Azioni per prevenire attacchi SQLi - XSS:

- **Utilizzare Prepared Statements:** usare query parametrizzate o prepared statements per separare il codice SQL dai dati.
- Limitare i Privilegi del Database: assicurarsi che le credenziali del database abbiano il minimo privilegio necessario.
- Monitoraggio e Logging: monitorare le query e registrare eventuali accessi anomali o tentativi di attacco.
- Escaping dei Dati: è una misura di sicurezza essenziale per garantire che i dati siano trattati in modo sicuro e che le vulnerabilità siano minimizzate. Preparare/modificare i dati che vengono restituiti al browser per evitare l'esecuzione di codice JavaScript.
- "Sanitizzazione" dell'Input: validare e sanificare tutti gli input dell'utente, specialmente in campi di testo e aree dove l'output viene visualizzato ed utilizzare delle blacklist di caratteri da non accettare in input.
- Content Security Policy (CSP): implementare una Content Security Policy per limitare le fonti da cui il browser può caricare contenuti.
- Formattazione delle Risposte: impostare correttamente gli header delle risposte HTTP
- Non Fidarsi dell'Input: non dare per scontato che i dati dell'utente siano sempre sicuri, piuttosto trattarli come non attendibili.
- Utilizzo di WAF: implementare un Web Application Firewall (WAF) per rilevare e
 bloccare attacchi SQLi e/o XSS. Il WAF lo implementeremo tra la nostra webapp ed
 Internet, allo stesso modo del già presente firewall. Come un normale firewall può
 essere di tipo hardware o software con la differenza che il primo può avere dei costi più
 alti mentre il secondo inficerà sulle prestazioni della macchina. Una soluzione ottimale
 potrebbe essere un WAF su cloud.

Attacco DDos

Spesa media al minuto: € 1.500,00
 Durata dell'interruzione: 10 minuti

Impatto = Spesa media al minuto × Durata dell'interruzione Impatto = € 1.500×10minuti = 15.000€ Quindi, l'impatto economico dell'attacco DDoS è di **15.000** €.

Azioni Preventive Contro Attacchi DDoS

Per mitigare il rischio e gli effetti di attacchi DDoS, possiamo implementare diverse misure preventive:

- Implementare un WAF (Web Application Firewall):anche in questo caso un WAF può filtrare il traffico malevolo e bloccare richieste sospette prima che raggiungano l'applicazione.
- Rate Limiting: implementare limiti di frequenza per le richieste degli utenti per prevenire picchi improvvisi di traffico.
- Rete di Protezione DDoS: considerare l'uso di servizi di protezione DDoS offerti da provider specializzati (come Cloudflare, AWS Shield) per rilevare e mitigare attacchi.
- Architettura Scalabile/Failover Cluster: sviluppare un'architettura scalabile che consenta di aumentare le risorse in caso di attacchi, cioè se il nostro server primario smetterà di funzionare il secondo nodo del cluster(gruppo di pc/server) si attiverà.
- **Monitoraggio e Alert**: monitorare costantemente il traffico di rete e impostare degli alert per attività sospette o picchi di traffico anomali.
- **Backup:** avere una strategia di come copiare i dati e le configurazioni attualmente in uso per recuperare l'attività in seguito ad un disastro.
- Piani di Risposta agli Incidenti: avere un BPC (Business Continuity Plan) e un Disaster Recovery che definiscano le procedure da seguire in caso di attacco.

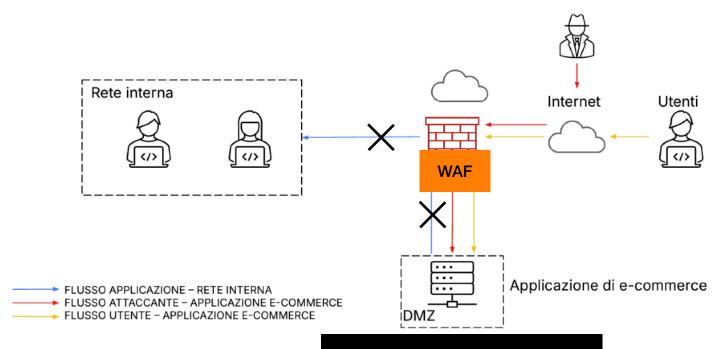
Conclusione

L'attacco DDoS ha un impatto significativo sul business, in questo caso pari a 15.000 €. Implementare misure preventive può non solo ridurre la probabilità di un attacco, ma anche limitare i danni economici e la perdita di reputazione associata a downtime imprevisti.

Response a malware

Se l'applicazione è infettata da malware e la vogliamo contrastare la propagazione nella rete interna, si possono adottare le seguenti misure:

- Segmentazione della Rete: isolare il server dalla rete interna, creando un rete di "quarantena", in modo da consentire comunque l'accesso ad Internet. Se pensiamo che non sia abbastanza sicuro o temiamo che l'attaccante possa comunque accedere alla rete interna o che il malware possa riprodursi allora il server infetto verrà "isolato" quindi avrà accesso ad internet ma sarà totalmente disconnesso dalla rete interna.
- **Firewall e VLAN**: configurare firewall/WAF e VLAN per impedire il traffico non autorizzato dalla macchina infetta alla rete interna.
- Monitoraggio del Traffico: implementare un sistema di monitoraggio che registri l'attività della macchina infettata e rilevi attività sospette o tentativi di propagazione del malware.
- **Backup e ripristino**: indicare un sistema di backup per garantire che i dati non vengano compromessi in caso di ulteriore propagazione. Procedere quindi con l'applicazione di patch di sicurezza aggiornate, revisione di politiche dei firewall/IPS/IDS e aggiornamento delle firme degli antivirus.



Quarantena / Isolamento del server