# HackEDU

Ridurre il rischio di vulnerabilità nel software con i corsi di programmazione sicura

Online e on demand

## WHITEPAPER

HackEDU
Online Cybersecurity Training

ADVANCTION

# INDICE

# HACKEDU: LA FORMAZIONE EFFICACE

Il costo delle violazioni di sicurezza cresce sempre più, i programmi di bug bounty sono costosi, i professionisti della sicurezza informatica sono difficili da trovare e gli sviluppatori non vogliono seguire corsi di formazione sulla sicurezza o sono "troppo occupati" a lavorare su nuove funzionalità. E per finire, la società sta diventando sempre più dipendente da tecnologie che sviluppatori poco formati in questo ambito stanno costruendo.

## Presentazione di HackEDU!

Uno degli obiettivi di HackEDU è di rendere la formazione su vari temi della sicurezza applicativa più efficace. Ecco alcuni dei problemi che stiamo risolvendo.

- ### Gli sviluppatori non vogliono seguire la formazione

La formazione HackEDU è diversa in quanto si concentra sulla sicurezza offensiva, più interessante della formazione difensiva e stimola l'interesse dello sviluppatore nella risoluzione dei problemi.

Per creare ulteriori incentivi possiamo istituire premi per gli sviluppatori: con la nostra piattaforma è possibile creare un *contest* in modo che gli sviluppatori possano competere per aggiudicarsi un premio finale. Gli sviluppatori dovranno seguire le lezioni in modo da essere preparati per la competizione.

- ### I video non sono coinvolgenti

Gli sviluppatori sono inventori. Non imparano guardando i video, imparano attraverso la sperimentazione. I tassi di abbandono dei video di formazione sulla sicurezza sono circa dell'83%.

- ### Gli sviluppatori sono già impegnati a lavorare sulle funzionalità del prodotto

Ci siamo passati tutti, è vero. Gli sviluppatori sono impegnati e la tua azienda deve continuare a rilasciare nuove funzionalità e supportare i tuoi prodotti attuali.

Sarà vero questo trimestre, ma anche nel Q2, nel Q3, nel Q4… Questa è la realtà!

Il punto è che hai bisogno che i tuoi sviluppatori siano efficienti, il che significa che devono capire come sviluppare codice sicuro. Una vulnerabilità, se non fissata, sarà presente in ogni rilascio del software. Un approccio allo sviluppo "sicuro alla fonte" (cioè al momento della scrittura del codice) ha avuto un ritorno quadruplo sugli investimenti in sicurezza delle applicazioni (fonte: Aberdeen Group).

Le violazioni dei dati sono costose. Perdi la fiducia dei consumatori, paghi cause legali, ti affretti a correggere i bug, e l'elenco delle conseguenze negative non finisce qui. Una violazione dei dati costa alle aziende in media 3,5 milioni di dollari.

- Le soluzioni difensive non sono efficaci

Abbiamo scoperto che quando gli sviluppatori comprendono come un utente malintenzionato esamina la loro applicazione riescono in modo più efficace a ridurre il numero di vulnerabilità. È un approccio diverso rispetto al tradizionale addestramento difensivo. Gli sviluppatori apprendono i problemi di sicurezza comuni molto più rapidamente e possono proteggere il codice in modo più efficace. Questo evita anche il divario che si crea tra team di sicurezza e software engineer quando i primi hanno il compito di trovare e correggere le vulnerabilità senza il supporto degli sviluppatori.

- C'è un divario tra sviluppatori e sicurezza

In molte organizzazioni, non sembra che sviluppatori e sicurezza facciano parte della stessa squadra.

La sicurezza comprende quali sono rischi della distribuzione di codice vulnerabile, ma gli sviluppatori sono sottoposti a un'estrema pressione per rilasciare nuove funzionalità e considerano la sicurezza come un elemento che porta restrizioni e burocrazia che li rallenta.

