# OWASP ZAP 2.7
# Gabay sa pagsisimula

## Overview

Ang dokumentong ito ay itinatabi upang tumayo bilang isang pangunahing pagpapakilala sa paggamit ng kasangkapan ng Zed Attack Proxy (ZAP) ng OWASP upang maisagawa ang pagsusuri sa kaligtasan, kahit na wala kang background sa pagsusuri sa kaligtasan. Upang tapusin iyon, Ang mga konsepto ng kaligtasan sa pagsubok at terminolohiya ay kasama subalit ang dokumentong ito ay hindi itinatabi upang maging isang kumpletong gabay sa anoman sa ZAP o pagsubok ng kaligtasan.

kapag pamilyar ka sa kaligtasan o pagsubok ng pagtagos, ikaw ay maaring magsimula Ipinapakilala ang ZAP.

See Useful Links para sa karagdagang mga pagkukunan at mga impormasyon ng ZAP.

## Security Testing Basics

Ang pagsubok ng seguridad ng Software ay proseso ng pag assess at pag subok ng sistema nang ma diskobre ng pagsusuri ng seguridad at mga kahinaan ng sistema at kanyang mga datos. Walang pangakalawakan o pangkalahatang terminolohiya pero para sa ating mga layunin, tinutukoy natin ang pag tasa bilang pag analisa at pag diskobre sa mga kahinaan ng walang sinusubukan sa aktwal na pagsasamantala sa mga kahinaan. Tinanggap natin na ang pag subok ay isang pag diskobre at pag tangka sa pagtangka sa mga kahinaan.

Ang seguridad ng pag subok ay madalas ng nasisira sa labas, medyo arbitrarily, ayon sa tipo ng kahinaan at nasubukan na o ang tipo ng pag subok na natapos na. ang mga karaniwan na breakout ay:

- **Vulnerability Assessment** – Ang sistema ay na scan ang naanalisa na para sa seguridad ng mga issues.
- **Penetration Testing** – Ang sostema na sa ilalim ng mga nag aanalisa at mga atake ay galing sa pang gagaya ng malisyosong umaatake.
- **Runtime Testing** – Ang sistema ay nasa ilalim ng pag analisa ng seguridad ng pag subok galing sa huling gumagamit o user.
- **Code Review** – Ang sistema ng code ay na sa ilalim ng mga na review na detalye at ang pag analisa sa pag tingin ng specific na seguridad na kahinaan.

Tandaan na ang pagtatasa ng panganib, na karaniwang nakalista bilang bahagi ng pagsusuri ng seguridad, ay hindi kasama sa listahang ito. Ito ay dahil ang isang pagtatasa ng panganib ay hindi talaga isang pagsubok kundi ang pagtatasa ng pinaghihinalaan ng sari saring mga panganib (kaligtasan ng software, kaligtasan ng mga tauhan, kaligtasan ng hardware, atbp.) At alinmang mga hakbang sa pagpapagaan para sa mga panganib.

### Ang mga tungkol sa pagtagos ng testing

Ang Pagpasok ng pagsusuri (pentesting) ay isinasagawa na kung ang tagasuri ay isang panlabas na pag atake na nakakahamak na ang layuning sirain ang sistema at alinman sa pagnanakaw ng datos o sa ilang uri ng pagtangi sa atake ng serbisyo.

Pentesting ay may kalamangan sa pagiging tumpak o sakto dahil mayroon itong mas mababang antas ng maling positibo (ang mga resulta na nagsasabi ng isang kahinaan na pangkasalukuyan), ngunit maaaring makaubos ito ng oras para tumakbo.

Pentesting ay maari ring gamitin para subukan pagtatangol ang mekanismo, siyasatin ang plano ng pagtugon, at kumpirmahin ang patakarang pangseguridad na masunod.

Ang automated pentesting ay isang mahalagang bahagi ng patuloy na pagsasama sa mga balidasyon. Ito ay nakakatulong sa mga bagong panganib maging ang mga regresyon sa mga nakaraang panganib sa sa kapaligiran kung saan ay mabilis na nagbabago, at kung saan ang pag develop ay maaring mas mataas na colaborative at nadistribute.

