OWASP ZAP 2.3
Panduan Petunjuk Awal

Tinjauan

Dokumen ini dimaksudkan untuk melayani sebagai dasar pengenalan untuk menggunakan OWASP ini Zed Attack Proxy (ZAP) alat untuk melakukan pengujian keamanan, bahkan jika anda tidak memiliki latar belakang dalam pengujian keamanan. Untuk itu, beberapa pengujian keamanan konsep-konsep dan terminologi ini termasuk tetapi dokumen ini tidak dimaksudkan untuk menjadi panduan komprehensif untuk ZAP atau pengujian keamanan.

Jika Anda sudah familiar dengan keamanan atau penetrasi pengujian, Anda mungkin ingin memulai dengan Memperkenalkan ZAP .

Lihat Link yang berguna untuk sumber daya tambahan dan informasi tentang ZAP.

Keamanan pengujian dasar-dasar

Keamanan perangkat lunak pengujian adalah proses penilaian dan pengujian sistem untuk menemukan risiko keamanan dan kerentanan sistem dan data. Tidak ada yang universal terminologi tetapi untuk tujuan kita, kita mendefinisikan penilaian sebagai analisis dan penemuan ke-rentanan tanpa mencoba untuk benar-benar mengeksploitasi ke-rentanan mereka. Kita mendefinisikan pengujian sebagai penemuan dan percobaan eksploitasi dari kerentanan.

Pengujian keamanan sering pecah, agak sewenang-wenang, menurut salah satu jenis kerentanan yang diuji jenis pengujian yang dilakukan. Umum breakout adalah:

- **Kajian kerentanan** – Sistem ini scan dan dianalisis untuk masalah keamanan.
- **Pengujian penetrasi** -Sistem mengalami analisis dan serangan dari simulasi berbahaya penyerang.
- **Pengujian penetrasi** -Sistem mengalami analisis dan serangan dari simulasi berbahaya penyerang.
- **Tinjauan kode** -Kode sistem mengalami tinjauan rinci dan analisis secara khusus mencari kerentanan keamanan.

Perhatikan bahwa penilaian risiko, yang umumnya tercantum sebagai bagian dari pengujian keamanan, tidak termasuk dalam daftar ini. Itu karena penilaian risiko adalah tidak benar-benar menguji melainkan analisis persepsi keparahan risiko yang berbeda (perangkat lunak keamanan, personel keamanan, keamanan perangkat keras, dll.) dan setiap langkah-langkah untuk mitigasi risiko tersebut.

Lebih lanjut tentang pengujian penetrasi

Pengujian penetrasi (pentesting) dilakukan seolah-olah tester berbahaya eksternal penyerang dengan gol dari melanggar ke dalam sistem dan mencuri data atau melakukan beberapa jenis denial-of-service attack.

Kelonggaran memiliki keuntungan menjadi lebih akurat karena memiliki lebih sedikit positif palsu (hasil bahwa laporan kelonggaran yang tidak benar-benar hadir), tetapi dapat memakan waktu untuk menjalankan.

Pentesting ini juga digunakan untuk menguji pertahanan mekanisme, memverifikasi rencana tanggap, dan mengkonfirmasi kebijakan keamanan kepatuhan.

Otomatis pentesting adalah bagian penting dari integrasi berkesinambungan validasi. Hal ini membantu untuk mengungkap kerentanan baru serta regresi untuk sebelumnya kerentanan

dalam lingkungan yang cepat berubah, dan untuk yang pengembangan mungkin sangat kolaboratif dan didistribusikan.

Proses Pentesting

Baik manual dan otomatis pentesting digunakan, sering bersamaan, untuk menguji segala sesuatu dari server, jaringan, perangkat, untuk endpoint. Dokumen ini berfokus pada aplikasi web atau situs web pentesting.

