Web Basics 2

Authentication & Authorization & Cookies

Authentication

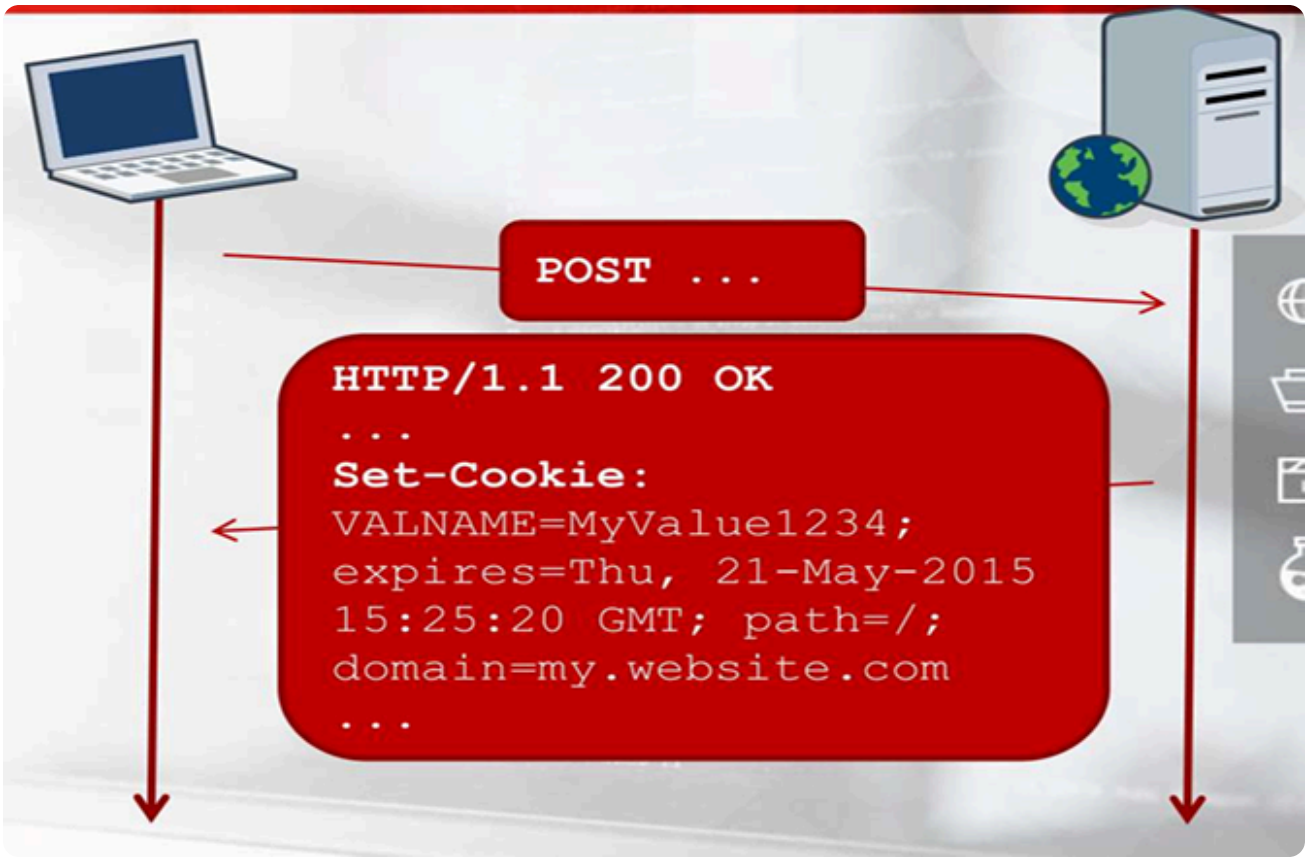
- بص ياباشا دا الحاجه اللي بتخليك تخش الموقع اللي هوا الemail وال pass مثلا طبيعي طول منتا معاك الايميل والباس تقدر تخش الموقع وده بنقول عليه انك authenticated انك تخش
- يعني مثلا تخيل معايا صحيت الصبح ونزلت الجامعه ونسيت الكارنيه بتاعك فالبيت فا لما وصلت الامن سألك قالك وريني الكارنيه قولتلو معلش والله نسيتو فالبيت فا هيقولك اسف مش هقدر ادخلك انتnot authenticated انك تخش في واحد جه من وراك وراهم الكارنيه ودخل يبقي ده authenticated