### Ang pag proseso ng Prentesting

Parehong manwal at automated pentesting ay ginagamit, kadalasang kasabay. para sa pag subok ng lahat galing sa server, papuntang mga network sa mga devices hanggang sa endpoints. Ang dokyumentong ito ay nag fofocus sa mga web aplikasyon o sa website na pentesting.

Ang pentesting ay kalimitang sumusunod sa mga stages:

- **Explore** – Ang pag test ay pag pagtukso ng malaman ang tungkol sa sistema bilang mga nasubukan na. Kasama na rito ang pag subok ng malaman kung anong software ang ginamit, kung anong endpoints ang nag eexist, at kung anong mga patches ang na install, etc. Kasama rito ang pag hanap ng mga site sa mga nakatagong nilalaman, kilalang kahinaan, at iba pang mga indicators sa mga kahinaan.
- **Attack** – Ang tester na nag exploit ay kilala o pinaghinalaan na kahinaan para ma prove na ito nag eexist.
- **Report** – Ang balik ng ng mga pagsubok ng mga resulta sa mga testing, kasama ang mga kahinaan. kung paano pagsamantalahan ito at kung paano kahirap ang pagsasamantala nito, at gaano na kalubha ang pagiging mapagsamantala.

### Pentesting Goals

Ang pinaka-Goal ng pentesting ay para masuri ang mga kahinaan upang ang mga kahinaan ay matukoy. Natutukoy din na ang system ay hindi mahina sa isang kilala o naturang depekto o kaya sa isang kaso ng kahinaan na maaring iniulat na maayos, upang matukoy na ang system ay hindi na kailanman problema sa naayong depekto.

## Introducing ZAP

Zed Attack Proxy (ZAP) ay libre, ito ay bukas para sa lahat ng gustong pumasok at subukan ang testing tool na patuloy na mapanatili ang kalasag ng Open Web Application Security Project (OWASP). ZAP ay dinisenyo lalo na para sa pagsusuri ng mga web application at ang parehong flexible at extensible.

At ang pinaka- gitna, ZAP ay kilala bilang “man-in-the-middle proxy." ito ay tumatayo sa pagitan ng tagasubok ng browser at ang web application upang maharang at masiyasat ang mga mensaheng natatanggap sa pagitan ng browser at web application, baguhin ang nilalaman kung kinakailangan, at pagtapos dumeretso sa mga packets sa mga naturang destinasyon. It c ito ay maaring magamit bilang magisang application, at bilang daemon process.


Kung may isa pang network proxy ay nagamit na, tulad ng nasa maraming corporate environments, ang ZAP ay maaring isaayos para makonekta sa kapalit.


ZAP nagbibigay pang andar para sa saklaw ng antas ng mga kasanayan - mula sa mga gumawa, tagasiyasat ng bago sa pagsubok ng seguridad, sa dalubhasa sa pagsubok ng seguridad. ZAP ay mayroong ibang salin sa bawat pangunahing OS at Docker, upang kayo'y hindi matali sa isang solong OS. Ang karagdagang pag-andar o paggana ay malayang magagamit mula sa iba't ibang mga karagdagang-ons sa ZAP Marketplace, na nagiging daan mula sa loob ng ZAP client.

Dahil bukas na pnagmulan ang ZAP, ang batayan ng kowd ay maaaring masuri upang makita ang kung paano ito saktong mapatutupad. Kahit sino ay maaaring magtrabaho ng boluntaryo sa ZAP ayusin ang bug, magdagdag ng mga tampok, makalikha ng pahintulot upang makahatak sa pagsasaayos ng mga proyekto, at makadagdag ang may akda upang masuportahan ang mga espesyal na sitwasyon.

Para sa karagdagang impormasyon, tingnan ang Pahina ng proyekto ng Paghalili sa paglusob ng Zed.

