Relazione sul Progetto Client-Server

David Moonsmee, Giovanni Pio Zullo

Sicurezza dei Sistemi

Abstract

La crescente sofisticazione degli attacchi informatici ha reso la sicurezza delle applicazioni una priorità fondamentale per la protezione delle informazioni sensibili. Questo documento descrive le misure implementate per rafforzare la sicurezza del sistema, con un focus sulle tecniche di protezione come la cifratura delle password, la gestione sicura delle sessioni, la protezione contro gli attacchi DDoS e la protezione contro gli attacchi di tipo SQL Injection. In particolare, viene esaminato come l'uso di SSL/TLS per la comunicazione sicura tra client e server contribuisca a garantire la riservatezza dei dati scambiati. Le misure adottate sono state progettate per ridurre al minimo le vulnerabilità comuni e aumentare la protezione degli utenti contro gli accessi non autorizzati.

Contents

1 Introduzione

Nel contesto digitale contemporaneo, la protezione dei dati degli utenti e delle applicazioni è di primaria importanza. La crescente complessità degli attacchi informatici e la continua evoluzione delle minacce richiedono misure di sicurezza avanzate per prevenire accessi non autorizzati e proteggere le informazioni sensibili. In questo contesto, il nostro sistema ha implementato diverse tecniche di protezione che mirano a garantire l'autenticazione sicura degli utenti, la difesa contro minacce comuni e la cifratura sicura dei dati durante la trasmissione.

Le principali misure adottate comprendono il rafforzamento delle credenziali di accesso tramite l'implementazione di politiche di complessità per le password, l'uso di cifratura e hashing delle stesse, la protezione delle sessioni utente e l'adozione di SSL/TLS per la cifratura delle comunicazioni. Inoltre, sono state introdotte difese contro gli attacchi DDoS e tentativi di accesso fraudolenti per garantire la disponibilità e l'integrità del sistema.

2 Miglioramenti alla Sicurezza

1. **Rafforzamento di Username e Password**
2. **Modifica di Username e Password durante l'Accesso**
3. **Cifratura e Hashing delle Password**
4. **Mascheramento delle Password**
5. **Timeout per la Gestione delle Risorse**
6. **Connessione Sicura SSL/TLS**
7. **Protezione contro Attacchi DDoS e Accessi Fraudolenti**

2.1 Rafforzamento di Username e Password

Il rafforzamento delle credenziali di accesso è stato ottenuto attraverso l'adozione di politiche di complessità avanzata. Ogni password deve soddisfare specifici requisiti, inclusi caratteri maiuscoli, minuscoli, numeri, caratteri speciali e una lunghezza minima di 8 caratteri. Questa misura ha l'obiettivo di prevenire attacchi di tipo "brute force", rendendo le password più difficili da indovinare o forzare.

Motivazione: L'implementazione di requisiti di complessità per le password è una strategia preventiva contro attacchi automatizzati che tentano di indovinare la password mediante l'uso di combinazioni di caratteri comuni.

2.2 Modifica di Username e Password durante l'Accesso

Per consentire agli utenti di aggiornare le proprie credenziali in caso di necessità, è stata introdotta una funzionalità che permette di modificare sia il nome utente che la password durante la sessione di accesso.

Motivazione: Consentire agli utenti di aggiornare le loro credenziali in caso di sospetta compromissione rappresenta una misura preventiva utile per ridurre i rischi legati a password compromesse.

2.3 Cifratura e Hashing delle Password

Le password degli utenti vengono cifrate e hashate utilizzando l'algoritmo SHA-256 al momento della registrazione e del login. Questo significa che il sistema memorizza solo la versione "hashata" della password, rendendo impossibile il recupero della password originale.

Motivazione: L'uso dell'hashing unidirezionale impedisce la decodifica delle password, riducendo il rischio che, anche in caso di accesso non autorizzato ai dati del sistema, le credenziali degli utenti vengano compromesse.

2.4 Mascherazione della Password

Per proteggere le credenziali dell'utente durante l'inserimento, le password vengono mascherate (ad esempio, tramite asterischi) sia durante la registrazione che durante il login.

Motivazione: La mascheratura impedisce che terze persone possano vedere le password mentre vengono inserite, aumentando la protezione durante il processo di autenticazione.

2.5 Timeout per la Gestione delle Risorse

Il sistema è stato configurato con un timeout che termina automaticamente le sessioni inattive dopo un determinato periodo di tempo. Questo aiuta a liberare risorse server non utilizzate e previene il rischio di accessi non autorizzati durante sessioni lasciate aperte accidentalmente.

Motivazione: Il timeout per le sessioni inattive ottimizza l'uso delle risorse del server e riduce il rischio che utenti non autorizzati possano prendere il controllo di una sessione non attivamente monitorata.

2.6 Connessione Sicura tramite SSL/TLS

Tutta la comunicazione tra client e server è protetta da SSL/TLS, garantendo che i dati siano cifrati durante il trasferimento, prevenendo così attacchi di tipo "man-in-the-middle" e assicurando che le informazioni non vengano intercettate o alterate.

Motivazione: L'adozione di SSL/TLS per le comunicazioni protegge la riservatezza e l'integrità dei dati, rendendo più difficile per i malintenzionati compromettere le informazioni in transito.

2.7 Protezione contro Attacchi DDoS e Accessi Fraudolenti

Il sistema è dotato di misure di protezione contro gli attacchi DDoS e limitazioni sui tentativi di login falliti. È stato implementato un monitoraggio per identificare e bloccare gli indirizzi IP sospetti e prevenire tentativi di accesso non autorizzato.

Motivazione: La difesa contro gli attacchi DDoS e la protezione contro i tentativi di login ripetuti sono essenziali per mantenere l'affidabilità e l'integrità del sistema, impedendo che il server venga sopraffatto o che si verifichino accessi non autorizzati.

3 Conclusioni

Nel contesto attuale delle applicazioni web, caratterizzato da minacce alla sicurezza sempre più sofisticate, l'adozione di misure di protezione avanzate risulta imprescindibile per tutelare le informazioni sensibili degli utenti. Tecniche quali la cifratura e l'hashing delle password, la protezione contro attacchi SQL Injection e la gestione sicura delle sessioni costituiscono una solida base per proteggere il sistema da vulnerabilità comuni.

Le politiche di complessità delle password e la possibilità di modificarle facilmente durante l'accesso, insieme alla mascheratura delle password e al timeout per le sessioni inattive, rafforzano ulteriormente le difese contro accessi non autorizzati. Tali misure, oltre a migliorare la sicurezza, contribuiscono a un'esperienza utente ottimale.

Un elemento cruciale nella protezione delle applicazioni web è la salvaguardia della comunicazione tra client e server, ottenuta tramite l'implementazione di SSL/TLS. Questo approccio previene attacchi di tipo "man-in-the-middle", garantendo la riservatezza e l'integrità dei dati scambiati. Le difese contro attacchi DDoS e i tentativi di accesso fraudolenti, inoltre, migliorano la resilienza complessiva del sistema, riducendo il rischio di compromissione dell'accesso a livello di rete.

In conclusione, l'attuazione di queste misure contribuisce significativamente a rendere l'applicazione web più sicura, riducendo le vulnerabilità e incrementando la fiducia degli utenti nel sistema. Poiché le minacce informatiche sono in continua evoluzione, è essenziale che la sicurezza rimanga una priorità costante, con l'aggiornamento e il miglioramento continuo delle tecnologie e delle pratiche di protezione.