Burp Suite

هو أداة لاختبار أمان تطبيقات الويب، تستخدم على نطاق واسع من ال pentesteration testers لاكتشاف الثغرات الأمنية وتحليل حركة مرور الشبكة بين ال browser وال server.

ايه اللي ممكن اعمله بيه ؟

1- اعتراض الطلبات سواء HTTP أو HTTPS بين ال browser وال server مباشرة يسمح لك بتحليل البيانات وتعديلها قبل إرسالها

2- Burp بيسجل جميع الطلبات التي يرسلها ال browser إلى server مما يتيح لك رؤية كل البيانات المتبادلة بين اليوزر والسيرفر بما في ذلك الكوكيز، الهيدر

3- تستخدم في اختبار الثغرات بناءً على إدخال البيانات Input validation tests مثل ال SQL insection، XSS، Command injection

4- يمكنك فك تشفير البيانات المشفرة مثلا ب Base64 أو مثلا URL Encoding

5- تجربة طرق انتحال الهوية (session Hijacking) أو تجاوز ال (Authentication) عبر التلاعب في ال Tokens أو ال Cookies

7- تنفيذ هجمات Brute force لمحاولة تخمين ال password أو ال users name من خلال إرسال طلبات تلقائية بسرعة كبيرة.

Target Tab

التبويب دى بتساعدك ع فهم هيكلية الموقع المستهدف وانك تحدد الأهداف اللى عاوز تختبرها وتنظم معلوماتك بحيث تسهل عليك عملية الاختراق

1) Site Map

ده المكان اللى بيتم فيه عرض جميع الـ requests (HTTP/HTTPS) التى تم اعتراضها أثناء الاختبار ، ويتم تنظيمها فى هيكل هرمى

+ ع كل الـ Domains أو المواقع اللى اتعاملت معاها أثناء الاختبار أو حتى اللى ممكن يكون موقع انت مختتهوش بس الموقع اللى انت فتحته مثلا هو اللى طلبه

لو الموقع انت مش طلبه بس موقع تانى هو اللى طلبه هتلاقيه اسمها كدا بخط خفيف

+ كمان المكان دا بيحتوى على تفاصيل كل Request من headers و Parameters ، Cookies ، tokens

أقدر كمان استخدم filtration علشان اتحكم ف اللى يتعرض لى

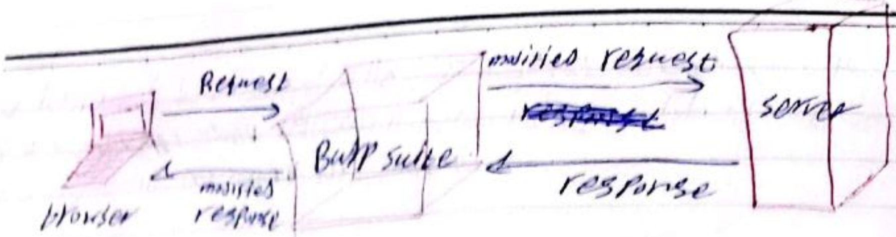
① Filter by request type

show only in-scope item بيستخدم من خانة الـ filter لو انا حاطط حاجة ف خانة scope علشان اعرض Domains معينه مثلا

show only requested item علشان اعرض الـ requests اللى انا عاملها يدويا فقط

show only parameters requests بيعرض فقط الـ requests اللى بتحتوى على باراميترز فقط

← اسم اليوزر أو الباسورد اللى بتبعته أو مثلا كلمة بتبحث عنها ف page حاجة انت دخلتها كـ input بعت واتحول للسيرفر



Proxy Tab

المسئوله عن اعتراض وتعديل الـ requests بين الـ browser والـ server.

الاستخدامات:

* التقاط جميع الـ requests التي يرسلها الـ browser
* تعديل الـ requests قبل ارسالها
* تحليل البيانات المستلمة من السيرفر (Responses)
* الاستناد لفحص sessions حركة البيانات بين العميل والسيرفر

[1] Intercept

دا المكان اللي ممكن فيه توقف الـ requests قبل ارسالها إلى السيرفر مما يسمح لك بتعديلها يدويًا قبل أن تصل للهدف

① forward ← ارسال الطلب كما هو إلى السيرفر
② Drop ← حذف الـ request وعدم ارساله
③ Intercept is on/off ← يشغل او يقفل الاعتراض
④ Action ← * send to repeater ← يقوم بإرسال الطلب إلى الـ Repeater tab بحيث تعدل فيه أو ترساله أكثر من مره لرؤية تأثيره
* send to intruder ← يقوم بإرسال الطلب إلى intruder tab لاستخدامه في تنفيذ هجوم Brute Force أو الفحص التلقائي يعني مثلاً نبعت الـ request وبحط فيه قائمة passwords يجربهم
* send to Scanner ← يقوم بإرسال الـ request إلى Burp Scanner لفحصه تلقائيًا بحثًا عن ثغرات أمنية
* send to Comparer ← لإرسال الـ request إلى Comparer tab لمقارنة الطلب مع طلب آخر لرؤية الفروق بينهم
* change request method ← يتيح لك تغيير نوع الـ request مثلاً من GET لـ POST أو العكس ودا مفيد عند اختبار كيف يتعامل السيرفر مع تغيير الطرق HTTP Methods Tampering