La chiave per colmare questa lacuna è:

  - ottenere che chi sviluppa comprenda adeguatamente i rischi
  - spostare *l'ownership* della sicurezza al team di sviluppo software

- La configurazione degli ambienti per la formazione sulla sicurezza è complessa

Certo, sono disponibili macchine virtuali (VM) per far pratica con le tecniche di sicurezza delle applicazioni. Ma se sei un esperto di sicurezza che cerca di organizzare la formazione per la tua azienda, devi provare a configurare l'intero team in un ambiente in cui hai accesso a queste VM o fargli eseguire le VM in locale. Gli sviluppatori devono configurare proxy e altri strumenti e tutto questo costituisce un enorme impegno di tempo e risorse, solo per la configurazione.

La piattaforma di HackEDU ti consente di saltare l'intero processo di configurazione dell'ambiente e passare direttamente alla formazione pratica.

- L'impostazione della formazione sulla sicurezza interna richiede molto tempo

Abbiamo trascorso migliaia di ore a creare strumenti e contenuti per formare i team di sviluppo.

Puoi pensare a noi come un'estensione del tuo team di sicurezza. Saremo quelli che si dedicano alla creazione di ottimi contenuti su una fantastica piattaforma che si adatta alle esigenze della tua organizzazione. Lavoreremo con te per personalizzare la formazione in base alle tue esigenze.

# ABOUT HACKEDU

La missione di HackEDU è fornire la migliore formazione interattiva sulla sicurezza informatica. Il nostro obiettivo è abbassare le barriere per apprendere la sicurezza e fornire ambienti sicuri e legali per far pratica. Solo allora il settore prospererà con più professionisti e *champion* della sicurezza.

La nostra esperienza decennale nella sicurezza informatica ci permette di adattare la nostra piattaforma e i nostri contenuti alle nuove minacce che mergono nell'ambito della cybersecurity.

## Linguaggi e framework

| | | | | | |
|---|---|---|---|---|---|
| Python | Ruby | PHP | Laravel | C# | .NET |
| Go | Node.JS | Angular | React | Java | C++ |

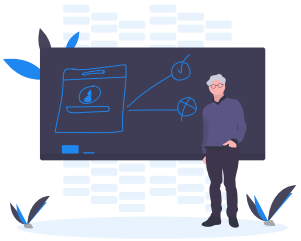
## Più di 115 argomenti di programmazione sicura

I corsi di HackEDU coprono molto più delle 10 principali vulnerabilità web di OWASP . Su richiesta, è possibile aggiungere ulteriori vulnerabilità.

| | | | |
|---|---|---|---|
| SQL Injection | NoSQL Injection | Command Injection | Remote Code Execution |
| XSS | Autenticazione e gestione delle sessioni difettose | Authentication Rate Limits | Gestione debole delle sessioni |
| Gestione e conservazione delle password | Cross-Site Request Forgery | Clickjacking | Controllo accessi difettoso |
| Condifugarzioni errate di sicurezza | Esposizione di dati sensibili | Best practice di crittografia | Utilizzo di componenti con vulnerabilità note |
| XML External Entities | Buffer Overflow | Heap Overflow | |

## Le caratteristiche di HackEDU

### Approccio offensivo e difensivo



Approccio più efficace e coinvolgente del solo allenamento difensivo.

### Gamification

È possibile organizzare *challenge* in cui gli sviluppatori possono competere, sfidare e guadagnare punti per catturare le sfide in stile bandiera. Questo impegna ulteriormente gli sviluppatori ad apprendere pratiche di codifica sicure.

### Risparmio sui tempi di sviluppo

Questa formazione ha un ROI di 4,4 volte sul risparmio di tempo per gli sviluppatori. Gli sviluppatori possono seguire queste lezioni secondo i propri ritmi.

### Certificazione degli sviluppatori

Gli sviluppatori ottengono la certificazione HackEDU per il completamento e il superamento di tutte le patch del codice.

### Responsabilità nella risoluzione

Gli sviluppatori devono correggere correttamente il codice vulnerabile per passare le lezioni. Per poter addestrare gli sviluppatori in modo efficace, è necessario farli programmare.

### Compliance

Soddisfa e gestisci i requisiti di formazione per gli sviluppatori come prescritto da PCI-DSS, GDPR, NIST 800-53, SOC.

