Report sull'esercitazione W20D4

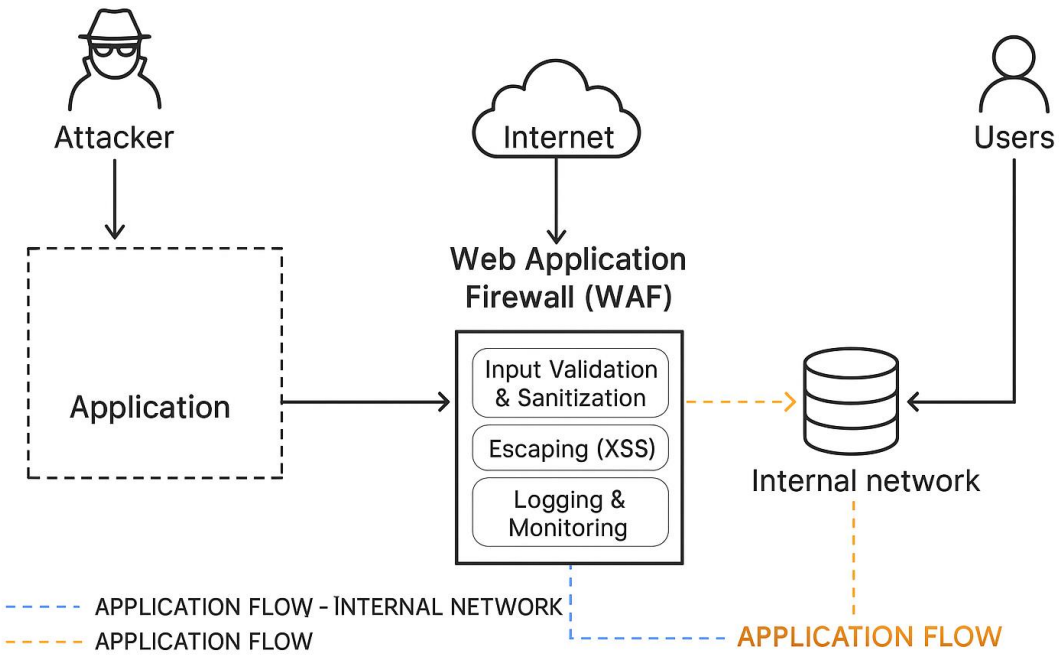
1. Azioni preventive:

Input Validation & Sanitization
Validare **tutti i dati in input**.

Web Application Firewall (WAF)
Posizionare un **WAF tra internet e la DMZ**, per filtrare richieste HTTP sospette o malevole (es. richieste contenenti payload XSS o SQLi).

Escaping dell'output (XSS)
Codificare correttamente l'**output HTML** generato dinamicamente con input dell'utente.

Logging e Monitoraggio
Implementare un sistema di logging che rilevi tentativi di injection o di accesso non autorizzato.



2. Azioni preventive:

Calcolo dell’impatto economico diretto:

Spesa media per minuto: 1.500 €;

Durata del disservizio: 10 minuti;

Perdita totale:

$$1.500\ €/\text{min} \times 10\ \text{min} = 15.000€.$$

Impatto diretto sul fatturato: 15.000 € persi in 10 minuti.

Altri impatti indiretti:

Diminuzione della fiducia degli utenti;

Danni all’immagine del brand.

Azioni preventive contro attacchi DDoS:

Firewall di nuova generazione;