Ang katulad sa karamihan ng open source projects, Ang tulong para sa gastos ng proyekto ay pinapaunlakan. Maaari mong makita ang pindutan ng donasyon sa owasp.org pahinahan para sa ZAP sa https://www.owasp.org/index.php/ZAP.

## Kabitan at i-configure ang ZAP

ZAP ay may installers para sa Windows, Linux, at MAC OS/X. Mayroondin itong larawan ng Dockers na makukuha sa lugar ng download na nakalista sa ibaba.

### Kabitan ng ZAP

Ang unang bagay na dapat gawin ay ikabit ang ZAp sa sistem kung saan mo balak isagawa ang pentesting. Idownload ang angkop na installer mula sa lugar ng ZAP's download https://github.com/zaproxy/zaproxy/wiki/Downloads at isagawa ang installer.

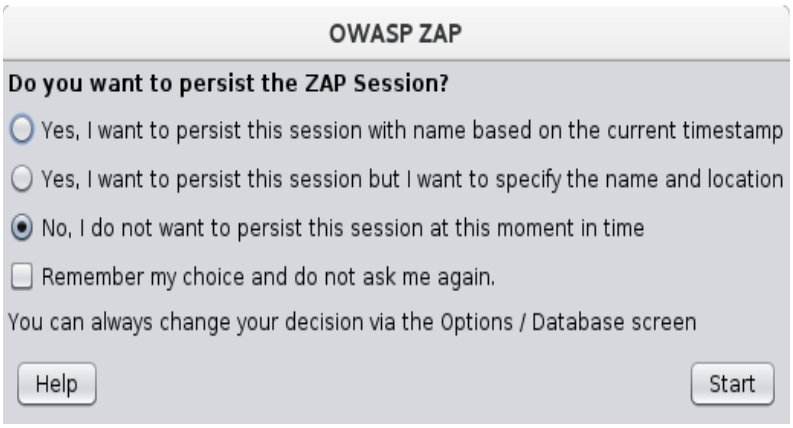
Tandaan na ang ZAP ay nangangailangan ng Java 8+ upang ito'y gumana. Ang MAC OS/X installer ay sinasama ang angkop na bersyon ng Java pero dapat mong iinstall ang Java 8+ nang bukod sa beryon ng Windows, Linux, at Cross-Platform. Ang bersyon ng Dockers ay hindi na kailangan pang iinstall ang Java.

Kapag ang pag-install ay nakumpleto, Ilunsad ang ZAP at basahin ang lisensya ng termino. Pindutin ang**Sang ayon** kung pumapayag ka sa mga tuntuning ito, at ang ZAP na ang magtatapos ng pag-iinstall, pag natapos ito ang ZAP ay kusang magsisimula.

magtiyaga sa isang sesyon

Kapag una mong simulan ang ZAP, ikaw ay tatanungin kung nais mong manatili sa sesyon. Sa Default, ang ZAP sesyon ay laging nakatala sa disk sa HSQLDB database na mayroong gamit na nakadefault na pangalan at lokasyon. Kpag ikaw ay hindi magpumilit sa ang sesyon, ang lahat ng mga file ay buburahin kapag ang ZAP ay umiiral.

Kung pipiliin mong magpumilit sa isang sesyon, ang impormasyon ng sesyon ay maaaring i-sayb sa lokal na databe pwedi mo nang ma-access ito mamaya, at maaari ka nang mag-bigay ng pasadyang mga pangalan at mga lokasyon para sa pag-sayb ng mga file.

