Security Operation

1. Difese contro SQL Injection (SQLi)

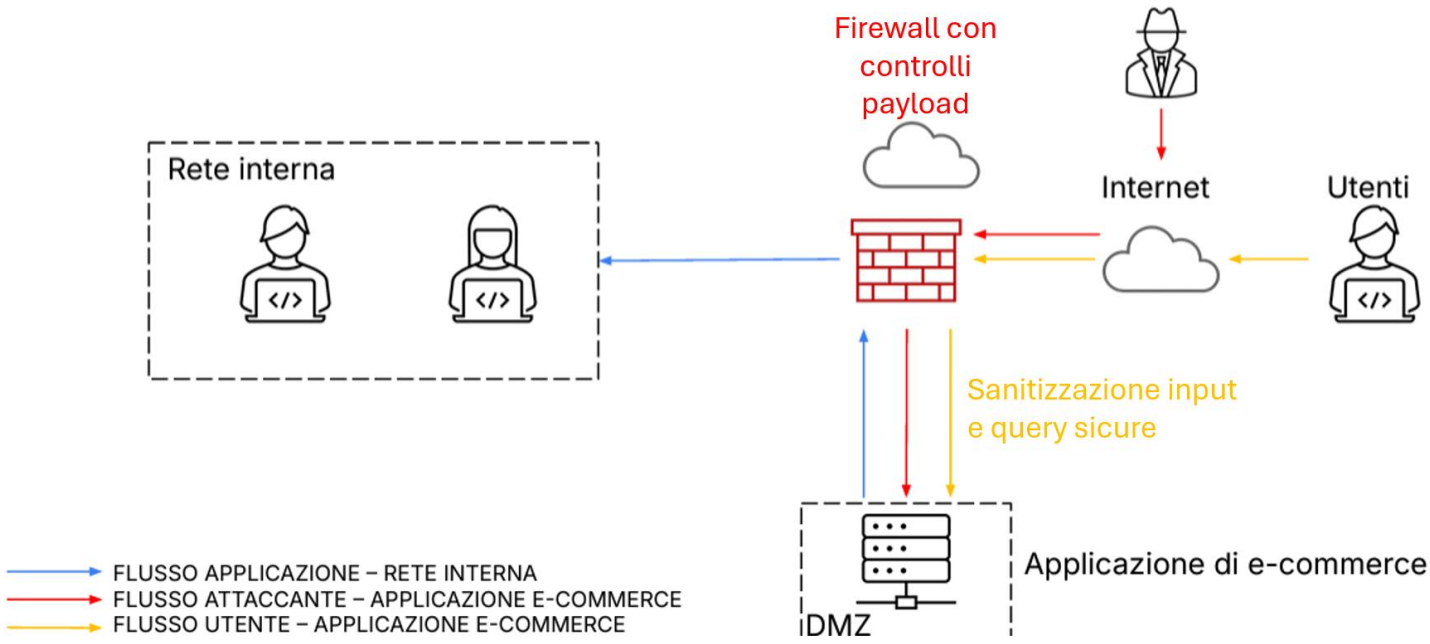
- Utilizzo di query parametrizzate (prepared statements).
- Adozione di ORM (Object-Relational Mapping) per gestire le query.
- Validazione e sanitizzazione degli input da parte dell'utente.
- Limitazione dei privilegi dell'utente del database.

2. Difese contro Cross-Site Scripting (XSS)

- Escape dell'output HTML, JavaScript e CSS.
- Implementazione di Content Security Policy (CSP) tramite header HTTP.
- Sanitizzazione dell'input HTML usando librerie come DOMPurify.
- Utilizzo dei flag HttpOnly e Secure nei cookie.

3. Architettura e punti di applicazione delle difese

Nell'immagine seguente vengono indicati i punti in cui le difese contro SQLi e XSS devono essere applicate all'interno dell'architettura. Le protezioni si applicano sia a livello di codice dell'applicazione, sia tramite configurazioni infrastrutturali come firewall, WAF e policy di rete.



1. Impatto economico di un attacco DDoS

Scenario: L'applicazione web subisce un attacco DDoS (Distributed Denial of Service) che la rende non raggiungibile per 10 minuti.
Spesa media degli utenti per minuto: 1.500 €
Durata del disservizio: 10 minuti
Perdita stimata: 10 × 1.500 € = 15.000 €

2. Azioni preventive contro attacchi DDoS

- Monitoraggio e rilevamento precoce tramite strumenti come Zabbix, Prometheus o Datadog.
- Utilizzo di servizi anti-DDoS come Cloudflare, AWS Shield, Azure DDoS Protection.
- Web Application Firewall (WAF) per bloccare traffico sospetto.
- Load balancing e ridondanza geografica per distribuire il traffico.
- Rate limiting e CAPTCHA per limitare l'impatto di bot e richieste anomale.
- CDN per caching dei contenuti e assorbimento del traffico distribuito.
- Piano di risposta agli incidenti e simulazioni periodiche di attacco.

Difesa da attacco Malware

Scenario: una macchina viene infettata da un malware.

Azioni di risposta:

- Disconnettere immediatamente la macchina infetta dalla rete interna
- Bloccare il traffico attraverso il firewall
- Verificare se il computer infetto ha account con privilegi amministrativi e/o ad altri sistemi. In questo caso ridurre i privilegi in modo da limitare I danni.
- Monitorare traffico di rete
- Dato che non abbiamo rimosso l'accesso dell'attaccante alla macchina infettata possiamo monitorare e studiare i suoi comportamenti, andando ad aggiornare le tecniche di difesa future.
- Consigliato creare una copia completa della macchina infetta per ulteriori analisi