Pentesting biasanya mengikuti tahap-tahap ini:

- **Jelajahi** -Tester upaya untuk belajar tentang sistem yang sedang diuji. Ini termasuk mencoba untuk menentukan software apa yang digunakan, apa yang endpoint ada, apa patch diinstal dan lain lain. Hal ini juga termasuk mencari situs untuk konten tersembunyi, yang dikenal kerentanan, dan indikasi lain dari kelemahan.
- **Serangan** -Tester upaya untuk mengeksploitasi kerentanan pelanggaran atau dugaan untuk membuktikan mereka ada.
- **Laporan** -Tester melaporkan kembali hasil pengujian mereka, termasuk kerentanan, bagaimana mereka dimanfaatkan mereka dan betapa sulitnya eksploitasi, dan keparahan dari eksploitasi.

Pentesting tujuan

Tujuan akhir dari pentesting adalah untuk mencari kerentanan sehingga kelemahan ini dapat diatasi. Hal ini juga dapat memverifikasi bahwa sistem ini tidak rentan untuk diketahui kelas atau cacat tertentu; atau, dalam kasus kerentanan yang telah dilaporkan sebagai tetap, memverifikasi bahwa sistem ini tidak lagi rentan untuk yang cacat.

Memperkenalkan ZAP

Zed serangan Proxy (ZAP) adalah gratis, open source penetrasi pengujian alat yang dipelihara di bawah payung dari membuka Web aplikasi keamanan proyek (OWASP). ZAP ini dirancang khusus untuk pengujian aplikasi web dan fleksibel dan extensible.

Pada intinya, ZAP adalah apa yang dikenal sebagai "manusia-di-the-tengah proxy." Ini berdiri antara tester browser dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang dikirim antara browser dan aplikasi web, memodifikasi isi jika diperlukan, dan kemudian meneruskan paket-paketnya mereka ke tujuan. Aku t dapat digunakan sebagai aplikasi yang berdiri sendiri, dan sebagai proses daemon.

Jika ada jaringan lain proxy yang sudah di gunakan, seperti di banyak lingkungan perusahaan, ZAP dapat dikonfigurasi untuk terhubung ke proxy.

ZAP menyediakan fungsi untuk berbagai macam tingkat keahlian – dari pengembang, ke penguji baru untuk keamanan pengujian, pengujian spesialis keamanan. ZAP memiliki versi untuk setiap OS utama dan Docker, sehingga Anda tidak terikat dengan OS yang tunggal. Fungsi tambahan yang tersedia secara bebas dari berbagai add-ons pada ZAP Pasar, dapat diakses dari dalam ZAP klien.

Karena ZAP adalah open-source, source code dapat diperiksa untuk melihat persis bagaimana fungsi tersebut dilaksanakan. Siapa pun bisa menjadi sukarelawan untuk bekerja di ZAP, memperbaiki bug, menambahkan fitur, membuat permintaan tarik untuk menarik perbaikan ke proyek, dan penulis add-ons untuk dukungan berupa situasi.

Untuk informasi lebih lanjut, lihat Zed serangan Proxy halaman proyek .

Seperti kebanyakan proyek open source, sumbangan yang diterima untuk membantu dengan biaya untuk proyek-proyek. Anda dapat menemukan tombol donate di halaman owasp.org untuk ZAP di https://www.owasp.org/index.php/ZAP .

Menginstal dan mengkonfigurasi ZAP

ZAP memiliki installer untuk Windows, Linux dan Mac OS / X. Ada yang juga Docker gambar s tersedia pada situs download tercantum di bawah ini.

Memperkenalkan ZAP

Hal pertama yang harus lakukan adalah menginstal ZAP pada sistem Anda berniat untuk melakukan pentesting. Download installer sesuai dari ZAP's lokasi download di https://github.com/zaproxy/zaproxy/wiki/Downloads dan menjalankan installer.

