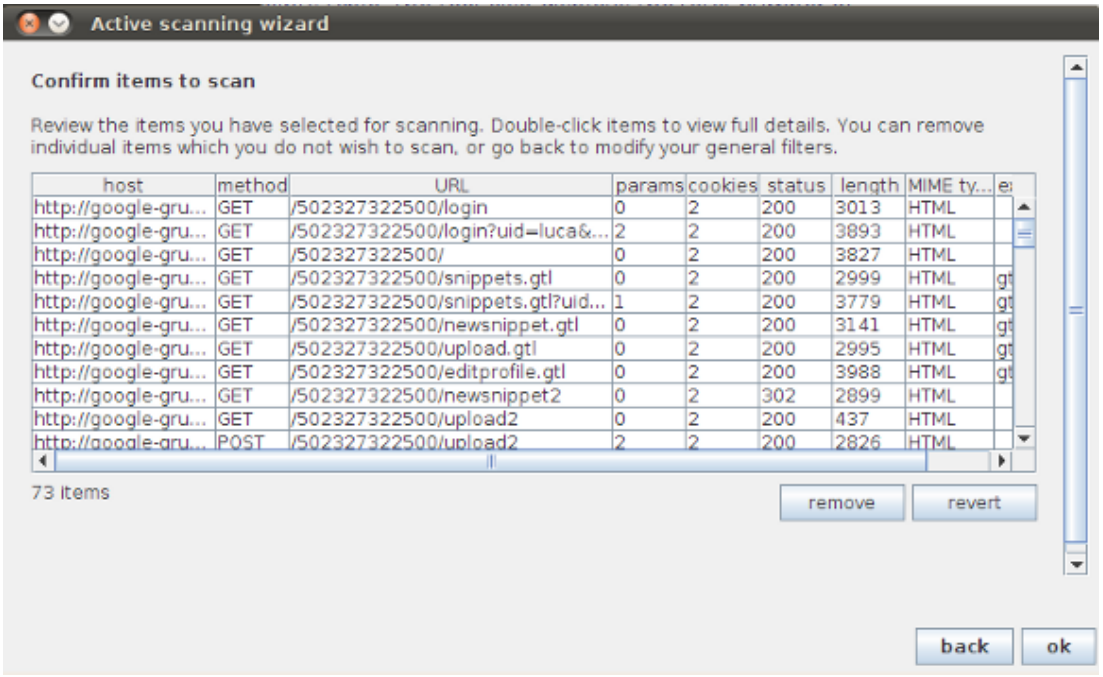
Pengaturan lanjutan yang penting

- Insertion points: menentukan bagian request mana saja yang boleh dimodifikasi, misalnya parameter URL, body POST, cookie, nama parameter, header, dan parameter pada URL gaya REST.
- Scanning areas: memilih kategori kelemahan apa saja yang ingin dicari.
- Scanning engine: mengatur jumlah thread dan kecepatan request agar sesuai dengan kondisi server.

Peringatan: Active scan dapat memicu perubahan data atau gangguan aplikasi. Karena itu, lakukan backup jika perlu, pantau prosesnya, dan pastikan Anda benar-benar punya izin menguji target tersebut.

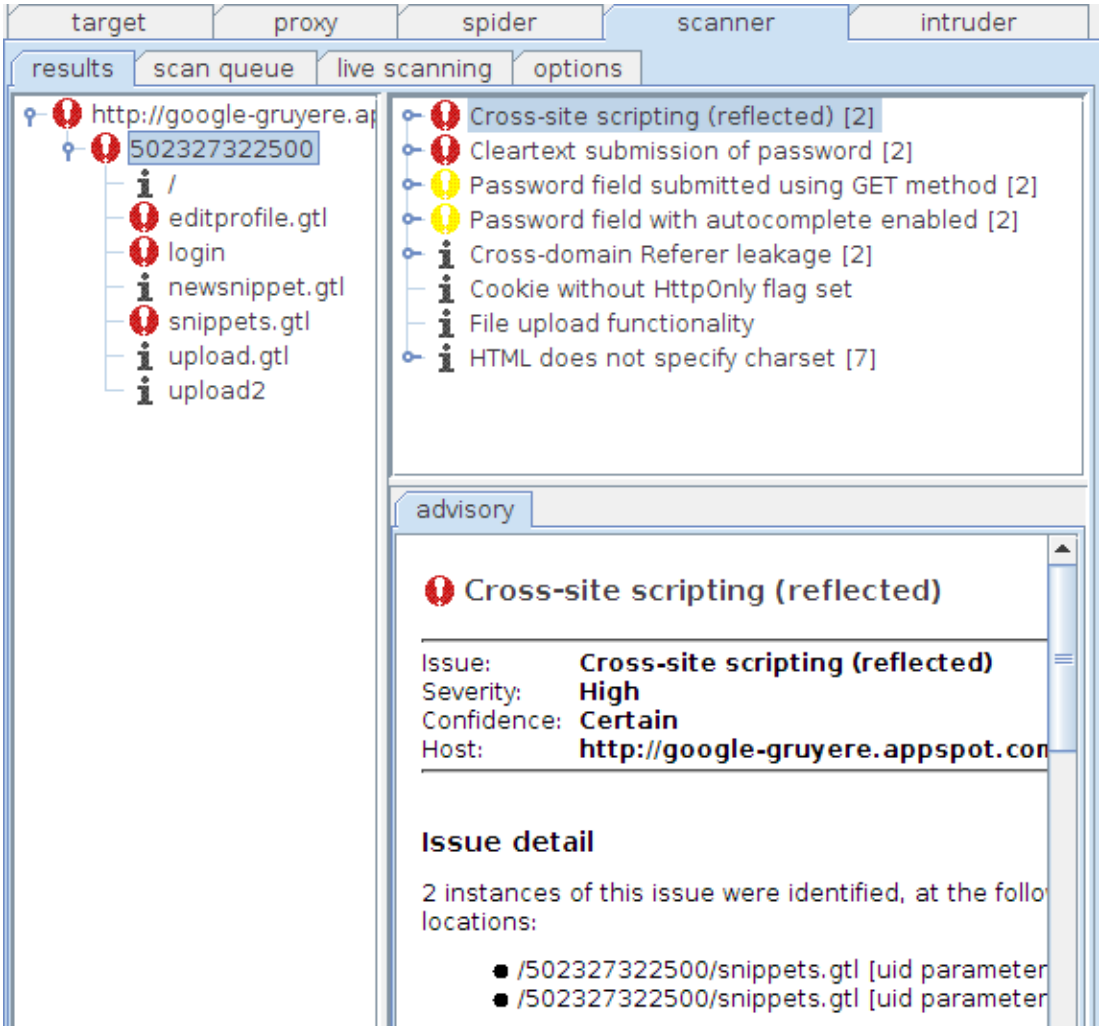
Membaca hasil scan

Selama scan berjalan, Anda bisa melihat antrean proses pada scan queue. Di sana terlihat request mana yang sedang dikerjakan, mana yang sudah selesai, dan berapa banyak temuan yang sudah muncul.



Gambar 8. Contoh antrean pekerjaan pada Burp Scanner.

Hasil akhir ditampilkan dalam bentuk findings tree. Setiap temuan biasanya disertai penjelasan kategori masalah, tingkat keparahan, tingkat keyakinan, host, dan path yang terkena.



Gambar 9. Contoh hasil temuan pada Burp Scanner.

- Severity menunjukkan seberapa besar dampak masalah tersebut.
- Confidence menunjukkan seberapa yakin Burp terhadap temuan itu.
- Beberapa hasil masih perlu diverifikasi manual, terutama bila confidence belum tinggi.

Jika perlu, hasil scan dapat diekspor ke laporan HTML atau XML. Fitur ini berguna untuk dokumentasi, pelacakan bug, atau dibagikan ke tim lain.