## Lezioni avanzate

Queste lezioni si basano sulle vulnerabilità individuate in applicazioni reali dal programma bug bounty di HackerOne.

| | | | | |
|---|---|---|---|---|
| Clickjacking | Blind XXE | Esecuzione di codice remoto | SQL Injection con SQLMap | XSS utilizzando PostMessage |

## Vulnerabilità pubbliche incluse

HackEDU dispone di sandbox con vulnerabilità pubbliche per apprendere tecniche di sicurezza offensive e difensive nel mondo reale in un ambiente sicuro.

| Drupalgeddon2 | Struts | Zip slip |
|---|---|---|
| Questa sandbox replica una vulnerabilità pubblica RCE (Remote Code Execution) in Drupal (CVE-2018-7600). | Questa sandbox replica una vulnerabilità pubblica RCE (Remote Code Execution) in Apache Struts 2 (CVE-2018-11776). | Questa sandbox replica le vulnerabilità pubbliche con il software di archiviazione / compressionee. |

## Integrazione con SAST / DAST e Bug Bounty

SAST, DAST e IAST sono ottimi strumenti che possono completarsi a vicenda. Idealmente, sarebbe meglio utilizzare una combinazione di strumenti per garantire una migliore copertura e ridurre il rischio di vulnerabilità nelle applicazioni di produzione. L'SDLC si è notevolmente accelerato negli ultimi anni ei metodi di test tradizionali non riescono a tenere il passo con il ritmo dello sviluppo web. L'utilizzo di strumenti di test automatizzati nelle prime fasi può migliorare significativamente la sicurezza con un costo minimo.

Tuttavia, tieni presente che questi strumenti non intendono sostituire tutte le altre pratiche di codifica sicura, ma piuttosto fanno parte di un più ampio sforzo di sicurezza dell'applicazione.

HackEDU si integra con i più popolari strumenti SAST e DAST, piattaforme bug bounty, strumenti SCA, repository di codice e tracker di problemi. Un piano di formazione adattivo viene creato automaticamente con le lezioni pratiche di HackEDU per ogni sviluppatore di software basate sulle vulnerabilità trovate nelle tue applicazioni e sulle prestazioni del singolo sviluppatore.

## Dashboard di gestione


La dashboard di amministrazione di HackEDU semplifica la gestione e il monitoraggio della formazione della tua organizzazione.

Caratteristiche della dashboard

- Monitoraggio dei progressi del team
- Creazione di piani di training personalizzati
- Impostazione di Single Sign-on
- Pianificazione della formazione dei team in base alle proprie esigenze
- Generazione di certificati di superamento del corso

## Vantaggi di HackEDU

- **Prevenzione delle vulnerabilità nel Software di produzione**
  - Promuove l'adesione agli standard di programmazione sicura
  - Migliora la capacità degli sviluppatori di trovare e correggere le vulnerabilità nel codice
  - Migliorare la tua postura di sicurezza
- **Riduzione dei costi operativi**
  - Riduce gli errori di codifica
  - Fornisce agli sviluppatori la conoscenza di cui hanno bisogno per essere in grado di bloccare le vulnerabilità nella fase iniziale del loro SDLC
  - Riduce i tempi di rilascio del codice in produzione
- **La formazione di persona è spessp una perdita di tempo ed è inefficace (oggi è quasi impossibile a causa del COVID)**
  - Consente agli sviluppatori di esercitarsi e testare le proprie capacità in un ambiente reale
  - Permette di creare piani di formazione personalizzati basati sui punti deboli identificati
  - Trasmette agli sviluppatori la responsabilità sui temi della programmazione sicura

# PERCHÉ È NECESSARIA LA FORMAZIONE SULLO SVILUPPO SICURO?

Il training per la programmazione sicura è un tipo di formazione per sviluppatori di software in cui è possibile imparare a sviluppare codice più sicuro. Di norma viene mostrato come affrontare le principali vulnerabilità come OWASP Top 10 o CWE / SANS Top 25 e scrivere codice in modo difensivo contro queste vulnerabilità, esplorando le migliori pratiche di programmazione sicura.

