HAWKTESTERS

Everyone should ***feel secure*** online.

We emulate threat ***adversaries.***

Conducendo simulazioni di attacchi reali, le organizzazioni hanno l'opportunità di scoprire e affrontare vulnerabilità nei loro sistemi prima che i cybercriminali agiscano.

Questa strategia preventiva non è solo cruciale per proteggere le informazioni confidenziali e gli asset intellettuali, ma costituisce anche una difesa essenziale contro i rischi finanziari e il deterioramento dell'immagine aziendale.

I test di penetrazione sono fondamentali per rispettare gli standard regolatori e di conformità, in quanto offrono una dimostrazione concreta dell'impegno di un'organizzazione per la sicurezza.

Mediante la realizzazione periodica di questi test, le organizzazioni possono valutare continuamente il loro approccio alla sicurezza, perfezionare le loro strategie di difesa e mantenere una posizione resistente di fronte alle minacce cibernetiche in costante evoluzione.

Security, ***Safety,*** Stability.

Metodo ***Hawktesters.***

HAWKTESTERS è un'azienda specializzata in cybersecurity, reti aziendali e gestione dei rischi IT, con un'ampia esperienza nei test di penetrazione per aziende di tutte le dimensioni.

I nostri test possono coprire ogni aspetto della vostra rete e sistemi, inclusi i test di sicurezza e di garanzia per applicazioni personalizzate. Identifichiamo e segnaliamo vulnerabilità e rischi in un formato chiaro e priorizzato, con raccomandazioni.

L'approccio ai test di penetrazione di HAWKTESTERS è strettamente allineato alle linee guida del Open Web Application Security Project (OWASP). Per fornire un risultato consistente, ripetibile e di alta qualità, utilizziamo una serie di metodologie a seconda dell'organizzazione e degli obiettivi.

Queste includono standard ben definiti come:

OWASP Top 10 (Web, Mobile and API - últimas versiones)

OWASP Testing Guide

SANS 25 & SANS CSV

MITRE ATT&CK

Benefici *chiave.*

1.

Valida la sua **cybersecurity** su tutta la superficie di attacco e allinei la gestione delle vulnerabilità agli obiettivi commerciali chiave.

2.

Report **prioritizzati** e **attuabili** per guidare la rimediazione delle vulnerabilità e la gestione dei rischi.

3.

*Migliora la comprensione delle **forze** e delle **debolezze** nella gestione dei suoi sistemi e nello sviluppo delle applicazioni per guidare il miglioramento continuo del processo di sicurezza.*

4.

***Rivalidazione** dei **test** entro tre mesi per assicurarsi che le patch siano applicate, il firmware sia aggiornato e le lacune di sicurezza siano chiuse.*

5.

***Rispetti le normative** incluse la privacy e la sicurezza dei dati, per costruire la fiducia del cliente e proteggere la sua organizzazione da sanzioni.*

1 Valutazione delle Applicazioni web

Le prove web si basano sulle linee guida dell'industria del Open Web Application Security Project (OWASP) così come sul Common Weakness Enumeration (CWE) Top 25.

