3. Advices for Altoro Mutual bank to close the vulnerabilities:

Altoro Mutual bank website can utilize certain strategies to prevent attackers from attacking the website and in securing the data. It is very important to build applications with utmost care to prevent it from attackers, few practices that could help to make it less susceptible to attacker's are:

- **By Implementing a Security Development Lifecycle:**

  They have to use a Security Development Lifecycle (SDL) while developing the application so that it limits the amount of coding errors as well as security flaws in the application. Thereby making the website less prone to Cross-site scripting XSS attack.

  The Security Development Cycle assumes that the data received by the web application is coming from untrusted source, even from the users who have logged and used the website multiple times.

- **By Investing in Website Vulnerability Scanners:**

  Altoro Mutual bank could make use of Website vulnerability scanners while developing the application that helps in identifying the security weaknesses and flaws in the website. This could have made the website less vulnerable to attackers. They should also ensure that the scanners are updated on regular basis.

- **By Adopting a crossing boundaries policy:**

  They should have adopted crossing boundaries policy so that they could make any authenticated users in their website to re-enter their credential details before they access certain pages and services within their website.

  For already authenticated users who has a cookie that allows them to login automatically, they can still design in such a way that they also have to re-enter their username and credentials prior to accessing certain pages within the website.

- **By Shielding website against SQL injection:**

  SQL Injection attack is where a hacker uses a URL parameter to manipulate the database and thereby gaining access to the site. In order to prevent the Altoro website from SQL injection, they should have implemented parameterized query instead of using a standard transact SQL as it is easy for an attacker to type few rogue code into the query to obtain access to website data.

- **By using the right META tags:**

  They could have use META tags to reduce the number of potential forms that a Cross-site script (XSS) injection can take.

- **By installing a Security Socket Layer:**

  The best way to use a Security Socket Layer into the website will be to use HTTPS protocol that helps us to have a secure communication over the network. So, it is very important that Altoro should implement HTTPS protocol on the website pages where users will be

submitting their sensitive information such as credentials, credit card details, financial details. If not, the attacker will be able to steal the data and impersonate the user.