4. Mengotomatiskan Serangan Kustom dengan Burp Intruder

Burp Intruder dipakai ketika Anda ingin menguji satu request dengan banyak variasi nilai. Misalnya, Anda menduga suatu parameter rentan terhadap SQL Injection, maka Intruder bisa membantu mengirim request yang sama berulang kali dengan payload yang berbeda-beda.

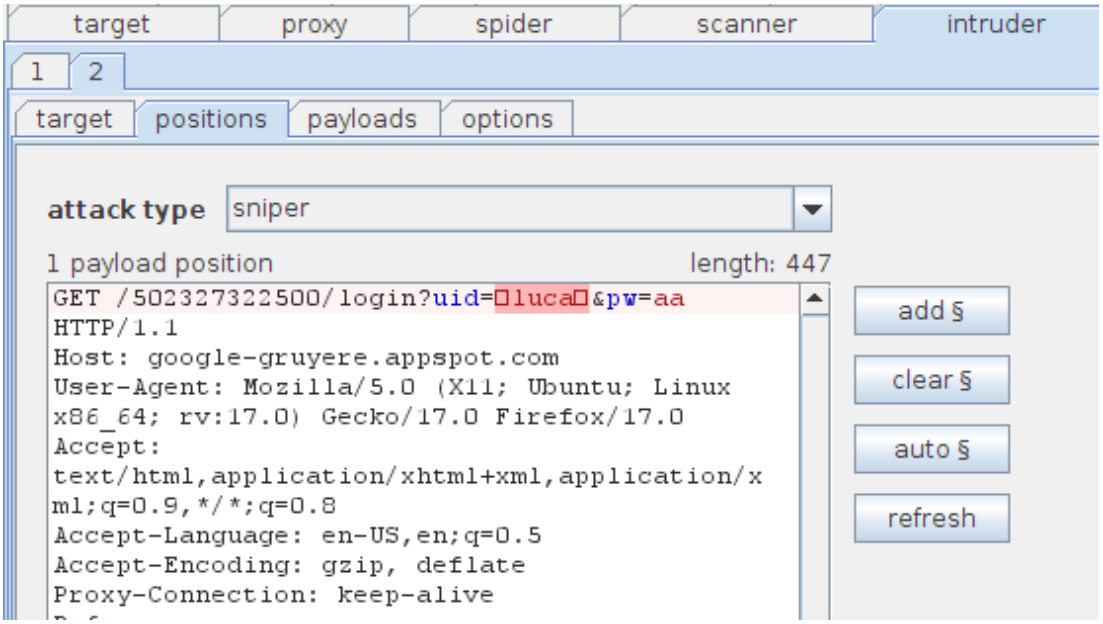
Secara sederhana, Intruder cocok untuk brute force, pengujian input, enumerasi, dan eksperimen terhadap parameter tertentu. Dibanding Scanner, Intruder memberi kontrol lebih besar terhadap isi request dan pola serangan.

Empat langkah besar penggunaan Intruder

- Memasukkan request yang ingin diuji.
- Menentukan posisi parameter yang akan diganti payload.
- Memilih tipe serangan.
- Menentukan daftar payload dan opsi tambahan.

Menentukan posisi dan tipe serangan

14. Kirim request ke Intruder, misalnya dari Proxy History dengan klik kanan lalu pilih send to intruder.
15. Buka tab Positions.
16. Hapus marker otomatis bila perlu, lalu tandai bagian request yang benar-benar ingin diuji.
17. Pilih attack type yang sesuai.



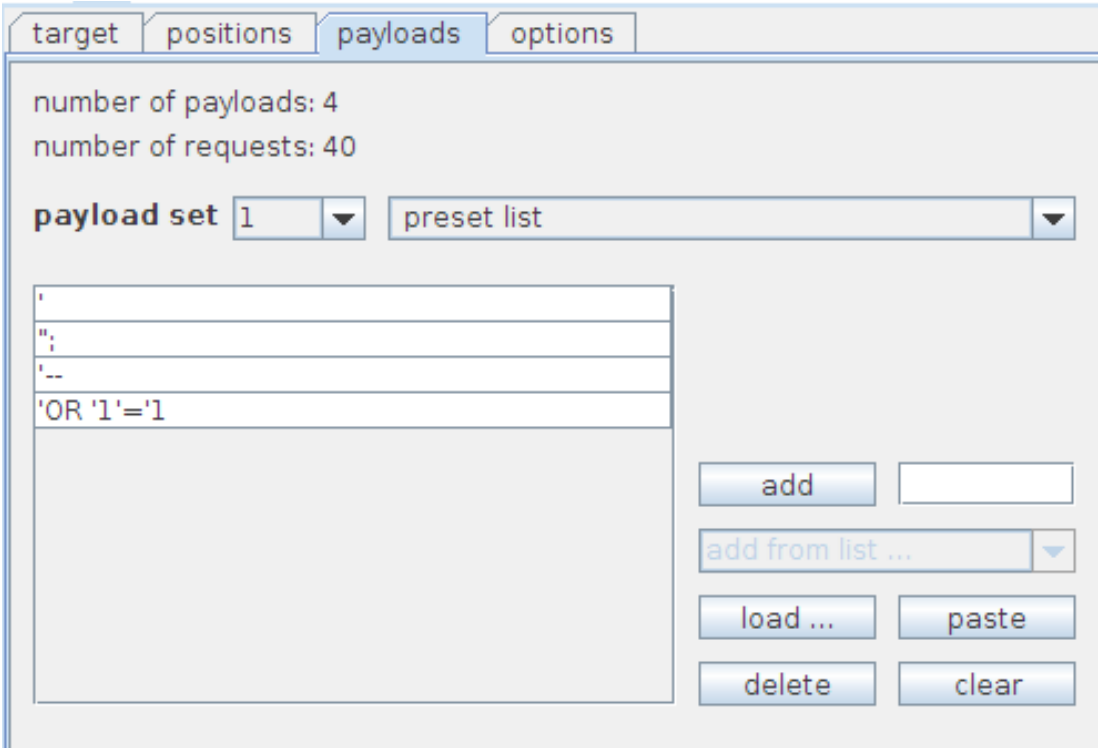
Gambar 10. Menentukan posisi parameter yang akan diuji pada Intruder.

Burp Intruder menyediakan empat jenis attack type. Masing-masing cocok untuk kebutuhan yang berbeda.

- Sniper: menguji satu posisi demi satu posisi dengan payload dari satu daftar. Cocok untuk mencari parameter mana yang paling menarik.
- Battering ram: mengisi semua posisi dengan payload yang sama secara bersamaan.
- Pitchfork: memakai beberapa daftar payload secara paralel, satu daftar untuk satu posisi.
- Cluster bomb: mencoba semua kombinasi dari beberapa daftar payload. Sangat kuat, tetapi jumlah request bisa sangat banyak.

Menentukan payload

Pada tab Payloads, Anda menentukan nilai apa saja yang akan dipakai untuk menguji parameter. Payload bisa berupa daftar kata, angka, tanggal, atau hasil brute force. Anda juga bisa menulis daftar sendiri secara manual.



