Azioni e Preventivo Difesa da SQLi/XSS

1 - Azioni Preventive - SQLi e XSS

Obiettivo

Difesa dell'applicazione web da attacchi **SQL Injection** e **Cross-Site Scripting**, si rendono necessarie le seguenti azioni.

Il punto di partenza deve essere la formazione del personale a cui possiamo poi applicare le seguenti correzioni. Alcune informazioni necessarie per la corretta fruizione della documentazione

SQL Injection (SQLi): attacco in cui un utente inserisce codice SQL malevolo in un campo di input dell'applicazione, ingannando il database per eseguire query non autorizzate (es. furto di dati, bypass dell'autenticazione).

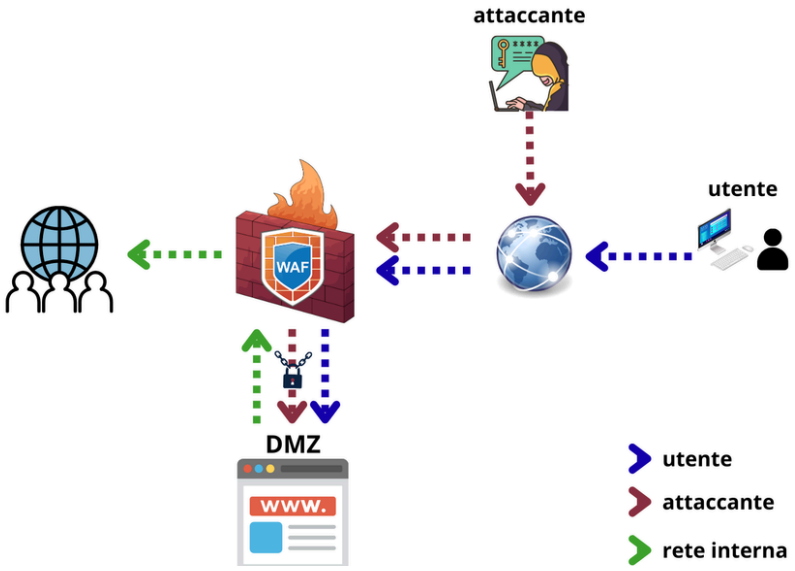
Cross-Site Scripting (XSS): attacco in cui script malevoli vengono iniettati in pagine web visualizzate da altri utenti. Può avvenire in tre forme: Stored XSS, Reflected XSS e DOM-based XSS.

DOM (Document Object Model): rappresentazione ad albero della pagina HTML creata dal browser in memoria. Nel DOM-based XSS, il payload malevolo viene iniettato ed eseguito direttamente nel DOM lato client (es. via document.location o innerHTML), senza passare dal server

Livello applicativo:

Installazione di un **WAF** (Web Application Firewall-agisce al livello 7 del modello **OSI**) da inserire in **DMZ** (zona demilitarizzata) davanti all'applicazione e-commerce. Questo misura filtra le richieste HTTP/HTTPS bloccando **payload** malevoli (SQLi, XSS, attacchi bot ecc.)

Lato codice dell'applicativo, nessun dato utente deve poter essere usato direttamente in **query SQL** o nel **DOM** (Document Object Model) senza sanificazione. Si applica un processo di pulizia e filtraggio dei contenuti dinamici (come input utente, HTML generato o script).



2 -Impatto sul Business - attacco DDoS

Simuliano che l'applicazione Web subisca un attacco **DDoS** dall'esterno che la rende non raggiungibile per 10 minuti. Gli utenti spendono in media 1.500 € al minuto sulla piattaforma di e-commerce.

Tabella calcolo impatto

Evento	*Valore*
Downtime	**10 minuti**
Spesa al minuto	**€1.500,00**
Perdita totale	**-€15.000,00**

calcolo: 10 minuti x 1.500€/minuto = 15.000€ di mancato fatturato diretto.

Conseguenze per l'azienda:

Danno reputazionale: perdita di fiducia da parte degli utenti, con possibile abbandono della piattaforma a favore di competitor.

Costi di risposta all'incidente: costi importanti per l'intervento del team tecnico, analisi post-attacco.

Penali: possibile violazione delle normative sulla cyber sicurezza aziendale con possibili multe.

Azioni preventive:

Definire e garantire la continuità dei servizi.

Una prima operazione consisterà nel attivare un servizio Anti-DDoS (es. cloudflare).

Limitare il numero di richieste per un determinato utente in un determinato lasso di tempo.

Distribuire il traffico su più server, così da scoraggiare e/o impedire che attacchi alla web app possano metterla offline.

