Secure Coding Phase 2

Team 7

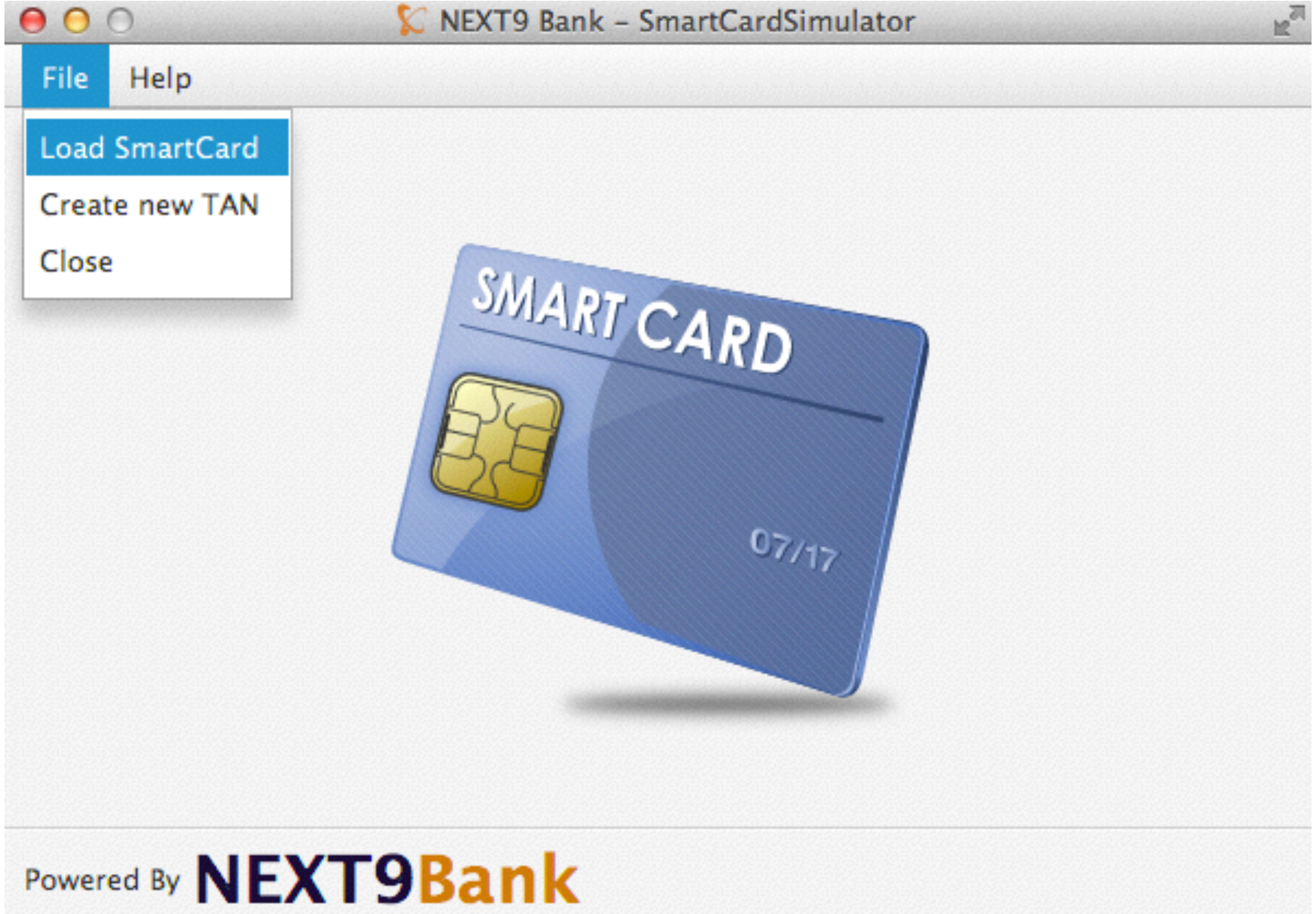
Magnus Jahnen, Thomas Krex, Elias Tatros

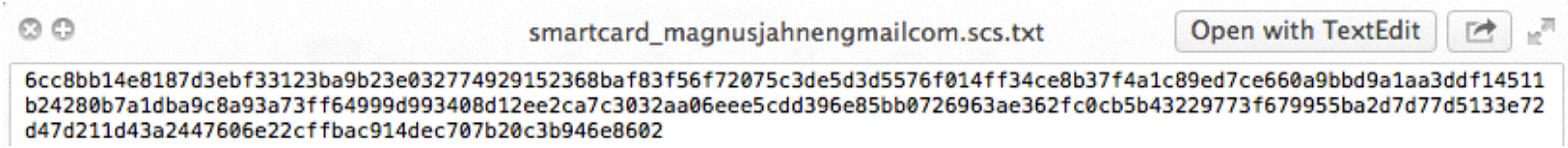
Analysed Application from **Team 8**

Vulnerabilities

Name	Impact	Likelihood
CWE-329 (Static IV in AES/CBC)	high	low - medium
OTG-CRYPST-001 (Weak AES Key)	high	low - medium
OTG-CRYPST-003 (Memory Scan Attack)	high	low