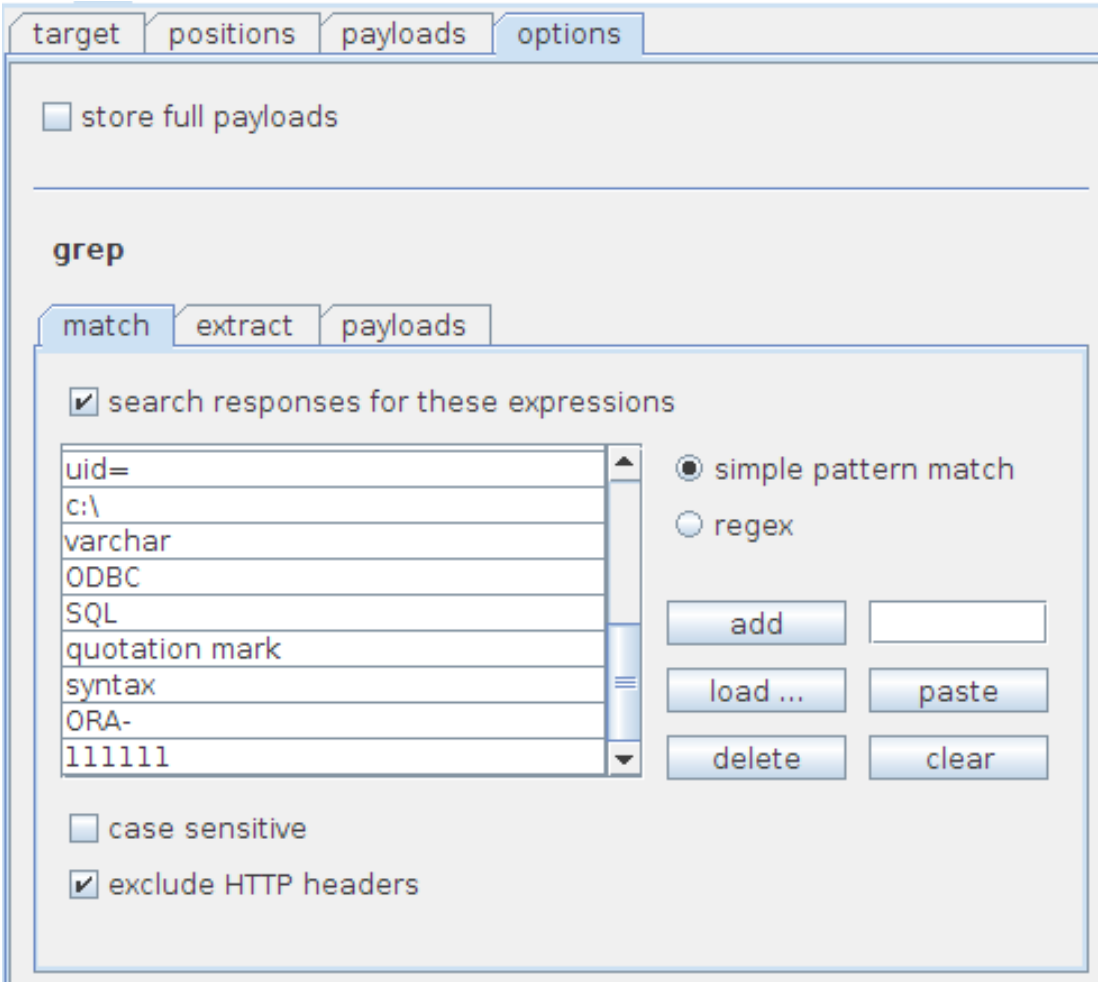
Gambar 11. Menyusun daftar payload untuk Burp Intruder.

- Preset list: memuat wordlist atau daftar string dari file atau dari input manual.
- Numbers: menghasilkan angka berurutan otomatis.
- Dates: menghasilkan nilai tanggal.
- Bruteforce: menghasilkan semua kombinasi karakter dalam batas panjang tertentu.

Secara bawaan, Burp dapat melakukan URL-encode terhadap karakter tertentu dalam payload. Ini penting dipahami, karena kadang hasil uji berubah bila karakter seperti tanda kutip otomatis diubah menjadi format encoded.

Opsi tambahan yang berguna

Intruder punya fitur grep yang sangat membantu. Dengan grep, kita dapat mencari kata atau pola tertentu di dalam response, misalnya error, invalid, unauthorized, incorrect, dan sebagainya. Kata-kata ini dapat membantu menandai respons yang menarik untuk diperiksa lebih lanjut.



Gambar 12. Menambahkan pola pencarian pada response Intruder.

Cara membaca hasil: Perhatikan perbedaan panjang response, kode status HTTP, waktu respons, dan kemunculan kata tertentu. Kadang perubahan kecil justru menjadi petunjuk bahwa sebuah payload berhasil memengaruhi aplikasi.

Setelah semua siap, jalankan serangan dari menu Intruder > Start Attack. Burp akan membuka jendela hasil dan menampilkan daftar request serta respons yang dihasilkan.

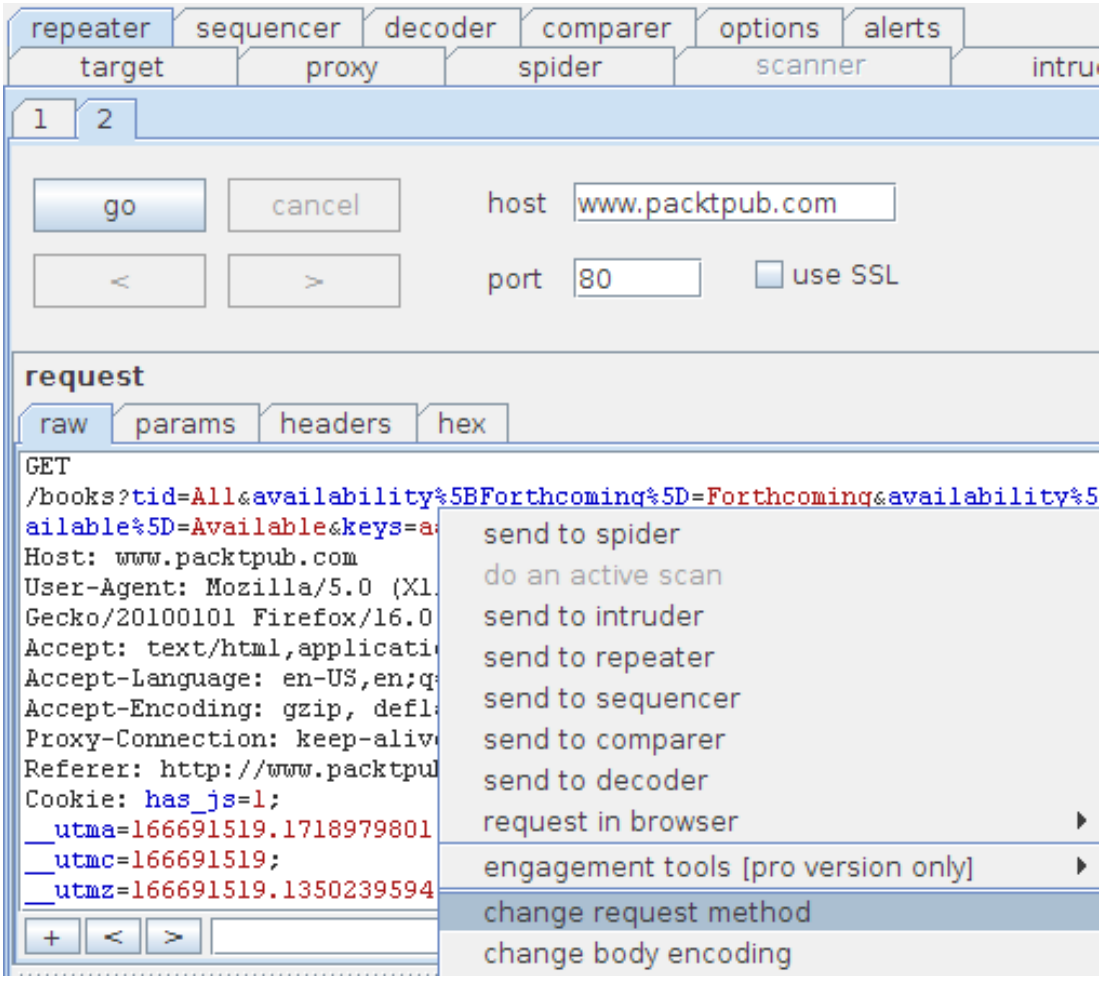
5. Mengubah dan Mengulang Request dengan Burp Repeater

Jika Intruder lebih cocok untuk percobaan massal, maka Repeater lebih cocok untuk eksperimen manual. Tool ini dipakai ketika Anda ingin mengambil satu request, mengubahnya sedikit demi sedikit, lalu mengirimkannya berulang kali untuk melihat dampaknya.

