Report Programma Tester Verbi HTTP - Azienda Theta

Azienda Theta Committente: Azienda Theta S.r.l.
Fornitore del servizio: Landa Tracker S.p.A.
Progetto: Progettazione e implementazione di un programma in linguaggio Python per la scansione delle porte.
Settore Cliente: Moda
Data: 25 Luglio 2025
Ideazione e progettazione a carico di Falchi Marco (PM), Lucchesi Marco, Matera Cristian, Meloni Alessandro, Mondelci Marco, Saad Patrick

Realizzazione a carico di Falchi Marco, Meloni Alessandro, Matera Cristian

Panoramica della richiesta

Questo documento presenta l'analisi completa di un programma Python progettato per effettuare testing sistematico dei metodi HTTP su risorse web specifiche.

Obiettivo principale: Analizzare una pagina HTML per identificare risorse target specifiche e testare tutti i metodi HTTP supportati, confrontando i metodi dichiarati con quelli effettivamente funzionanti per identificare potenziali vulnerabilità di sicurezza web.

1. Panoramica del Programma

Il programma sviluppato è un tester avanzato di metodi HTTP implementato in Python che permette di analizzare la sicurezza web attraverso il testing sistematico dei verbi HTTP supportati da risorse specifiche. Il software utilizza librerie moderne per offrire un'interfaccia utente elegante e funzionalità di reporting professionale specializzate nell'audit di sicurezza web.

1.1 Funzionalità

Il programma offre le seguenti funzionalità principali:

Parsing HTML Intelligente: Utilizza la libreria BeautifulSoup per analizzare documenti HTML e identificare automaticamente risorse target specifiche, in questo caso per l'immagine con pattern "logo_right.png".

Validazione URL Robusta: Implementa controlli di validità degli URL tramite espressioni regolari, garantendo che gli input rispettino gli standard HTTP/HTTPS e prevenendo errori di formato.

Testing Sistematico dei Verbi HTTP: Esegue test completi sui sette metodi HTTP principali (GET, POST, PUT, DELETE, HEAD, OPTIONS, TRACE), fornendo una copertura completa per l'analisi di sicurezza.

Analisi Comparativa Allow vs Reale: Confronta i metodi dichiarati nell'header "Allow" della risposta OPTIONS con quelli effettivamente funzionanti, identificando discrepanze di configurazione.

Reporting Statistico: Genera automaticamente statistiche aggregate sui risultati, includendo conteggi di metodi testati, funzionanti e dichiarati.

Risoluzione URL Dinamica: Utilizza **urljoin** per costruire correttamente URL assoluti da percorsi relativi, gestendo diverse strutture di siti web.

Gestione Avanzata degli Errori: Implementa **try-catch** specifici per diversi tipi di errori (connessione, timeout, HTTP), garantendo continuità nell'esecuzione anche in caso di problemi.

1.2 Utilità

Lo strumento rappresenta una risorsa fondamentale per diverse categorie di utenti:

Security Auditor Web: Possono identificare configurazioni HTTP pericolose che potrebbero esporre per esempio l'infrastruttura e-commerce a attacchi di tipo privilege escalation.

Sviluppatori Full-Stack: Utilizzano il tool per verificare che le API e le risorse web implementino correttamente le policy di sicurezza HTTP, garantendo che solo i metodi necessari siano esposti.

DevOps: Impiegano lo scanner per monitorare la conformità delle configurazioni server durante la distribuzione di nuove funzionalità dell'ecosistema digitale.

Penetration Tester: Sfruttano il programma per identificare vettori di attacco basati su metodi HTTP non sicuri, particolarmente critici per proteggere i sistemi di pagamento e gestione ordini.

Compliance Manager: Utilizzano i report per documentare la conformità agli standard di sicurezza web richiesti nel settore fashion retail, dove la protezione dei dati clienti è prioritaria.

1.3 Ragioni di Sicurezza

L'implementazione del programma segue principi di sicurezza responsabile:

Testing Non Distruttivo: Il programma esegue solo richieste di verifica senza modificare o compromettere le risorse target, mantenendo l'integrità dei sistemi durante l'audit.

Controllo Granulare delle Richieste: Ogni metodo HTTP viene testato individualmente con gestione specifica degli errori, evitando comportamenti imprevisti che potrebbero impattare la produzione.

Logging Trasparente: Tutte le operazioni sono documentate con output dettagliato, facilitando la tracciabilità e l'audit delle attività di security testing.

Gestione Responsabile degli Errori: Gli errori di connessione e timeout sono gestiti **gracefully** senza generare traffico eccessivo o comportamenti anomali verso i server target.

Focus su Risorse Specifiche: Il targeting selettivo di risorse specifiche (logo_right.png) dimostra un approccio mirato e professionale, evitando scansioni massive non autorizzate.

Attenzione: è fondamentale utilizzare questo strumento esclusivamente su domini e risorse di proprietà o con autorizzazione esplicita, poiché il testing non autorizzato può violare policy aziendali e normative legali.

1.4 Implementazioni Grafiche Realizzate

Il programma implementa diverse soluzioni tecniche per migliorare significativamente l'esperienza visiva e l'usabilità, trasformando l'analisi di sicurezza HTTP in uno strumento professionale e user-friendly:

Libreria Rich per Output Avanzato: Il programma utilizza la **libreria Rich** (from rich.console import Console, from rich.table import Table) per trasformare l'output testuale grezzo in presentazioni grafiche professionali. Questa implementazione sostituisce i tradizionali print() con rendering avanzato che supporta colori, formattazione e layout strutturati.