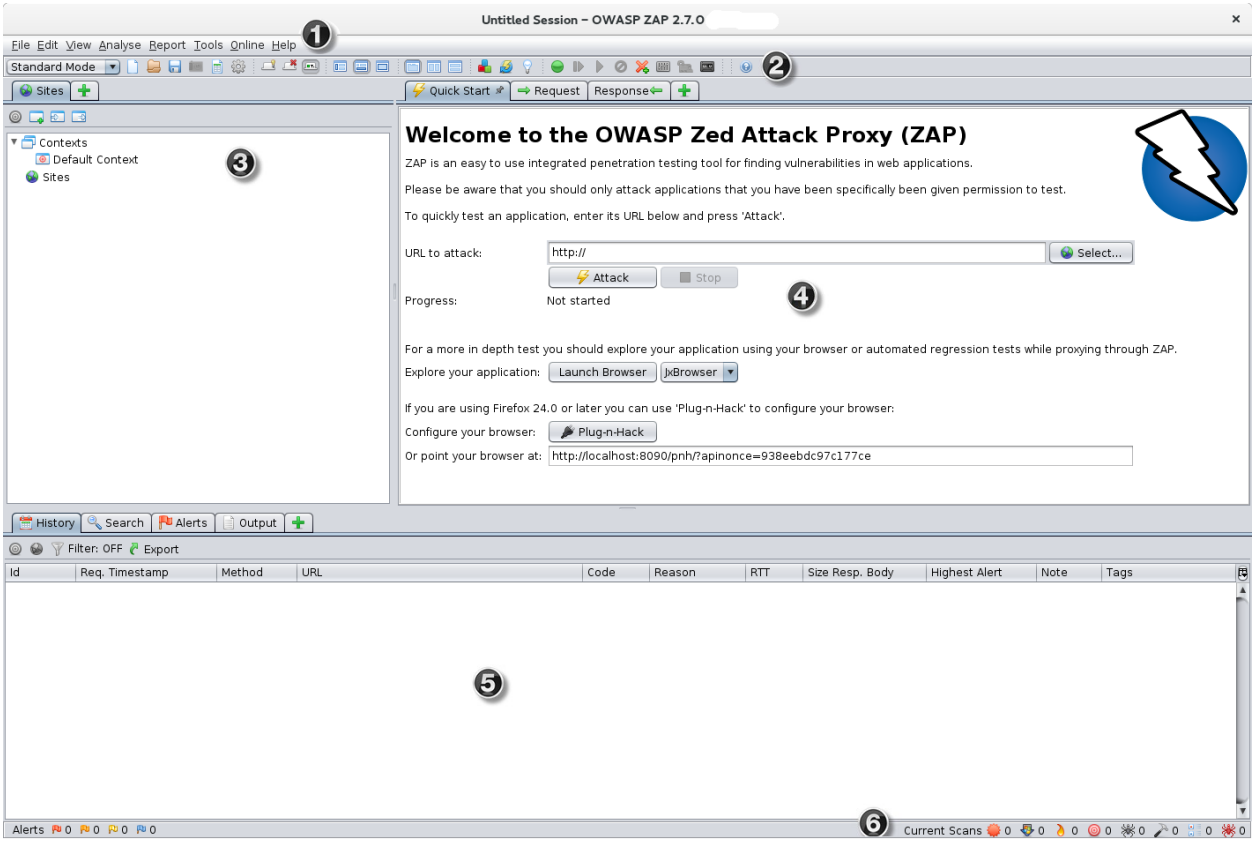



para sa ngayon, pumili **hindi, hindi ako nag-pupumilit sa sesyon sa sandaling oras na ito** , pagkatapos pindutin **Start**. Ang mga sesyon ng ZAP ay hindi maaaring i-pagpilitan sa ngayon.

## Ang ZAP UI

Ang ZAP UI ay binubuo ng sumusunod na mga elemento:

1. **Ang Menu Bar** – Nagbibigay ng daan sa maraming kilusan at mano manong kasangkapan.
2. **Ang Toolbar** – kasama sa pindutan kung saan nagbibigay ito ng madaling daan sa mas kilalang ginagamit na mga tampok.
3. **Ang Tree Window** – Ang display ng mga sayt tree at Ang script ng punong kahoy.
4. **Ang Workspace ng Window** – Ipakita ang kahilingan, ang mga tugon, at scripts at pinapayagan kang baguhin ito.
5. **Ang impormasyon ng Window** – Ipakita ang paliwanag ng kilusan at mano manong mga kasangkapan.
6. **Ang Footer** – Ipakita ang isang buod ng mga alerto upang makita ang katayuan ng pangunahing kasangkapan ng kilusan.




habang ginagamit ang ZAP, pwedin mong pindutin **tumulong** sa Menu Bar o pindutin ang F1 upang ma-access ang context-sensitive tulong mula sa ZAP na gabay ng user.