Repeater sangat berguna untuk mengonfirmasi dugaan kerentanan, menyempurnakan payload, atau memahami logika aplikasi secara lebih detail. Ini adalah tool favorit banyak penguji karena sederhana tetapi sangat fleksibel.

18. Pilih request dari tool mana saja, misalnya dari Proxy History.
19. Klik kanan lalu pilih send to repeater.

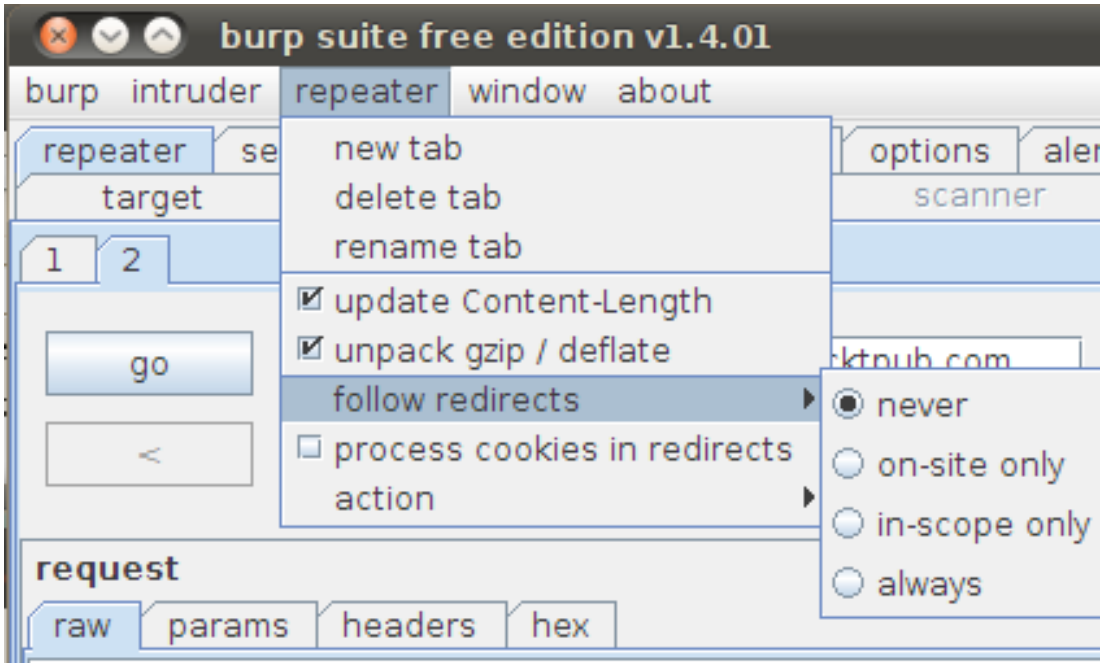
20. Di tab Repeater, ubah bagian request yang ingin diuji.
21. Klik Go untuk mengirim request dan lihat response.



Gambar 13. Mengubah metode request di Burp Repeater.

Contoh sederhana adalah mengubah request GET menjadi POST, menambah parameter baru, atau mengganti nilai parameter lama. Dari response yang dihasilkan, kita bisa menilai apakah server menerima perubahan itu atau justru menolaknya.

Fitur tambahan pada Repeater



Gambar 14. Opsi tambahan yang tersedia pada Burp Repeater.

- Update Content-Length: memperbarui header Content-Length secara otomatis saat isi request berubah.
- Follow redirects: membuat Burp mengikuti redirect dan menampilkan halaman akhirnya.
- Process cookies in redirects: membantu mengelola cookie saat terjadi redirect.
- Tab management: Anda bisa membuat, mengganti nama, atau menghapus tab untuk memisahkan percobaan.

Repeater juga berguna untuk membuat proof of concept pada beberapa jenis serangan, misalnya CSRF. Dengan cara ini, penguji bisa membuat contoh eksploitasi sederhana untuk menunjukkan dampak masalah secara lebih jelas.

Kapan Repeater dipakai? Gunakan Repeater saat Anda sudah menemukan request menarik dan ingin menyelidikinya secara manual, perlahan, dan terkontrol.

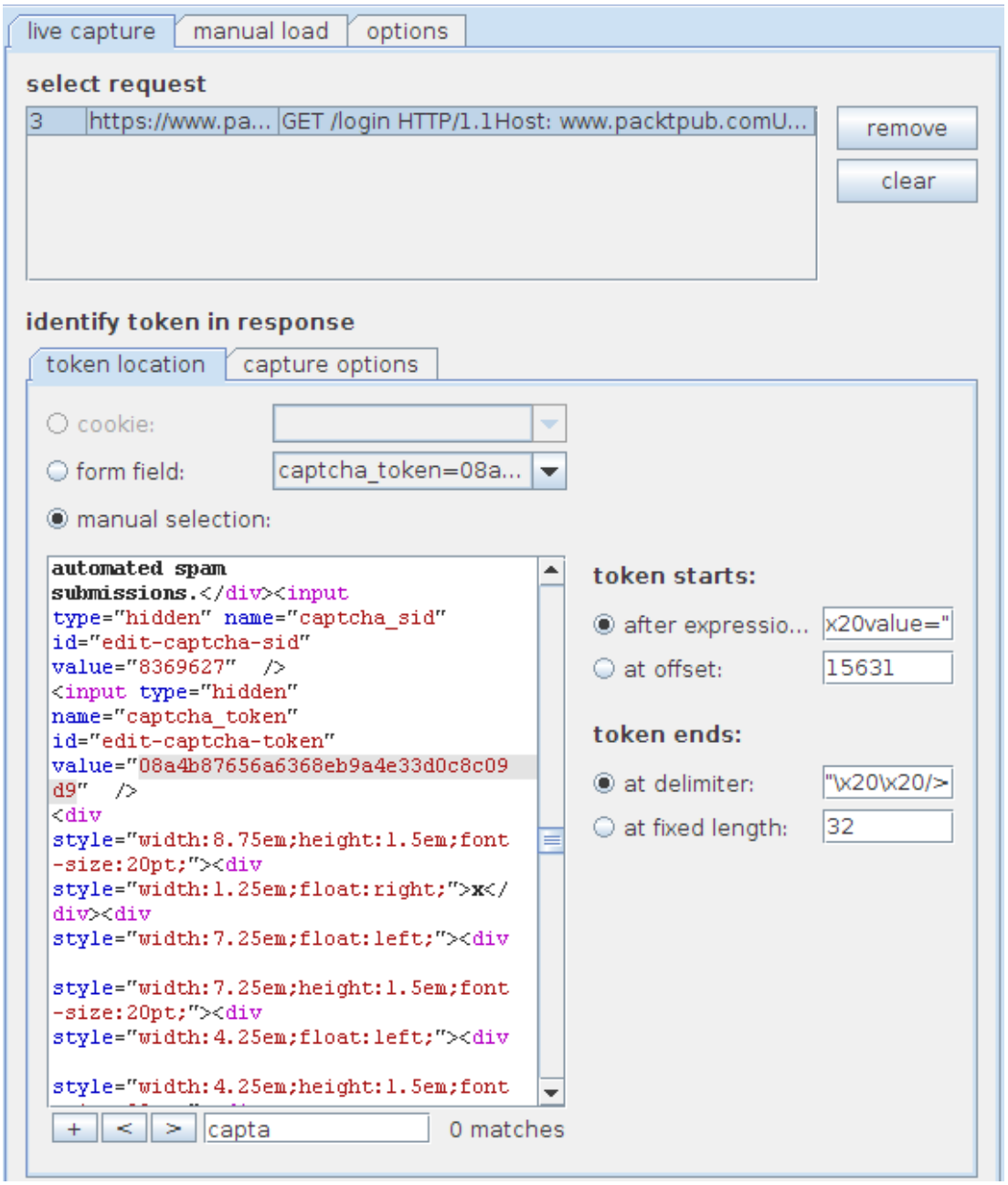
6. Menganalisis Keacakan Data dengan Burp Sequencer

Burp Sequencer dipakai untuk menilai apakah data tertentu—terutama token sesi atau token anti-CSRF—cukup acak atau justru mudah ditebak. Jika token terlalu mudah diprediksi, keamanan aplikasi bisa lemah karena penyerang berpotensi menebak token milik pengguna lain.