Java SCS

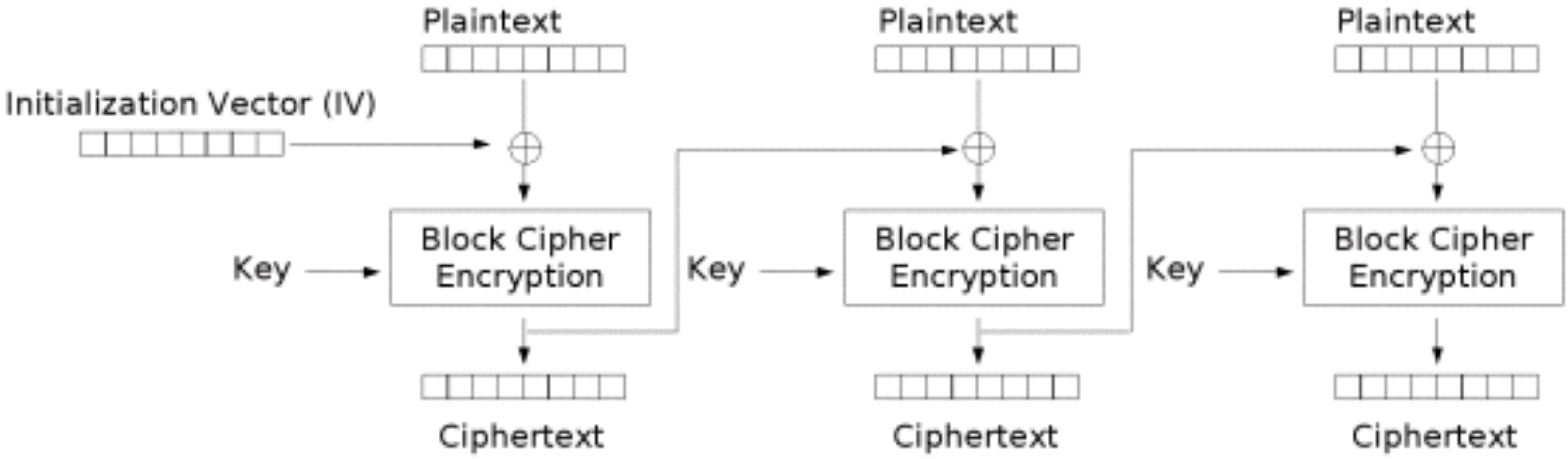




```
6cc8bb14e8187d3ebf33123ba9b23e032774929152368baf83f56f72075c3de5d3d5576f014ff34ce8b37f4a1c89ed7ce660a9bbd9a1aa3ddf14511
b24280b7a1dba9c8a93a73ff64999d993408d12ee2ca7c3032aa06eee5cdd396e85bb0726963ae362fc0cb5b43229773f679955ba2d7d77d5133e72
d47d211d43a2447606e22cffbac914dec707b20c3b946e8602
```

Static IV

```
public class MCrypt
{
    private String iv = “fedcba9876543210”;
    …
}
```



