



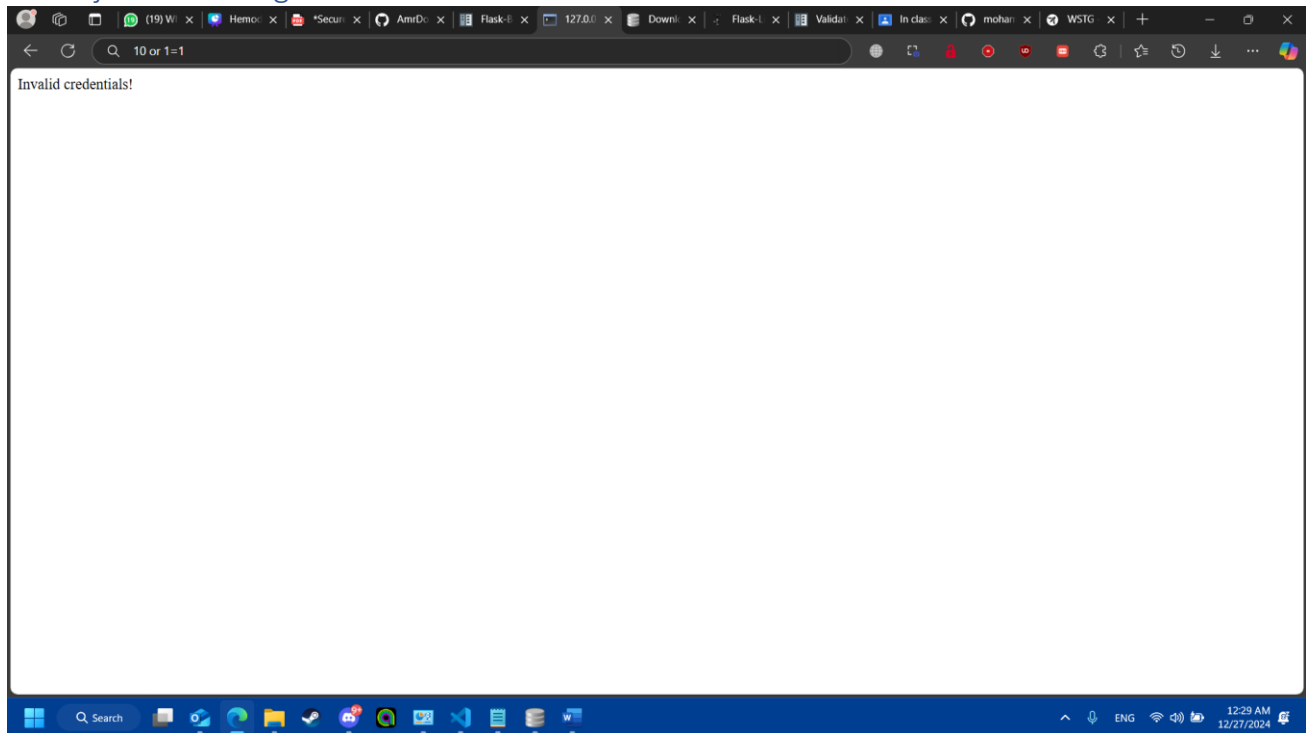
Security Task

To: Eng. Mohamed Abdelhalim
Team Members:

Amr Doma (1210273)
Tarek Waleed (1210246)
Habiba Walid (1210215)