Konsep dasarnya sederhana: Burp mengambil banyak contoh token dari response aplikasi, lalu menganalisis kualitas keacakannya.

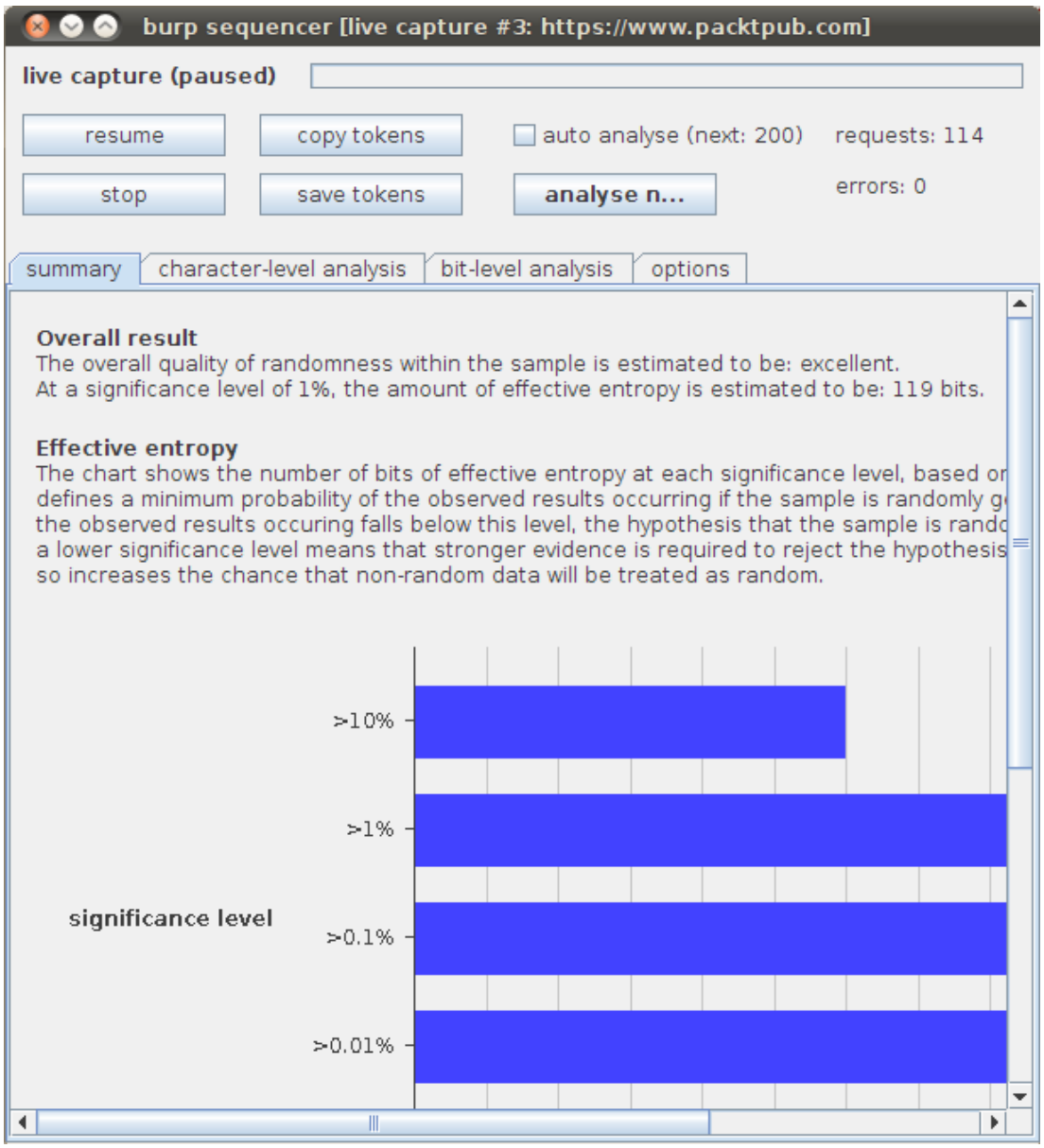
22. Arahkan browser ke aplikasi target melalui Burp Proxy.
23. Cari request yang relevan, misalnya halaman login yang memunculkan token.
24. Klik kanan request tersebut lalu pilih send to sequencer.

25. Di Sequencer, tentukan token mana yang ingin dianalisis. Token bisa dipilih dari cookie, form field, atau ditandai manual dari response.
26. Mulai pengambilan sampel. Burp akan mengulang request dan mengumpulkan banyak token.



Gambar 15. Menentukan token yang akan dianalisis dengan Burp Sequencer.

Setelah sampel cukup banyak—biasanya minimal sekitar seratus—analisis dapat dijalankan. Hasilnya akan menunjukkan penilaian umum terhadap kualitas keacakan token tersebut.



Gambar 16. Contoh tampilan hasil analisis pada Burp Sequencer.

- Summary tab: memberi penilaian umum, misalnya excellent atau extremely poor.
- Character-level analysis: melihat pola karakter dalam token.
- Bit-level analysis: melihat tingkat keacakan sampai level bit.