La stragrande maggioranza dei laureati in informatica non ha mai seguito una formazione sullo sviluppo sicuro e non conosce i tipi di vulnerabilità o come difendersi da esse. Gli sviluppatori si laureano e accettano un lavoro in cui, nella maggior parte delle volte, non ricevono una formazione sullo sviluppo sicuro. Molti software engineer continuano a progredire nella loro carriera senza mai affrontare i fondamenti della sicurezza, che però sono vitali per sviluppare e mantenere prodotti affidabili. Parliamo degli stessi software engineer che stanno sviluppando il software delle vostre automobili, dei pacemaker, di social network, di applicazioni finanziarie, di software per la gestione delle reti elettriche o delle acque, o che sviluppano codice nella vostra azienda. Le vulnerabilità aumentano il rischio di violazioni dei dati, perdite finanziarie e, negli scenari più estremi, possono persino causare vittime. La formazione sullo sviluppo sicuro è in grado di ridurre il rischio di questi incidenti.

È questa la soluzione per eliminare tutte le vulnerabilità? No. Tuttavia, è il primo passo per ridurre il rischio di vulnerabilità nel software. Gli sviluppatori di software devono far parte della soluzione e assumersi la responsabilità del proprio codice. Troppe volte le organizzazioni di ingegneria del software si aspettano che il proprio team di sicurezza conduca test delle applicazioni e corregga il codice quando vengono rilevati problemi. Ma ciò non funziona per vari motivi: in primis, nessuno conosce il software meglio dello sviluppatore che lo ha codificato. In secondo luogo, gli sviluppatori di software e di sicurezza dovrebbero essere nella stessa squadra e entrambi dovrebbero assumersi la responsabilità della sicurezza dell'applicazione. Più tardi viene rilevata una vulnerabilità durante il processo di sviluppo o quando un software è già in produzione, più diventa costoso risolverla. È necessario fare il più possibile all'inizio per bloccare le vulnerabilità alla fonte.

Molte aziende non dispongono di una formazione per la programmazione sicuro. Spesso pagano bug bounty per lo stesso tipo di vulnerabilità più e più volte, e i prodotti/servizi che hanno gli stessi tipi di vulnerabilità vengono visualizzati ripetutamente nelle Common Vulnerability Exposures (CVE).

La formazione allo sviluppo sicuro interrompe questo schema, permette di risparmiare denaro, riduce il rischio di una violazione della sicurezza del software e fa risparmiare tempo.

Infine, una considerazione sull'aggiornamento. Se gli sviluppatori hanno ricevuto una formazione di sviluppo sicuro in passato, non significa necessariamente che ricordino tutto e potrebbero non essere all'altezza degli attacchi e delle tecniche difensive più recenti. È importante ricevere la formazione su base continuativa per aggiornare le proprie capacità e apprendere le minacce più recenti.

# PERCHÉ È PIÙ EFFICACE UN APPROCCIO OFFENSIVO ALLA FORMAZIONE SULLA SICUREZZA?

C'è un modo di dire nel mondo della sicurezza: i difensori devono avere ragione il 100% delle volte, ma gli aggressori devono avere ragione solo una volta. Sebbene questa possa sembrare una semplificazione eccessiva, spiega come i difensori devono capire come pensano gli attaccanti in modo da poter anticipare gli attacchi: i migliori difensori sono quelli che comprendono veramente cosa vuol fare un aggressore.

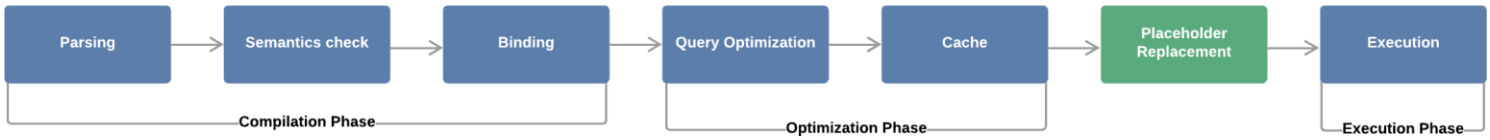
Sfortunatamente, la maggior parte del training si concentra solo sulla difesa, in particolare nella formazione sulla programmazione sicura. Molti corsi in questo ambito prendono in esame le vulnerabilità del codice e come scrivere codice sicuro oppure dettagliano quali librerie utilizzare e come gestire un ciclo di vita di sviluppo software sicuro (SDLC). Questo tipo di formazione manca di una spiegazione degli attacchi e quindi offre agli sviluppatori di software una visione unilaterale della codifica sicura. Tuttavia, per scrivere codice protetto, gli sviluppatori devono comprendere le menti di un aggressore: come pensa alle applicazioni e come riesce a sfruttare i loro punti deboli.

