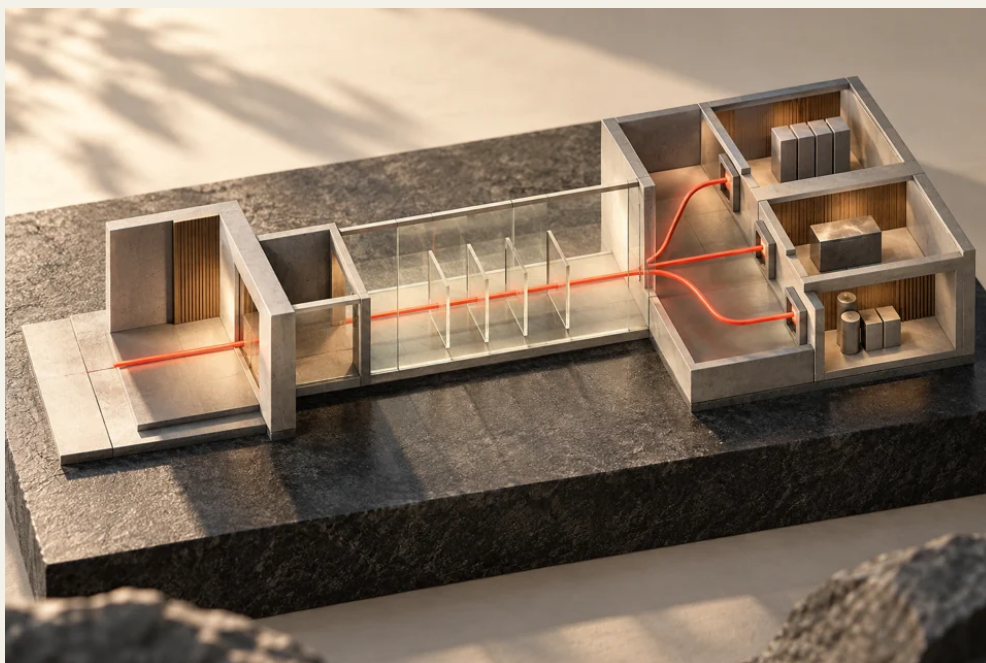


ESEMPIO DI CONSEGNA / PENTESTING

Penetration testing

Evidenza tecnica. Impatto contestuale. Retest.



Perimetro del campione

Applicazione fittizia <https://demo.example.invalid>, due account di prova A e B. Il dominio è riservato agli esempi; nessuna scansione è stata svolta contro un sistema esterno.

Come leggere questo documento

Questo estratto rende visibile la struttura di una consegna. Riscontri, attività e date del racconto sono sintetici, salvo l'impronta del file campione ricalcolabile. Il contenuto di un incarico effettivo viene definito con il committente.

Il percorso documentato.

01 / Regole di ingaggio

Obiettivo didattico: controllare l'autorizzazione su un documento. Sono ammessi solo account e record sintetici. Sono esclusi carico, persistenza, social engineering e accesso a dati reali.

02 / Rilievo sintetico DEMO-PT-01

Precondizione: l'account A possiede il documento 101; B non dovrebbe poterlo leggere. Nel risultato simulato, una richiesta autenticata come B restituisce il documento 101 con stato 200. È un esempio costruito, non un finding del sito Consuleria.

03 / Impatto e correzione

Possibile lettura tra account nel solo scenario. La priorità dipende da dati coinvolti, ampiezza e controlli effettivi; non viene assegnato un punteggio CVSS privo di vettore. Correzione proposta: verificare sul server il diritto dell'utente per ogni oggetto richiesto.

04 / Piano di retest

Con B, il documento di A deve restituire 403 o una risposta equivalente che non riveli il contenuto. Con A, l'accesso legittimo resta disponibile. Ripetere sui ruoli previsti e registrare richiesta, risposta depurata, versione e data.

Criterio di riesame

La relazione finale distingue test eseguiti, prove riproducibili, esclusioni, finding confermati, correzioni suggerite e retest svolti. Un esito del test non costituisce garanzia di assenza di vulnerabilità.

Approfondisci: <https://consuleria.org/penetration-testing/>