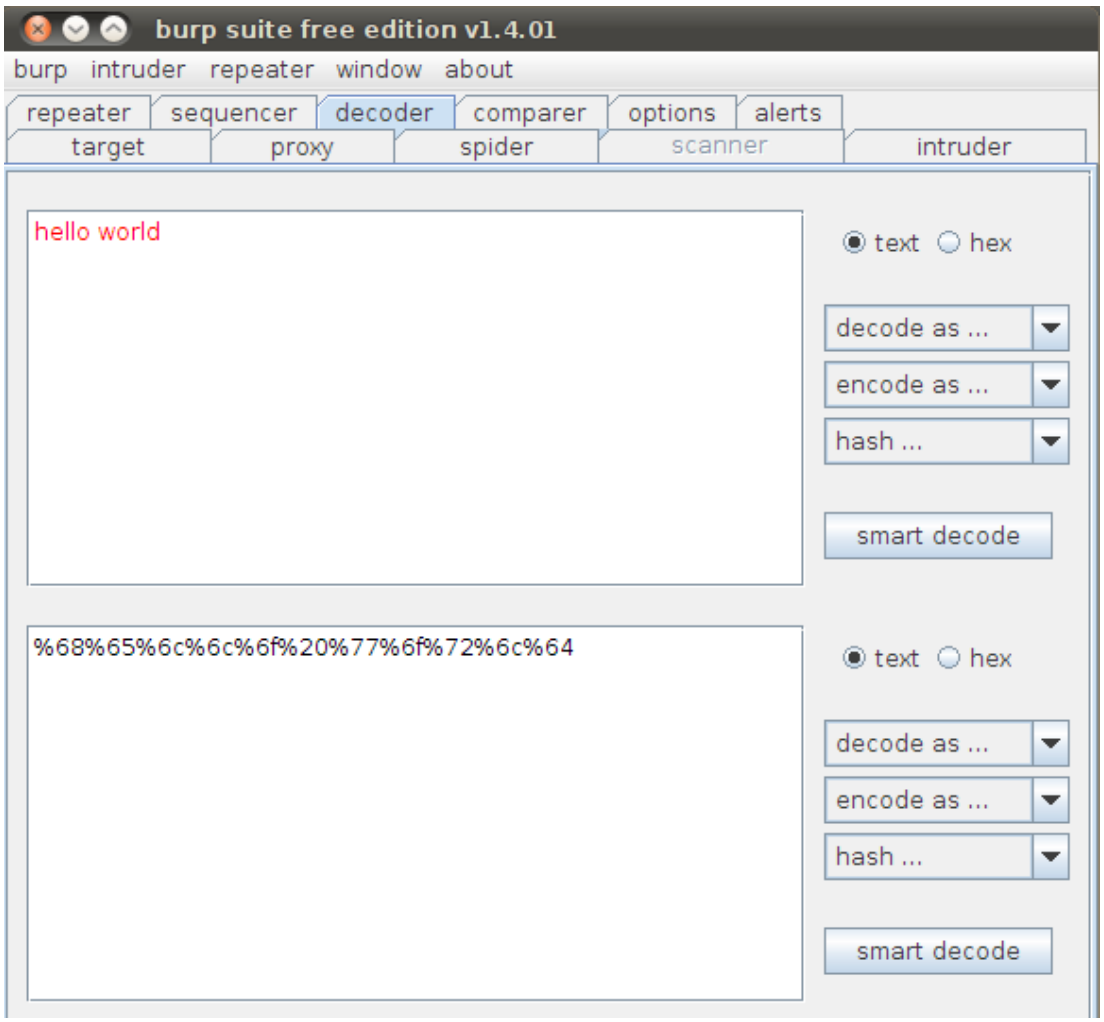
Hal yang perlu diingat: Hasil Sequencer sangat membantu, tetapi bukan satu-satunya penentu. Untuk kasus penting, hasil otomatis tetap perlu ditinjau dengan pemahaman teknis yang baik.

7. Melakukan Encode dan Decode dengan Burp Decoder

Burp Decoder adalah tool kecil tetapi sering dipakai. Fungsinya untuk mengubah data dari satu format ke format lain. Dalam pengujian aplikasi web, hal ini penting karena data kadang dikirim dalam bentuk URL-encoded, Base64, hex, HTML entities, atau bahkan data terkompresi.

Dengan Decoder, penguji dapat memahami isi data yang terlihat aneh, menyusun payload dalam format tertentu, atau mencoba beberapa lapisan encoding untuk melihat apakah filter aplikasi bisa dilewati.

27. Pilih bagian string yang ingin diuji dari request atau response.
28. Klik kanan lalu pilih send to decoder.
29. Di tab Decoder, pilih apakah string ingin di-decode atau di-encode.
30. Lihat hasilnya pada panel output.



Gambar 17. Tampilan Burp Decoder untuk proses encode dan decode.

- Format umum yang didukung: URL encoding, HTML entities, Base64, hex, dan GZIP.
- Decoder juga bisa membuat hash seperti MD5, SHA, SHA-256, dan SHA-512.
- Fitur smart decode mencoba menebak format data secara otomatis.

Keluaran dari satu proses bisa langsung dipakai sebagai input ke proses berikutnya. Artinya, Anda bisa melakukan decode berlapis jika data memang melewati beberapa tahapan encoding.

8. Membandingkan Dua Site Map

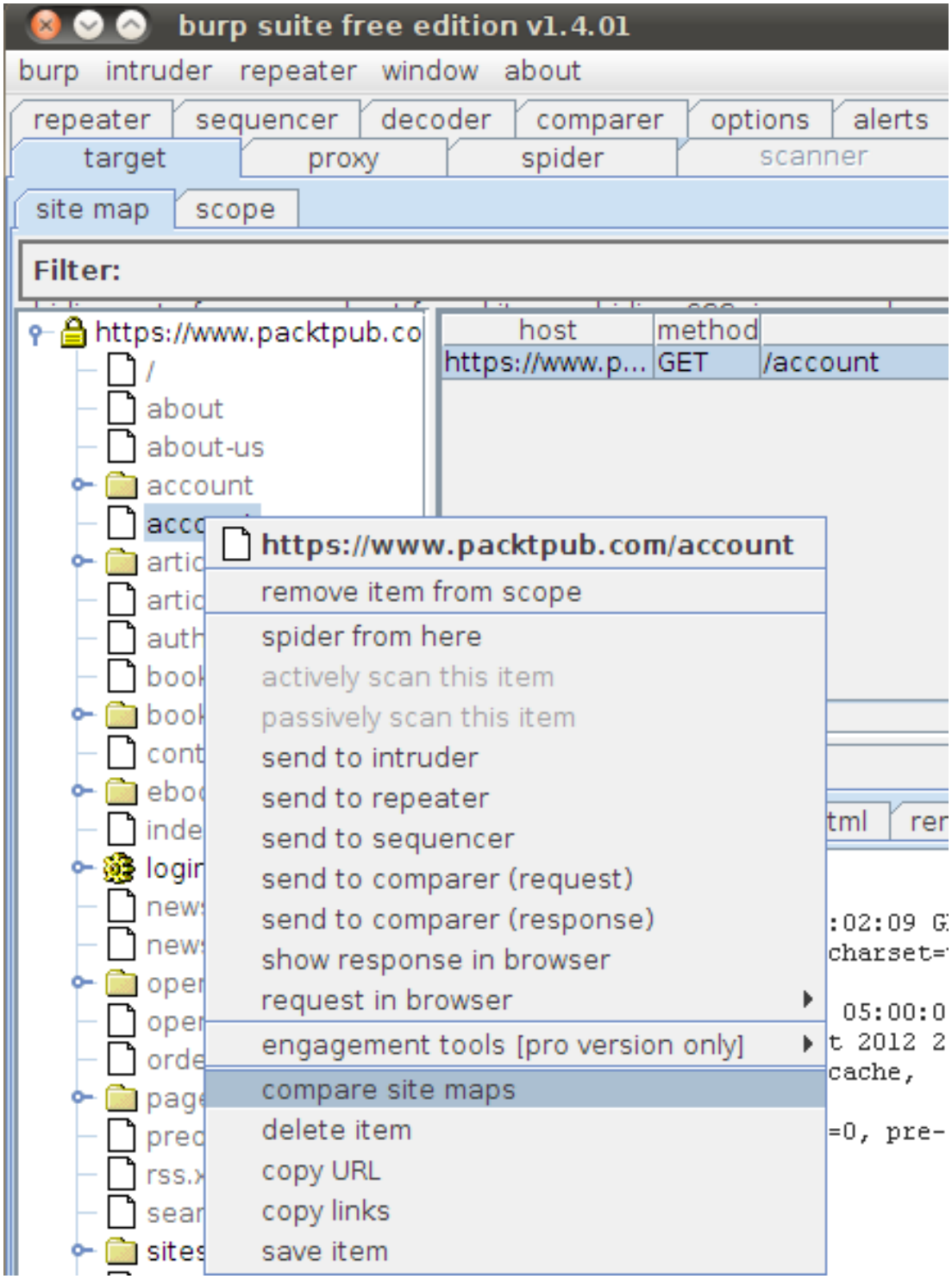
Fitur compare site maps berguna untuk menemukan perbedaan akses atau perbedaan respons antara dua kondisi. Contoh paling umum adalah membandingkan apa yang terlihat oleh pengguna biasa dengan apa yang terlihat oleh admin, atau membandingkan pengguna yang sudah login dengan pengguna yang belum login.

