- **Analisi dinamica**: attraverso l'attuazione di test dinamici di sicurezza sull'applicazione in esecuzione in ambiente controllato;
- **Penetration Test**: attraverso l'esecuzione di scansioni ed analisi della superficie di attacco;
- **Test di autenticazione multilivello**: attraverso la verifica delle modalità di gestione dell'accesso degli utenti;
- **Business Logic test**: attraverso l'esecuzione di test manuali sulle applicazioni in fase di esecuzione;
- **Analisi dei risultati**: attraverso l'individuazione e la rimozione dei falsi positivi;
- **Remediation Plan**: attraverso la definizione del piano di rientro e la produzione di reportistica di sintesi e di dettaglio; Proof of Concept delle vulnerabilità riscontrate comprensiva di azioni per la riduzione della superficie d'attacco.

L'esame delle Applicazioni in esecuzione in ambiente di test, deve portare alla produzione, mediante la Dinamic Analysis delle seguenti tipologie di documenti:

- **Vulnerability Assessment**: report di dettaglio delle vulnerabilità riscontrate nella fase di analisi dinamica dell'applicazione tramite gli strumenti a supporto;
- **Remediation Plan:** report che analizza i falsi positivi ed indirizza la risoluzione delle problematiche riscontrate nell'analisi stessa.

La figura che segue sintetizza gli elementi in input e l'output prodotto dal processo DAST:

Figura 25 - Input e Output della fase Dynamic Analysis

9.4.1 Identificazione degli strumenti a supporto

Nel paragrafo 6.6.1 sono stati presentati i tool a supporto di questa fase. Si riporta di seguito un estratto:

- closed source
  - IBM App Scan (versione DAST),
  - Veracode,
  - CodeDx.
- open source
  - OWASP Zed Attack Proxy.

9.5 Supporto per la manutenzione di applicazioni sicure

L'obiettivo di questa fase è mantenere un prodotto sicuro, a partire dai nuovi trend sugli attacchi/minacce. Il team deve quindi analizzare le nuove minacce e individuare le contromisure necessarie rilasciando nuovi aggiornamenti/patch laddove necessario attraverso un processo di 'Continuous Security':