Oauth

تعريفه: هو Authorization Framework بيسمح لل Third party Apps إنها تـ access معلومات محددة من تطبيق ما، زي لما تيجي تسجل دخول في موقع Quora بتلاقي تسجيل بالفيس بوك وهنا انت بتسمح إنه ياخد معلومات محددة من فيس بوك عشان يعملك اميل في موقع Quora بدون ما تعمل Signup في كورا.

- الـ Acces Token ده بتستخدمه عشان تقدر تـ access الـ resources بتاعة موقع تاني

إحنا عندنا 4 أدوار بيتعاملوا مع بعض عشان يحققوا بروتوكل الـ Oauth.

- التطبيق الي عايز يوصل لمعلوماتي في تطبيق تاني وده إسمه |Third Party Application|

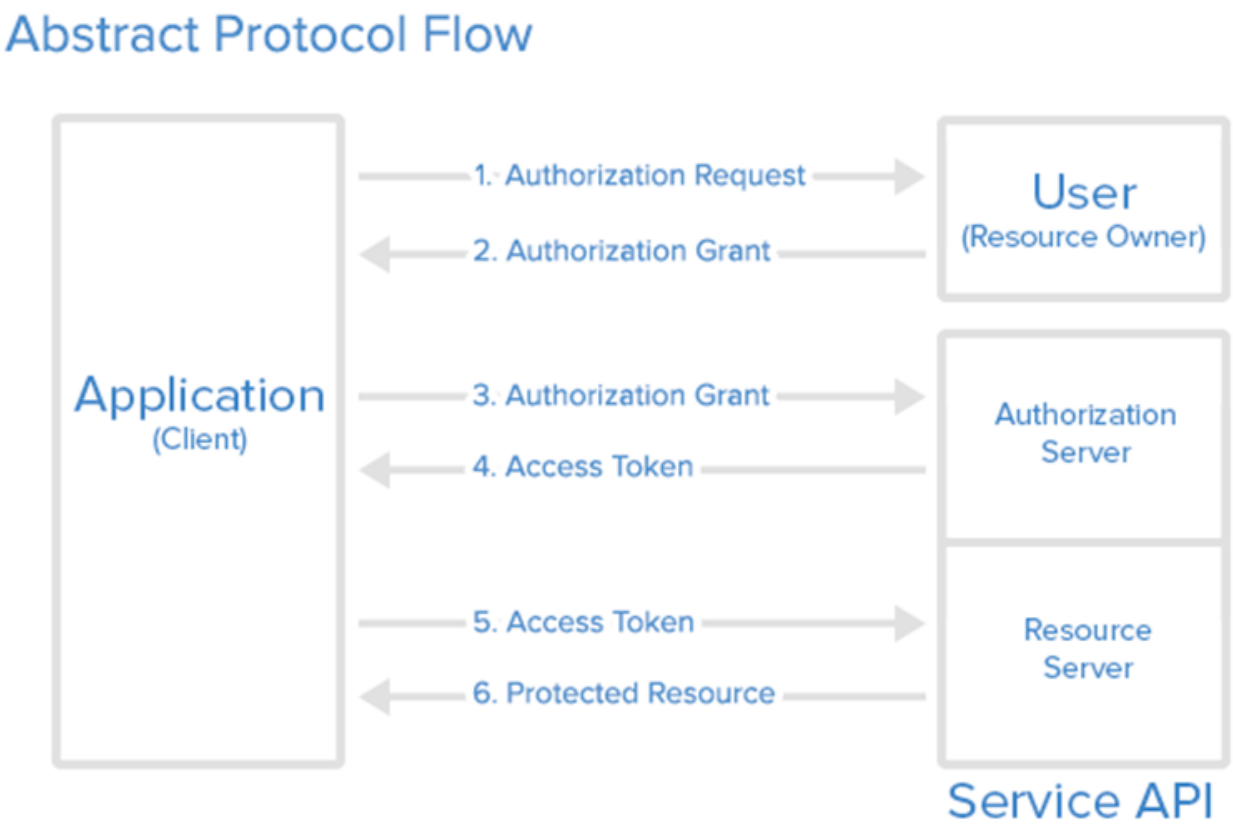
Ex. Quora Application

- التطبيق الي هيتاخد منه معلومات للتطبيق الأول وده إسمه | Authorization Server | وده الي بيعرضلك Interface عشان توافق أو ترفض عملية Oauth