Pendekatan ini sangat berguna untuk menguji access control. Dengan kata lain, kita ingin tahu apakah ada halaman yang seharusnya tidak bisa diakses, tetapi ternyata tetap terbuka untuk pengguna yang salah.

Skenario penggunaan yang umum

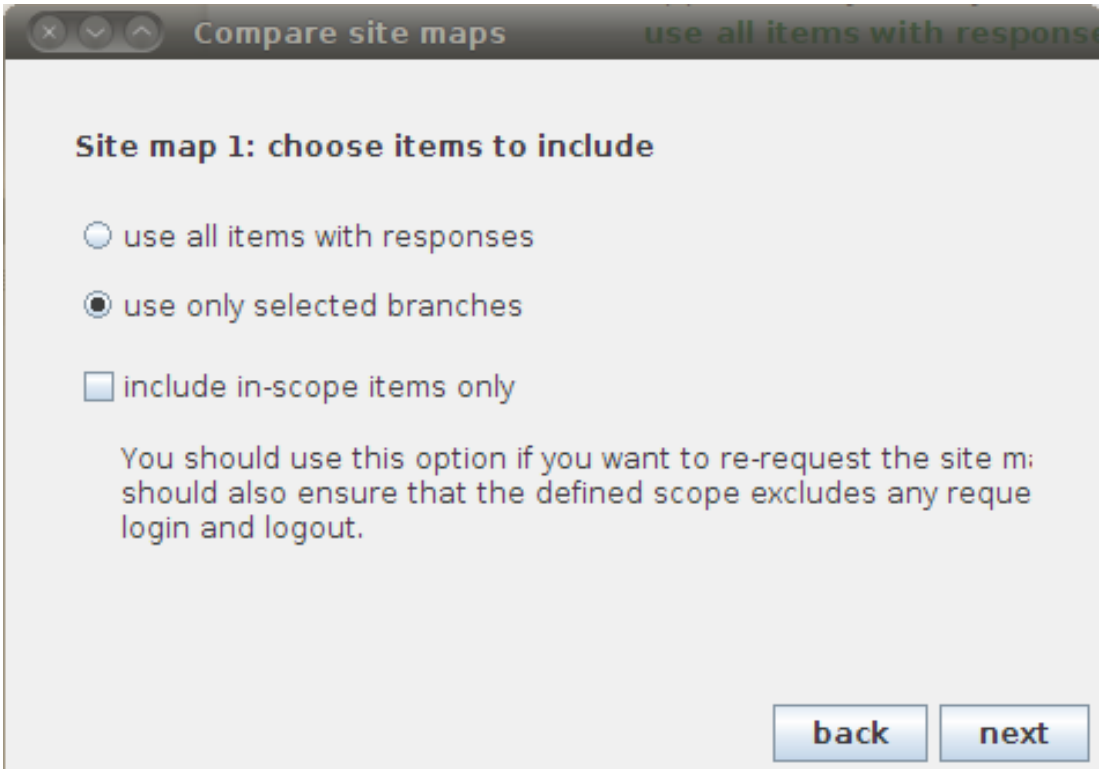
- Membandingkan sesi login dan non-login untuk melihat halaman yang seharusnya hanya muncul setelah autentikasi.
- Membandingkan dua pengguna dengan level yang sama untuk mencari kebocoran akses horizontal.
- Membandingkan user biasa dengan admin untuk mencari kenaikan hak akses vertikal.

31. Rekam dahulu resource yang ingin dijadikan pembanding pada site map pertama.
32. Dari Target Site Map, pilih endpoint terkait lalu klik kanan dan pilih compare site maps.



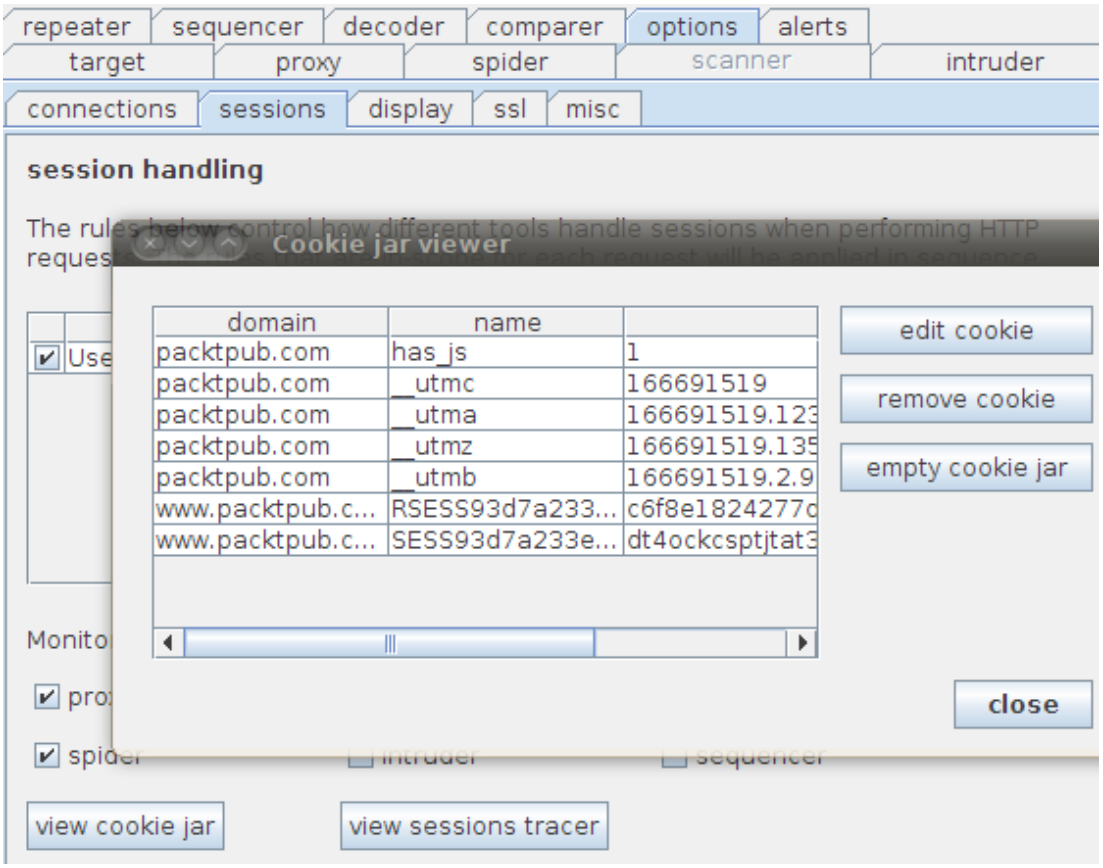
Gambar 18. Menjalankan fitur Compare Site Maps dari menu Target.

33. Pilih sumber site map pertama sebagai baseline.
34. Tentukan apakah ingin membandingkan semua item atau hanya cabang yang dipilih.