---

Hide-not-found items ← يخفي الـ requests اللي أرجعت كود 404 not found

② filter by MIME Type ← فلتره على حسب نوع المحتوى MIME typ
* زي HTML (ذي html, php) أو script, CSS, Images وحاجات تانيه كتير

③ filter by status code
على حسب الـ status code

③ filter by file Extension ← فلترة حسب امتداد الملفات
عندك خيار الـ show والـ Hide

[2] Scope

دا المكان اللي بتكتب فيه الـ Domains اللي عاوز تركز عليه أو الـ Domains اللي مش عاوزهم بحيث تعمل فلترة باستخدام الـ scope دا

4. HTTP history : بتسجيل كل الـ requests اللي تم اعتراضها أو مرت عبر Burp Suite سواء GET أو POST عشان تقدر ترجعلها وتحللها

3. Options : دي تعتبر الـ settings بتاعت الـ Intercept يعني ممكن منها تحدد ايه الـ requests اللي تعترضها
* تلغي الـ validation أي مثلاً تحول الـ HTTPS لـ HTTP
تخفي مثلاً الـ form fields اللي بتبقا مخفية في الـ page

intruder Tab

واحدة من أقوى الـ tools في الـ Burp Suite حيث يستخدم لتنفيذ الهجمات التلقائية على المواقع زي الـ Brute Force Attacks أو اختبار ادخال القيم العشوائية أو Fuzzing أو تجربة قيم مختلفة في الـ Parameters

أزاي استخدمه ؟ بعد الـ request المستهدف من الـ Proxy أو الـ Repeater ويبعت ببيعته للـ intruder ونبعته باختيار الـ Attack وبعد القيم اللي هدخلها أو الملف اللي فيه القيم يبدأ ويبعت بشغل الـ Attack

1. Positions : في الجزء ده انت بتحدد الأجزاء المتغيرة في الـ request التي سيقوم intruder باختبارها
* بيتم وضع أقواس {} حول المعلمات المستهدفة تلقائياً وكمان ممكن تضيف أو تحذف أجزاء من الـ request أو تعدل فيه

2. Payloads : هنا بيتم إدخال القيم التي سيتم استخدامها في الهجوم وهي التي سيتم استبدالها بالجزء اللي كنت حددته في الـ Positions tab
* يمكن إضافة القيم يدوياً أو تحميل قائمة جاهزة

Repeater tab

يستخدم لإعادة وإرسال الـ requests يدوياً الى السيرفر بدل ما ابعته من الـ browser. يعني مع امكانية التعديل عليها و مراقبة الاستجابات.

* بتستخدمه في انا نحلل كل response لكل تغيير في الـ request و في اختبار الثغرات الأمنية و تحليل بيانات الـ sessions والـ cookies

* لازم الأول ننقل الـ request يدوي من الـ proxy tab أو من الـ intruder tab

نلاقيه منقسم لـ الـ request والـ response

Sequencer tab

تستخدم لتحليل عشوائية الرموز الأمنية وقوتها زي الـ session tokens والـ cookies مثلاً

عشان لو الرموز دي مش عشوائية بشكل كافي، فالـ Attacker ممكن يخمنها ويخترق الـ sessions مثلاً

* كل اللي بيعمله انه بيحلل القيمة العشوائية دي كنظرية كذا حاجة بحيث يرى هل ممكن نقدر نتوقع مثلا القيم الجديدة ولا لا والقيمة قوية وعشوائية جداً بس هو مش بيجرب حاجة ولا بيبعت مثلاً requests

Decoder Tab

عبارة عن Tab ممكن نبعا أحول النصوص بين encoding أو decoding أو حتى hashing

ايه الفائدة: باستخدمها عشان احلل البيانات المشفرة في الـ requests مثلاً أو تحويل الـ strings بين عدة صيغ

بنستخدمه في الـ reverse engineering لمعرفة كيف يتم تشفير البيانات.

Comparer Tab

عبارة عن tool تستخدم لمقارنة اتنين requests أو النصوص العادية أو الـ responses عشان أعرف الفرق بينهم

* بيعرفك ايه الفرق بين الاتنين بحيث يلون كل شئ مختلف

Extender Tab

يسمح لك بإضافة وتخصيص ميزات جديدة للأداة من خلال الإضافات (Plugins) اللي يمكنك استخدامها في تحميل الـ Plugins من الـ BApp store

ممكن تعتبرها زي الـ extensions كدا

أو انك انت اللي تعمل plugins (عبارة عن كود مخصص) لتمديد وظائف الـ Burp حسب احتياجك

* API Tab ← دي اللي ممكن فيها تكتب اسكريبت تعدل سلوك الـ Burp بتدعم python