**NISM – Assignment 2 (Body)**

Brief Summary of the work performed:

* To include some items from the recommendations section
* Fingerprinting (From 1st assignment)
* GDPR compliance
* AWS scan
* Open-Source scan (Available tools to be used here: <https://owasp.org/www-community/Vulnerability_Scanning_Tools>) which one would you prefer?
* DNS Forwarding
* All IP scans,
* OWASP guidelines used
* Appendix 1 (graphical presentation of all errors in an easy-to-comprehend format)

Findings:

* Consult Sam’s reports results from 1st assignment
* Present our findings from the open-scan tool we will use from above
* Security Problems findings (encryption, open ports, etc.)
* Privacy problems findings [GDPR + Payment Card Industry Data Security Standard (PCI-DSS)]
* Traceroute graph (Appendix 2)

Conclusion:

* A summary of the work performed (consult first section)
* What we found (consult findings)
* Limitations (consult 1st assignment limitations section)
* Any future scans we might have to perform (only if this would happen in a real-life situation. E.g. New scan after implementing new security and privacy models)

Recommendations:

* Easy-to-read non-technical recommendations (Ahmad’s document but in a paragraph structure)
* GDPR recommendations (I will write this section, along with the above GDPR section)

\*New page for the two appendix parts\*