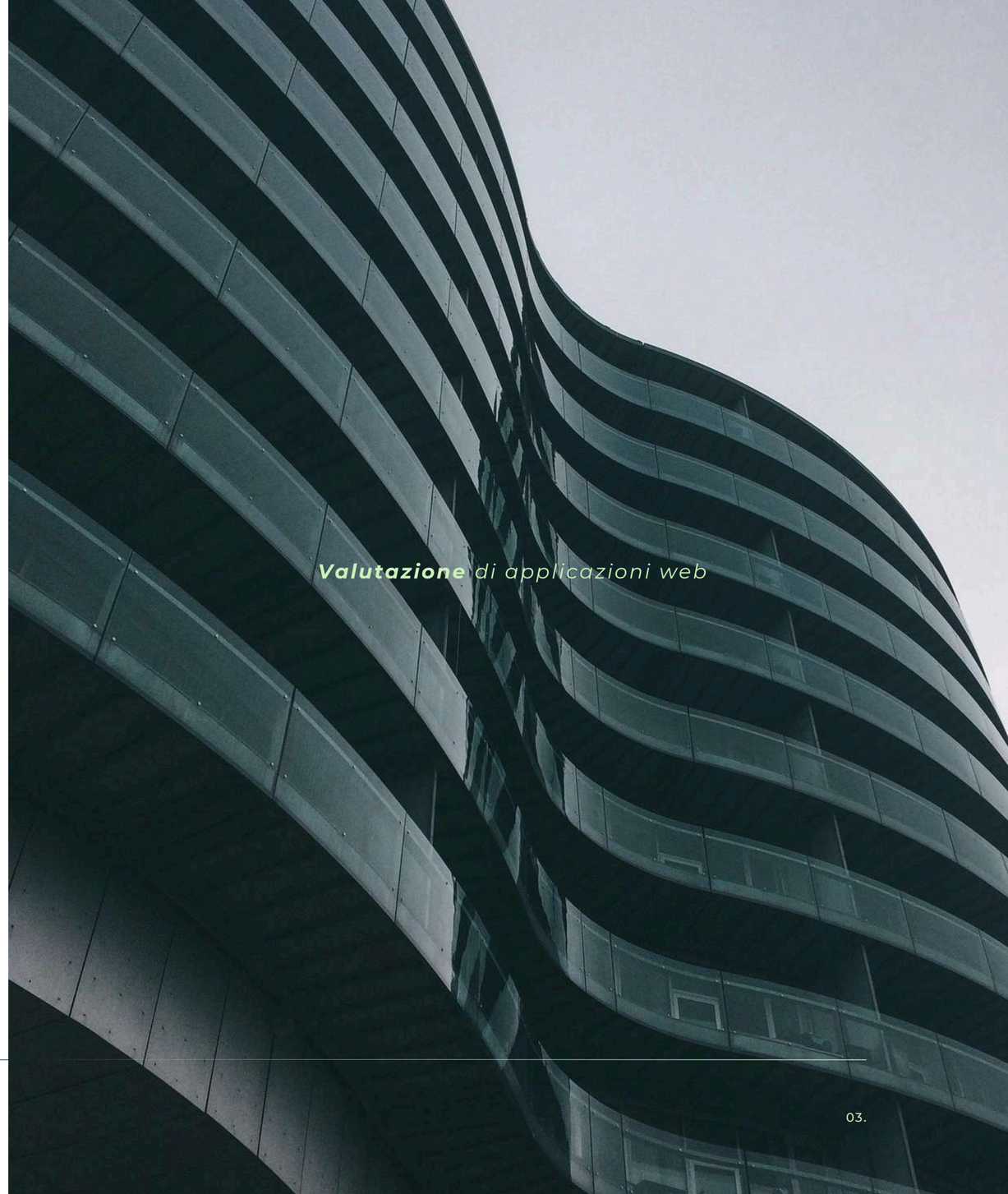
I risultati dei test delle applicazioni sono indicatori preziosi delle competenze e delle lacune nello sviluppo delle applicazioni interne, offrendo opportunità per la formazione e il miglioramento degli strumenti di fronte a problemi futuri.

Con ogni test che utilizza lo stesso flusso di lavoro e pratiche, inclusivo di un esteso processo di controllo di qualità realizzato da un tester senior, può essere sicuro di ottenere risultati esaustivi e consistenti.

Inclusioni

Hawktesters può testare tutte le sue applicazioni web, siano esse:

- Siti piccoli di tipo landing page, Wordpress o simili.
- Applicazioni di dimensioni medie
- Applicazioni grandi e complesse



Valutazione di applicazioni web

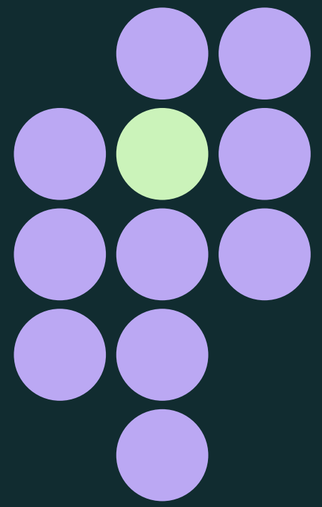
2 Valutazione della sicurezza *inalámbrica (Wireless)*

Le reti wireless possono offrire una superficie di attacco che si estende ben oltre il limite fisico delle strutture di un'organizzazione. Questo le rende un bersaglio attraente per un attaccante determinato.

