Fuzzing a Local Client Application

Write a Python Script to Crash the VUPlayer Application

In this Lab we want to write some code to cause the VUPlayer application to crash. But this time we will be using Python instead of SPIKE (will get back there later, no worries :D). On the desktop of your VM, you should find a basic starting point for our python script.

Ask your instructor to explain the basics of this code.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
buffer = "\x41" * 500
payload=buffer
f = open ("bad.m3u", "w")
f.write(payload)
f.close()
```

Task #1: Creating a bad playlist

Open the file using the Python IDLE and just hit the “F5” button. This should create the bad.m3u file. Start VUPlayer and load the playlist in the application.

A) Did the application crash?

Task #2: Debugging using Immunity Debugger

This time open the application and then use your Immunity Debugging skills to load the VUPlayer and then resume its execution. After that open the bad playlist that we just created.

B) Did the application crash?

C) Did you find any of the data sent in Immunity? Where?

Task #3: Repeat, repeat, repeat…..

If the application did not crash, go back to Task #1 and double the buffer size (increase it). Then repeat Task #2 again.

Keeping repeating Task #3, which is actually just a loop to repeat Task #1 and Task #2 until you get VUPlayer to crash. This will lead Immunity Debugger to pause the application. Then we can inspect the memory, stack, registers, etc.

When your application crashes and Immunity shows the "**Paused**" in the lower right panel, move on to the next Task.

Task #4: Exploitable?

Now, based on the rules of exploitability found in "Bug Hunting" slide #20. Is any of those situations valid? Which ones are they?

Task #5: Reflection

Please reflect on what you have learned from this lab.

Exploiting VUPlayer will be done in our next sessions… The fun is coming, we are just getting started :D