Comprendendo i metodi offensivi, gli sviluppatori diventano difensori migliori, apprendendo i fondamenti delle vulnerabilità e dei meccanismi molto più che dal lato difensivo. Questo non solo ha senso concettualmente, ma c'è anche uno studio che lo dimostra. Lo studio dell'Università di Mannheim, *Evaluation of the Offensive Approach in Information Security Education*, ha rilevato che gli studenti che hanno ricevuto una formazione offensiva hanno scoperto più vulnerabilità e hanno ottenuto punteggi più alti nei test di sicurezza rispetto agli studenti che avevano solo un addestramento difensivo.

Lo studio ha scoperto che la formazione pratica sulla sicurezza offensiva ha portato a:

- migliore capacità di scrivere software sicuro;
- migliore comprensione di come vengono violati i sistemi software;
- capacità di risolvere i problemi relativi alla sicurezza più velocemente.

Il Secure Development Training di HackEDU utilizza tecniche pratiche di formazione sulla sicurezza offensiva unitamente all'istruzioni su come impostare la programmazione difensiva.




*Rappresentazione semplificata dell'elaborazione di una prepared statement SQL*

# COME CONDURRE UN PROGRAMMA EFFICACE DI APPLICATION SECURITY DA REMOTO

La buona notizia è che eseguire in remoto un programma di application security efficace non è diverso dall'eseguirlo in ufficio. Tuttavia, la realtà è che la maggior parte delle aziende non si trova nella situazione di condurre un efficace programma di sicurezza delle applicazioni. Punto. Questo perché la sicurezza delle applicazioni spesso viene implementata attraverso processi manuali.

Invece, le tre componenti più importanti nella sicurezza delle applicazioni dovrebbero essere automazione, automazione e automazione.

### Integrazione negli strumenti di comunicazione e monitoraggio

Un primo passo importante è integrare le notifiche e le attività di sicurezza negli strumenti e nei flussi di lavoro SaaS già esistenti, come JIRA, Slack, PagerDuty, MS Teams, ecc. Tutte le attività e le notifiche dovrebbero essere aggiunte a questi strumenti invece di essere gestite manualmente. Ciò garantisce che il team di sicurezza e gli sviluppatori di software ricevano avvisi e facciano fronte alle loro attività, poiché esse si trovano negli strumenti che già utilizzano.

