Università degli Studi di Padova

Corso di Laurea in Informatica

Applicazioni web vulnerabili: Implementazione di un Web Application Firewall con F5 per la mitigazione di attacchi informatici

Tesi di laurea triennale

Laureando:

Soranzo Mendez Andrea Jesus
2075539

Anno Accademco 2024-2025

Indice

1. Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage aziendale, con l'obiettivo di fornire una soluzione efficace per la protezione delle applicazioni web dagli attacchi informatici. La tesi affronta la sfida di analizzare i più noti vettori d'attacco e di comprendere come possano consentire a un utente malintenzionato di compromettere l'intera applicazione o di acquisire il possesso di informazioni sensibili degli utenti. La soluzione adottata consiste nell'implementazione di un ***Web Application Firewall (WAF)***$_g$, progettato per analizzare le richieste inviate dal client al server. Attraverso un set di regole predefinite, il ***WAF***$_g$ è in grado di identificare e bloccare le richieste sospette. Lo sviluppo del prodotto finale ha seguito diverse fasi: dall'analisi approfondita dell'applicazione web, con la creazione di una dettagliata lista di vulnerabilità, alla costruzione e definizione delle regole necessarie per mitigarle in maniera efficiente ed efficace, riducendo al minimo i falsi positivi. Questa esperienza ha offerto un contributo significativo nel campo della cyber-sicurezza, attraverso l'analisi e lo studio dei vari tipi di attacchi, e delle reti informatiche, tramite la creazione di una piccola rete dedicata a rendere più sicura la comunicazione client-server.

2. Struttura e organizzazione del documento

- Il **terzo capitolo** è dedicato alla presentazione dell'azienda presso cui ho avuto l'opportunità di svolgere il periodo di stage, contestualizzando l'ambiente lavorativo e illustrando le motivazioni che mi hanno spinto a scegliere questa specifica esperienza formativa.
- Il **quarto capitolo** descrive nel dettaglio i processi e le metodologie adottate per lo sviluppo del progetto. Include l'analisi dei requisiti e la pianificazione del lavoro.
- Il **quinto capitolo** presenta gli studi e delle ricerche condotte nella fase antecedente l'avvio del progetto. Include l'analisi delle tecnologie scelte e l'infrastruttura di rete adottata.
- Il **sesto capitolo** descrive il funzionamento generale dei firewall tradizionali e dei ***WAF***$_g$, evidenziandone le principali differenze operative e funzionali.
- Il **settimo capitolo** illustra gli attacchi studiati, fornendo una spiegazione sul loro meccanismo operativo e sulle potenziali implicazioni in termini di compromissione dell'applicazione.
- Il **ottavo capitolo** approfondisce la fase di creazione delle regole del ***WAF***$_g$ e delle strategie adottate per la loro ottimizzazione in termini di prestazioni e tempo di elaborazione.
- Il **nono capitolo** contiene le conclusioni personali e generali sull'esperienza svolta.

3. Lavoro in KIREY SRL

3.1. L' azienda

Kirey
Data Made Human

KIREY SRL è un system integrator con radici italiane che si è affermato come un attore globale nel guidare le imprese attraverso il loro percorso di trasformazione digitale. La sua missione principale consiste nell'accompagnare le organizzazioni verso la realizzazione di strutture data-driven, riconoscendo nei dati un asset strategico fondamentale per lo sviluppo del business. L'offerta di servizi di KIREY SRL è completa, con un filo conduttore incentrato sui dati e l'intelligenza artificiale, e si estende a settori cruciali quali Cloud, Software Development, Cybersecurity, Infrastructure & Automation, e Monitoring.
Nata come una piccola realtà locale, ha saputo espandersi a livello internazionale attraverso acquisizioni strategiche, consolidando la sua presenza in paesi come Spagna, Portogallo, Croazia, Romania, Bulgaria, Serbia, Albania, Messico e Kenya.
Oggi, KIREY SRL vanta un team di quasi 1100 dipendenti, servendo oltre 100 clienti in tutto il mondo con più di 10000 contratti attivi. Sebbene il suo target principale di mercato sia rivolto a soluzioni finanziarie per settori come assicurazioni e banche, l'azienda è estremamente attiva anche nel commercio al dettaglio, nella pubblica amministrazione e al mondo della moda, dimostrando una notevole versatilità e una profonda comprensione delle diverse esigenze settoriali.

