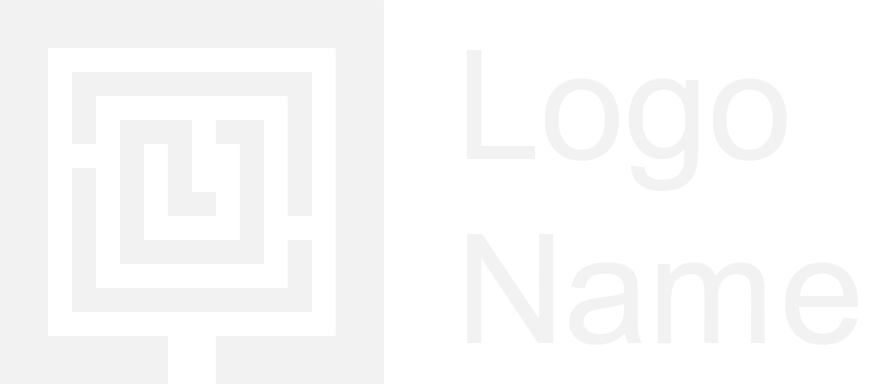
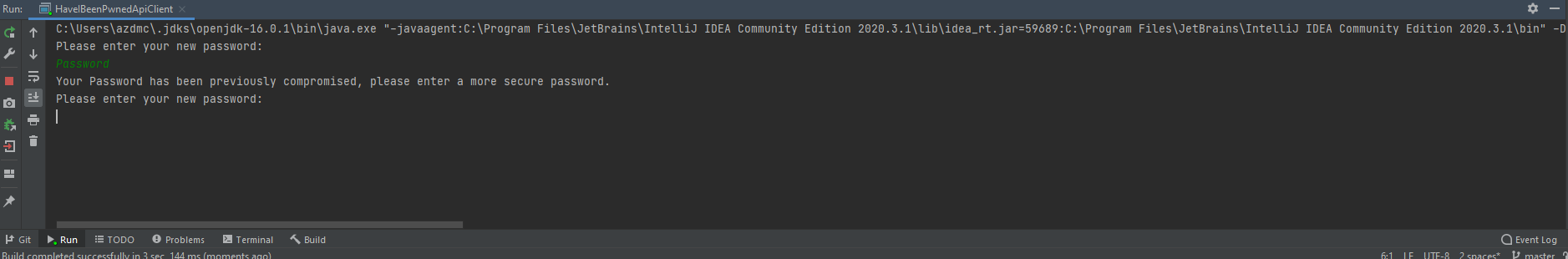


|  |
| --- |
| Broken Authentication Mitigation |
|  |
| May 3  The companies company.  Authored by: Derek McPeak |

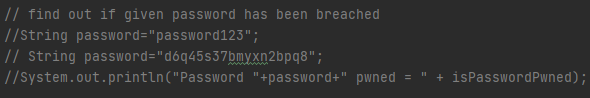


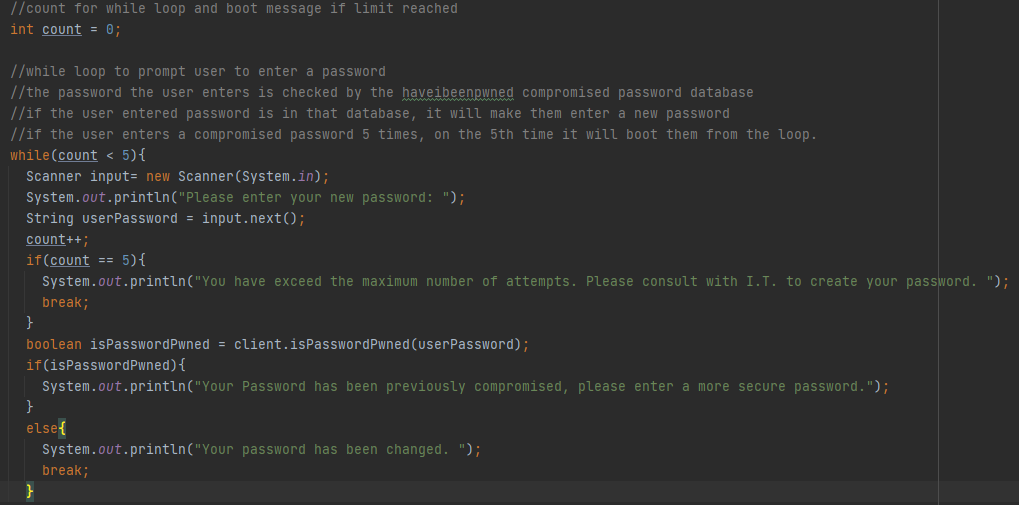
Vulnerability – Employees creating passwords that have been compromised and leaked. This will give bad actors a head-start into getting credentials for a user.

Company risk - The risk of broken authentication to the company is an employee’s credentials being leaked causing a bad actor to being able to access company systems allowing for a data spill.



Correction – The current state of the code, it will allow a user to generate a password of any quality and length. This creates a security vulnerability for our company by proxy of our employee’s password. The new password will force the user to create a password that has not been previously compromised.





The first screen shot, shows the password being tested. This will just tell if it has been compromised, there are no rules in place if a password has been compromised.

The second screen shot, shows a loop that will run a maximum of five times. If an employee is unable to create a password in five attempts, that has not been compromised, it directs them to contact IT who will create a secure password for them.

The code will be tested for further vulnerabilities, passing those tests the code will be moved into production.

Approval granted by Manager.