**Task 1 answer**

Password are often the weakest link in the security chain. A weak password is often a re-used password, and it is easily exploitable with a brute-force attack reading from a list of common weak passwords. These weak password lists have been catalogued over the years from case studies in hacked sites and are widely available.

**Task 2: Command injection**

1. flag{command\_injection\_is\_a\_serious\_vulnerability}
2. Navigated to URL <http://192.168.56.102/hackable/uploads/> then <http://192.168.56.102/hackable/uploads/flag.txt>
3. Because the website’s security level is very low to nil, I figured the file directory from the root of the web application was available. Tried the hackable/uploads path and it got me to the directory. It looks like the web server is not configured to deny admin user the ability to browse and request any file type.

**Task 3: Local file inclusion**

**Task 4: File upload**

**Task 5: SQL injection**

**Task 6: Weak Session ID**