Università Degli Studi Di Salerno

Progetto di Ingegneria del software 2018/2019

Security Testing

Sommario

Componenti del team di progetto

Partecipanti	Matricola
Cosimo Bacco	**0512104516**
Michele Castellaneta	**0512104804**
Domenico Trotta	**0512104882**

1. Introduzione

Il Security o Penetration test è il processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. L'analisi comprende più fasi ed ha come obiettivo evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che ne hanno permesso l'accesso non autorizzato. L'analisi è condotta dal punto di vista di un potenziale attaccante e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente al sistema.

2. Fasi

Nel caso di GamesHub, il Security test è stato suddiviso in 2 fasi:

- SQL Injection test
- Privilege Escalation test

3. SQL Injection

Un SQL injection (SQLi) è un attacco mirato a colpire le applicazioni web che si appoggiano su un DBMS di tipo SQL. Questo attacco sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL. Le conseguenze prodotte sono imprevedibili per il programmatore, l'SQL injection permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito anche senza essere in possesso delle credenziali di accesso e di visualizzare e/o alterare dati presenti del database.
GamesHub interagisce con un'utente, che può inserire dei dati, e quindi potenzialmente effettuare una SQLi. La SQLi in sé, deve contenere dei caratteri specifici della sintassi SQL, come ad esempio ' (l'apostrofo), "" (gli apici), ; (punto e virgola) ecc... La verifica dell'esistenza di questi caratteri nell' input, garantisce l'impossibilità di effettuare una iniezione.
Tutti i campi input di GamesHub, prima di essere inseriti nella query verso il db, vengono validati con dei pattern regex.
La validazione avviene nei due momenti diversi: lato client e lato server. Lato client non è sicuro, siccome un malintenzionato potrebbe eseguire una richiesta direttamente al server sorpassando validazione con jquery. La seconda verifica, lato server, impossibile sorpassarla, quindi rende il sistema sicuro.

4. Privilege Escalation test

Il Privilege Escalation consiste nel tentativo di ottenere i privilegi più alti nel sistema. Ad esempio, un utente potrebbe tentare di eseguire una richiesta alle pagine del gestore catalogo o gestore ordini.
Però prima che l'utente venga reindirizzato alla pagina viene controllato se un utente può o meno accedere ad una determinata pagina. Nel caso in cui l'utente non ha l'autorizzazione ad accedere a quella pagina viene immediatamente reindirizzato alla pagina di login di GamesHub.

5. Conclusione

Durante lo sviluppo di GamesHub sono state adottate diverse tecniche per garantire la sicurezza e stabilità del sistema stesso. Tutte le tecniche citate in questo documento sono state testate e all'atto del rilascio del sistema tutto risulta funzionante e coerente con i requisiti non funzionali definiti all'interno del requirements analysis document.