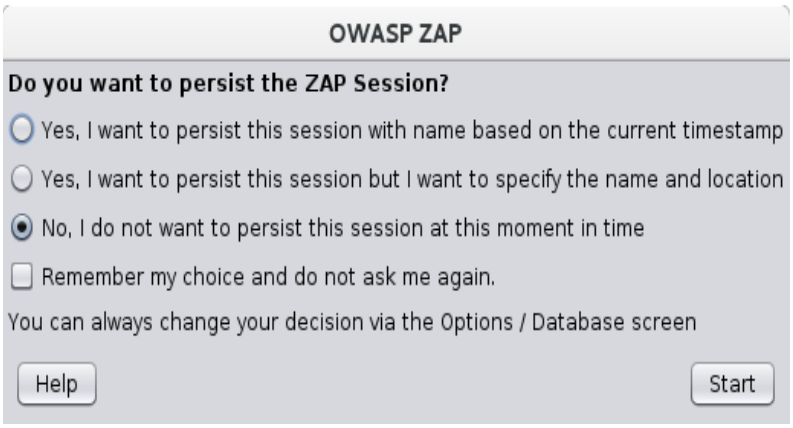
Catatan bahwa ZAP memerlukan Java 8 + untuk menjalankan. Mac OS / X installer mencakup versi yang sesuai dari Jawa, namun Anda harus menginstal Java 8 + secara terpisah untuk versi Windows, Linux, dan Cross-Platform. Versi Docker s tidak mengharuskan Anda untuk menginstal Java.

Setelah instalasi selesai, peluncuran ZAP dan baca ketentuan lisensi. Klik **setuju** jika Anda menyetujui persyaratan, dan ZAP akan selesai menginstal, maka secara otomatis akan mulai ZAP.

Pentesting tujuan

Ketika Anda pertama kali ZAP, Anda akan diminta jika Anda ingin bertahan ZAP sesi. Secara default, ZAP sesi selalu dicatat ke disk dalam database HSQLDB dengan nama default dan lokasi. Jika Anda tidak bertahan sidang, file-file tersebut akan dihapus ketika Anda keluar ZAP.

Jika Anda memilih untuk bertahan sesi, sesi informasi akan disimpan dalam database lokal sehingga Anda dapat mengaksesnya kemudian, dan Anda akan mampu memberikan kustom nama dan lokasi untuk menyimpan file.