### Automazione delle attività

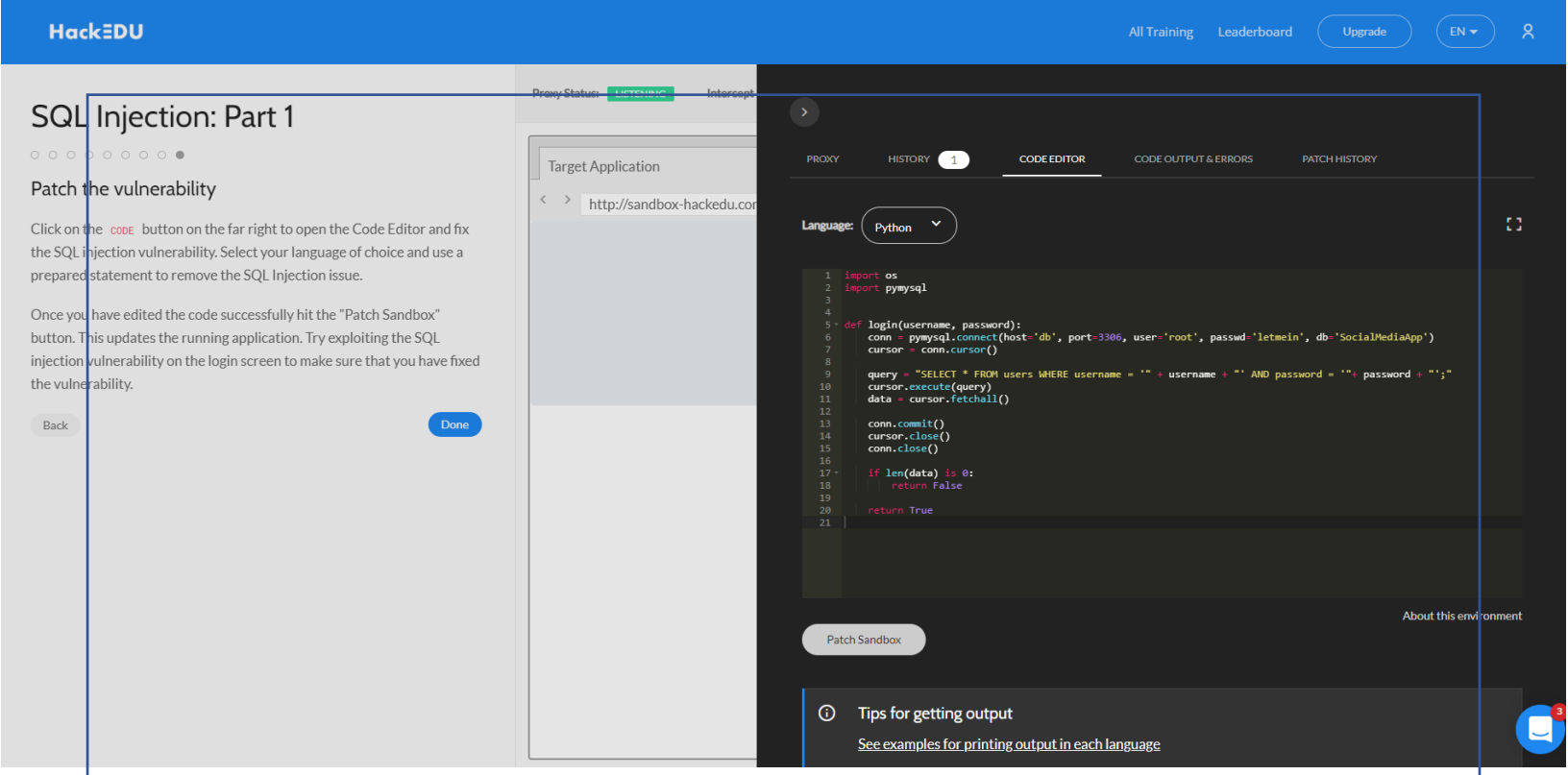
Gli strumenti di sicurezza dovrebbero essere eseguiti quando necessario attraverso un workflow automatizzato. Strumenti come Static Application Security Testing (SAST) e Dynamic Application Security Testing (DAST) devono essere usati quando il codice viene archiviato o distribuito negli ambienti di sviluppo. L'integrazione degli strumenti SAST e DAST in software CI / CD come Jenkins o CircleCI ne permetterà l'esecuzione automatica. I problemi rilevati da questi strumenti dovrebbero essere assegnati automaticamente e tracciati nella loro risoluzione, operazioni che possono essere svolte quando gli strumenti di sicurezza sono già integrati nel software di comunicazione e tracking.

### Automazione dell'applicazione delle regole

L'applicazione delle regole e delle politiche di sicurezza può essere automatizzata in modo che qualcuno non debba per forza assicurarsi che siano soddisfatte. Ciò si applica in special modo quando tutti lavorano in remoto e il monitoraggio delle policy è quasi impossibile. Ad esempio, è possibile non consentire agli sviluppatori di eseguire il check-in o di distribuire il codice se sono presenti vulnerabilità note che sono state individuate tramite test SAST / DAST. O anche monitorare la notifica e il tracciamento delle attività per garantire che le vulnerabilità vengano risolte in base al periodo di tempo richiesto nelle politiche di sicurezza. Provare a farlo manualmente quando si è in ufficio è già abbastanza difficile, ma farlo mentre tutti lavorano in remoto è quasi impossibile per qualsiasi team, in particolar modo per team di grandi dimensioni.