Para sa higit pang impormasyon tungkol sa UI, tignan ZAP UI Overview ang online na dokumentasyon ng ZAP.

Maging ang ZAP ay sumusuporta sa isang mabisang API at pag-andar ng utos sa linya, Ang kapwa na kung saan lampas ang saklaw sa gabay na ito.

## Ang pag-lulunsad ng mga browser

Maari kang mabilis at madaling mag-lunsad ng mga browser na pre-configure para sa proxy sa pamamagitan ng ZAP via sa mabilis na pagsimula ng tab. Ang mga browser na nailunsad sa ganitong paraan ay hindi mapapansin sa kahit na anong sertipiko ng validation ng mga babala kung sakali ito ay maaaring iulat.

Ang opsyon ay Ang pag-lunsad ng kahit anong pinaka kilalang mga browser na pinaka bagong nai-install sa iyong propayl.

Kung gusto mong gumamit ng kahit na anong mga browser sa iyong umiiral na propayl, para sa halimbawa sa ibang browser ng naka-install na add-ons, kung gayon kinakailangan mong mano-mano i-configure ang iyong browser tungo sa proxy via ZAP at i-angkat at magtiwala sa ZAP Root CA Certificate. Tignan ang ang gabay ng taga-gamit ng ZAP para sa mas maraming paliwanag.

Subukang ikoneta ang iyong web na aplikasyon

Sa sandaling magkaroon ka matagumpay na i-ayos ang iyong ang browser upang magamit ang proxy nito, subukan upang maka konekta sa web na aplikasyon ng iyong sinusubukan.

Kung mo magawang abutin ang iyong web na aplikasyon, suriin ang sumusunod:

1. I-verify ang proxy setting ng browser na ginagamit upang maka konekta sa ZAP.
2. Ang pag-verify ng proxy setting sa ZAP ang ginagamit ng browser upang subukang makanekta sa ZAP.
3. I-verify ang web aplikasyon na gusto mong subukan upang paganahin.
4. Ang pag-suri upang makita kung ang iyong network ay kinakailangan ng proxy upang maabot ang web aplikasyon. kung gayon, Kinakailangan mong i-configure ang ZAP upang magamit ang proxy.

I-configure ang ZAP upang magamit ang papalabas na proxy:

1. Simulan ang ZAP at ang Menu Bar, pindutin **Tools** -> **Options**.
2. pumili **koneksyon** sa kaliwang pinto.
3. sa mga **gamitin ang pamalit na kadena**seksyon ng **koneksyon**mga setting, tignan ang **Gamitin ang pagpapalabas ng pamalit server checkbox**.
4. Pasukin ang **direksyon/Pangalang Domino**at **daungan** para sa iyong pamalit network.
5. Pindutin **OK** para masalba ang mga settings at mapatunayan na ka nang makakonekta sa iyong web aplikasyon.

Kapag ang iyong browser ay matagumpay na naka konekta sa iyong web applikasyon, ikaw ay maghanda na upang patakbuhin ang pag-subok.

## Simulan ang Pentesting sa ZAP

Ang pinakamadaling paraan upang masimulang gamitin ang ZAP ay patakbuhin ang Mabilisang Simulang Subok. Ang mabilisang Simula ay isang ZAP add-on na kung saan itoy awtomatikong naikakabit kapag ikinabit mo ang ZAP.

