Home Assignment 0

Advanced Web Security

2017

Assignment

1 Some assignments will require you to interpret and print data in different ways, more specifically as integers, (hexadecimal) strings and byte arrays. This can lead to some confusion and headache, though the conversion typically only require one line of code. In this assignment you shall implement 6 functions to convert between these different representations. You will also use the SHA-1 hash function, which you will find built into many programming languages (so do not implement it yourself).

Example:

- The integer 500 can be written in its 4-byte (big-endian) representation `00 00 01 f4`, which is printed as an 8-byte string "`000001f4`". Hash functions typically operate on, and returns, byte arrays. Taking the SHA-1 hash of the 4-byte array above will return an array of 20 bytes (SHA-1 output is 160 bits). When printed this must be converted to e.g., a 40-byte hexadecimal string, in this case "`c6c5da207269aa4a59743ded27105b13bc8dd384`".
- The 16-byte string of hexadecimal characters "`fedcba9876543210`" can be interpreted as an 8-byte array, i.e., `fe dc ba 98 76 54 32 10`. This can in turn be interpreted as the integer 18364758544493064720. The SHA-1 hash of the 8-byte array will return byte array (of 20 bytes) which can be interpreted as the integer 946229717077375328329532411653585908948565005770.

Assessment:

- There will be one Moodle question, in a test quiz, following the problem statement and examples above. You can try this quiz as many times as you like. The test quiz will not be graded.