SSRF

تعريفها

ببساطة هي ثغرة بتخليك تـ access internal resources جوا شركة عن طريق سيرفر خارجي(الي هو انا), للتوضيح , مثلا انا بعمل هاك على شركة معينة ولنفترض فيسبوك وانا عارف إن عندهم URL زي ده (services.mail.facebook.com)ولكن لما بحاول أوصل بيقولي فوربيدن او مش موجود وده بسبب الفايرول, هنا بقى يظهر دور الثغرة إن بحاول اشوف سيرفر داخلي في الشركة يقدر يـ access الـ URL الي فوق عادي بما انه على نفس الشبكة وابعت معاه الـ URL الي فوق وبالتالي انا قدرت ادخل عليه من سيرفر خارجي.
- مثال واقعي, وهو اني عايز أوصل رسالة لـحد ف البيت الأبيض وبالتالي انا مقدرش ادخل جوا ف بروح اشوف حد يقدر يدخل جوا وابعت معاه الرسالة وكده.

!#الثغرة دي بتخليك تبعت ريكوست من سيرفر التطبيق المصاب فالريكوست ممكن يروح لسيرفر خارجي زي جوجل او فيس بوك وغيرهم ولكن الاستغلال الأمثل ليها بيكون إنك تبعت الريكوست لـ أنظمة داخلية موجودة ورا فايروول من الصعب إنك تعملها access في الوضع العادي - لانك في الحالة دي سيرفر خارجي وهي بتقبل الي على نفس الشبكة -.

External service interaction :!#ببساطة هي الـ intended functionality الي بيعملها السيرفر, يعني لما ترجمة جوجل تديها لينك وتروح تترجم الموقع, هنا جوجل اخد اللينك وراح زار الموقع يترجمه بس دي الوظيفة الأساسية أصلا مش ثغرة ولا حاجة والفيس نفس الحوار لما تضيف لينك ويروح يزور اللينك يجيب اسم الموقع او رأس الموضوع,ودي طبعا مش عليها أي ضرر ومفيش خطورة خالص, العادي أصلا إن السيرفر سواء جوجل او فيس بوك يعمل كده لإن لو ده محصلش كده الـ functionality أصلا هتقف.

- في نوعين من الـ EXI وهما الـ HTTP والـ , DNS الـ HTTP عشان بتم عن طريق الويب من خلال بورت 80 او 443 والـ DNS كذلك.
- الضرر الوحيد منها وهو إنك بتستغل السيرفر المصاب بالـ EXI في إنك تبعت ريكوستات كتير لسيرفر خارجي وبالتالي بتضر بسمعة الشركة صاحبة السيرفر ده.
- أي HTTP interaction لازم تسبقها DNS interaction عشان تعرف الـ IP بتاع الموقع المطلوب وبالتالي الـ EXI-DNS مش ثغرة ابداً.

أنواعها

عندنا نوعين من الـ : SSRF

- Based:ودي معناها إن لو الموقع مصاب بـ SSRF وعملت ريكوست إنه يزور موقع تاني بيروح يعمل ريكوست ويعرضلك الـ response بتاعة الموقع ده قدامك (بيعرضلك الموقع كأنك دخلت ع الموقع نفسه يعني لو اديته Url بتاع جوجل بيعرضلك الـ index بتاع جوجل)
- Blind:هنا بقى مفيش حاجة بتظهر يعني انت عملت ريكوست بالـ URL بس مظهرش حاجة, ف بنلجأ لاستخدام Burp collaborator عشان نشوف ايه الي حصل.

ايه سبب حدوثها

- اول نقطة وهي إن الكود لما بيجي يتنفذ بياخد قيمة بارامتر الـ URL ايان كانت ويروح يعمل ريكوست بالـ URLده ويجيب الريسبونس ويعرضها , ف هنا مفيش أي فتلرة.

أماكن تواجدها دي أهم نقطة وهي فين بلاقي الثغرة دي.

- الثغرة دي بتلاقيها في أي بارامتر بيقبل URL يعني ولنفترض كام مثال كده
★ www.facebook.com/home?imageUrl=https://infographic.com/bingoo.jpg
★ www.google.com/services?redirect_to=https://google.com/home

يعني أي بارامتر بيقبل URL خارجي أو داخلي تجرب فيه.

- ممكن تكون عن طريق إن في Endpoint معينة بتجيب المحتوى عن طريق الـ HOST + Endpoint وبالتالي تغير الـ HOST لموقع خارجي (البرب سويت.)
- أحيانا بيكون الـ parameter في الـ Body بتاع الريكوست ف شوف الريكوستات كلها.
- غالبا بيكون في تفعيل الاشعارات وتفعيل أي حاجة بتبعتلك رسايل وهكذا.

