

# ALLEGATO 1

## CARATTERISTICHE TECNICO – FUNZIONALI

### Caratteristiche tecnico - funzionali del servizio di una consulenza per attività di Vulnerability Scan.

Svolgimento dei seguenti test:

- Ricerca e test di vulnerabilità nella validazione dell'input al fine di rilevare eventuali vulnerabilità di tipo XSS (Cross-site scripting), SQL injection e command injection, utilizzando tool di scanning e/o fuzzer.
- Port scanning del server web con Nmap al fine di individuare Porte/servizi critici che vengono aperti in fase di installazione del server.
- Ricerca e test di vulnerabilità di tipo authorization al fine di rilevare eventuali vulnerabilità di tipo directory traversal e forceful browsing utilizzando tool di fuzzing.
- Ricerca e test di vulnerabilità nel sistema di autenticazione attraverso la simulazione di attacchi di tipo username enumeration e brute force.
- Ricerca e test di vulnerabilità lato client: test su URL Redirection e Cross Origin Resource Sharing (CORS)
- Ricerca e test di vulnerabilità nella gestione delle sessioni: verificando la robustezza ad attacchi di tipo CSRF (Cross-site Request Forgery).

1. Al termine dell'attività di analisi le eventuali vulnerabilità individuate per ogni applicazione dovranno essere classificate assegnandogli un livello di gravità e per ogni vulnerabilità dovranno essere riportate le relative misure di mitigazione. Redazione di un report in lingua inglese (metodologia, test vulnerabilità eseguiti).

2. Partecipazione alla redazione di un documento "Linee guida per lo sviluppo di software sicuro" che, rifacendosi ai principali standard internazionali in materia, contenga indicazioni sulle procedure e tecniche da adottare per la progettazione e implementazione di applicazioni web sicure e che sia specifico per l'ambiente di sviluppo adottato.

Durata servizio: i servizi dovranno essere conclusi entro la scadenza progettuale prevista per il 14/09/2024.

Presenza di eventuali certificazioni internazionali;  
Adesione a codici di condotta o standard;  
Obblighi in materia di policy e formazione del personale.