**MAHALAGA**: Dapat mo lang gamitin ang ZAP para atakihin ang aplikasyon na magkaroon ka ng kapahintulutan sa pasususbok sa aktibong atake. Dahil sa ito ay isang pakunwari, ang aktwal na pinsala ay maaaring mangyari sa mga sayt ng tungkulin, datos, atbp. Kung nag-aalala ka tungkol sa pag-gamit ng ZAP, mapipigilan mo isang sanhi ng pagkasira( bagaman ang ZAP's ay pagaganahin maaaring ito ay maliwanag na mabawasan). sa pag-lipat sa ligtas na anyo.

Upang ilipat ang ZAP sa ligtas na anyo, pindutin ang arrow sa anyo I-drop pababa ang pangunahing kasangkapan ng bar upang mapalawak ang dropdown sa listahan at pag-pipilian **ligtas na anyo**.

### Patakbuhin ang isang mabilis na pag-simula ng pagsubok

Upang paganahin ang isang mabilis na pagsisimula ng pagsubok:

1. Simulan ang ZAP at pindutin ang **Ang mabilis napag-simula** Ang tab ng workspace ng window.
2. Ang mga **pag-atake ng URL** Ang kahon ng teksto, Ipasok ang buong URL ng web na aplikasyon na gusto mong atakihin.
3. Pindutin ang**Atake** pindutan.

Ang ZAP ay magpapatuloy sa pag-gapang sa aplikasyon ng web gamit ang spider nito, pagkatapos passively scan ang bawat pahina ng paghahanap. Ang ZAP ay magagamit sa madalas na pag-scan sa pag-atake sa lahat ng na diskubring pahina, ang kakayahan at parameter.

## Ang kahulugan ng resulta ng iyong pagsubok

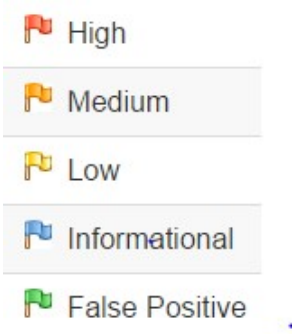
At sa ZAP spiders ang iyong web na aplikasyon, ito ay bumubuo ng isang mapa ng iyong web na aplikasyon' pahina at ang pagkukunan na magagamit sa pag-render ng lahat ng mga pahina. Pagkatapos ito ay nagtatala ng mga kahilingan at ang tugon na ipadala ang bawat pahina at gumawa ng mga alerto kung mayroong potensyal na mali sa isang kahilingan o tugon.

### Tignan ang mga Pangsaliksikang Pahina

Para suriin ang punong pananaw sa mga pahinang pangsaliksik, pindutin ang **mga Site** tab sa mga punong bintana. Ang nodes ay maaari mong palawakin para makita ang indibidwal na URL upang maaccess.

### Tignan ang Alerto at mga detalye ng Alerto

Ang kaliwang bahagi ng pampaa ay may nilalamang bilang ng mga alerto na matatagpuan habang ito'y sinusuri, nasira sa mga panahong mapanganib na kategorya. Ang mga mapanganib na kategorya ay ang mga:




Upang maipakita ang alerto na nagawa habang ito'y sinusubukan:

1. Pindutin ang **Alerto**tab sa impormasyong bintana.
2. Pindutin ang bawat alerto ng display sa window upang ma display ang URL at ang kahinaan sa pag-detek sa tamang gilid ng impormasyon ng window.
3. ang para sa workspace window, pindutin ang **Response** tab upang makita ang mga nilalaman ng header at katawan ng tugon. Ang bahagi ng tugon na magenerate ang alerto na maaaring i-highlight.