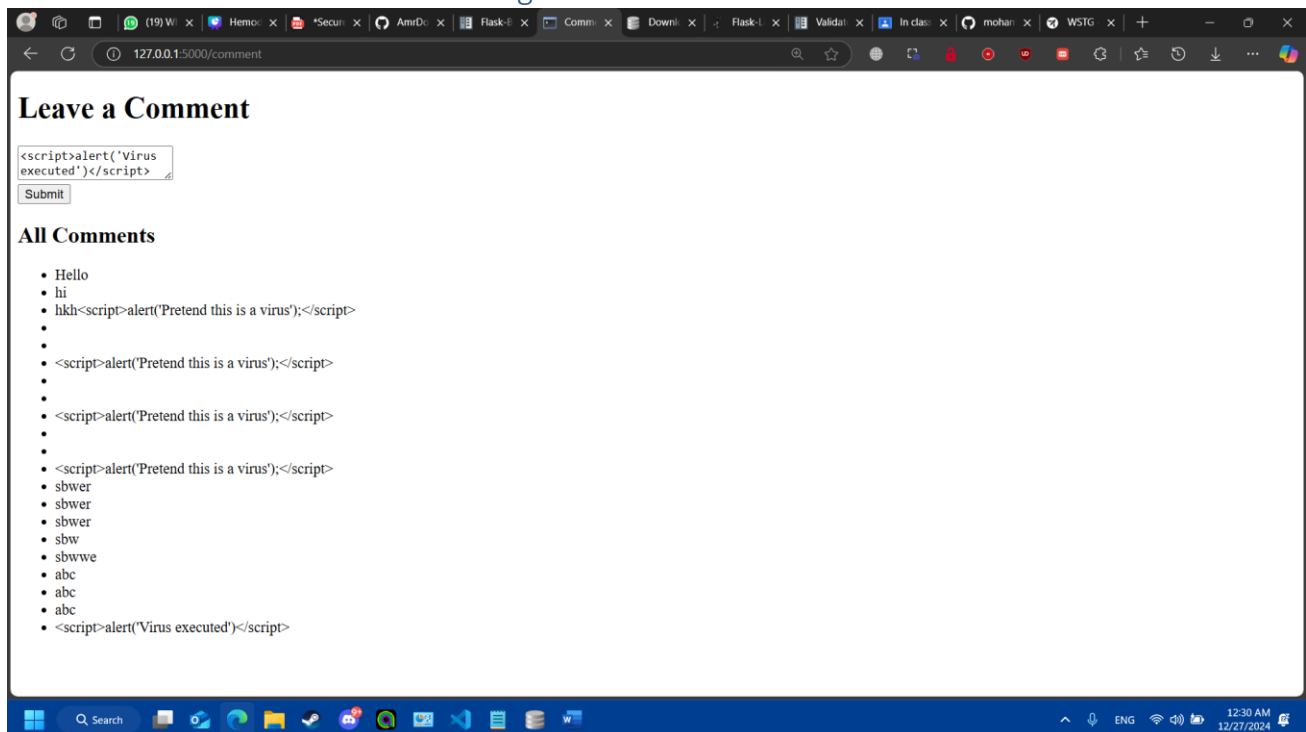
Test Vulnerabilities

SQL Injection on Login



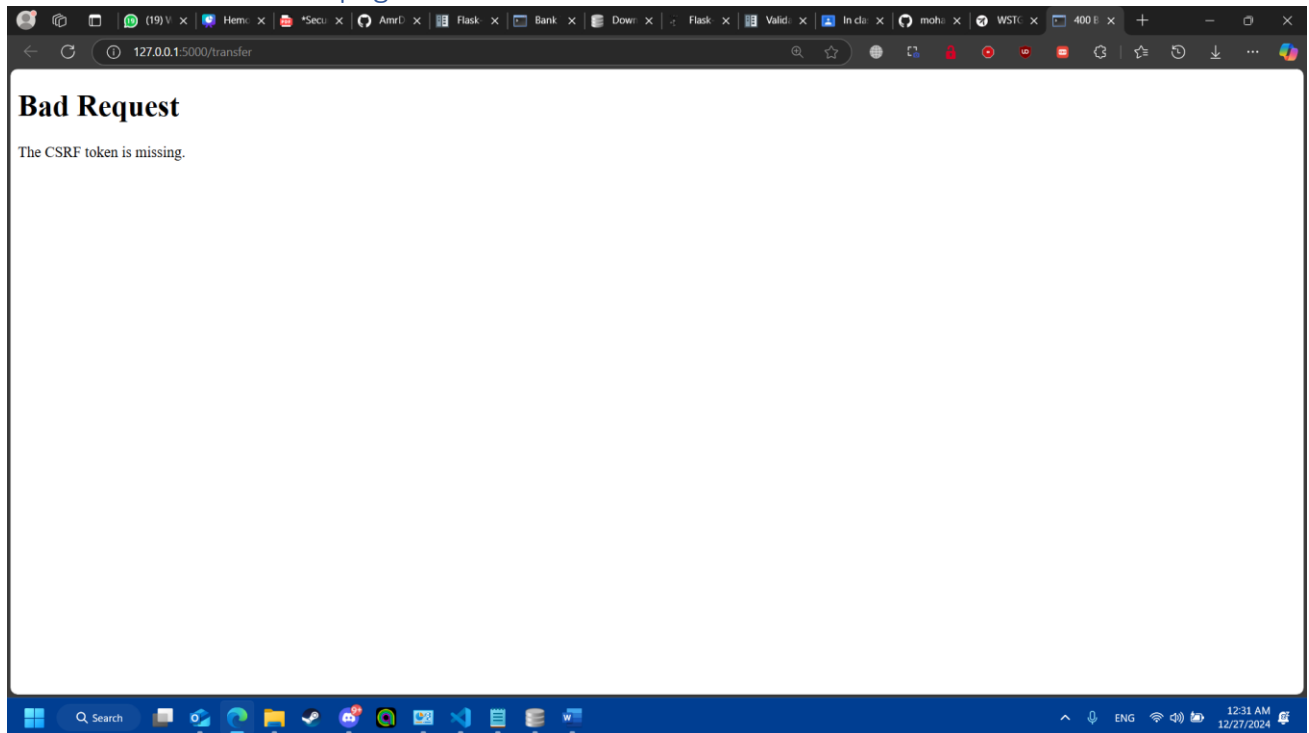
On using username that exists in database and the password “10 or 1=1”, we get invalid credentials because we have escaped the inputs and also we compare for hashes so that’s not a hashed value which returns none

Unsanitized comments for XSS testing



The comment `<script>alert('Virus executed')</script>` is converted to markdown text so that it is not executed

CSRF attack on transfer page



The page is missing a CSRF token which is only granted through the server when redirecting