# Question 1

The Registration.name() function is pasted below.

Text

Description automatically generated

The tests for assignment 3 part 1 are pasted below.

Text

Description automatically generated

Text

Description automatically generatedText

Description automatically generated

The results for the tests are pasted here.

Graphical user interface, text

Description automatically generated

# Question 2

1. Five high alert vulnerabilities are.
   * <http://testasp.vulnweb.com/>
     1. Path Traversal
     2. Reflected Cross Site Scripting
     3. SQL Injection
     4. External Redirect
2. The five vulnerabilities have the following description and were found with OWASP ZAP 2.12.0
   * Path Traversal – an attack where the attacker has access to files and directories outside of the web document root directory. Per OWASP ZAP this attack is often carried out by using “../” which changes the current directory to the parent directory to access files anywhere on the web server.
   * Reflected Cross Site Scripting- Attack that has attacker supplied code entered into a browser to be executed.
   * SQL Injection – Attack where attacker enters an SQL query as input to run on website’s database.
   * External Redirect- External redirection itself is not an attack. However, an attacker can use social engineering to make users believe that they are at a site that is trusted when in reality it is an entirely different site. This different site can pose as another site and prompt the user to login with their account details at which point, they are at risk of being stolen
3. The vulnerabilities are critical weaknesses and can be exploited in the following ways.
   * Path Traversal- Is a critical weakness because it allows for files on the web server to be revealed. It can be executed by using a special sequence of characters used to refer to a parent directory “../”
   * Reflected Cross Site Scripting
   * SQL injection- An attacker can use SQL injection to reveal the usernames and passwords if they are stored on a database used by the website in plain text
   * External Redirect- An external redirect may lead an unsuspecting user to a phishing site where they are tricked into revealing their username and password to an attacker. This becomes more dangerous if a user uses the same login credentials for other sites or all the logins of the users for the site follow a pattern such as firstname\_lastname for the username, and a user’s year of birth for the password.
4. The vulnerabilities can be exploited in the following ways
   * <http://testasp.vulnweb.com/>
     1. Path Traversal- Enter ../ Into registration fields to get to a higher directory and to sign in to an account that you didn’t create with a valid email. Graphical user interface, text, application, email

        Description automatically generated
     2. Reflected Cross Site Scripting
     3. SQL Injection – Enter SQL
     4. External Redirect
5. To fix the issues the following strategies are recommended:
   * Path Traversal- We can assume that all input is malicious and allow only certain inputs to be used that agree with the requirements of the website. We most likely don’t need to allow the specific sequence “../” on our website. So we will validate inputs to make sure that “../” cannot be entered
   * Reflected Cross Site Scripting- To prevent cross site scripting I would perform input validation to ensure that no attacker supplied code is entered. I would also recommend doing security checks on both the client side and server side.
   * SQL Injection- To prevent this I would have a list of allowed input and reject any input with disallowed characters such as “=”
   * External Redirect- To fight against this I would recommend a list of allowed redirects on the site in question. I would also include a warning for when users are being redirected off site as seen on many 3rd party shopping sites