KIREY SRL si posiziona come un partner strategico per le aziende che desiderano sfruttare al meglio il potenziale dei propri dati e dell'intelligenza artificiale per innovare e competere nel panorama digitale odierno.

3.2. La sede di Padova

Durante il mio periodo di tirocinio, ho avuto l'opportunità di immergermi nell'ambiente lavorativo di KIREY SRL presso la sede di Padova, frequentandola in presenza una volta a settimana. Questa esperienza mi ha permesso di approfondire il loro way of working, grazie anche al prezioso supporto del tutor aziendale, Marchetti Stefano, che mi ha garantito un'introduzione completa all'ambiente e alle dinamiche interne.
Le sede di Padova adotta un modello di lavoro ibrido, prediligendo il lavoro da remoto e dedicando un giorno a settimana all'incontro in presenza per un allineamento generale del team, a cui ho regolarmente partecipato, inoltre conta circa 15 dipendenti, a cui si aggiunge un numero variabile di stagisti, contribuendo a un ambiente dinamico e collaborativo.
Un aspetto particolarmente arricchente del tirocinio è stata la possibilità di collaborare con un altro stagista allo stesso progetto. Questa scelta aziendale mirava a valutare le nostre capacità di lavoro di gruppo e a favorire la collaborazione nell'approccio a un settore per noi nuovo. L'esperienza è stata fondamentale sia sul piano personale che professionale, permettendomi di ampliare la mia visione del mondo del lavoro e di approfondire conoscenze in ambiti dell'informatica precedentemente poco esplorati.
Ho avuto modo di osservare da vicino l'organizzazione interna di una realtà di grandi dimensioni come KIREY SRL e di comprenderne le modalità operative. La sede di Padova è strutturata in tre settori principali – Sicurezza, Dev-Ops e Data & AI – ciascuno con i propri sotto-team. Per gestire la complessità derivante dalla creazione e manutenzione di numerosi progetti e contratti, l'azienda fa leva su strumenti digitali

avanzati che assicurano una comunicazione rapida e una gestione efficiente delle attività.
In particolare, ***Microsoft Teams***$_g$ si è rivelato la piattaforma di comunicazione interna centrale. Consente una condivisione istantanea di informazioni, documenti e aggiornamenti sui progetti, fungendo anche da calendario del team. Questa integrazione tecnologica non solo ottimizza la comunicazione e la pianificazione, ma offre anche una visione chiara delle risorse disponibili, garantendo una gestione ottimale dei tempi e delle competenze.

3.3. Il progetto

3.3.1. Le necessità aziendali

L'azienda ha individuato nella protezione delle applicazioni web una priorità strategica, proponendo l'implementazione e la configurazione di un ***WAF***$_g$ ***F5***$_g$ che risolvesse le ***Open Worldwide Application Security Project (OWASP)***$_g$ top 10. L'obiettivo principale delle WASP Top 10 è aumentare la consapevolezza sui rischi di sicurezza delle applicazioni web e fornire una base comune per la protezione contro gli attacchi più diffusi. Non è un elenco esaustivo di tutte le vulnerabilità, ma si concentra su quelle che hanno il maggiore impatto potenziale e sono più frequentemente sfruttate. Questa scelta mira a fornire ai clienti un'opzione di sicurezza avanzata a livello applicativo e per la protezione delle API utilizzate. Di conseguenza, il progetto di tirocinio è stato specificamente concepito per formare risorse interne capaci di operare con questa tecnologia all'avanguardia, rispondendo all'esigenza aziendale di diversificare e rafforzare le proprie competenze in cybersecurity.