تلاقيها ازاي

- أول حاجة بتبدأ تشوف بارامتر بيقبل URL
- بتروح تجرب تديله سيرفر خارجي ولنفترض هنشغل الكالي كسيرفر ونشوفه هيـ access ولا ولا
- لو عمل aceess فعلا يبقى حتى الآن هي External service interaction
- بتروح تجرب بقى تـ access الـ localhost بتاع الموقع بتاعهم لو حصل يبقى ديSSRF

ممكن نحولها لإيه

- الـ SSRF ممكن تتحول لـ local File Inclusion بإنك تجرب الـ PHP wrapper الي اسمه file:// وبعدين تديله ملف معين يقراه, وعلى حسب الـ privilege بتاعتك هتقدر تقرأ ملف معين.
- ممكن نستعملها في الـ Port scanning في إننا بنديله URL خارجي ومعاه البورت ونشوف هل هيرد ولا لا, في حالة الـرد هيبقى مفتوح وفي حالة إنه مرجعش حاجة هيبقى البورت غالبا closed هنا مثال للـURL:

Url=http://google.com:80وبعدين تبدأ تغير في الـ port وتشوف الـresponse.

- وممكن نستعملها في إننا نعمل host discovering / network scanning وندیله IPs ونشوف الي هيرد هيبقى شغال أو مش هيرد ف مش شغال.
-

!#الـ Meta-data file ده عبارة عن ملف بيكون تبع الـ cloud providers زي , Microsoft Azure , AWS) (وهكذا , الملف بيحتوي على secret keys خاصة بالسيرفر بتاعك الي انت عامله host على AWS مثلا, في بيكون في معلومات حساسة.

- في لو الموقع مصاب بـ SSRF وهو hosted على AWS او أي خدمة تاني, جرب تغير قيمة البارامتر لـإنك تقرأ ملف الـ Meta-data file ودي بعض اللينكات :
  - ★ AWS => http://169.254.169.254/latest/meta-data/
  - ★ Digital ocean => http://169.254.169.254/metadata/v1.json

سيناريوهات

- طرق الحماية في الثغرة دي يا اما balcklisted أو whitelisted
- في حالة وانت بتيست وجربت تكتب موقع خارجي في الـ URL واشتغل بعدين جيت تكتب الـ localhost ف رفض لإنه, black listed هنا ممكن تجرب طريقة | Domain pointing to localhost | وده معناه إن طالما السيرفر بيرفض الـ 127.0.0.1 ف انا هبعتلك دومين لما تيجي تعمله ترانسليت هيبقى الـ localhost وبالتالي قدرت اتخطى ده, الي هو زي لما تيجي تتصل بحد صاحبك مش بيرد غير على الي يعرفهم ف انت بتتصل من رقم جديد وهو مش عارف مين ده ف بيرفض ف تروح مسجل رقمك ف التروكولر باسمك وبالتالي لما تتصل هيظهرله.
- تاني حاجة تقدر تعمل بيها bypass لو كلمة Localhost او 127.0.0.1 معمولهم black listed هي الـ IP hexadecimalاو بمعنى تاني الـ Long IP وهو انك تحول الـ IP لـ hexadecimal.
- لو كان بيبلوك كل حاجة ف جرب تعمل access لـ corp domains ودي محدش يقدر يعملها access غير موظفين الشركة, زيcorp.yahoo.com
- لو حصل بلوك لكل حاجة زي (127.0.0.1 , ::1 , 127.1 , localhost) وكل ده, جرب تخلي الـ URL كده http://127.1/%25%36%31dminيعني تعمل encoding لحرف الـ a او كل الكلمة.
- لو ثغرة الـ SSRF بتقبل endpoint بس مش URL كامل فـ انت محتاج تلاقي endpoint فيها open redirectionبحيث لما تدي الـ enpoint للـ SSRF هيروح منفذها عادي وبعدين يعمل redirection للـ URLالي انت محتاجه.
- ممكن لو في ثغرة XXE تحولها أو تستغلها في إنك تنفذ SSRF Attacks.
- ممكن تستغل الثغرة في إنك تعرف الـ IPs الي شغالة مع نفس الموقع على نفس السيرفر.
- أحيانا السيرفر بيعمل check على إن البارامتر موجود ولا لا, ف ممكن نضيف نفس البارامتير بالدومين الخارجي بتاعنا ونخليه البارامتر الأول.
- في الـ Input field الي بتكون فيها إضافة URL والـ Input الي بتضيف فيها URL خارجي علشان يبعتولك عليها notifications وكده.
- لو كتبت 127.0.0.1 ورجعلك الـ status code 404 جرب تضيف بورت بعد الـ IP وتشوف الرد لو كان بإن البورت مقفول يبقى هو كده بينفذ الـ SSRF.
- جرب تكتب 0.0.0.0:22 كـ Bypass للـ 127.0.0.1.
-
-