1. Information disclosure in error messages:
   * The application disclosed the version of the backend server when we forced an exception to occur by submitting a string value in place of an integer as the server expected an integer so it returned the entire error with full stack trace.
2. Information disclosure on debug page:
   * We used BurpSuite’s Target tab and then to site map tab and then in engagement tools we selected find comments.
   * It helped us find a HTML comment which contained a link called Debug and when hitting on that end point, we got some debug secret key info.
3. Source code disclosure via backup files:
   * Using the content discovery option in BurpSuite we managed to get into robots.txt and there we found a backup folder.
   * In there we found a file which contained all the source code of the application in which we found the POSTGRE SQL’s password for the backend database.
4. Authentication bypass via information disclosure:
   * Using BurpSuite’s Repeater we browsed to the admin page and got to know that the admin page can only be accessed if we’re on application’s network so now instead of a GET request, we sent TRACE request to the admin page.
   * In the response we found **X-Custom-IP-Authorization** header containing my IP address which was automatically appended to the request.
   * So, we went to Proxy’s Options and then in Match and Replace, left the Match condition blank and in Replace field we entered **X-Custom-IP-Authorization: 127.0.0.1.** So, now the proxy will append this to every request we send.
5. Information disclosure in version control history:
   * In this case we browsed to **/.git** to get the Git version control data so we cloned the entire directory using **Cygwin.**
   * Now while exploring the directory, we found that there was a commit about password so we started undoing all commits one by one until we get anything important in **admin.conf** file.