## Introduction:

This document is a list of prerequisite requirements needed prior to performing the web application security assessment.

## Prerequisite Requirements/Checklist:

1. Get permission to perform scans from the vendor who is hosting the noted web application.
   1. If the web application is not hosted in a third party cloud environment (e.g., AWS, Azure, Google, etc.) you can skip this step.
   2. If you have to request permission, and if you are approached, be sure to review the rules of engagements for that cloud vendor.
2. Provide a target list comprised of IPs, and URLs.
   1. You may need you to compile an exclusion list.
      1. This will contain any sections of the web application, entire URLs or IPs that are off-limits.
   2. You will need to know if any load balancers or any security appliances (NGFW, WAF, IDS/IPS, etc.) are in line with the noted web application.
3. Provide a set of relevant test credentials (username, password) for each user access levels (e.g., standard user, administrator, etc.).
   1. You only need test credentials for sections of the web application used by your employer or client.
4. Provide a scan window.
   1. When would you like us to perform the scan(s)?
   2. What time would you like us to perform the scan(s)?
   3. What time would you like us to stop scanning?
5. Provide a point of contact in case of emergencies and/or to respond to requests from your employer or client cyber security team.

NOTE: The tools used in application security assessments may create spurious data records during the course of the assessment. So, please ensure that only test date or a copy of production data is present on the target system at the time of the test.