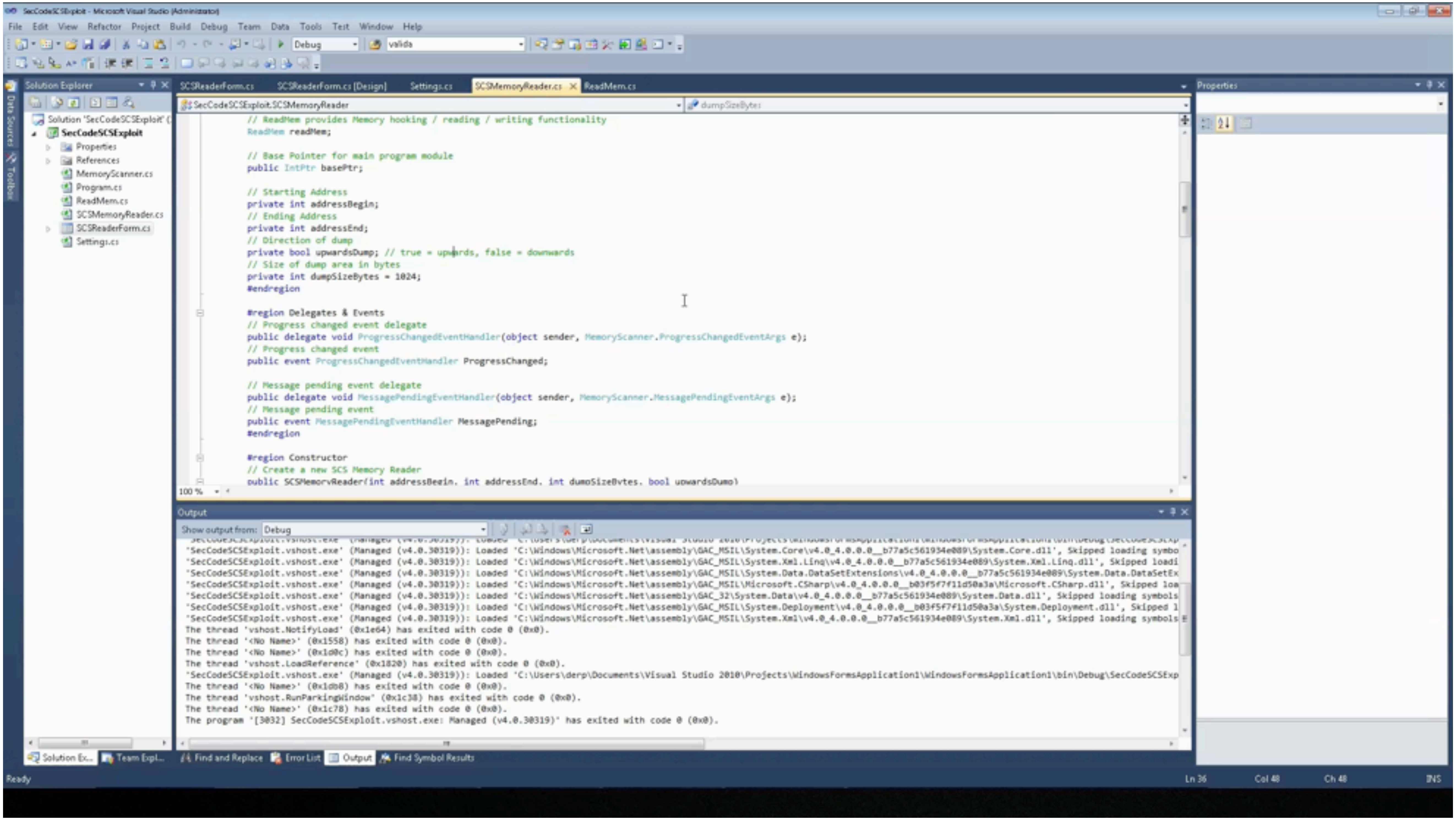
Cipher Block Chaining (CBC) mode encryption

Weak AES Key

```
public class Encryption
{
  public static String Encrypt(String data, String password)
  {
    MCrypt mcrypt = new MCrypt(password + “0000000000”);
    …
  }
}
```

- Password consists only of six digits
- Most characters of AES key are zeros

Memory Scan Attack



```
        // ReadMem provides Memory hooking / reading / writing functionality
        ReadMem readMem;

        // Base Pointer for main program module
        public IntPtr basePtr;

        // Starting Address
        private int addressBegin;
        // Ending Address
        private int addressEnd;
        // Direction of dump
        private bool upwardsDump; // true = upwards, false = downwards
        // Size of dump area in bytes
        private int dumpSizeBytes = 1024;
        #endregion

        #region Delegates & Events
        // Progress changed event delegate
        public delegate void ProgressChangedEventHandler(object sender, MemoryScanner.ProgressChangedEventArgs e);
        // Progress changed event
        public event ProgressChangedEventHandler ProgressChanged;

        // Message pending event delegate
        public delegate void MessagePendingEventHandler(object sender, MemoryScanner.MessagePendingEventArgs e);
        // Message pending event
        public event MessagePendingEventHandler MessagePending;
        #endregion

        #region Constructor
        // Create a new SCS Memory Reader
        public SCSMemoryReader(int addressBegin, int addressEnd, int dumpSizeBytes, bool upwardsDump)
```

Show output from: Debug

```
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll', Skipped loading symbo
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml.Linq\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.Linq.dll', Skipped loadi
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Data.DataSetExtensions\v4.0_4.0.0.0__b77a5c561934e089\System.Data.DataSetEx
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.CSharp\v4.0_4.0.0.0__b03f5f7f11d50a3a\Microsoft.CSharp.dll', Skipped loa
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_32\System.Data\v4.0_4.0.0.0__b77a5c561934e089\System.Data.dll', Skipped loading symbols
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Deployment\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Deployment.dll', Skipped l
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll', Skipped loading symbols
The thread 'vshost.NotifyLoad' (0x1e64) has exited with code 0 (0x0).
The thread '<No Name>' (0x1558) has exited with code 0 (0x0).
The thread '<No Name>' (0x1d0c) has exited with code 0 (0x0).
The thread 'vshost.LoadReference' (0x1820) has exited with code 0 (0x0).
'SecCodeSCSExploit.vshost.exe' (Managed (v4.0.30319)): Loaded 'C:\Users\derp\Documents\Visual Studio 2010\Projects\WindowsFormsApplication1\WindowsFormsApplication1\bin\Debug\SecCodeSCSExp
The thread '<No Name>' (0x1db8) has exited with code 0 (0x0).
The thread 'vshost.RunParkingWindow' (0x1c38) has exited with code 0 (0x0).
The thread '<No Name>' (0x1c78) has exited with code 0 (0x0).
The program '[3032] SecCodeSCSExploit.vshost.exe: Managed (v4.0.30319)' has exited with code 0 (0x0).
```

Thank you

Any Questions?