Inclusioni

Le audit di sicurezza wireless si concentrano sui seguenti componenti:

- ***Ambiente wireless:*** *Scansione e scoperta.*
- ***Infrastruttura wireless:*** *Revisione della configurazione dei dispositivi.*
- ***Infrastruttura wireless:*** *Valutazione dell'implementazione e delle operazioni.*
- Validazione della segregazione della rete tra reti wireless, come le reti per ospiti e aziendali.
- Dopo aver completato la revisione iniziale e affrontato eventuali problemi, ciò costituirà una base di sicurezza.

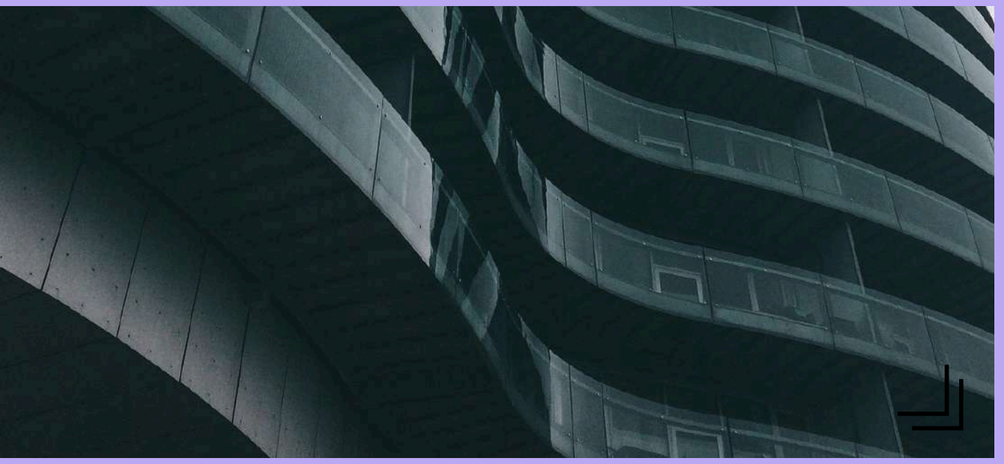


3.Valutazione della *sicurezza delle API*

Il nostro approccio si basa sulle linee guida dell'industria del Open Web Application Security Project (OWASP) per i test delle API.

Inclusioni

I test possono essere effettuati indipendentemente (utilizzando una specifica di Postman o Open API) o come parte di un test più ampio che includa l'applicazione web o un altro client API. Tutti i test sono realizzati secondo le migliori pratiche dell'industria, e i risultati sono mappati con l'ultimo OWASP API Top 10.



4. Valutazione della *configurazione dell'host*

La valutazione della configurazione dell'host prende in considerazione la configurazione di dispositivi server specifici (e applicazioni di supporto) o altri dispositivi.

Inclusioni

Le aree di focus e revisione durante questa attività possono includere:

- **Aggiornamenti e patch del sistema operativo (o equivalente)**
- **Configurazioni predefinite**
- **Permessi del sistema di file**
- **Configurazione errata e vulnerabilità note con servizi installati**
- **Controlli di sicurezza impiegati nella prestazione di servizi sui server di file**
- **Configurazioni di applicazioni di supporto**
- **Superficie di attacco minimizzata (non vengono eseguiti servizi non necessari)**
- **Confronto contro una linea base fornita/configurazioni documentate**
- **Accesso a dati sensibili, come file di configurazione che contengono credenziali**

5 *Valutazione della **sicurezza** mobile (Android & iOS)*

Inclusioni

Dato che molte applicazioni vengono attualmente distribuite tramite dispositivi mobili, rispondiamo ai loro requisiti di test di sicurezza, sia che si tratti di applicazioni native, web o ibride.

Tutti i test sono realizzati secondo le migliori pratiche dell'industria, e i risultati sono mappati con l'ultimo OWASP Mobile Top 10.