Successivamente bisognerà strutturare **BCP - Business Continuity Plan (garantisce la continuità del business), BIA - Business Impact Analysis (identificare le aree critiche e definirne il costo possibile), IRP - Incident Response Plan (piano di riposta ad un incidente).**

3 - Response - Malware sull'Applicazione Web

Possibilità:

L'applicazione web viene infettata da un malware. Massima priorità, impedire la propagazione sulla rete interna.

IRP - Incident Response Plan

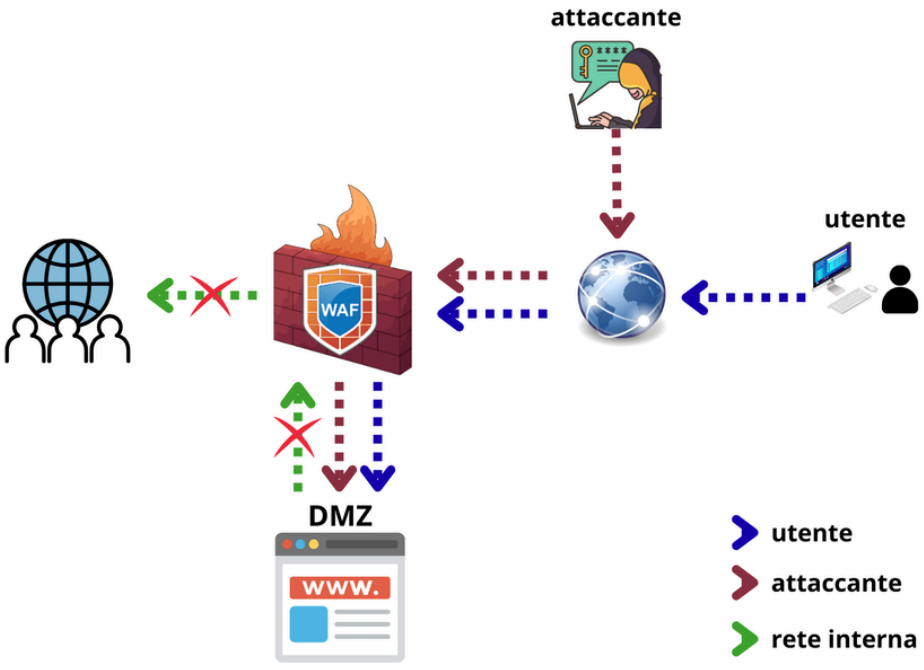
Esempio di comportamento appropriato, una volta eseguiti gli step, è possibile depennarli

Azione Immediata - isolamento:

- [ ] Modificare le regole del firewall (Aggiungere una regola esplicita di blocco es. DMZ verso Rete Interna (traffico bloccato) per bloccare immediatamente qualsiasi traffico dalla DMZ verso la rete interna (rappresentato dall'interruzione della freccia verde nella figura)
- [ ] Mantenere attivo il traffico da internet verso **DMZ**. Questo punto può apparire controverso, ma è molto importante non allertare l'attaccante in modo da poter monitare le sue azioni.

Azione di monitoraggio e analisi:

- [ ] Attivare il monitoraggio intensivo del traffico generato dalla macchina infetta tramite **SIEM (Security Information and Event Management)** e dato che l'attacco è già avvenuto e che momentaneamente non vogliamo allertare l'attaccante, utilizzare il sistema **IDS (Intrusion Detection System).** Li sfruttiamo per rilevare movimenti sospetti, tracciare tentativi di connessi ad host esterni , analizzare la logica dell'attaco e ideare misure di difesa e risposta.
- [ ] Attivare analisi forense della macchina e il suo isolamento
- [ ] Documentare tutte le attivita osservate dall'attacante per comprende il vettore di attacco e per eventuali procedure legali



Brevemente, in risposta all'incidente, la prima azione è attuare un modifica selettiva delle regole del firewall: si procede a bloccare esclusivamente il traffico in uscita dalla DMZ verso la rete interna, lasciando invece attivo il flusso dati proveniente dall'attaccante verso la DMZ. Questa scelta intenzionale. Interrompere tutto il traffico allerterebbe l'attaccante che rendendosi conto di essere stato scoperto, interromperebbe l'attacco. L'eventuale interruzione dell'attacco impedirebbe qualsiasi attività di analisi e studio del comportamento malevolo.

