Hayley Cohen
Assignment 4
Technical Risk Analysis

Risk ID	Technical Risk	Technical Risk Indicator	Related CVE, CWE or OSVDB IDs	Impact Rating	Impact	Mitigation	Validation Steps
1	Cross-site scripting	Modified content, improper error messages, improper page redirects	CWE ID 80	H	HTTP response contains compromised information or modified content	Ignore </script> tags by flipping the direction of the arrows	Set a flag to alert when something that should not be modified is.
2	Code Injection	Code is being implemented that was not originally in the source code	CWE ID 95	L	Code is executed that might produce unexpected results	Authenticate users before they have access to the source code	Set a flag to alert when code that should not be modified is.
3	SQL injection	Restricted content is presented and the database is visible to the user	CWE ID 89	H	Provides user with the ability to access and modify restricted content	Filter input to check that SQL injection is not being used	Require a second form of validation
4	Information leakage	Sensitive information is present on a page if not properly logged out	CWE ID 209	L	If a user forgets to logout, someone can see the sensitive information	The page should time out if the user does not authenticate themselves again	Redirect to the login page and remove the information from the page
5	Hard coded password	Successful login attempts to accounts or excessive access to protected sites	CWE ID 259	L	Provides access to accounts and sites that should not be easily accessed	Use strong password protection and hashing methods	Check the logs that no one suspicious is being authenticated
6	Information exposed through error messages	Improper error message appears on site	CWE ID 209	H	Exposes information about the site and can be used to exploit it	Do not allow error messages except ones with general information	Only simple information can be presented to validated users
7	Cookie tampering	Cookies are able to be modified on the web browser	CWE ID 565	H	Parameters can be changed to alter restrictions of a page	Encrypt the cookies so that they cannot be easily encrypted	Validate cookies if they are modified
8	Brute force user authentication	Restricted accounts are accessed without proper credentials	CWE ID 259	H	User will have access to information and accounts	Set a number of allowed logins to prevent brute force	System locks and alerts when the allowed logins are exceeded