vault-door-1

Medium Reverse Engineering picoCTF 2019

AUTHOR: MARK E. HAASE

Description

This vault uses some complicated arrays! I hope you can make sense of it, special agent. The source code for this vault is here: VaultDoor1.java

Hints

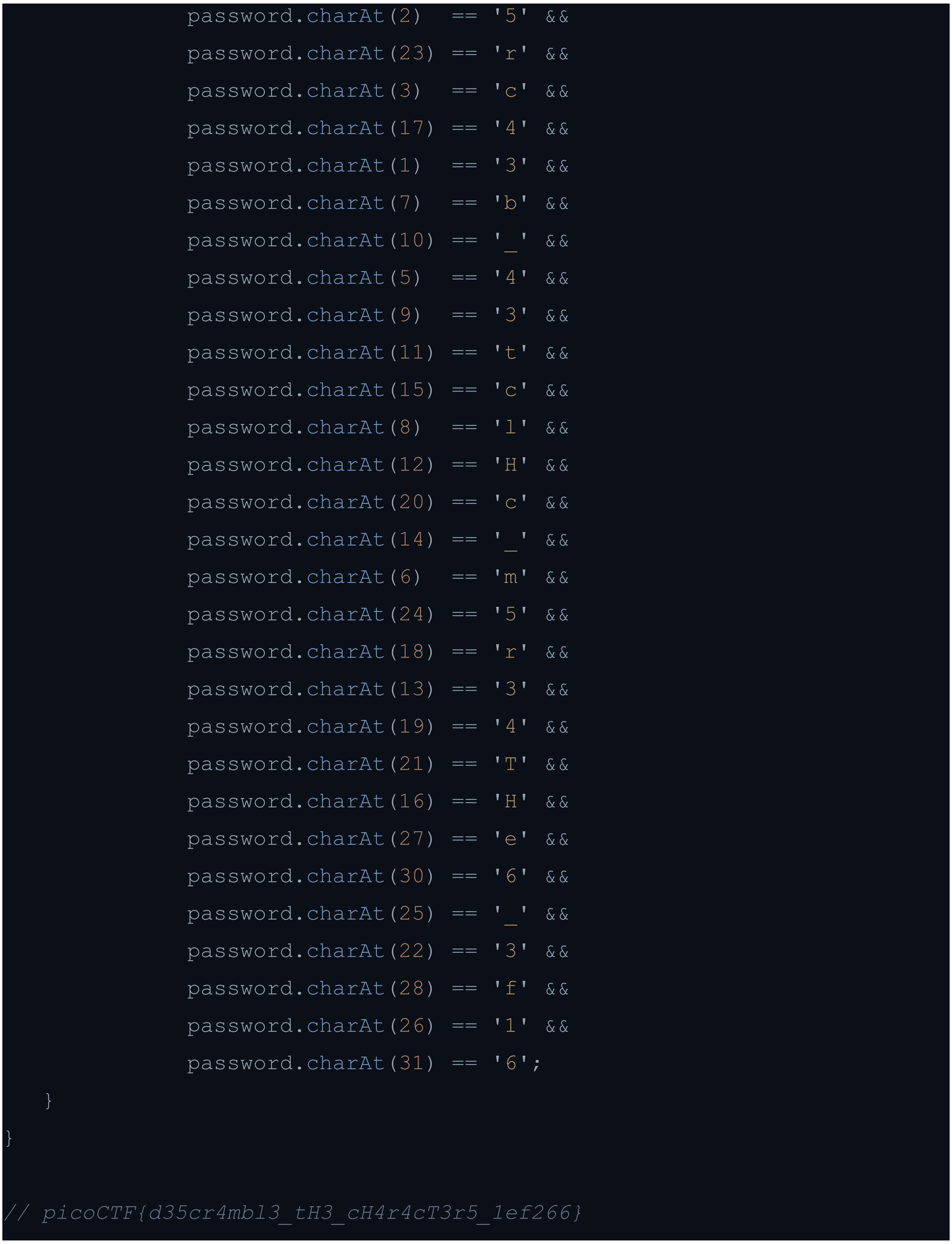
1

Look up the charAt() method online.

```
import java.util.*;

class VaultDoor1 {
    public static void main(String args[]) {
        VaultDoor1 vaultDoor = new VaultDoor1();
        Scanner scanner = new Scanner(System.in);
        System.out.print("Enter vault password: ");
    String userInput = scanner.next();
                                    String          input          = userInput.substring("picoCTF{".length(),userInput.length()-1);
    if (vaultDoor.checkPassword(input)) {
        System.out.println("Access granted.");
    } else {
        System.out.println("Access denied!");
    }
    }

    // I came up with a more secure way to check the password without putting
    // the password itself in the source code. I think this is going to be
    // UNHACKABLE!! I hope Dr. Evil agrees...
    //
    // -Minion #8728
    public boolean checkPassword(String password) {
        return password.length() == 32 &&
               password.charAt(0)  == 'd' &&
               password.charAt(29) == '2' &&
               password.charAt(4)  == 'r' &&
```



```
              password.charAt(2)  == '5' &&
              password.charAt(23) == 'r' &&
              password.charAt(3)  == 'c' &&
              password.charAt(17) == '4' &&
              password.charAt(1)  == '3' &&
              password.charAt(7)  == 'b' &&
              password.charAt(10) == '_' &&
              password.charAt(5)  == '4' &&
              password.charAt(9)  == '3' &&
              password.charAt(11) == 't' &&
              password.charAt(15) == 'c' &&
              password.charAt(8)  == 'l' &&
              password.charAt(12) == 'H' &&
              password.charAt(20) == 'c' &&
              password.charAt(14) == '_' &&
              password.charAt(6)  == 'm' &&
              password.charAt(24) == '5' &&
              password.charAt(18) == 'r' &&
              password.charAt(13) == '3' &&
              password.charAt(19) == '4' &&
              password.charAt(21) == 'T' &&
              password.charAt(16) == 'H' &&
              password.charAt(27) == 'e' &&
              password.charAt(30) == '6' &&
              password.charAt(25) == '_' &&
              password.charAt(22) == '3' &&
              password.charAt(28) == 'f' &&
              password.charAt(26) == '1' &&
              password.charAt(31) == '6';
   }
}

// picoCTF{d35cr4mbl3_tH3_cH4r4cT3r5_1ef266}
```