السلام عليكم ورحمة الله وبركاته

IDOR

سنقدم في هذا التقرير شرح عن ثغرة IDOR ماهي الثغرة وكيف يمكن الحماية منها وكيف يمكن استغلالها

ثغرة IDOR، التي تعني Insecure Direct Object Reference، هي نوع من الثغرات الأمنية التي تحدث عندما يكون من الممكن للمستخدمين الوصول إلى موارد معينة من خلال الإشارة المباشرة إلى هذه الموارد باستخدام معرفات يمكن التنبؤ بها، مثل أرقام أو معرفات فريدة (IDs)، دون التحقق المناسب من الصلاحيات.

مثال بسيط على الثغرة :

لديك رابط URL للوصول إلى ملف معين: example.com/files/1234

إذا قام مستخدم بتغيير الرقم في URL إلى example.com/files/1235 وتمكن من الوصول إلى ملف لا ينبغي له رؤيته، فهذا يعني أن الموقع يعاني من ثغرة IDOR.

كيف استطيع حماية موقعي من الثغرة ؟ :

التحقق من الصلاحيات (Authorization):

تأكد من التحقق من صلاحيات المستخدم قبل السماح له بالوصول إلى أي ملف او يوزر

التحقق من الملكية (Ownership Checks):

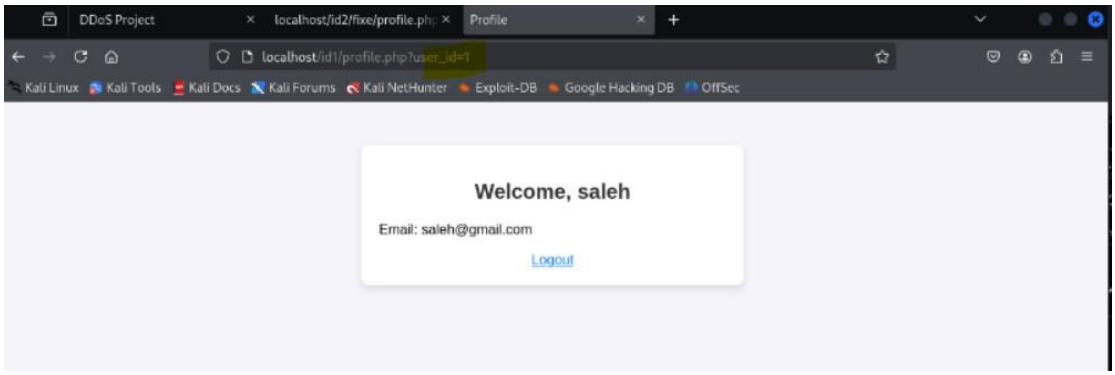
عند الوصول إلى الموارد الحساسة، تأكد من أن المستخدم الحالي هو المالك الفعلي للمورد أو لديه الحق في الوصول إليه

تشفير المعرفات (Object References):

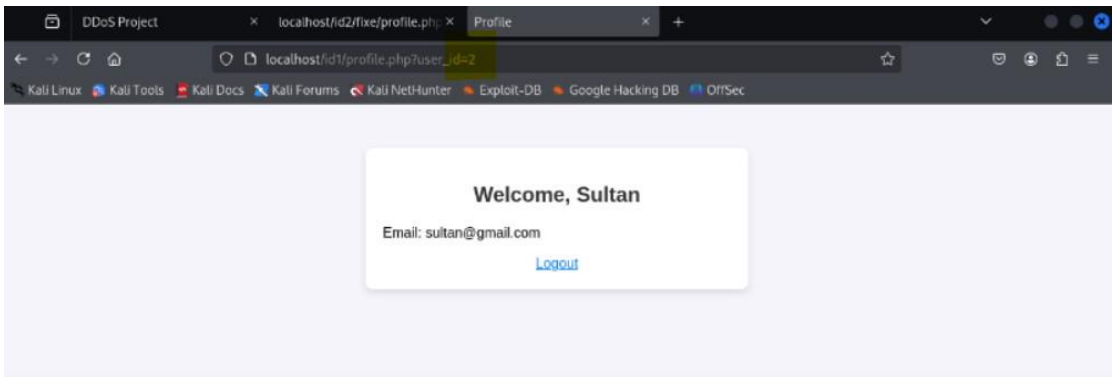
يمكنك تشفير المعرفات أو استخدام رموز موقعة (signed tokens) لمنع التلاعب بها

وسنقوم بشرح ذلك بشكل افضل بالجزء العملي لكي تتوضح الصورة

الجزء العملي :