# Palawakin sa ZAP ang iyong PENTESTING

Ang pasibong pag-scan at pag atake ng awtomatikong pag andar ay isang mabisang paraan upang makapag umpisa ng isang kahinaang pagtatasa ng iyong web aplikasyon ngunit ito mayroong mga iilang limitasyon. Kabilang sa mga ito ay:

- Anumang pahina na protektado ng pahina ng login ay hindi matutuklasan sa panahong pasibong masuri dahil, maliban kung isasaayos ito ng ZAP pagpapatunay ng pag andar, ang ZAP ay hindi mahahawakan ng kailangang pagpapatunay.
- Anumang pahina na hindi mahahanap sa pagitan ng ZAP default gagamba ay hindi nasubok habang sinusuring posibo. ZAP ay nagbibigay ng karagdagang pagpipilian para sa pagtuklas at sakop sa labas ng posibong pagsusuri.
- Wala kang maraming kontrol na higit sa pagkakasunod ng pagsaliksik sa posibong pagsuri o anumang uri ng atake na isinagawa sa awtomatikong pag atake. ZAP ay nagbibigay ng maraming karagdagang pagpipilian para masaliksik at panglabas na atake ng posibong pasuri.

## I-configure at patakbuhin ang gagamba sa ZAP

Isang daan upang palawakin at pagbutihin ang iyong pagsuri na mapabago ang gagambang ZAP upang gamitin sa pagsiyasat ng iyong mga wen aplikasyon. Ang Mabilisang pagsusuri ay gumagamit ng mga gagambang ZAP na tradisyunal, kung saan ay nadiskubre ang links sa pamamagitan ng pagsusuri ng HTML sa pagtugon mula sa WEB aplikasyon. Ang gagamba ay mabilis, ngunit ito ay hindi laging epektibo kung sinasaliksik ang AJAX web Aplikasyon na lumilikha o gumagawa ng mga links gamit ang java.

Para sa aplikasyong ng AJAX, gagambang ZAP's AJAX ay maaaring mas epektibo. Itong gagamba ay sinasaliksik ang Aplikasyong web sa pamamagitan ng nanawagang browser kung saan kailangan sundin ang links na nalilikha. Ang gagambang AJAX ay mas mabagal kaysa sa gagambang tradisyunal at nangangailangan ng karagdagang pagsasaayos para magamit sa "headless" na kapaligiran.

Ang simpleng paraan upang lumipat pabalik balik sa pagitan ng mga gagamba ay upang paganahin ang tab sa bawat isang gagamba sa Impormasyong window at gamitin ang tab upang ilunsad ang mga sinuri.

1. sa impormasyong bintana, pindutin ang isang berdeng dagdag na tanda (**+**.
2. pindutin**gagamba**upang makalikha o makagawa ng gagambang tab.
3. Ulitin ang hakbang 1, tapos pindutin **AJAX Gagamba**ng makalikha ng **AJAX gagamba**tab.
4. Pindutin ang tulak pin na simbolo sa parehong **gagamba**at**AJAX gagamba** tabs upang i-pin sila sa mga bintanang impormasyon.

Tandaan na ang pareho sa mga tabs ay kasama ang **Bagong Suri**pindutan.

## Siyasatin ang mga Site

Ang mga gagamba ay mabisang paraan upang saliksikin ang iyong batayang site, ngunit dapat nilang pagsamahin sa manu-manong pagsisiyasat para maging mas epektibo. Gagamba, halimbawa, ay papasok lamang sa pinagbabatayang defaultna datus sa mga anyong aplikasyons web ngunit ang gumagamit ay maaring makapasok ng higit sa angkop na impormasyon kung saan maaari, sa pagliko, ibunyag pa ng maraming web aplikasyon sa ZAP. Ang mga bagay na ito ay lalong totoo tulad ng mga anyong rehistro kung saan ay wastong email address na kailangan. Ang gagamba ay maaaring makapasok sa isang

sinalang pisi, kung saan ay magiging sanhi ng pagkakamali. Ang gumagamit ay dapat umipekto sa mga mali at magbigay ng tamang wastong ayos-pisi, na maaaring lalong magdulot pa sa aplikasyon na malantad kung saan ang ayos ay naipasa at natanggap.

Dahil sa nai-configure mo na ang iyong browser para magamit ang ZAP bilang pamalit, dapat mong saliksikin ang lahat ng iyong aplikasyong web sa ganung browser. Habang ginagawa ito, ZAP ay sinusuring mabuti ang lahat ng mga hiling at mga sagot na ginawa habang ginagalugad ang mga ito para sa kahinaan, patuloy na pagtatayo ng punong lugar, at maalerto ang rekord na potensyal na kahinaan na natagpuan habang may paggalugad.