Tabelle Dinamiche per Audit: La funzione generate_report() utilizza rich.table.Table per creare visualizzazioni tabellari professionali con:

- Intestazioni categorizzate (Metodo, Status Code, Supportato, Dichiarato)
- Colorazione basata sui codici di stato HTTP
- Icone intuitive (✅ per supportato, 📋 per dichiarato, ❌ per errori)
- Allineamento ottimizzato per la scansione visiva rapida dei risultati

Progress Bar Interattiva: L'implementazione di from rich.progress import track nella fase di testing fornisce feedback visivo real-time durante l'esecuzione:

- Barra di progresso animata con descrizione contestuale (" 🧪 Testando metodi HTTP...")
- Indicatori di completamento che mantengono l'utente informato durante operazioni di rete
- Visualizzazione del progresso particolarmente utile per testing su risorse remote

Sistema di Icone ed Emoji: Il codice integra strategicamente emoji e simboli per comunicazione visiva immediata:

- 🌐 per input URL
- 📸 per risorse immagine identificate
- 🔧 per operazioni OPTIONS
- 📋 per metodi dichiarati
- 🧪 per fase di testing
- 🎯 per report finale
- 📊 per statistiche aggregate

Colorazione Condizionale Intelligente: Il sistema di colori implementa:

- Codici di stato HTTP colorati semanticamente (verde=successo, giallo=redirect, rosso=errore)
- Evidenziazione automatica delle discrepanze di sicurezza

Dashboard Statistico Integrato: Il report finale include le metriche presentate visivamente:

- Contatori colorati per metodi testati, funzionanti e dichiarati
- Layout strutturato che facilita la comprensione immediata delle implicazioni di sicurezza
- Formato ideale per inclusione in report executive e documentazione di compliance

2. Spiegazione semplificata

Il programma rappresenta una soluzione specializzata per l'analisi della sicurezza delle configurazioni HTTP. La sua architettura modulare e l'implementazione chiara lo rendono uno strumento versatile per identificare vulnerabilità specifiche dei metodi HTTP.

Come Funziona in Pratica: Il workflow del programma è stato progettato per essere intuitivo ma completo. L'utente inserisce l'URL di una pagina web del sito Theta (ad esempio, una landing page prodotto o una sezione del catalogo), il sistema analizza automaticamente il codice HTML per identificare risorse specifiche come immagini o componenti grafici, quindi esegue una batteria completa di test sui metodi HTTP. Il risultato è un report dettagliato che evidenzia immediatamente eventuali discrepanze tra configurazione dichiarata e comportamento reale del server, cruciali per identificare potenziali vettori di attacco.

Punti di Forza: La capacità di confrontare automaticamente i metodi dichiarati nell'header "Allow" con quelli effettivamente funzionanti rappresenta un vantaggio unico per rilevare discrepanze di configurazione. L'integrazione di parsing HTML intelligente con testing HTTP sistematico offre un approccio completo all'audit di sicurezza web. L'utilizzo della libreria Rich trasforma analisi complesse in report visivamente comprensibili.

Potenziale di Sviluppo: Il codice attuale fornisce una base solida per **espansioni future**.

Considerazioni Finali

Il programma HTTP Verbs Tester sviluppato per Theta, azienda leader nel settore moda, rappresenta una soluzione di security auditing su misura che combina precisione tecnica e presentazione elegante, riflettendo l'approccio qualitativo che caratterizza il brand nel settore moda.

Rilevanza Strategica per il Business Theta: Nel contesto dell'e-commerce fashion, questo strumento supporta la sicurezza di componenti critici dell'infrastruttura digitale:

- Protezione Asset Multimediali: Verifica che le immagini prodotto, e contenuti visual non siano esposti a manipolazioni tramite metodi HTTP non sicuri
- Sicurezza API : Analizza le configurazioni HTTP delle API che gestiscono catalogo prodotti, prezzi e disponibilità per prevenire modifiche non autorizzate

Abbiamo voluto dare un valore aggiunto per Theta: Il tester fornisce al team di cybersecurity di Theta uno strumento specifico per identificare configurazioni HTTP errate che potrebbero passare inosservate durante audit tradizionali. La capacità di analizzare automaticamente discrepanze tra metodi dichiarati e supportati permette di scoprire vulnerabilità sottili ma critiche, garantendo che l'infrastruttura web sia configurata secondo le best practices di sicurezza.

La funzionalità di reporting statistico consente di tracciare nel tempo l'evoluzione della postura di sicurezza HTTP, supportando decisioni strategiche e di compliance.

Conclusione

Questo HTTP Verbs Tester rappresenta un tassello fondamentale nella strategia di cybersecurity di Theta, specificamente progettato per proteggere l'esperienza digitale dei clienti. In un settore dove la fiducia del consumatore è essenziale per il successo commerciale, strumenti specializzati come questo garantiscono che ogni aspetto dell'infrastruttura web sia sicuro e affidabile.

Il programma dimostra come l'innovazione tecnologica possa essere applicata con la stessa cura artigianale che Theta dedica alle sue creazioni fashion. La combinazione di funzionalità avanzate di security testing con un'interfaccia elegante e intuitiva riflette perfettamente i valori del brand: eccellenza tecnica, attenzione al dettaglio e user experience superiore.

L'approccio metodico del programma nel testare sistematicamente i metodi HTTP e confrontare configurazioni dichiarate vs reali permette al team IT di mantenere standard di sicurezza elevati senza compromettere l'agilità operativa, essenziale in un mercato dinamico come quello della moda dove velocità di distribuzione e sicurezza devono coesistere in armonia.