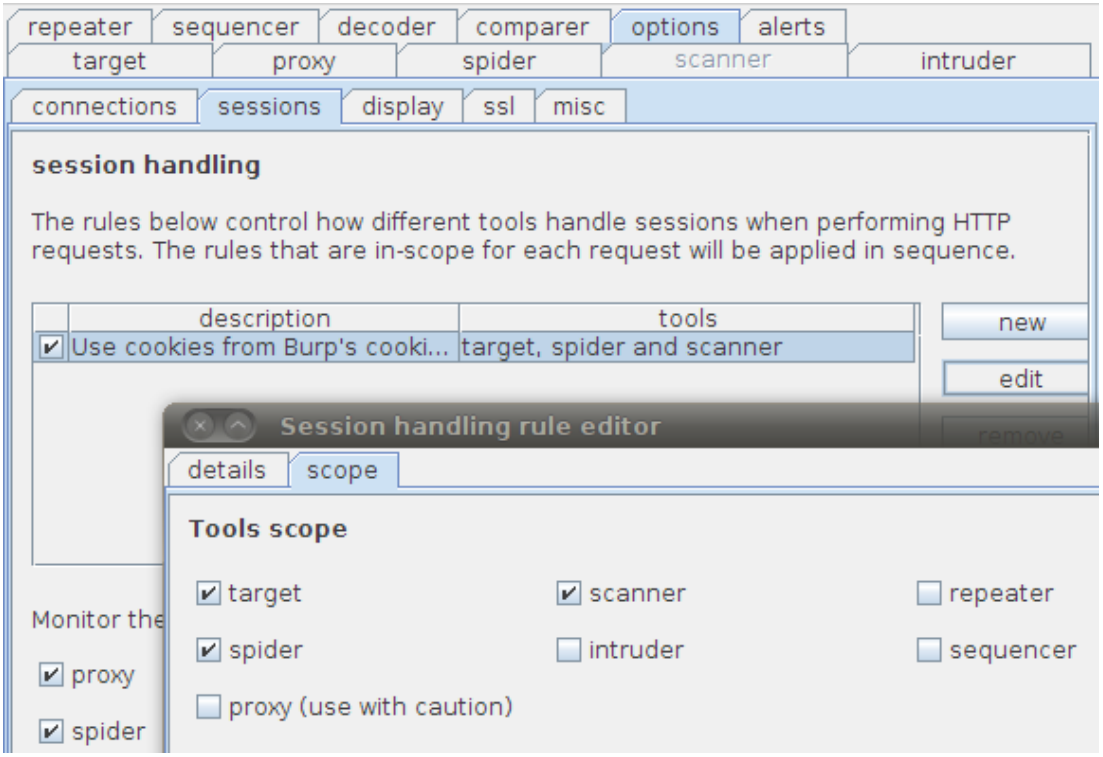
Gambar 19. Menentukan item yang dimasukkan ke dalam proses perbandingan.

Jika ingin membandingkan kondisi login dan non-login, maka sesi yang dipakai untuk site map kedua harus diubah. Pada contoh buku, cookie pada cookie jar dimodifikasi agar mensimulasikan kondisi pengguna yang tidak lagi terautentikasi.



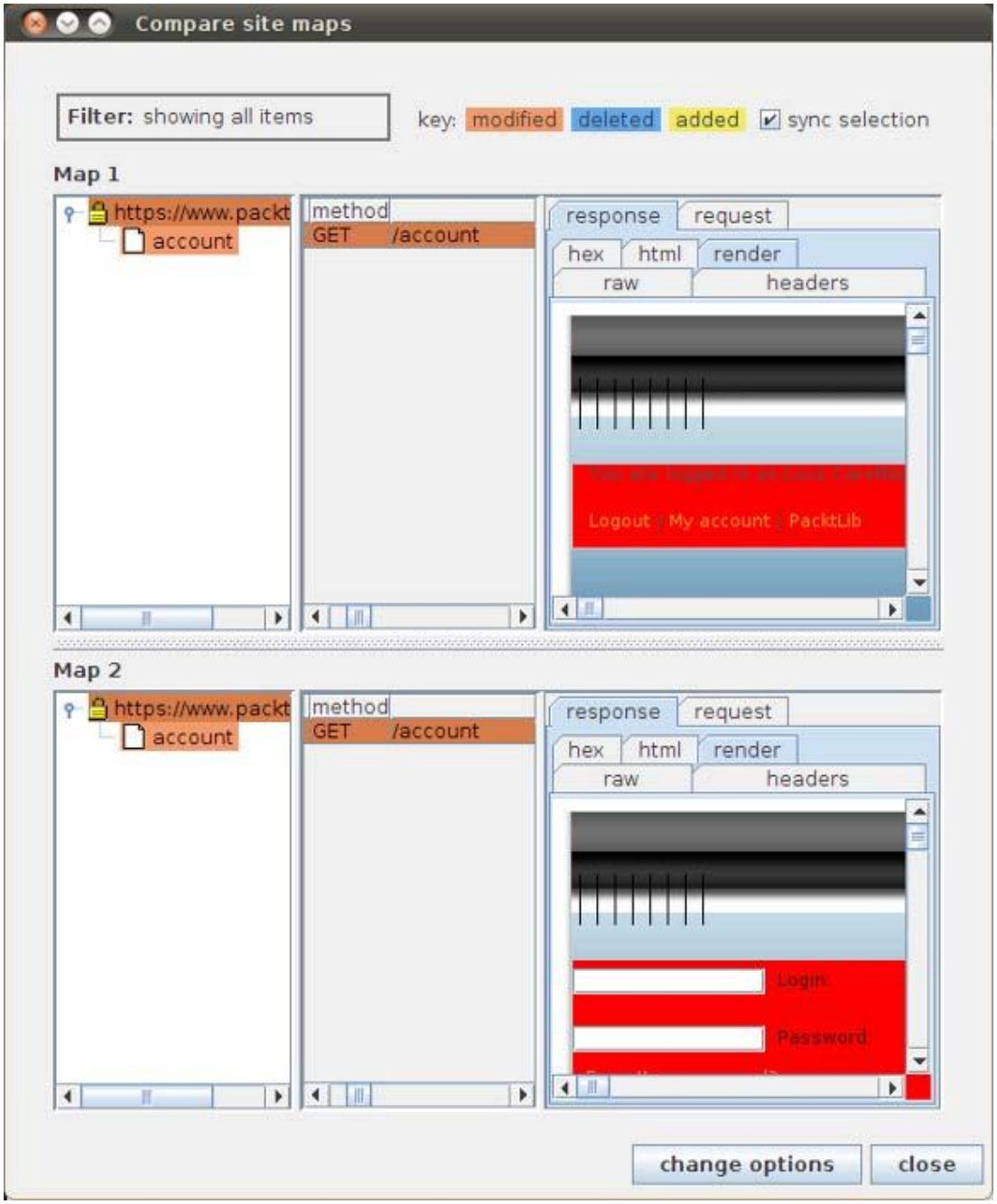
Gambar 20. Cookie jar Burp yang dipakai untuk mengelola sesi.

Setelah itu, aturan session handling juga perlu diarahkan agar proses compare memakai konteks sesi yang sudah diubah tadi.



Gambar 21. Pengaturan session handling rule untuk proses perbandingan.

Saat perbandingan selesai, Burp akan menampilkan dua panel yang bisa disinkronkan. Dari sini, Anda bisa melihat apakah sebuah endpoint memberikan respons yang berbeda pada dua kondisi yang dibandingkan.



Gambar 22. Contoh hasil Compare Site Maps yang menunjukkan perbedaan respons.

Cara membaca hasil: Fokuslah pada resource yang bertambah, hilang, atau responsnya berubah secara signifikan. Perbedaan kecil kadang hanya berasal dari token sekali pakai atau elemen halaman yang dinamis.

Penutup

Delapan fitur pada bab ini menunjukkan bahwa Burp Suite bukan hanya proxy untuk menangkap request, tetapi juga sebuah rangkaian tool yang saling terhubung. Site Map membantu memahami aplikasi, Spider membantu menemukan resource, Scanner membantu mencari celah umum, Intruder dan Repeater membantu pengujian manual yang lebih dalam, Sequencer menilai token, Decoder membantu membaca data, dan Compare Site Maps membantu menguji kontrol akses.

Untuk pembaca pemula, kunci utamanya adalah memahami kapan sebuah tool dipakai. Tidak semua pengujian harus dimulai dengan serangan. Sering kali, langkah terbaik justru dimulai dari memetakan aplikasi dengan rapi, menetapkan scope dengan benar, lalu bergerak pelan dari pengamatan ke pengujian.

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