### Formazione on demand

La formazione pratica on demand offre agli sviluppatori di software che lavorano da casa un break e offre un po' di varietà nella loro giornata. Lavorare da casa per alcune persone può essere difficile e aiutare a spezzare la giornata con qualcosa di diverso è molto utile. HackEDU ha riscontrato un netto aumento dell'utilizzo del servizio quando le persone lavoravano da casa.




# CASO STUDIO: LA FORMAZIONE DI HACKEDU PERMETTE DI INDIVIDUARE 5 VOLTE PIÙ VULNERABILITÀ

## Riepilogo dei risultati

I principali vantaggi raggiunti

- Il 100% degli sviluppatori ha migliorato la propria capacità di trovare e correggere le vulnerabilità del software
- L'81% delle vulnerabilità è stato trovato e risolto correttamente
- Aumento del 452% delle competenze di scrittura di codice sicuro

## La sfida

Una società di tecnologia software che ha come clienti molte aziende Fortune 500 archivia oltre 41 milioni di record di dati di utenti finali. L'azienda desiderava una soluzione di formazione per soddisfare i requisiti di codifica sicura PCI e ridurre le vulnerabilità nel software per proteggere le proprie applicazioni e, in ultima analisi, i dati degli utenti finali.

L'azienda voleva dimostrare l'efficacia della soluzione di formazione in modo da poter giustificare alla direzione che valeva la pena trascorrere del tempo lontano dallo sviluppo, mostrare il ROI per il budget di sicurezza interno e misurare l'efficacia della sua leadership.

Prima di intraprendere qualsiasi formazione, l'azienda ha chiesto a tutti gli sviluppatori di rispondere a un assessment sullo sviluppo sicuro. La valutazione consisteva in una serie di domande relative alla ricerca di una semplice vulnerabilità OWASP Top 10 in una funzione specifica e nel risolverla, in due vulnerabilità SQL Injection, una vulnerabilità XML External Entities (XXE) e una vulnerabilità Cross-Site Scripting. Inoltre,

era presente una domanda sulla deserializzazione insicura. Agli sviluppatori non sono state date le risposte alle domande, ma solo un punteggio finale.

Gli sviluppatori hanno ottenuto in media un punteggio di appena il 19% e hanno trovato e risolto una media di appena il 14% delle vulnerabilità. Il 58% degli sviluppatori non è stato in grado di trovare e correggere con successo una sola vulnerabilità.

### Soluzione

L'azienda ha deciso di sottoporre tutto il proprio team di sviluppo software ai corsi di formazione pratici sullo sviluppo sicuro di HackEDU. Gli sviluppatori dell'azienda hanno superato una media di 12 delle 35 lezioni e 12 sfide di HackEDU. La formazione di HackEDU aiuta gli sviluppatori a migliorare la loro capacità di scrivere software sicuro, aumentare la loro comprensione di come i sistemi software vengono hackerati e ridurre il tempo necessario per risolvere i problemi relativi alla sicurezza. Inoltre, la formazione ha aiutato l'azienda a soddisfare i requisiti di conformità della formazione sulla codifica protetta PCI.

Successivamente alla formazione e circa 9 mesi dopo la valutazione iniziale, gli sviluppatori sono stati sottoposti a un'altra valutazione. Questa volta il punteggio medio è stato dell'85% e gli sviluppatori hanno rilevato l'81% delle vulnerabilità. Il 100% degli sviluppatori ha trovato e risolto la maggior parte delle vulnerabilità nella valutazione e tutti quanti hanno migliorato la loro capacità di trovare e correggere le vulnerabilità nel codice.

### Risultati e vantaggi

Il team di sviluppo ha migliorato non solo la capacità di scrivere codice in modo sicuro, ma ha anche pensato che il training sia interessante e illuminante. Uno sviluppatore ha scritto "Non sapevo che l'algoritmo MD5 non fosse considerato sicuro" e un altro sviluppatore ha commentato: "La parte pratica è stata fantastica!"

---

Advanction è partner di HackEDU per l'Italia e la Svizzera.

Contattaci per avere maggiori informazioni

**Advanction S.A.**

Via Nuaa, 20

6873 Corteglia – Castel San Pietro

Svizzera

www.advanction.com

info@advanction.com