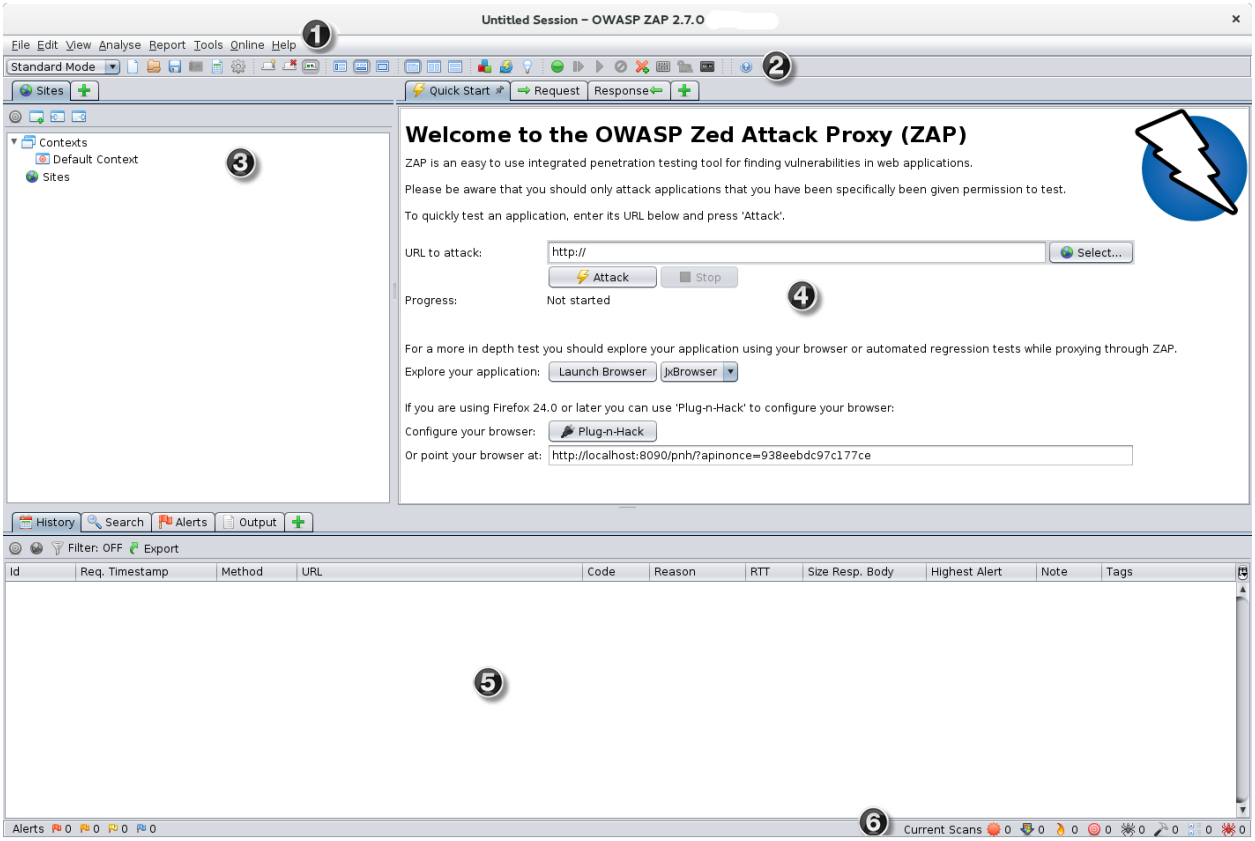


Untuk saat ini, pilih **tidak, saya tidak ingin untuk bertahan sesi ini pada saat ini dalam waktu** kemudian klik **mulai** . ZAP sesi tidak akan bertahan untuk sekarang.

ZAP UI

ZAP UI terdiri dari unsur-unsur berikut:

1. **Menu Bar** -Menyediakan akses ke banyak alat-alat otomatis dan manual.
2. **Toolbar** -Termasuk tombol yang menyediakan akses mudah ke sebagian besar fitur yang umum digunakan.
3. **Pohon jendela** – Menampilkan situs pohon dan pohon skrip.
4. **Jendela ruang kerja** -Menampilkan permintaan, tanggapan, dan skrip dan memungkinkan Anda untuk mengedit mereka.
5. **Informasi jendela** – Menampilkan rincian alat otomatis dan manual.
6. **Footer** – Menampilkan ringkasan tanda yang ditemukan dan status otomatis alat utama.



Saat menggunakan ZAP, Anda dapat klik **Membantu** pada Menu Bar atau Tekan F1 untuk mengakses context-sensitive membantu dari panduan pengguna ZAP.

Untuk informasi lebih lanjut tentang UI, lihat ZAP UI Gambaran di ZAP dokumentasi online.

ZAP juga mendukung API yang kuat dan perintah baris fungsi, keduanya berada di luar cakupan dari panduan ini.

Meluncurkan browser

Anda dapat dengan cepat dan mudah meluncurkan browser yang pra-dikonfigurasi untuk proxy melalui ZAP melalui Cepat Mulai tab. Browser yang diluncurkan pada cara ini juga akan mengabaikan validasi sertifikat peringatan yang seharusnya dilaporkan.

Ini pilihan akan meluncurkan salah satu browser yang paling umum yang telah Anda instal dengan profil baru.

Jika anda ingin menggunakan salah satu browser anda dengan profil yang ada, misalnya dengan browser lain add-ons yang terinstal, maka anda akan perlu untuk secara manual mengkonfigurasi browser anda untuk proxy via ZAP dan impor dan mempercayai ZAP Root CA Sertifikat. Lihat ZAP panduan pengguna untuk lebih jelasnya.

Cobalah untuk menghubungkan aplikasi Web Anda

Setelah Anda memiliki berhasil mendirikan Anda browser untuk menggunakan ZAP sebagai kuasa, mencoba untuk terhubung ke aplikasi web Anda akan menguji.