3.3.2. Modalità di lavoro

Il tirocinio ha avuto una durata complessiva di 300 ore, svolte prevalentemente in modalità da remoto, in linea con l'organizzazione aziendale. L'orario di lavoro, dal lunedì al venerdì, prevedeva otto ore giornaliere con un'ora di pausa pranzo. Per facilitare lo

svolgimento del progetto e lo studio, l'azienda ha fornito un computer portatile aziendale, indispensabile data la necessità di licenze a pagamento per i software utilizzati. Fin dal primo giorno, ho avuto accesso a un'ampia risorsa bibliografica e al corso ufficiale completo di ***F5***$_g$ [1], elementi che hanno costituito la base per il mio percorso di studio e apprendimento. Oltre a queste risorse, sono stato affiancato da due tutor: uno con un'orientamento più specifico sulla creazione di firewall e quello aziendale. Entrambi mi hanno seguito quotidianamente tramite stand-up meeting e si sono dimostrati costantemente disponibili per chiarire ogni dubbio. Questi confronti regolari sono stati cruciali per riadattare e scalare il progetto in base al tempo a disposizione e al nostro ritmo di apprendimento. Inoltre, durante il periodo di formazione, ho avuto l'opportunità di confrontarmi, tramite ***Microsoft Teams***$_g$, con uno specialista di ***F5***$_g$ per affrontare e risolvere le problematiche e le incertezze più complesse.

3.3.3. Il motivo della scelta

Ho optato per un tirocinio esterno con l'obiettivo di confrontarmi con la realtà del mondo del lavoro, diversa dall'ambiente universitario, e maturare una scelta più consapevole riguardo al prosieguo dei miei studi. Inoltre il settore della sicurezza informatica ha rappresentato per me, fino a tempi recenti, un'area poco chiara e raramente esaminata nel percorso accademico tradizionale. È stato solo a partire dal secondo anno universitario, grazie alla partecipazione a un corso facoltativo, che ho potuto acquisire una comprensione basilare e un'esperienza pratica delle sue dinamiche. Questa esposizione ha acceso in me un profondo interesse e la volontà di proseguire lo studio in questo ambito. Tuttavia, la sicurezza informatica si rivela essere una disciplina intrinsecamente complessa, e la ricerca di risorse di apprendimento efficaci, specialmente quelle gratuite o che offrano un affiancamento costante da parte di esperti, è ardua. Nonostante fossi a conoscenza dell'esistenza di percorsi di laurea magistrale interamente dedicati a questi argomenti, il mio intento era quello di iniziare a familiarizzare con le tematiche fondamentali. Questo mi ha permesso di gettare le basi per una possibile futura specializzazione e di comprendere

l'applicabilità pratica nel settore, verificando al contempo il mio effettivo interesse per un'eventuale mansione in quest'ambito.

Bibliografia e Sitografia

1. F5: Configuring F5 Advanced Web Application Firewall for Modern Applications. OnFulfillment F5 Network Ltd (2022).

Glossario

WAF : Firewall specializzato che protegge le applicazioni web da attacchi e traffico internet indesiderato (es. botnet, attacchi DoS), analizzando il traffico HTTP e HTTPS.. 2,3, 6.

Microsoft Teams : Piattaforma di collaborazione sviluppata da Microsoft basata su cloud che integra chat, riunioni video, chiamate, condivisione di file e applicazioni, progettata per facilitare la comunicazione e il lavoro di squadra all'interno delle organizzazioni.. 6, 7.

F5 : Azienda leader nella fornitura di soluzioni per la sicurezza delle applicazioni, l'ottimizzazione della rete e la gestione del traffico. I suoi prodotti principali, come i Big-IP, sono spesso utilizzati per il bilanciamento del carico, creazione di Web Application Firewall (WAF) e la gestione delle API.. 6, 7.

OWASP : Organizzazione no-profit che si dedica a migliorare la sicurezza del software.. 6.

Acronimi e abbreviazioni

WAF : Web Application Firewall. 2, 3, 6.

OWASP : Open Worldwide Application Security Project. 6.