6 *Test di penetrazione della rete interna*

Inclusioni

Questo viene tipicamente realizzato sotto uno dei seguenti tre approcci:

- Vivere del territorio (Living off the Land), dove al tester viene fornito accesso alla rete interna e poi utilizza strumenti e tecniche standard per accedere ai sistemi, esplorando vulnerabilità identificate e opportunità di movimento laterale.
- Valutazione di vulnerabilità, dove tutti gli obiettivi entro l'ambito vengono scannerizzati utilizzando strumenti leader nell'industria, e tutti i risultati sono revisionati manualmente e categorizzati per aiutare a valutare il rischio generale.
- Test basato su obiettivi, dove al tester viene fornita un'account utente standard all'interno della rete, e ha l'obiettivo di ottenere accesso a un obiettivo concordato (come Active Directory, dati finanziari o dei clienti).

7 *Test di penetrazione della rete esterna*

Il test di penetrazione della rete esterna valuta la postura di sicurezza dell'infrastruttura esposta a Internet in generale.

Inclusioni

Questo viene realizzato in due ampie categorie:

- Scansione automatica: esamina tutti i servizi esposti alla ricerca di configurazioni errate o vulnerabilità note.
- Test manuali: applica tecniche di test manuali e l'esperienza per revisionare gli host e i servizi esposti. I dispositivi identificati vengono interrogati utilizzando una varietà di strumenti per identificare porte aperte, servizi e vulnerabilità.

Le aree di focus e revisione includono:

- Configurazioni errate dell'infrastruttura
- Vulnerabilità note relative ai servizi esposti
- Configurazioni dei certificati SSL
- Analisi dei risultati degli strumenti di valutazione della sicurezza della rete come Nessus e Nmap
- Analisi manuale delle vulnerabilità segnalate per valutare l'esploitabilità e la criticità

8 *Simulazione di avversari (Red Team)*

Pianificazione, coordinazione, esecuzione, valutazione, analisi e rapporto di un attacco simulato del mondo reale utilizzando tecniche di squadra rossa. Utilizziamo strumenti di attacco e penetrazione progettati per testare in modo occulto i controlli tecnologici e i processi organizzativi contro attacchi, inclusi phishing, malware, attacchi ad applicazioni o infrastrutture.

Inclusioni

Nell'eseguire un esercizio di squadra rossa, ci concentreremo su obiettivi specifici che sono fondamentali per le operazioni attuali e future della vostra organizzazione. L'obiettivo durante questo esercizio è migliorare la vostra postura generale di sicurezza, dimostrando l'impatto di un attacco mirato e fornendo raccomandazioni e opportunità di apprendimento per migliorare la risposta agli incidenti di sicurezza.

Si prevede che questo impegno segua un approccio per fasi:

- **Pianificazione e preparazione**
- **Ottenimento di un primo punto di appoggio (attività di attacco esterno)**
- **Identificazione di percorsi interni verso obiettivi specifici**
- **Conquista degli obiettivi (attività di attacco interno)**
- **Aumento del 'rumore' per tentare di validare la risposta del team blu**
- **Report**
- **Team viola (opzionale)**
- **Formazione sulla consapevolezza della sicurezza per i dipendenti (opzionale)**

9 *Revisione del codice delle applicazioni*

Hawktesters può eseguire revisioni focalizzate sulla sicurezza di applicazioni sviluppate utilizzando una vasta gamma di linguaggi e piattaforme.

Inclusioni

- Revisione manuale di alto livello in cui si cercano nel codice problemi e debolezze di sicurezza comuni.
- Le valutazioni di scansione del codice più profonde possono essere implementate utilizzando strumenti SAST o DAST.
- Identificazione di debolezze e vulnerabilità di sicurezza a livello di codice sorgente e dimostrazione di come queste risultino in difetti di sicurezza.
- Revisione aggiuntiva del codice per applicazioni che operano su basi di codice e framework antichi per identificare nuove e emergenti classi di vulnerabilità di codifica.

10 *Revisione della sicurezza dei servizi Cloud*

Valutazione della sicurezza dei servizi basati su cloud (SaaS/PaaS/IaaS) come AWS, Azure e O365 basata su una revisione di configurazione e implementazione.

Inclusioni

- Rivedere la configurazione e le opzioni contro le migliori pratiche del fornitore e dell'industria.
- Esaminare le pratiche e l'efficacia della gestione degli utenti e dei gruppi.
- Analizzare le misure di protezione dei dati.
- Valutare le politiche di conservazione, eDiscovery e i registri di audit come parte dei controlli di conformità e audit.
- Documentazione e rapporto dei risultati con raccomandazioni attuabili.