Ito'y mahalaga namagkaroon ng ZAP salikisin ang bawat pahina ng iyong aplikasyon Web, maging ito'y linked sa isa pang pahina o hindi, para sa kahinaan. Kadiliman ay hindi seguridad, at nakatagong pahina kung mabuhay ng walang babala o mapansin. Pwed maging masinsin ka hangga't maaari kapag tutuklasin ang iyong sayt.

## patakbuhin ang madalas na pag-scan ng ZAP

Sa ngayon ang ZAP ay nag-dadala lamang ng passive scan ng iyong web aplikasyon. Ang passive na pag-scan ay hindi mapapalitan kinakailangan ng kahit ano at kinokonsedera na ligtas. Isinasagawa din ang pag-scan sa isang thread sa background para hindi bumabagal ang paghahanap. Ang passive scanning ay mabuti sa paghahanap ng ilang mga kahinaan at ang paraan upang maramdaman ang pangunahin na estado ng seguradad sa web aplikasyon at ang lokasyon kung saan ang imbestigasyon ay maaring ginagarantiya.

Ang aktibong pag-scan, datapwa't, ang pag-tatangka na makakita ng iba pang mga kahinaan sa pamamagitan ng paggamit ng mga kilalang pag-atake laban sa mga piniling target. Ang madalas na pag-iskan ay totoong pag-atake sa lahat ng mga target at maaaring mailagay ang mga target sa kapahamakan, kaya huwag gamitin ang madalas na pag-iskan laban sa target ikaw ay walang pahintulot upang mag-subok.

Upang magsimula sa aktibong pag-iskan:

1. Ang mga tanaw na puno, Ang mga **mga sayt** tab, piliin ang sayt na gusto mong magsagawa ng madalas na pag-iskan dito.
2. Pindutin sa kanan ang piniling mga sayt **Ang madalas na pag-iskan**.

o

1. Ang impormasyon ng Window, piliin ang **Madalas na pag-iskan** tab.
2. Pindutin **bagong pag-iskan**.

Upang masuri at ma-modify ang iyong setting, pagkatapos simulan ang madalas na pag-iskan:

1. Ang Menu Bar, pindutin **Mga kasangkapan** -> **madalas na pag-iskan**.
2. Ang pag-suri ng mga setting at gumawa ng kahit anong pag-iba sa iyong kahilangan sa.
3. Pindutin **simulan ang iskan**upang simulan ang madalas na pag-iskan sa setting na ito.

Maaari mong suriin ang resulta ng iyong madalas na pag-iskan sa parehong paraan paraan ng pagsusuri ang resulta ng iyong passive iskan, sa pinapakita sa iwasto ang resulta ng iyong pagsubok.

## Mas matuto ng marami tungkol sa ZAP

Ngayon na pamilyar kana sa i-ilang pangunahing mga abilidad ng ZAP, ikaw ay maaaring matuto tungkol sa abilidad ng ZAP at kung paano ito gamitin sa ZAP Ang gabay ng user. Ang gabay ng user ay ginawa ng sunod sunod na instraksyon. Ang mga reference para sa API at Command-line programming, Ang instraksyunal na video, at mga tip at trick para sa pag-gamit ng ZAP.

### Ang mapapakinabangang mga link

OWASP Zed Attack Proxy Project – ZAP's main project page

OWASP ZAP Wiki – Ang ZAP Wiki

Ang gabay ng user ng OWASP ZAP - Ang gabay ng user ZAP

OWASP ZAP Hot Keys - Ang listahan ng ZAP hotkeys

Ang mga grupo ng user ng ZAP– Grupo ng Google para sa mga gumagamit ng ZAP

Ang Grupo na Developer ng ZAP – Ang Grupo ng google para sa mga developer at taga-ambag sa ZAP