Report – Analisi e funzionamento dello script di scansione HTTP

Lo script analizzato in questo report è stato sviluppato con l'obiettivo di osservare e documentare il comportamento di un servizio HTTP esposto su un host specifico. Il suo scopo principale non è quello di sfruttare vulnerabilità, ma di raccogliere informazioni utili durante una fase di reconnaissance.

Nel nostro caso verrà utilizzato per verificare se sono presenti eventuali vulnerabilità nel nostro servizio web

Durante l'esecuzione, lo script richiede all'utente l'inserimento dell'host di destinazione, della porta del servizio HTTP e del path da analizzare. Nel caso in cui la porta non venga specificata, viene automaticamente utilizzata la porta 80. Il path viene normalizzato per evitare errori comuni e garantire una richiesta HTTP corretta.

Uno degli aspetti centrali dello script è la produzione di un file di log strutturato e leggibile. Il log riporta chiaramente l'orario di avvio e di conclusione della scansione, oltre alla durata totale.

La scansione viene effettuata testando diversi metodi HTTP, con particolare attenzione al metodo OPTIONS, utilizzato per individuare i metodi supportati dal server tramite l'header Allow. Successivamente vengono analizzati i metodi GET, POST, PUT e DELETE, osservando gli status code, i messaggi di risposta e una porzione limitata del body.

Lo script include inoltre una gestione esplicita degli errori più comuni, come timeout di rete o connessioni rifiutate. Questo garantisce che eventuali problemi vengano comunque documentati nel file di log, rendendo l'analisi più completa e affidabile.

Nel complesso, lo script rappresenta uno strumento didattico efficace per comprendere il funzionamento del protocollo HTTP e per introdurre le fasi iniziali di analisi di un servizio web.