الفصل التاسع
ثغرة ال IDOR

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال IDOR

- حيث سنتعرف اليوم على ثغرة تصيب تطبيقات الويب وتتسبب في سرقه بياناتك الحساسه مثل الحسابات البنكيه او كلمات المرور واسم المستخدم ويتم ذلك من خلال السماح للمستخدم بإدخال input لمتغير دون ان يتم التحقق منه.
- ثغرة IDOR تعتبر من أخطر الثغرات ولها نصيب في OWASP Top 10 في سنة 2013 وتأخذ رقم CWE-639 وأصابت الكثير من المواقع العالمية مثل تويتر و فيسبوك و أوبر الخ.. .
- ثغرة IDOR تعتبر Web Parameter Tampering (Authorization Bug) وهي تحدث عندما يضع المبرمج متغيرا (user-input) والمستخدم يستطيع تغيير قيمة هذا المتغير, وهو غير مصرح بتغييره, ولهذا تم تسميتها (Insecure Direct Object References)

ثغرة ال IDOR (تكمله...)

- لمن لم يفهم ماذا اعني بكلمة "متغير" هو البراميترات مثلا لاللحصر عندما تشاهد موقع بهذا الشكل : http://evil.com/test?name=1337r00t
- ال name هو المتغير و 1337r00t هو قيمة المتغير .
- # شرح عملي :-
- رأيت موقع بيع هواتف وأحببت انت ان تشتري آيفون لكن قيمة الآيفون 5000 ريال وانت لاتمتلك هذا المبلغ, لكن عندما طلبت شراء الآيفون لاحظت ان رابط الطلب أصبح :-

```
https://phonemarket.com/buy/iphone?price=5000
```

ثغرة ال IDOR (تكمله...)

- قمت انت بتغيير قيمة متغير price الى 10 فتم وضع قيمة الآيفون 10 ريالات في سلة المشتريات وشريته فعليا بهذه القيمة ! هنا حدثت ثغرة IDOR
- مثلا أخر لكل منشور او تعليق على Facebook يوجد له id خاص به ويمكن للمستخدم حذف او تعديل اي منشور من خلال ذلك المعرف وهنا يقوم المهاجمين بإستغلال هذه النقطه من خلال إرسال request حذف او تعديل لمنشور ما، ثم يقوم بتغيير ال id وإدخال idمنشور الضحية وهنا تتم عمليه استبدال للبيانات
- ومن هنا يمكن للمهاجم حذف تعليق او تعديل نص او الاطلاع على بيانات اي شخص داخل مجموعة وذلك لأن الموقع هنا مصاب وسيقوم بتنفيذ الطلب دون التحقق منه!

ثغرة ال IDOR (تكمله...)

- مثلا اخر موقع او متجر شراء يستخدم username في الرابط
- www.example.com/username=MissAngela/details
- ومن المفترض ان هذا الرابط سيعرض معلومات بطاقة الدفع او visa لدي وهنا اذا كنت اعرف username مستخدم يقوم بعمليات شراء كثيرة اي يملك مال كثير وليكن اسم المستخدم مثلا majd
- هنا سأغير المدخل في الرابط واضع user الضحية
- www.example.com/username=majd/details
- فإذا كان الموقع مصاب سيعرض معلومات visa الضحية او بيانات الشراء
- او حتى يمكنني وضع users عشوائيا وسرقة جميع بيانات المستخدمين!

ثغرة ال IDOR (تكمله...)

- مثال اخر موقع لتحميل تطبيقات مدفوعة
- قمت بشراء تطبيق وكان رابط التحميل على الشكل التالي:
- www.example.com/app_id=11/download
- ويبدو من الرابط السابق ان كل تطبيق له رقم id خاص به واذا قمنا بتغيير id لنضع 12 سأستطيع الوصول إلى تطبيقات اخرى مدفوعة مجانا..!

ثغرة ال IDOR (تكمله...)

- # التجنب عن هذه الثغرة :-
- يجب عليك عزيزي المبرمج ان لاتعطي المستخدم الأمكانية على تغيير البيانات الحساسة او اللذي من الغير طبيعي تغييرها .
- ايضا يجب على المطور او مسؤول حمايه الموقع او المتجر تجنب إظهار الملفات المهمة بالموقع وان يكون التحقق من الطلبات وربطها بـ token مخصص (وهي قيمة يتم توليدها عشوائيا) خاصة بكل مستخدم منفرد حيث لايتم قبول اي طلب اذا لم يتوافق ال token الذي يكون مع الطلب
- يوجد بعض plug-ins المفيدة في burpsuite مثل
- Authz , AuthMatrix, Authorize لاختبار هذه الثغرة و الكشف عنها

تم بحمد الله انتهاء الفصل التاسع