Jika anda dapat mencapai aplikasi web anda, periksa hal-hal berikut:

1. Memverifikasi pengaturan proxy browser menggunakan untuk terhubung ke ZAP.
2. Memverifikasi pengaturan proxy browser menggunakan untuk terhubung ke ZAP.
3. Verifikasi aplikasi web yang anda inginkan untuk menguji berjalan.
4. Periksa untuk melihat apakah jaringan anda membutuhkan proxy untuk mencapai aplikasi web anda. Jika demikian, anda mungkin perlu mengkonfigurasi ZAP untuk menggunakan proxy.

Untuk mengkonfigurasi ZAP untuk menggunakan aplikasi yang keluar proxy:

1. Mulai ZAP dan pada bilah Menu, klik **Alat** -> **Pilihan** .
2. Pilih **Koneksi** dalam pane kiri.
3. Di **menggunakan proxy Jaringan** Bagian **Koneksi** pengaturan, periksa **Gunakan kotak centang server proxy keluar** .
4. Enter **Nama alamat Domain** dan **Port** untuk Anda jaringan proxy.
5. Klik **OK** untuk menyimpan pengaturan dan memverifikasi bahwa Anda sekarang dapat terhubung ke aplikasi web Anda.

Setelah browser Anda dapat berhasil tersambung ke aplikasi web Anda, Anda siap untuk menjalankan tes.

Proses Pentesting

Cara termudah untuk mulai menggunakan ZAP adalah untuk menjalankan Quick Start test. Quick Start adalah ZAP add-on yang dipasang secara otomatis ketika anda menginstal ZAP.

PENTING: Anda hanya harus menggunakan ZAP untuk menyerang aplikasi anda memiliki izin untuk tes dengan serangan aktif. Karena ini adalah simulasi yang bertindak seperti real serangan, kerusakan yang sebenarnya dapat dilakukan untuk fungsionalitas situs, data, dan lain lain. Jika anda khawatir tentang menggunakan ZAP, anda dapat mencegah hal itu menyebabkan kerugian (meskipun ZAP fungsi akan berkurang secara signifikan) dengan beralih ke mode aman.

Untuk beralih ZAP ke mode aman, klik tanda panah pada mode dropdown pada toolbar utama untuk memperluas daftar dropdown dan pilih **Safe Mode**.

Menjalankan Cepat Mulai Tes

Untuk menjalankan tes cepat mulai:

1. Mulai ZAP dan klik **Cepat mulai** tab jendela Workspace.
2. Di **URL untuk menyerang** teks kotak, masukkan URL lengkap aplikasi web yang ingin menyerang.
3. Klik **Menyerang** tombol.

ZAP akan melanjutkan untuk merangkak aplikasi web dengan laba-laba, kemudian secara pasif scan setiap halaman yang ditemukan. Kemudian ZAP akan menggunakan active scanner untuk menyerang semua menemukan halaman, fungsi, dan parameter.

Menafsirkan Hasil Tes Anda

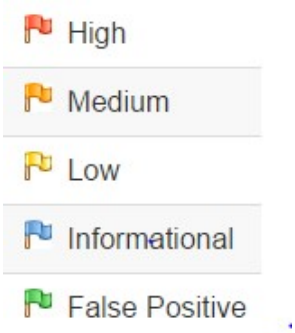
Sebagai ZAP laba-laba aplikasi web anda, itu akan membuat peta dari aplikasi web anda' pages dan sumber daya yang digunakan untuk membuat halaman-halaman tersebut. Maka rekaman permintaan dan tanggapan yang dikirim ke masing-masing halaman dan membuat peringatan jika ada sesuatu yang berpotensi salah dengan permintaan atau respon.

Melihat Dieksplorasi Halaman

Untuk memeriksa tampilan pohon dari dieksplorasi halaman, klik **Situs** tab di Jendela Pohon. Anda dapat memperluas simpul untuk melihat masing-masing Url yang diakses.

