**Macro**

بسم الله الرحمن الرحيم المقالة هذي بتكون تحليل لملف excel يحتوي على ماكرو

باختصار وشو الماكرو؟ هي خاصيه تتيح للي مسوي الملف التحكم بشكل اكبر سواء بالجداول و تعديلها و يكون فيه تفاعل مع المستخدم و طبعا الهكر ممكن يستغلها لأشياء لصالحه و يجيب شل على الجهاز

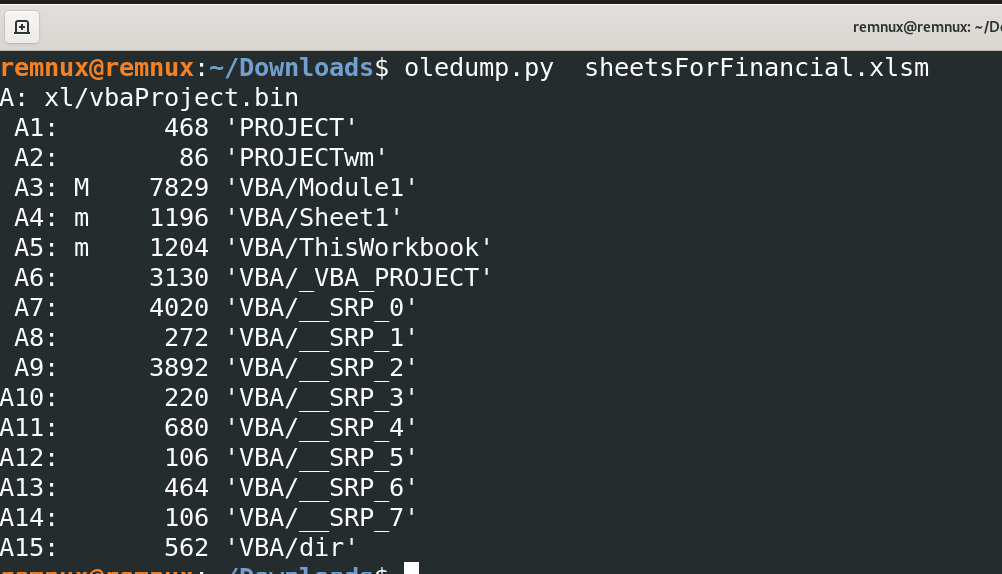
​

في البداية نشوف نوع الملف

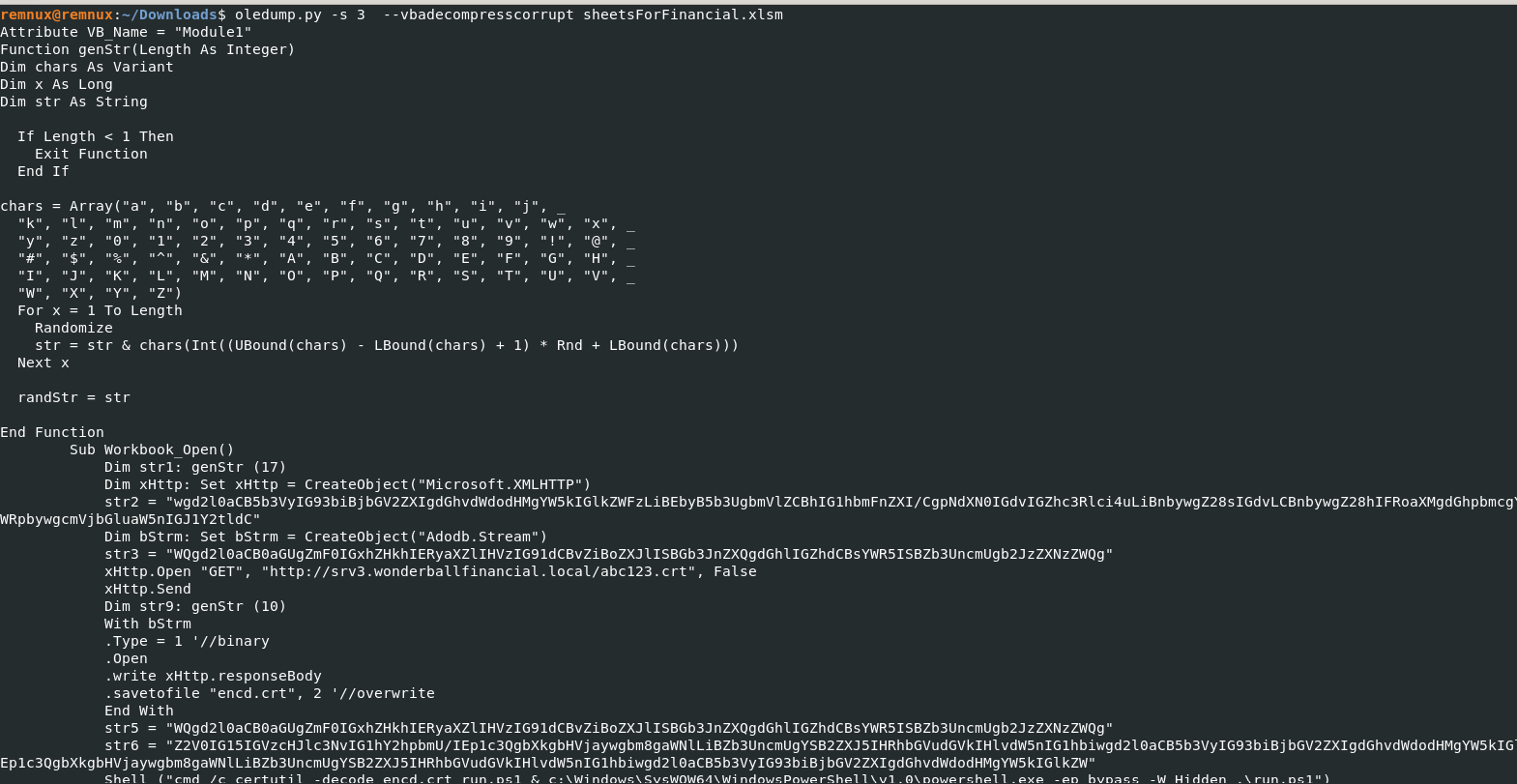
Text

Description automatically generated

عرفنا انه ملف excel و الاصدار حقه و الحين نشوف هل يحتوي على ماكرو او لا و نقدر نستعمل oledump.py

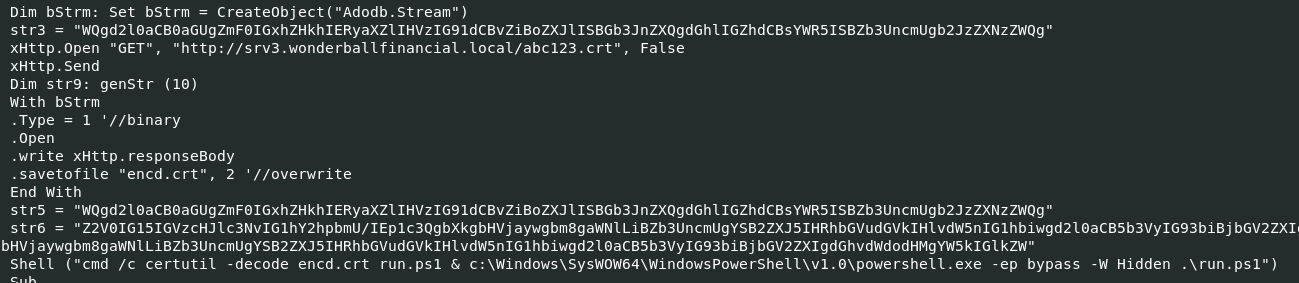


الماكرو اللي نبحث عنه يكون M و هذا يعني انه ماكرو طيب الرقم حقه هو A3 الحين نستخرج الكود حقه



شغلنا الاداة و حطينا 3 اللي هو A3 و vbadecompresscorrupt عشان نطلع الكود و بعدها الملف نفسه و طلعت لنا الاكواد

oledump.py -s 3 --vbadecompresscorrupt sheetsForFinacial.xlsm



لو نلاحظ عند Shell شغل cmd و حمل ملف من النت و بعدين سو decode له و شغله ك powershell file

​

الموضوع سهل بس مرات الهكر يخلي قرايه الكود اصعب ف يسوي يشفر الكود حقه ليكون اصعب تحليله

​

**الملخص**

شفنا نوع الملف و اكتشفنا فيه ماكرو استخرجنا الماكرو و حللنا الكود و اكتشفنا انه يشغل powershell

​

ان شاء الله تعجبكم و اذا فيه اخطاء نبهوني