Il **SIEM** (Security Information and Event Management) si occuperà di raccoglie e centralizzare in tempo reale tutti i log disponibili, quali: log del firewall, log dell'applicazione web, log di sistema della macchina infetta. Grazie alla correlazione automatica degli eventi è possibile ricostruire la timeline completa dell'attacco (quando è avvenuto l'accesso iniziale, quali azioni ha eseguito il malware, verso quali risorse ha tentato di spostarsi). Questa ricostruzione è fondamentale sia per contenere l'incidente in corso che per prevenire simili attacchi futuri.

L'**IDS** (Intrusion Detection System) posizionato nella DMZ monitora sia il traffico in entrata che quello in uscita dalla macchina compromessa. Quest'ultimo aspetto è particolarmente critico: molti malware, una volta installati, tentano di contattare server esterni di controllo per ricevere istruzioni o estrarre dati. L'IDS rileva questi tentativi e genera alert immediati al team di sicurezza. A differenza dell'**IPS** (Intrusion Prevention System), che blocca automaticamente il traffico sospetto in tempo reale, in questa occasione scegliamo un **IDS** perché vogliamo osservare il comportamento dell'attaccante senza interromperlo o insospettirlo. Bloccare il traffico automaticamente significherebbe allertarlo e perdere la possibilità di anallizare le tecniche/strategie di attacco, raccogliere prove e aggiornare le difese di conseguenza.

Le informazioni raccolte da SIEM e IDS servono a quattro obiettivi principali: studiare i **pattern dell'attacco**, difendersi attivamente dal tentativo in corso, identificare il **vettore di attacco iniziale** (es. una vulnerabilità nell'applicazione web) per applicare le patch necessarie prima del ripristino del servizio, e infine aggiornare l'**IRP (Incident Response Plan)** il documento che definisce ruoli, responsabilità e procedure di escalation da seguire durante un incidente di sicurezza.

4 -Riassunto delle operazioni/modifiche svolte

Aggiunto	Valore	Punto riferimento
Anti-DDoS	Intercetta attacchi prima che raggiungano il firewall	**Punto 2**
Firewall	Regole accesso DMZ	**Punto 1, 3**
WAF	filtra attacchi SQLi XSS	**punto 1**

Soluzione alternativa:

Nel caso in cui decidessimo di applicare una soluzione più drastica, portemmo:

Aggiungere un ulteriore firewall tra DMZ e rete interna.

Aumentare le misure di autentificazione utente. Essere nella rete non è più sufficiente per avere accesso alle successive risorse, è necessario riautenticarsi per l'accesso ad ogni dispositivo/software ecc. Applicchiamo il principio del Minimo Privilegio, ogni utente nella rete ha accesso solo alle area strettamente necessarie (l'attacco risulterà più difficle da svolgere e non si rischia di diffondere informazioni riservate).

E' possibile anche utilizzare dei software in grado di "studiare" le operazioni quoitidiane e necessarie degli utenti e se necessario bloccare quelle che risultano sospette.

Se non siamo sotto attacco potremmo anche valutare l'utilizzo dell'IPS.

5 - Costo implementazioni - costo in caso di attacco

Formazione del personale

Trattandosi di un'azienda con oltre 50 dipendenti, il costo della formazione del personale è più incisivo. Grazie al principio del minimo privilegio citato precedentemente possiamo chiaramente decidere di investire su formazione più complete solo per quegli utenti che effettivamente maneggiano dati importanti e lavorano giornalmente con le macchine, un 30% su 100 dipendenti.

- Costo formazione per 70 dipendenti standard: Corso base online su piattaforme come coursera €30 per dipendente, **totale €2.100**
- Corso formazione dipendenti esperti/team IT: corsi di formazione su misura erogati da epicode + piattaforma epicode microlearn. Il costo varia in base al preventivo per l'azienda, costo stimato per formazione premium €300 - €500 per dipendente, **totale max €15.000**

Anti-DDoS

La scelta suggerita è cloudflare Business, uno dei più noti nel settore, offre difesa contro svariate tipologie di attacchi. La licenza al software include WAF, difesa da DDoS e supporto 24/7. Costo annuo **€2.400**

Firewall

Disponibilità di scegliere tra opzioni più basilari come pfSense al costo di **€480 annui**. Fattibile, ma meno consigliato per aziende di queste dimensioni.

Soluzioni più complete e premium:

Fortinet - offre soluzioni come FortiGate 60F che prevede fino a 200 utenti al costo di **€1.200 una tantum** + **€800 annui.**

Cisco Firepower - software completo, utile se si vuole integrazione tra i vari software, costo **€2.500 una tantum** + **€1.500 annui.**

Per una maggiore sicurezza è possibile utilizzare un doppio firewall, chiaramente moltiplicando i prezzi.

