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

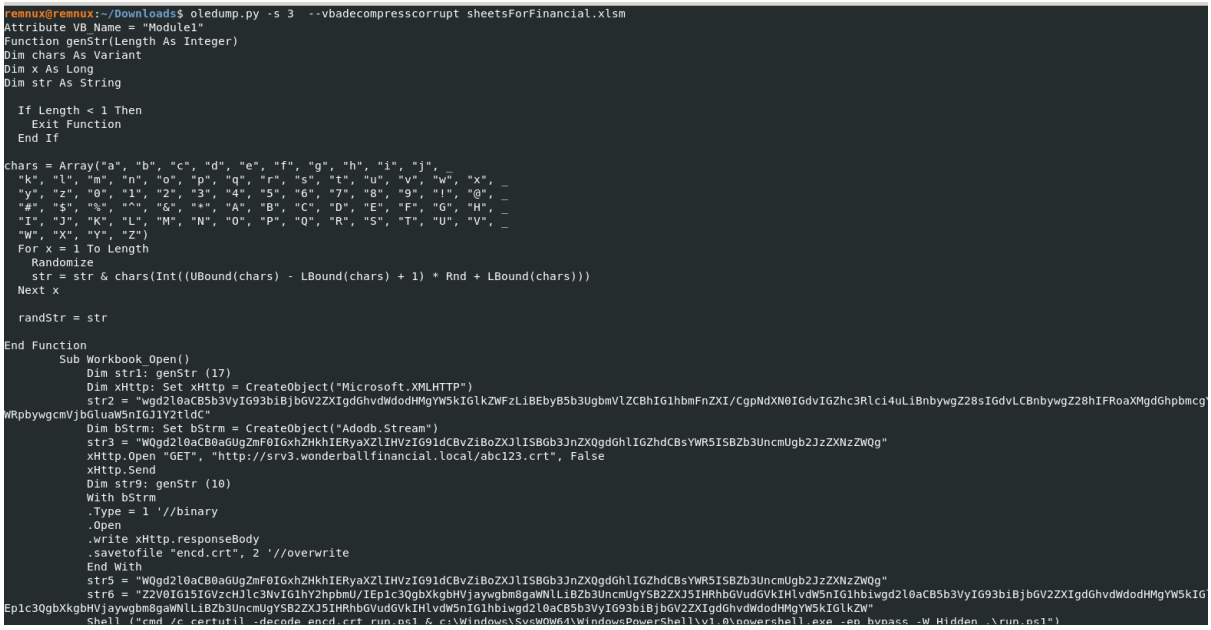
في البداية نشوف نوع الملف

```
remnux@remnux:~/Downloads$ file sheetsForFinancial.xlsm
sheetsForFinancial.xlsm: Microsoft Excel 2007+
remnux@remnux:~/Downloads$
```

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

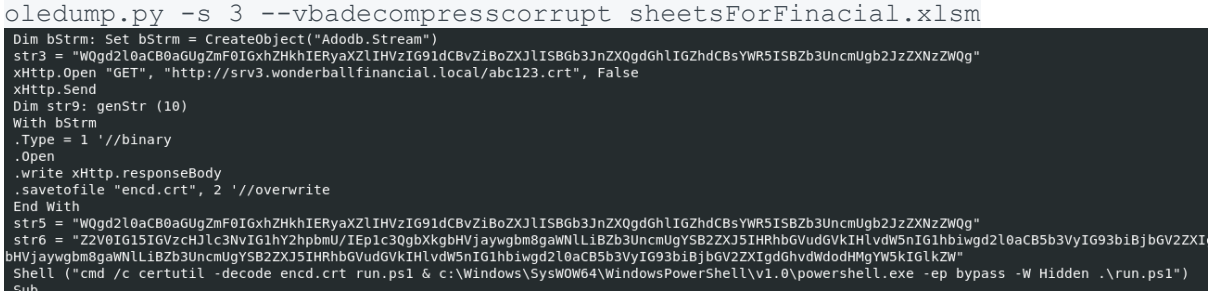
```
remnux@remnux:~/Downloads$ oledump.py  sheetsForFinancial.xlsm
A: xl/vbaProject.bin
 A1:       468 'PROJECT'
 A2:        86 'PROJECTwm'
 A3: M    7829 'VBA/Module1'
 A4: m    1196 'VBA/Sheet1'
 A5: m    1204 'VBA/ThisWorkbook'
 A6:      3130 'VBA/_VBA_PROJECT'
 A7:      4020 'VBA/__SRP_0'
 A8:       272 'VBA/__SRP_1'
 A9:      3892 'VBA/__SRP_2'
A10:       220 'VBA/__SRP_3'
A11:       680 'VBA/__SRP_4'
A12:       106 'VBA/__SRP_5'
A13:       464 'VBA/__SRP_6'
A14:       106 'VBA/__SRP_7'
A15:       562 'VBA/dir'
```

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