****

**YILDIZ TECHNICAL UNIVERSITY**

**FACULTY OF ELECTRICAL AND ELECTRONICS**

**SECURITY OF COMPUTER SYSTEMS**

**(BLM4011)**

**BUFFER OVERFLOW LAB REPORT**

20011901 – Muhammet Kayra Bulut  
19011707– Barış Can Yılmaz

kayra.bulut@std.yildiz.edu.tr  
can.yilmaz8@ std.yildiz.edu.tr

**DEPARTMENT OF COMPUTER ENGINEERING**

1. **INTRODUCTION**

The BufferOverflow attack occurs when the input value recieved from user is longer than the expected length of input, if this input values are to be stored statically. A hacker who knows the background of the system can easily enter the system. All it has to do is enter an input that is longer than the memory space allocated by the program. When we look at the example given to us, the 'isAdmin' value takes up 4 bytes, the 'userName' value takes up 20 bytes, and the 'password' value takes up 20 bytes. Since these variables are defined statically, the value corresponding to the largest address of the stack is 'idAdmin' followed by 'password' and 'username' in the stack.Therefore, when a value greater than 40 bytes is entered in the 'userName' field or a value greater than 20 bytes in the 'password' field, the hacker can manipulate the 'isAdmin' value as he wishes to gain unauthorized access to the system.

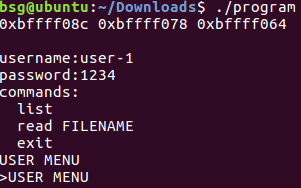
1. **METHOD**

The hacker obtains or tries to solve the systematics of the system to enter the system. Then, it determines the method according to the structure of the variables in the system and the memory organization of the system. If the variables in the system are defined statically and sequentially, the system is very vulnerable to an attack using Buffer Overflow. The hacker tries to access the system with certain lengths as brute-force. Finally, the hacker accesses the system and can perform operations such as deleting, copying, and manipulating data as he wishes. The hacker can intimidate with this and offer money in return.

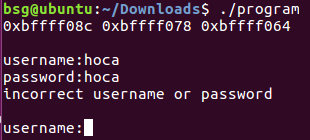


1. **RESULTS**

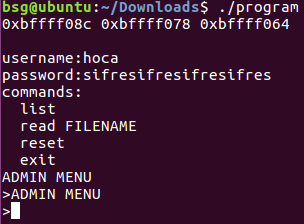
For the examples given, there is a 0x14 byte difference between 0xbffff08c and 0xbffff078, that is, 20 bytes in decimal. Similarly, there is a 0x14 byte difference between 0xbffff078 and 0xbffff064, that is, 20 bytes in decimal.

****

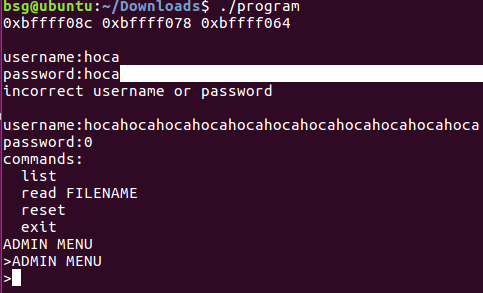
For the sample code given here, we logged in as normal



There we loggedin normally for given example code.

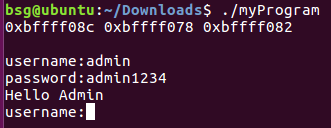


In this example we entered a very long password and occured a buffer overflow for given code.

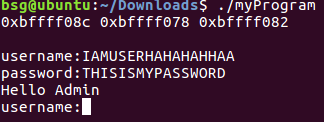


For the example code given here, we entered the user name long and overflowed the buffer.

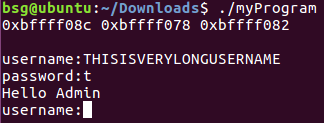




There we logged in normally for our code



In this code, we entered very long password and achieved buffer overflow attack



There we entered long username and occured a buffer overlfow attack successfully