Web audit deliverable 1:

Group Members: Angela Castronuovo, Ryan Brockway, Joshua Cominelli, Trent Chismar
Name of Website: Grammarly
URL: https://www.grammarly.com/
Link to Bug-Bounty Program: https://hackerone.com/grammarly?type=team

Grammarly has a very broad scope for their bug bounty program, including their website grammarly.com, Grammarly add ons for microsoft products, mobile keyboards, and extensions for various browsers. If you do make a free account to test their security, they ask that you tell them by filling out a form that links your HackerOne nickname with the email used for the account

To disclose a vulnerability to Grammarly, one should submit a form to Grammarly through the HackerOne website, and "follow disclosure guidelines". These disclosure guidelines for HackerOne are to "submit a Report to the appropriate program on the HackerOne platform. The Report should include a detailed description of your discovery with clear, concise reproducible steps or a working proof-of-concept". Additionally, Grammarly encourages public disclosure of vulnerabilities once the vulnerability is resolved. The website offers to help with the write-up by suggesting we send our write-up to security@grammarly.com.

After a vulnerability is disclosed to Grammarly, they "will respond within 3 business days", and they will "try to make a bounty determination after validating a legitimate security issue within 10 business days". If every effort was made not to act maliciously, such as not trying to access private user data, Grammarly will not take legal action. Grammarly lays out certain vulnerabilities that you cannot test for, such as "any activity that could lead to the disruption of our service". However, Grammarly states that "we will not pursue a civil action or initiate a complaint to law enforcement for accidental, good faith violations of this policy." As long as the policy is not intentionally violated, then Grammarly will not pursue any legal action against the researcher.