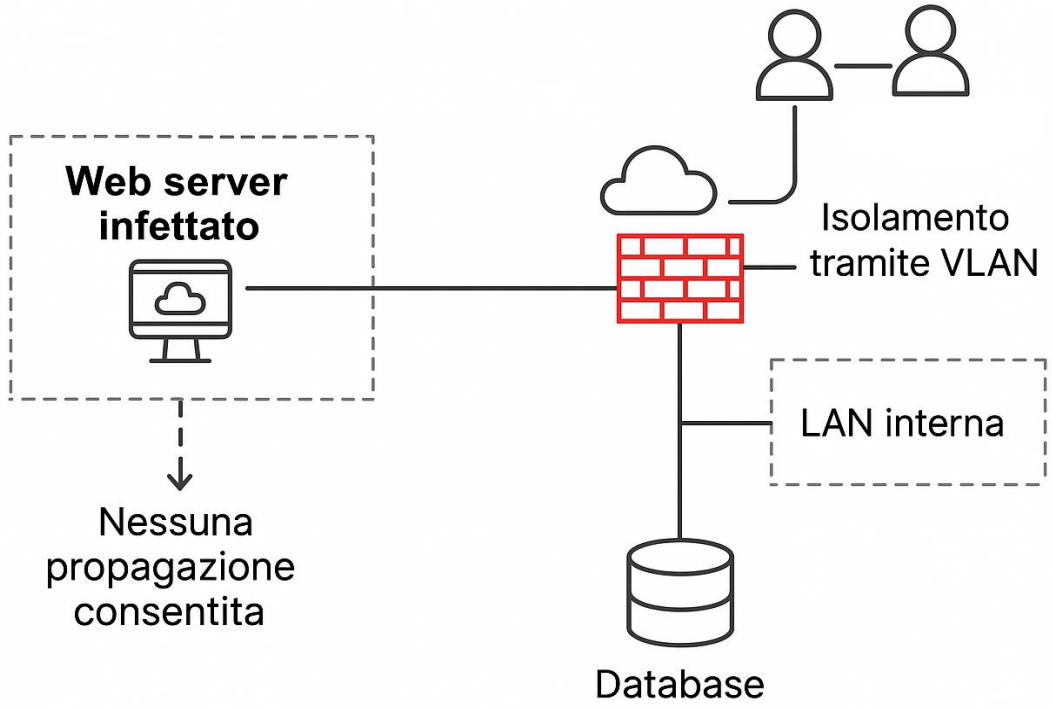
Servizi Anti-DDoS basati su cloud;

Load Balancer e ridondanza;

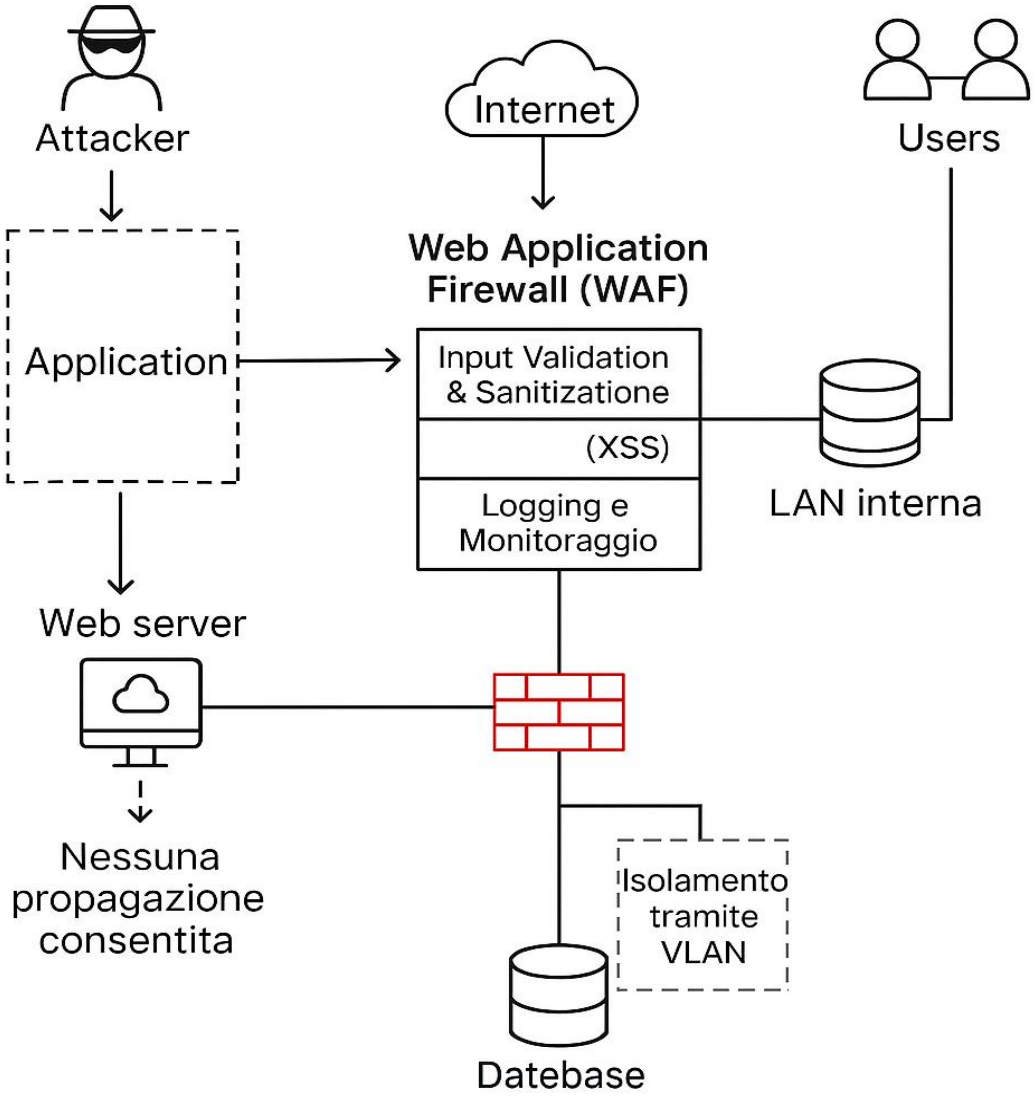
Sistema di rilevamento e risposta automatica;