Lihat Peringatan dan Waspada Detail

Sisi kiri Footer berisi hitungan Peringatan yang ditemukan selama tes anda, yang dikelompokkan ke dalam kategori risiko. Ini kategori risiko adalah:



Untuk melihat pemberitahuan yang dibuat selama tes anda:

1. Klik **Peringatan** tab dalam Jendela Informasi anda.
2. Klik setiap peringatan yang ditampilkan di jendela itu untuk menampilkan URL dan kerentanan terdeteksi di sisi kanan Jendela Informasi anda.
3. Dalam area Kerja Windows, klik **Respon** tab untuk melihat isi dari header dan body respon. Bagian dari respon yang dihasilkan waspada akan disorot.

Memperluas Pentesting dengan ZAP

Passive scanning dan otomatis menyerang fungsi adalah cara yang bagus untuk memulai penilaian kerentanan aplikasi web anda tetapi memiliki beberapa keterbatasan. Di antaranya adalah:

- Setiap halaman yang dilindungi dengan login halaman tidak dapat ditemukan selama pasif scan karena, kecuali jika anda telah dikonfigurasi ZAP otentikasi fungsi, ZAP tidak akan menangani autentikasi yang diperlukan.
- Setiap halaman yang tidak dapat ditemukan dengan ZAP default laba-laba tidak dapat diuji selama pasif scan. ZAP tidak memberikan opsi tambahan untuk penemuan dan cakupan luar passive scanning.
- Anda tidak memiliki banyak kontrol atas urutan eksplorasi secara pasif scan atau jenis serangan yang dilakukan secara otomatis menyerang. ZAP tidak memberikan banyak opsi tambahan untuk eksplorasi dan serangan luar passive scanning.

Mengkonfigurasi dan Menjalankan laba-Laba dengan ZAP

Salah satu cara untuk memperluas dan meningkatkan pengujian adalah untuk mengubah laba-laba ZAP menggunakan untuk mengeksplorasi aplikasi web anda. Quick Scan menggunakan tradisional ZAP laba-laba, yang menemukan link dengan memeriksa HTML dalam tanggapan dari aplikasi web. Laba-laba ini lebih cepat, tapi hal ini tidak selalu efektif ketika menjelajahi sebuah web AJAX aplikasi yang menghasilkan link menggunakan JavaScript.

Untuk aplikasi AJAX, ZAP AJAX laba-laba mungkin akan lebih efektif. Laba-laba ini mengeksplorasi aplikasi web dengan menerapkan browser yang kemudian mengikuti link yang telah dihasilkan. AJAX laba-laba lebih lambat dari yang tradisional laba-laba dan membutuhkan konfigurasi tambahan untuk digunakan dalam "headless" lingkungan.

Cara sederhana untuk beralih bolak-balik antara laba-laba adalah untuk mengaktifkan tab untuk setiap laba-laba dalam Jendela Informasi dan menggunakan tab untuk memulai scan.

1. Dalam Jendela Informasi anda, klik tanda plus hijau (**+**).
2. Klik **Spider** untuk membuat laba-Laba tab.
3. Ulangi langkah 1, kemudian klik **AJAX Spider** untuk membuat **AJAX Spider** tab.

4. Click the push-pin symbol on both the **Spider** and **AJAX Spider** tabs to pin them to the Information Window.

Perhatikan bahwa kedua tab ini mencakup **New Scan** tombol.

Menjelajahi Situs Anda

Laba-laba adalah cara yang bagus untuk menjelajahi dasar anda, tetapi mereka harus dikombinasikan dengan panduan eksplorasi menjadi lebih efektif. Laba-laba, misalnya, hanya akan memasukkan standar dasar data ke dalam bentuk aplikasi web anda, tetapi pengguna dapat memasukkan informasi yang lebih relevan yang dapat, pada gilirannya, mengekspos lebih dari aplikasi web untuk ZAP. Hal ini terutama berlaku dengan hal-hal seperti formulir pendaftaran di mana alamat email yang valid diperlukan. Laba-laba dapat memasukkan string acak, yang akan menyebabkan kesalahan. Pengguna akan dapat bereaksi terhadap kesalahan itu dan pasokan di hapus dengan benar string, yang dapat menyebabkan lebih banyak dari aplikasi yang akan terkena ketika formulir dikirimkan dan diterima.