Authorization

- دي الصلاحيات اللي بتكون معاك واللي تقدر تعملها فالموقع في حاجات بتكون مسموحه ليك وحاجات لأ
- بعد مرحلة الauth وانك دخلت الموقع تخيل معايا انك فتحت الفيس مثلا وروحت جربت تغير اسم اكونت صحبك فا اكيد مش هينفع عشان انت not Authorized انت مش صاحب الأكونت ولا حتي ادمن فالفيس عشان تعمل كده
- طب تعالي نغير اسم البروفايل بتاعنا كده هيغيرو عادي انت authorized بكده
- تخيل معايا انك دخلت الجامعه وجبت الكارنيه وبقيت authenticated ودخلت الجامعه وروحت قعدت ف اوضة المعيدين؟ هل هيبقي مسموح ليك؟ اكيد لا دي مش بيدخلها غير المعيدين بس يبقي انتnot authorized طب تعالي جرب خش المدرج بتاع المحاضره بتاعتك اه ده تقدر تخشو عادي يبقي كده انت authorized عادي

Cookies

- الـ Cookies دي عبارة عن ملفات صغيرة السيرفر بيخزنها جوه المتصفح بتاعك بتبقى عبارة عن بيانات بسيطة(زي: user ID, session token, language preference...) عشان لما تدخل تاني الموقع يفتكرك، أو عشان يحتفظ بحاجات ليك
- تخيل معايا كل مره تيجي تدخل علي الفيس يقولك سجل دخول هيبقي الموضوع بيض صح؟ هنا بقي بيجي دور الcookies وانها تقول للفيس اه ده طنطاوي اللي كان لسه داخل ودي بياناته فا الفيس يدخلك علاطول من غير login



- دي صوره فيها ازاي جهازك بيبعت ال cookies للسيرفر ودي القيم اللي بتكون فيها
- المفروض لما تيجي تعمل Logout من الأكونت الcookies بتتمسح بمجرد ماتعمل Logout طب لو متمسحتش؟ تبقي دي ثغره يامعلم اه دي تاني ثغره معانا بعد ال Host Header Injection اللي قولنا عليها فوق
- الCookies دي بيكون فيها حاجه اسمها Session ودي معناها بالعربي الجلسه ومتركزش ف معناها بالعربي بقي دي بيكون فيها انت بقالك قد ايه فاتح الموقع ده وهتفضل logged in لحد امتي اول ما الsession دي تخلص هتلاقي الموقع عمل Logout فا الكوكيز تتمسح ولما تسجل دخول تاني تتعمل واحده جديده وهكذا
- وهنا حد هيجي يقولي ياعم هو كل شويه الsession تخلص ويعملي Logout واعمل login تاني ايه القرف ده اقولك وانت بتسجل دخول ف اي موقع بتلاحظ كلمة remember me دي لو فعلتها وانت بتسجل دخول بتطول مدة ال session فالكوكيز وهتقعد فتره كبيره والكوكيز محفوظه عادي ومش هيعمل logout
- معني كلامك ده ان انا لو هاكر وعرفت اخد ال cookies بتاعتك اي حد هيبقي عندي full access علي اكونته اقولك اه عادي طبعا وهنتعلم نعمل كل ده مستقبلا
- بس عاوز الفت نظرك لحاجه بمجرد ما انت بتغير الباسورد بتاع اكونتك او تغير الايميل او تفعل ال 2FA الكوكيز بتتمسح فورا وبتعملك واحده جديده والأكونت يعمل logout لوحده طب لو معملش Logout؟ اقولك زي ماقولنا فوق دي تبقي ثغره اسمها improper session expiration
- الimproper session expiration دي بتحصل لما مثلا انت تكون عامل اكونت علي موقع وفتحت نفس الاكونت من براوزر تاني وغيرت الباسورد مثلا المفروض الكوكيز تتمسح والاكونت يعمل logout من كل الاجهزه اللي متسجل عليها الأكونت فا لو مخرجش من البراوزر الاولاني يبقي كده في ثغره اسمها improper session expiration

Proxy and Burpsuite

- ال Proxy عامل زي الكمين اللي بيكون ف نص الtraffic بينك وبين السيرفر
- هو بيشتغل كا وسيط بينك وبين السيرفر وهو اللي بيبعت الطلبات للسيرفر بدالك وهو اللي بيستقبلها ويبعتهالك
- انت لما بتفتح أي موقع، بتبعت request، والـ request ده بيروح للموقع، والموقع يرد عليك

لو فيه Proxy في النص:

