Assignment 0x05

Frank Kaiser – 1742945, Jan Martin – 1796943

January 20, 2018

Contents

1 Setting up the Environment

As username I was very creative and chose "frank". The IP-Address is: 10.136.0.114. The VM's address is: 10.137.2.170

2 Bypass the login

To bypass the login we used: `' or 1=1 -- `. It is important to include the whitespace after the SQL Injection. When visiting Daisy Duck's profile page, the URL changes to `http://10.137.2.170/index.php?page=profile&userid=6`. So now we know the userid of Daisy Duck is 6.

To successfully login as Daisy we used the injection: `' or id=6 -- `. Her favourite movie is:

2.1 Explain the underlying problem of the vulnerability and how to fix it. What advice would you give to a developer who uses SQL?

TODO: (Prepared SQL statements)