Ex. Gmail Application

- ال API Server وده السيرفر الي هيستخدمه موقع Quora عشان يـ access معلوماتي في موقع Gmail وده إسمه |Resource Server |
- وآخر حاجة الي هو " أنا " الي بسمح لـ Quora إنها تستخدم الـ API Server عشان تـ access معلوماتي في Gmail وده إسمه |Resource Owner|

طريقة عمله إزاي بقي؟



طريقة عمل الـ Authorization code grant 😆

- أول حاجة الـ Third Party app بيبعت Authorization request للـ Authorization server (يعني Quora بيبعت ريكوست لـفيس بوك) عن طريق الـ Browser.
- بعدين بيجي دور الـ Resource owner في إنه يوافق او يرفض العملية |User|
- لو اليوزر وافق, بيتبعت Authorization code من فيس بوك لموقع كورا عن طريق المتصفح
- بعدين موقع كورا يطلب من فيس بوك access token وبيعت في الريكوست الـ client-id و authorization code و والـ Redirect-URL
- ف يرد عليه الفيس ب access token
- في parameters لازم نخلي بالنا منها :
  - response-type= code وده معناه إن كورا بتطلب autorization code من فيس بوك
  - clint-id=xxxxxxx وده رقم مميز بيستخدمه الفيس بوك عشان يعرف كل App
  - scope وده بيوضح الـ Permission الي بيطلبها كورا من فيس
  - Redirect-URL وده فيه لينك بيوضح الـaccess token يتبعت فين بعد ما الـ user يوافق.

5- طريقة عمل الـ Implicit grant 😆

· نفس طريقة عمل Authorization code grant ولكن في الخطوة التالتة بتحصل على الـ access token ع طول.

6- فين الأماكن الي بنستخدم فيها Oauth؟.

· في بعض المواقع لما نيجي نعمل Import لصور او محتوى معين من موقع تاني

« او في صفحات Log-in

· في صفحات SSO

ليه بتحصل الـ attacks اصلا؟

- بسبب إن معظم الـ impelmentaions بتكون اختياري وده بيتضمن إجرءات حماية كتير وظيفتها حماية الداتا بتاعة اليوزر وبتكون اختياري برضو.
- نقص في ميزات الأمان الي المفروض تكون built-in في الـ configuration عشان تساعد في حماية الداتا، بل إن جزء كبير جداً من الحماية معتمد على الديفلوبر واختياره لمجموعة صحيحة من إجراءات الأمان، وكمان فلترة الـ Inputs وغيرها من أنواع الحماية.
- على حسب نوع الـ Grant ف بيتم إرسال البيانات عن طريق المتصفح وبالتالي بتكون عرضة للهجوم.

الثغرات الي بتحصل بتكون يا إما في الـ client application's الي بتستخدم الـ Oauth، أو في الـ Configuration الخاص بالـ Oauth نفسه.

- ثغرات الـ Client application:
  - 1. أحيانا الـ client بيستخدم الـ access-token كـ password، وبالتالي بعد ما تعمل success Oauth الـ auth server بيبعت الـ credentials ومعاها الـ access-token ف ممكن تغير الـ username, email وتحاول تدخل على أميل حد تاني.
  - 2. عدم وجود state parameter ووجود option إنك تعمل link للـ Oauth account ف ده معناه إنك تقدر تعمل CSRF attack وتربط الـ Oauth account الخاص بيك بيوزر تاني. (الـ State parameter بيُستخدم كـ CSRF token فالـ Oauth flow)
- ثغرات الـ Oauth Configuration:
  - 1. إنك بتقدر تتحكم في الـ URI_redirect param وبالتالي ممكن تحط external domain خاص بيك ولما اليوزر يتم تسجيل الدخول بالـ Oauth هيبعتلك الـ Access token
  - ولكن هنا في بعض الـ Metigiations والـ Bypasses:
    - أحيانا بيعمل check على الدومين بس وممكن تخطي الموضوع بإنك تلاقي open redirect في الـ Client نفسه وتخلي الـ uri_redirect يروح عليه.