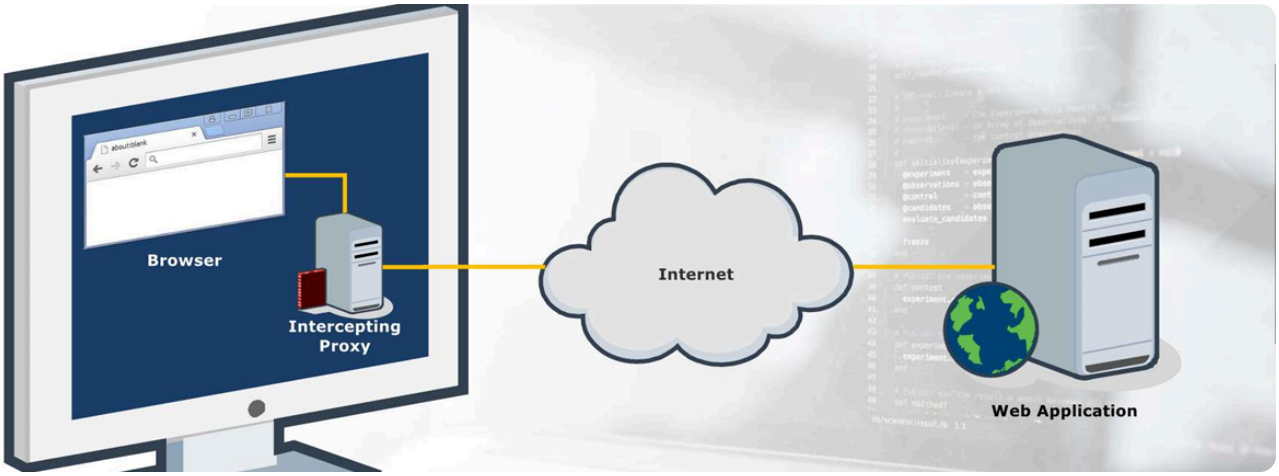
- انت تبعت للـ Proxy
- الـ Proxy ياخد الـ request بتاعك
- ويبعت بدل عنك للموقع
- وياخد الـ response
- ويرجعهولك

كأنك بتكلم الموقع عن طريق مندوب بالظبط

طب احنا ليه ممكن نستخدم Proxy اصلا؟

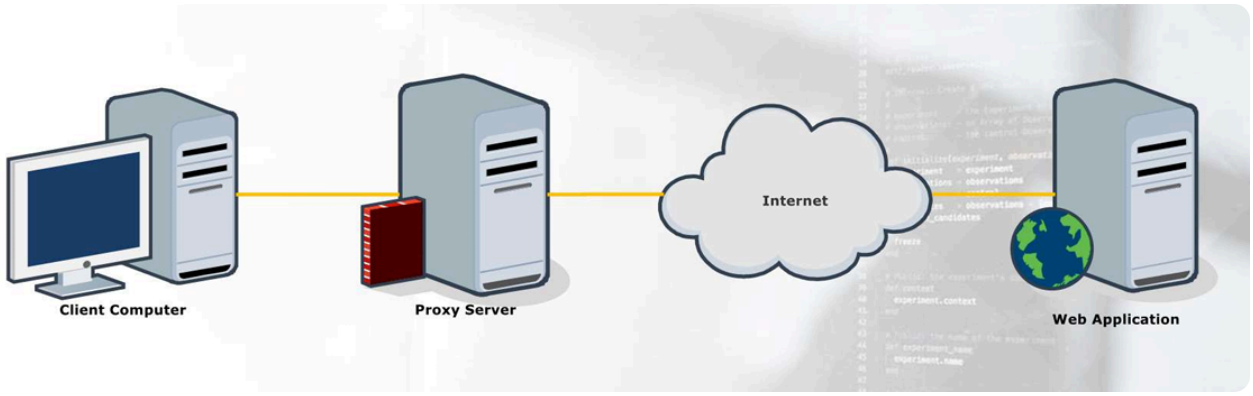
الاستخدام	الشرح
Privacy (إخفاء الهوية)	بيخفي الـ IP بتاعك عن السيرفر اللي بتتواصل معاه
Filtering (تصفية)	يمنع أو يسمح بمواقع معينة (زي الشبكات الداخلية في الشركات)
Security (حماية)	يحميك من مواقع خبيثة أو يحلل الـ traffic اللي خارج وداخل الشبكة
Caching (تسريع التصفح)	يخزن نسخ من المواقع عشان يسرّع التصفح للمستخدمين
Penetration Testing (اختبار اختراق)	يسمحلك تشوف وتعدل الـ requests والـ responses عشان تكتشف ثغرات

- واحنا فالمجال بتاعنا هنستخدم ال Proxy اللي هو BurpSuite عشان نقدر نوقف الطلبات ونعدل عليها وكل الكلام ده



FoxyProxy

- دلوقتي احنا عرفنا يعني ايه proxy وهنستعمله ف ايه بس احنا عاوزين نوجه اي حاجه بنبعتها او بنستقبلها للproxy ده عشان تروح عليه
- فا هنستخدم اضافه فالكروم اسمها Foxyproxy ودي اضافه بتعملي redirect لكل الترافيك بحيث انه يروح علي البروكسي بتاعي اللي هو ال Burpsuite وطبعا الburpsuite بيشتغل علي بورت 8080 فا هيوجه كل الترافيك علي البورت ده



اتفرج علي المحاضره Web Basics 2 و اللي بعدها عشان تعرف ازاي تظبط الاكستنشن بتاعت foxyproxy وكمان عشان تعرف ازاي تنزل اداة ال burpsuite