ARTICOLO DI ELEARNINGNEWS

Year 6 - number 227 Wednesday 7 december 2022

Come riconoscere un'app di eLearning sicura

In che modo gli sviluppatori di app per la formazione difendono la nostra sicurezza? Impariamo a individuare i segnali che indicano la sicurezza di un'app.

L'eLearning è cresciuto in popolarità per la sua capacità di far fronte alla crescente richiesta di una **formazione più veloce, mirata e accessibile**. Inoltre, le tecnologie di oggi permettono a chiunque abbia una connessione a internet di creare un sito o un'app per vendere i propri corsi. Questo spiega perché c'è stata negli ultimi anni una grande evoluzione nello sviluppo di applicazioni eLearning. Come sempre, ogni aspetto della tecnologia comporta una serie di minacce alla sicurezza.

La **sicurezza dei dati** è messa a dura prova anche nelle **applicazioni di eLearning**. Le ripercussioni di una violazione della sicurezza dei dati potrebbero essere problematiche per gli studenti i cui diritti vengono violati e devastanti per la reputazione di chi offre i corsi. In questo articolo esploriamo il dietro le quinte dello sviluppo delle app per capire in che modo gli sviluppatori difendono la nostra sicurezza e per imparare a individuare i segnali che indicano la sicurezza di un'app.

Le misure di sicurezza per difendere i dati

Ogni sviluppatore di applicazioni eLearning dovrebbe affrontare la questione della sicurezza dei dati con la massima attenzione. In caso contrario, l'applicazione sarà vulnerabile ad attacchi come furti di identità, frodi online, manomissione dei dati, fino ad arrivare alla perdita di proprietà intellettuale. Pertanto, la strategia migliore consiste nell'implementare **misure di sicurezza** per evitare che le vulnerabilità dei dati si infiltrino nelle app di eLearning. Questo articolo illustra alcuni suggerimenti essenziali che possono aiutare a proteggere le applicazioni eLearning dalle minacce alla sicurezza.

1. Scrivere un codice sicuro

La prima misura di sicurezza cruciale che gli sviluppatori di app dovrebbero adottare è la scrittura di un codice sicuro. Non c'è dubbio che i codici delle app siano vulnerabili a diverse falle nella sicurezza che spesso hanno ripercussioni devastanti, come danni alla reputazione, esposizione di dati sensibili degli utenti, furti di identità e violazioni della privacy. Per proteggere un codice da questi e molti altri problemi di sicurezza, è sempre essenziale seguire pratiche di scrittura sicura del codice.

La pratica di sicurezza più importante che ogni sviluppatore dovrebbe adottare quando scrive un codice è quella di firmare il codice utilizzando un **certificato di firma del codice**, chiamati certificati **code signing**. Questo certificato è fondamentale perché garantisce che il codice non venga corrotto o alterato da individui malintenzionati mentre si sposta tra i sistemi degli sviluppatori e quelli degli utenti. Se avete sviluppato la vostra app di eLearning ricordatevi che avete bisogno di questi certificati per proteggere i codici da un'eventuale corruzione. Fortunatamente ci sono vari prodotti online e non è necessario acquistarne uno costoso per assicurarti la massima sicurezza.

2. Valutare e prevenire le minacce legate al server

Uno sviluppatore di applicazioni eLearning deve assicurarsi di valutare e prevenire tutte le vulnerabilità legate al server. Questo dovrebbe essere fatto nelle prime fasi del ciclo di vita dell'applicazione. Le vulnerabilità legate al server aprono le porte a malintenzionati che possono infiltrarsi nel sito web e manometterne i contenuti. Queste vulnerabilità possono essere comunicazioni non sicure, malware e virus ecc., tutti elementi che possono rappresentare minacce per i server.

Ci sono tre metodi che gli sviluppatori possono utilizzare per prevenire le minacce alla sicurezza legate al server.

a. In primo luogo, gli sviluppatori di app di eLearning devono sempre attenersi alle migliori **pratiche di sicurezza del codice**. Una lista di alcune delle pratiche di controllo per una codifica sicura dei dati è riportata di seguito:

- Autenticazione con password sicura

- Gestione della sessione con i dettagli completi dell'utente
- Controllo e gestione degli accessi con adeguata verifica dell'utente
- Il caricamento dei file deve essere specifico per il contesto della pagina
- Trasmissione sicura con HTTPS

b. In secondo luogo, gli sviluppatori dovrebbero utilizzare uno **scanner automatico**. L'automazione è il modo migliore per ridurre le possibilità di errore umano. Una disattenzione può portare alla perdita di dati sensibili e l'automazione è come mettere il pilota automatico ai processi essenziali di sicurezza ed eliminare gli eventuali errori.
c. Lo scopo dell'automazione è quello di incoraggiare gli sviluppatori a correggere i bug nelle prime fasi dello sviluppo, piuttosto che effettuare una verifica di sicurezza alla fine del processo. Per questo è sempre utile effettuare una **valutazione manuale dei rischi** per la sicurezza delle app. Questo aiuta a distinguere le minacce dell'applicazione classificandole in base alla loro intensità e probabilità di verificarsi.

3. Utilizzo dei certificati SSL

I certificati SSL sono strumenti crittografici che si occupano di nascondere i dati da accessi non autorizzati. In parole più semplici sono dei pezzi di codice che garantiscono la sicurezza delle comunicazioni online. Quando un browser web contatta il vostro sito, il certificato SSL abilita una connessione crittografata. Non è così diverso dal sigillare una lettera in una busta prima di spedirla per posta. Il loro utilizzo non si limita a questo, sono utilizzati anche come strumenti per la sicurezza dei siti web nell'ambito della migrazione da HTTP a HTTPS. Questi ultimi sono considerati più sicuri perché consentono di crittografare le informazioni di un sito, tanto che Google usa gli HTTPS come standard per i siti presenti su Google Chrome.