- أحيانا بيعمل check على الدومين والـ path الي بعده ف ممكن تستخدم path traversal عشان ترجع للـ path الي عليه الـ open redirect
- لو بيعمل check على الدومين والـ path كويس وبيقارن إن الـ uri_redirect هو نفسه بالظبط الي موجود في الـ Oauth Configuration ف هنا مفيش ثغرة.
- أفضل جرب تغير في القيم وجرب تستخدم الـ SSRF techniques، وشوف إيه الي هيخلي التطبيق ميظهرلكش ايرور، متكتفيش بتغير قيمة واحدة ولو منفعتش تعديها.
- ممكن تجرب الـ Parameter pollution، أو إن الدومين يكون بيبدأ بالـ Localhost ف وقتها تسجل دومين localhost-evil.com وتبعت الريكوست عليه.

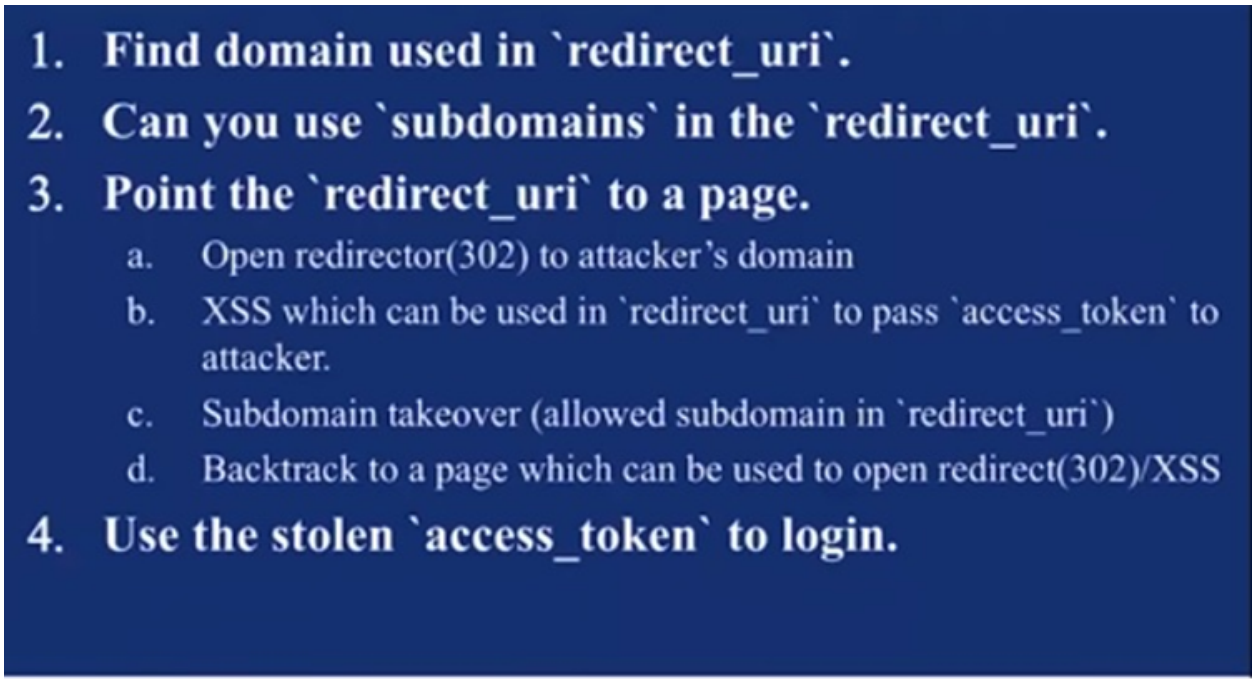
- خطأ في scope validation (وده بيعتمد على الـ grant type):
  - المفروض إن بعد ما اليوزر يسجل من خلال الـ Oauth ف الـ Client يقدر يوصل للحاجات المتفق عليه فالـ Scope من الأول قبل ما يوافق اليورز على الـ authorization، ولكن ف بعض الحالات بيحصل إن الـ Scope ده يحصله Upgrade وبالتالي الـ attacker يقدر يوصل لحاجات أكتر ويغير في الأسكوب.
  -

7- ايه هي الـ Attacks الي ممكن تحصل على صفحات Log-in؟.

· Token/code Stealing

» كل الي محتاجينه في الـ Attack ده هو إننا نعرف الـ access token ونستخدمه لتسجيل الدخول

» طيب وننفذ الـ Attack ده إزاي؟.



· CSRF

Token Impersonation ·

8

-9