IDS/IPS

Snort 3, software open source standard nel mercato. Il softare è gratuito ma il suo impiego, configurazione e gestione potrebbe avere un costo in un range di **€1.000-€1.500**

SIEM

Microsoft sentinel **€4.000 annui**

Costi annui

Voce	Minimo	Massimo
Formazione del personale	€11.100	€17.000
Anti-DDoS	€2.400	€2.400
Firewall	€480	€1.500
IDS/IPS	€1.000	€1.500
SIEM	€4.000	€4.000
Totale	**€18.980**	**€26.400**

Subire un attacco informatico ha costi molto più alti. Come da stime precedenti, un attacco DDoS da soli 10 minuti genera già **15.000 € di danno** (1.500 €/minuto × 10 minuti), e se il downtime si prolunga a un'ora si arriva a **90.000 €**. Nei casi più gravi, una violazione dei dati (data breach) costa in media **4,5 milioni di euro** secondo il rapporto IBM 2023, considerando i costi legali, le sanzioni GDPR, il risarcimento agli utenti e il danno reputazionale. Un attacco ransomware su una realtà medio-grande può invece bloccare l'intera operatività aziendale con danni stimati tra i **500.000 e i 2 milioni di euro**. A questi si aggiungono costi indiretti difficilmente quantificabili: perdita di clienti, recensioni negative e penali per violazione e per eventuale non rispetto delle normative.

Costo di due attacchi DDoS da 10 minuti = **€30.000**

Costo servizio di difesa premium = **€26.400**

glossario

SQL Injection - *Nella sicurezza informatica SQL injection è una tecnica di command injection, usata per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL. Il mancato controllo dell'input dell'utente permette di inserire artificiosamente delle stringhe di codice SQL che saranno eseguite dall'applicazione server: grazie a questo meccanismo è possibile far eseguire comandi SQL, anche molto complessi, dall'alterazione dei dati (es. creazione di nuovi utenti) al download completo dei contenuti nel database.*

Cross-Site Scripting - *Il cross-site scripting (XSS) è una vulnerabilità informatica che affligge siti web dinamici che impiegano un insufficiente controllo dell'input nei form. Un XSS permette a un cracker di inserire o eseguire codice lato client al fine di attuare un insieme variegato di attacchi quali, ad esempio, raccolta, manipolazione e reindirizzamento di informazioni riservate, visualizzazione e modifica di dati presenti sui server, alterazione del comportamento dinamico delle pagine web, ecc. Nell'accezione odierna, la tecnica ricomprende l'utilizzo di qualsiasi linguaggio di scripting lato client tra i quali JavaScript, VBScript, Flash. Il loro effetto può variare da un piccolo fastidio a un significativo rischio per la sicurezza, a seconda della sensibilità dei dati trattati nel sito vulnerabile e dalla natura delle strategie di sicurezza implementate dai proprietari del sito web. Secondo un rapporto di Symantec, nel 2007 l'80% di tutte le violazioni era dovuto ad attacchi XSS*

WAF - *Un firewall per applicazioni web (WAF) è una forma specifica di firewall applicativo che filtra, monitora e blocca il traffico HTTP da e verso un servizio web. Ispezionando il traffico HTTP, può impedire che gli attacchi sfruttino le vulnerabilità note di un'applicazione Web, come SQL injection, scripting cross-site (XSS), inclusione di file e configurazione del sistema impropria.*

DMZ - *Nell'ambito delle reti informatiche e della sicurezza informatica, una demilitarized zone o DMZ (in italiano zona demilitarizzata) è una sottorete fisica o logica che contiene ed espone dei servizi ad una rete esterna non ritenuta sicura, come ad esempio Internet. Lo scopo di una DMZ è di proteggere la rete LAN di un'organizzazione*

DDoS - *nel campo della sicurezza informatica, indica un malfunzionamento dovuto a un attacco informatico (abbreviato attacco DoS, lett. "attacco di diniego del servizio") in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un server web, fino a renderlo non più in grado di erogare il servizio ai client richiedente*

IDS - *Nella sicurezza informatica un sistema di rilevamento delle intrusioni o intrusion detection system (IDS) è un dispositivo software o hardware (o a volte la combinazione di entrambi, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.*

SIEM - (gestione delle informazioni e degli eventi sulla sicurezza) è una soluzione di sicurezza che aiuta le organizzazioni a riconoscere e affrontare potenziali minacce e vulnerabilità prima che possano interrompere le operazioni di business. (definizione IBM)