Tuttavia, il loro ambito di applicazione non è limitato ai siti web. I certificati SSL hanno un ruolo fondamentale anche nella sicurezza delle app. La mancanza di un certificato SSL, o anche solo la possibilità che il certificato non sia stato verificato correttamente, può invitare molti aggressori a sfruttare il vostro sito web. Senza questi strumenti, anche gli hacker non esperti hanno la possibilità di appropriarsi di dati e comunicazioni che avvengono nel vostro sito web.

4. Utilizzare un'autenticazione forte per le app

Il **Verizon Data Breach Investigation Report** del 2021 ha riportato alcune statistiche sorprendenti: l'81% delle violazioni di dati si verifica a causa di password deboli. Gli aggressori decodificano facilmente le password deboli per accedere ai dati privati. Per evitare che ciò accada, gli sviluppatori di app di eLearning dovrebbero stabilire una soglia che richieda agli utenti di utilizzare solo password forti e uniche. Gli sviluppatori dovrebbero anche ricordarsi di **integrare dei fattori di autenticazione** nel processo di accesso degli utenti. L'autenticazione a più fattori aumenta la sicurezza perché richiede agli utenti di utilizzare più di una singola password per accedere all'applicazione.

Altre pratiche utili per difendere dati

1. Proteggere le e-mail dagli attacchi di phishing

Gli hacker non attaccano solo attraverso malware nascosti in app o siti, ma anche in modo più diretto, per esempio mandando e-mail. Questo tipo di attacco è molto popolare e sfortunatamente miete molte vittime, tanto da aver ricevuto un nome proprio: **phishing.**

L'invio di e-mail infestate da malware è stato il segno distintivo degli hacker che cercano di creare scompiglio nel mondo informatico. Gli hacker possono bloccare i profili degli studenti e per contrastare questi attacchi è consigliabile installare certificati S/MIME.

2. Proteggere i documenti riservati

Un altro aspetto fondamentale per chi fa eLearning è impedire la manipolazione e la manomissione di certificati scolastici, come diplomi, trascrizioni ecc. Fortunatamente la pandemia ha costretto aziende, privati e la pubblica amministrazione ad adottare uno strumento utile ad assicurare la protezione di questo tipo di documenti. **La firma digitale dei documenti** ha garantito la sicurezza della firma remota dei documenti e, se combinata con i vantaggi della PKI, offre un alto livello di sicurezza nello scambio di certificati scolastici, come diplomi e trascrizioni. Infatti, una firma digitale non può essere falsificata a differenza di

una documento firmato a mano e scannerizzato. Inoltre, non ha una data di scadenza ed è valida per sempre.

Le regole di privacy negli store di app-mobile

Nonostante il tema della privacy e sicurezza dei dati sia sempre più importante per la politica e per gli utenti, i principali colossi della tecnologia non sembrano fare passi promettenti per difendere la sicurezza dei nostri dati.

I principali attori negli store di app-mobile, ovvero **Play Store** ed **Apple Store**, adottano costantemente nuove politiche di protezione dati con lo scopo di garantire ai propri utenti un sistema di sicurezza efficace. Ad esempio, Apple dichiara che i controlli eseguiti sul suo store sono così rigidi da riuscire ad intervenire subito nel caso venga rilevato un caso sospetto. Nonostante questo, nel 2022 sono uscite notizie riguardanti la presenza di **7 app presenti sullo store di Apple contenenti malware**. Apple è intervenuta prontamente eliminando queste app (dallo store, ma non dai dispositivi) ma il fatto che siano arrivate sullo store e siano state disponibili al download fa sorgere diversi dubbi sui canoni di sicurezza stabiliti dal colosso tecnologico. Anche Google non sembra fare passi in avanti per la difesa dei dati. Alcune regole di sicurezza su Play Store sono cambiate di recente. Fino a luglio 2022, nella pagina di download delle applicazioni era mostrato un elenco, scritto da un software creato da Google, contenente tutti i permessi richiesti. In questo modo, l'utente poteva intuire subito i rischi a cui andava in contro e valutare la sicurezza dell'applicazione. ??Oggi, quando si sfogliano le app o i giochi su Google Play, si può notare che **l'elenco delle autorizzazioni non è più disponibile**. Sembra che Google abbia deciso che il nuovo elenco sulla sicurezza dei dati sia sufficiente a questo proposito. Gli editori che vogliono vendere le loro app su questi store sono sempre tenuti a fornire informazioni sulla sicurezza dei dati, poiché Google le ha rese obbligatorie. Tuttavia, spetta all'editore compilare queste informazioni e non è spiegato all'utente finale come vengano controllate queste informazioni.

Conclusione

Dato che il tema della privacy e dell'utilizzo dei nostri dati necessitano di strumenti legali che sono ancora in fase di perfezionamento, e che non sempre le aziende sembrano prendere decisioni in favore degli utenti finali, è vitale che questi ultimi si tutelino da soli. La creazione di un'applicazione eLearning sicura dipende soprattutto dalle competenze e dalle conoscenze degli sviluppatori. Tuttavia, è necessario che anche gli utenti siano consapevoli dei rischi che si incorre a scaricare un'app priva di certificazioni di sicurezza e conoscano i modi per tutelarsi al meglio da questi rischi.