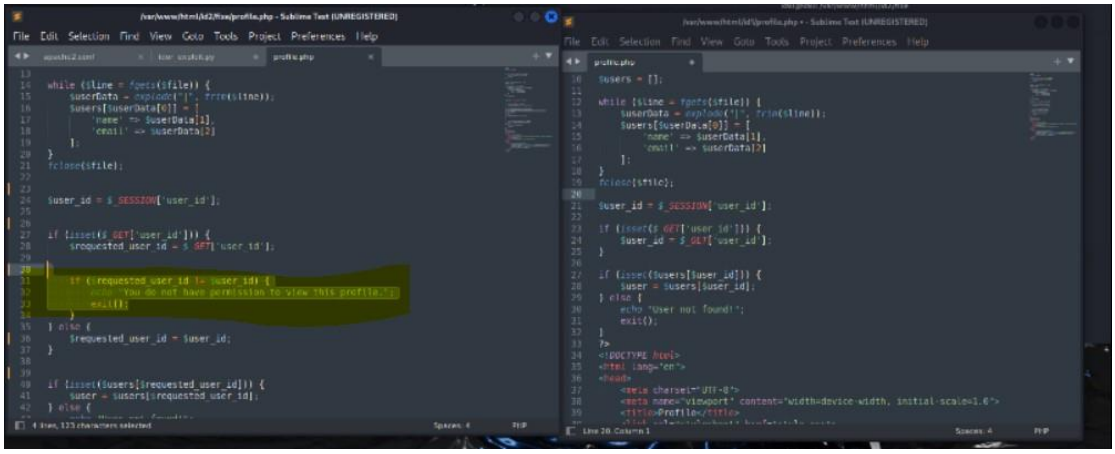


لدينا هنا موقع مصاب قمنا بتسجيل الدخول فيه وظهر لنا ال ID نقوم بالتلاعب فيه وتغييره للوصول لمستخدم اخر

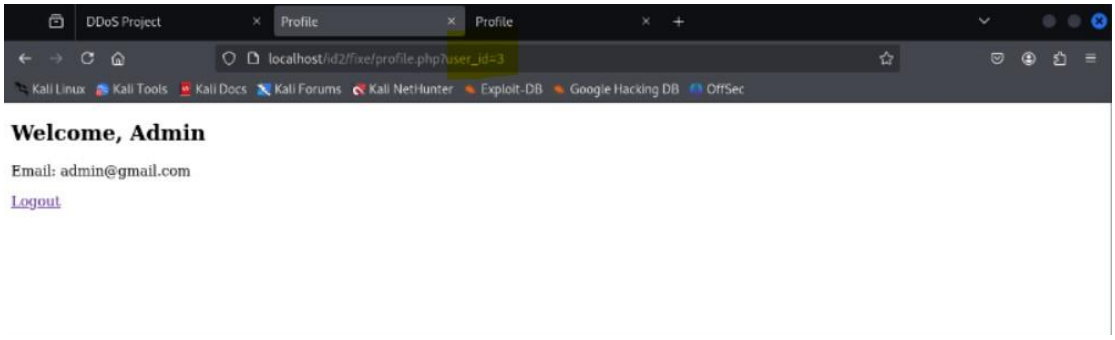


عندما قمنا بتغيير ال ID في الرابط استطعنا الدخول على يوزر اخر في الموقع

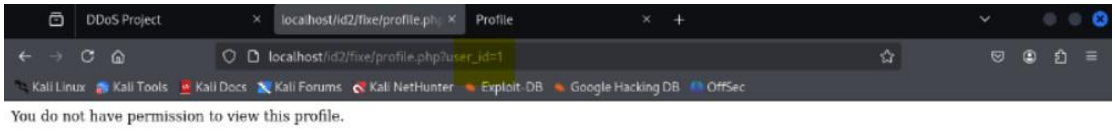
كيف يمكننا الحد من هذه الثغرة ؟



قمنا بإضافة هذا التعديل في كود الموقع واضافة وسيلة حماية لجعل الموقع يتاكد من قيمة ID قبل قبول الطلب



الان قمنا بالدخول للموقع بعد التعديل لنجرب هل مازالت الثغرة موجودة ام لا



بعدما حاولنا التلاعب مره أخرى بالرابط اظهر لنا اننا لانستطيع بسبب عدم وجود الصلاحيات ف هكذا قمنا بحماية موقعنا ووصلنا الى نهاية التقرير

أسماء الطلاب:
صالح النهابي
سلطان الحربي

إشراف: باسم الحربي