\* What is the Plan to perform the Pen Testing:

The goal of an intrusion test is the identification of security vulnerabilities in an application that could be used by attackers for a later remediation. Conduction intrusion testing is similar to hiring security consultants to attempt a cybersecurity attack to find out how real criminals might do it. Regarding the focus for testing web applications, the OWASP Top Ten (https://owasp.org/www-project-top-ten/) provide good orientation.

\* What should we do and what is the process to do the testing (PEN Test)

The tests are performed by company CERT/CDC or their external partners. As preparation, two mandatory documents are needed (checklist & signed permission to attack) in advance of a Technical Call which should take place at least two weeks before the test. During the test, it is recommended to have a contact from the project available for questions. This is useful as well in case of critical findings, which might be erased during the test. The effort for remediation after a test is determined by the identified vulnerabilities.

We can make a draft first by seeing previous findings and some explanations for preparing intrusion tests(If not then take the examples from other organizations).

**Penetration Testing Stages**

These phases are typically demarcated as:

(1) reconnaissance,

(2) vulnerability mapping,

(3) exploitation,

(4) post exploitation, and

(5) reporting.

**(**[**https://www.nettitude.com/us/what-is-penetration-testing/**](https://www.nettitude.com/us/what-is-penetration-testing/)**) -** Explanation is is the link

**Penetration Testing Tools** ( First thing to figure out which tool and why)

* Nmap,-- (Use for vulnerability scanning) -- open source utility for network discovery and security auditing -
* Burp Suite,-- Burp Suite Professional is one of the most popular penetration testing and vulnerability finder tools, and is often used for checking web application security. “Burp,” as it is commonly known, is a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing.
* Nikto,-- software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems.
* Metasploit, -- provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
* Other Kali Linux-related tooling, and/or
* PoshC2 (<https://github.com/nettitude/PoshC2>).

**Security and Testing OWASP Procedures:**

https://owasp.org/www-project-top-ten/

I) Second layer of authentication - Two step authentication using a phone number or email id.

II) Deal with removing the ability to put in SQL queries in the fields.

III)

**3rd Party Security Questionnaire:**

I) Have incident response plans which can be executed for cyber-security (CSIRP) or patient safety issues.