Limiti di rete e Captcha avanzati.

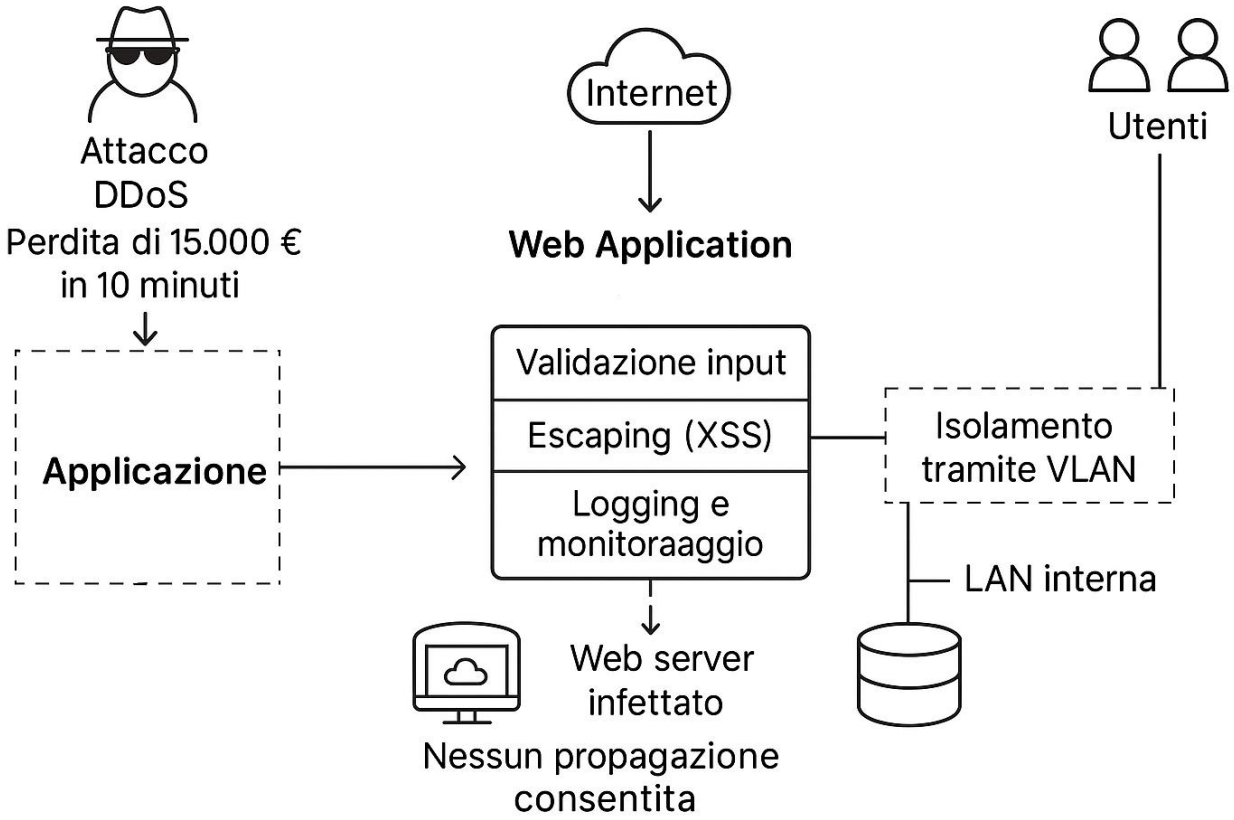
3. Response:



4. **Soluzione completa:**



5. Modifica più ‘aggressiva’ dell’infrastruttura:


Attacco
DDoS
Perdita di 15.000 €
in 10 minuti
Internet
Web Application
Utenti
Applicazione
Validazione input
Escaping (XSS)
Logging e
monitoraaggio
Isolamento
tramite VLAN
LAN interna
Web server
infettato
Nessun propagazione
consentita