11 *Campagne* di Phishing

Offriamo un servizio completo di campagne di phishing progettato per valutare e migliorare la consapevolezza sulla sicurezza dei dipendenti nella vostra organizzazione.

L'obiettivo di queste campagne è fornire una misurazione realistica del livello di consapevolezza sulla sicurezza tra i dipendenti, identificare aree di miglioramento e rafforzare le difese dell'organizzazione contro tattiche ingannevoli.

Inclusioni

Phishing: Realizziamo campagne di email simulate per misurare la risposta dei dipendenti di fronte a tentativi di phishing, fornendo una visione chiara della vulnerabilità organizzativa a questo tipo di attacchi.

Vishing: Implementiamo test di ingegneria sociale telefonica per valutare come i dipendenti rispondono alle richieste verbali di informazioni sensibili o azioni che potrebbero compromettere la sicurezza.

Smishing: Inviamo messaggi di testo che imitano tattiche utilizzate dai cybercriminali per determinare la suscettibilità dei dipendenti agli attacchi di phishing tramite SMS.

12 Formazioni su sviluppo sicuro

Hawktesters può realizzare revisioni focalizzate sulla sicurezza di applicazioni sviluppate utilizzando una vasta gamma di linguaggi e piattaforme.

Inclusioni

Formazione su Sviluppo Sicuro secondo ASVS: Adottiamo lo standard ASVS di OWASP per fornire una solida base nelle pratiche di sicurezza durante lo sviluppo di applicazioni, assicurando che i team comprendano e possano implementare i requisiti di sicurezza necessari.

Sessioni interattive e pratiche: I corsi di formazione sono progettati per essere dinamici, con esercizi pratici e analisi di casi reali che consentono di applicare le conoscenze in scenari concreti.

Contenuto aggiornato e rilevante: Ci assicuriamo che il contenuto della formazione rifletta le ultime tendenze e minacce nel campo della cybersecurity, preparando i team ad affrontare le sfide attuali.

Valutazione dell'apprendimento e miglioramento continuo: Misuriamo il progresso e la comprensione degli argomenti trattati, offrendo un feedback dettagliato e suggerimenti per il rafforzamento delle competenze e delle conoscenze.

Rapporti e analisi ↘

Il nostro rapporto standard include un **sommario esecutivo** dei risultati, insieme a:

↘ Una descrizione dettagliata di ciascun risultato

↘ Le classificazioni di rischio associate

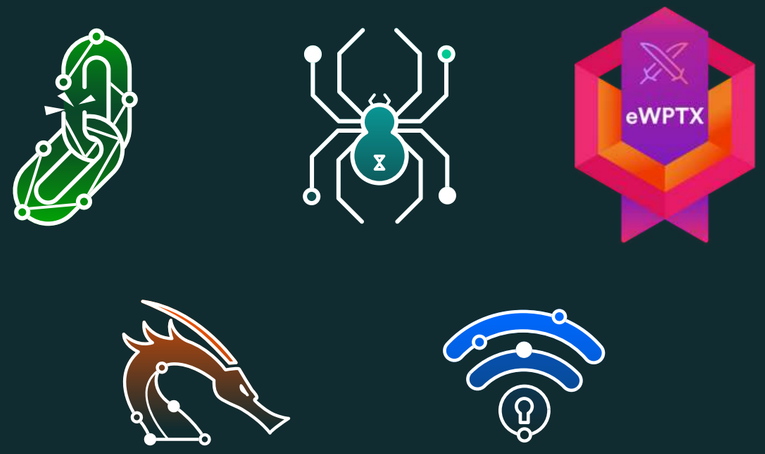
↘ Le raccomandazioni per risolvere la vulnerabilità

*Inoltre, organizziamo una **sessione** virtuale per condividere e **discutere i risultati** con il team tecnico dell'azienda, promuovendo così un approccio collaborativo nella **mitigazione dei rischi**.*

Le nostre credenziali nei test di penetrazione ↘

Hawktesters si distingue per la sua alta specializzazione e per il suo personale con ***più di 10 anni di esperienza*** nei test di penetrazione.

Il nostro team possiede una vasta gamma di certificazioni riconosciute nell'industria, tra cui:



Everyone should ***feel secure*** online.