You are working as a group of cyber security engineers for Company X.

There is a requirement for a browser-based password generator. The existing implementation has been provided and you need to build on this. You have been provided with a docker compose file that includes two existing services:

* Flask App (Python based)
* Nginx ingress controller

You can achieve the intended outcome with the provide infrastructure. You are free to change the Flask app / python coding language for something else, but the Nginx ingress controller must be utilised.

The following are required:

* Passwords generated need to be compliant with the Application Security and Development STIG[[1]](#footnote-1)
* Logging needs to be compliant with the Application Security and Development STIG
* TLS must be implemented using a NIST 800-52[[2]](#footnote-2) recommended cipher suite
  + TLS must be strictly enforced and the application should only be accessible via HTTPS
* Security assessment must be carried out on both the originally provided implementation and image(s) and the final implementation and image(s)
* A comparison between the two security assessments must also be provided

You are expected to check and ensure that the application is checked against any other relevant STIG or SRG not listed above

In any instance where compliance with the STIG or NIST guidelines is not possible a justification must be provided and where possible the timeline for a fix

1. https://public.cyber.mil/stigs/downloads/ [↑](#footnote-ref-1)
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf [↑](#footnote-ref-2)