Karena anda telah mengkonfigurasi browser anda untuk menggunakan ZAP sebagai proxy, anda harus memulai semua dari aplikasi web anda dengan browser tersebut. Ketika anda melakukan ini, ZAP pasif scan semua permintaan dan tanggapan yang dilakukan selama eksplorasi anda untuk kerentanan, terus membangun situs pohon, dan catatan peringatan untuk potensi kerentanan yang ditemukan selama eksplorasi.

Hal ini penting untuk memiliki ZAP jelajahi setiap halaman aplikasi web anda, apakah terhubung ke halaman lain atau tidak, untuk kerentanan. Ketidakjelasan ini tidak keamanan, dan tersembunyi halaman kadang-kadang pergi hidup tanpa peringatan atau pemberitahuan. Jadi seperti yang menyeluruh seperti yang anda dapat ketika anda menjelajahi situs anda.

Menjalankan Active Scan dengan ZAP

Sejauh ini ZAP telah dilakukan pasif scan aplikasi web anda. Passive scanning tidak respon perubahan dalam cara apapun dan dianggap aman. Pemindaian ini juga dilakukan di latar belakang benang untuk tidak memperlambat eksplorasi. Passive scanning lebih baik menemukan beberapa kerentanan dan sebagai cara untuk mendapatkan merasa untuk dasar negara keamanan aplikasi web dan menemukan di mana penyelidikan lebih lanjut mungkin diperlukan.

Active scanning, namun, upaya untuk menemukan kerentanan lainnya dengan menggunakan dikenal serangan terhadap target yang dipilih. Active scanning adalah serangan nyata pada target dan dapat menempatkan target pada risiko, sehingga tidak menggunakan active scanning terhadap target anda tidak memiliki izin untuk tes.

Untuk mulai aktif scan:

1. Dalam Tampilan struktur Pohon, di **Situs** tab, pilih situs yang anda inginkan untuk melakukan pemindaian aktif.
2. klik Kanan pada situs yang dipilih dan pilih **Active Scan**.

atau

1. Dalam Jendela Informasi anda, pilih **Active Scan** tab.
2. Klik **Scan Baru**.

Untuk meninjau dan mengubah pengaturan anda, kemudian mulai aktif scan:

1. Pada Menu Bar, klik **alat-Alat** -> **Active Scan**.

2. Meninjau pengaturan dan membuat perubahan yang anda inginkan.
3. Klik **Mulai memindai** untuk mulai aktif Scan dengan pengaturan ini.

Anda dapat memeriksa hasil Anda aktif scan dengan cara yang sama Anda memeriksa hasil scan Anda pasif, seperti yang ditunjukkan dalam Menginterpretasikan hasil tes Anda .

Pelajari lebih lanjut tentang ZAP

Sekarang bahwa Anda sudah familiar dengan beberapa kemampuan dasar dari ZAP, Anda dapat mempelajari lebih lanjut tentang ZAP's kemampuan dan bagaimana menggunakannya dari ZAP's Panduan pengguna . Panduan Pengguna memberikan langkah-demi-langkah petunjuk, referensi untuk API dan baris perintah pemrograman, video instruksi, dan tips dan trik untuk menggunakan ZAP.

Di Link Yang Berguna

OWASP Zed Attack Proxy Proyek – ZAP utama halaman proyek

OWASP ZAP Wiki – ZAP Wiki

OWASP ZAP Panduan Pengguna - ZAP Panduan Pengguna

OWASP ZAP Hot Keys - daftar ZAP hotkeys

ZAP Grup Pengguna – grup Google untuk pengguna ZAP

ZAP Pengembang Group – grup Google untuk pengembang dan kontributor untuk ZAP