Università degli Studi di Padova

Corso di Laurea in Informatica

Piano di Lavoro

Azienda:
KIREY Srl

Soranzo Mendez Andrea Jesus
2075539

06 maggio 2025

Indice

1. Contatti

Studente:

- Soranzo Mendez Andrea Jesus 2075539
  soranzoandrea.mj@gmail.com
  andreajesus.soranzomendez@studenti.unipd.it

Tutor aziendale:

- Stefano Marchetti
  stefano.marchetti@kireygroup.com

Azienda:

- KIREY Srl
  Corso Stati Uniti, 14/B, 35127 Padova PD
  HR@Kireygroup.com
  https://www.kireygroup.com/

2. Informazioni sull'azienda

Kirey è un system integrator che guida le aziende nel loro percorso di Digital Transformation, accompagnandole verso la realizzazione di organizzazioni data-driven. Facendo leva su una forte competenza in materia di Data & AI, Kirey riconosce nei dati un asset strategico per lo sviluppo del business, offrendo una gamma completa di servizi che hanno come filo conduttore i dati e l'intelligenza artificiale, e che coprono diversi settori tra cui Cloud, Software Development, Cybersecurity, Infrastructure & Automation e Monitoring.

3. Scopo dello stage

Il progetto mira all'implementazione e ottimizzazione di un Web Application Firewall (WAF) strategico per la protezione del perimetro applicativo web aziendale. Le fasi chiave del progetto includono:

- Analisi vulnerabilità e requisiti.
- Implementazione del WAF senza impatti operativi.
- Testing e ottimizzazione delle regole.
- Monitoraggio attacchi in tempo reale.

Il risultato atteso è un Web Application Firewall in grado di:

- Proteggere le applicazioni web aziendali da attacchi informatici come SQL injection, XSS, e DDoS.
- Garantire la continuità operativa riducendo i rischi di downtime dovuti ad attacchi informatici.
- Monitorare e analizzare il traffico web in tempo reale per identificare comportamenti sospetti.
- Rispettare gli standard di sicurezza e le normative, come il GDPR, proteggendo i dati sensibili degli utenti.

3.1. Contenuti formativi

Durante questo progetto di stage lo studente avrà occasione di approfondire le sue conoscenze nei seguenti ambiti:

- **Sicurezza ad attacchi:** SQL injection, XSS, DDoS e log analysis
- **Security testing:** Burp Suite, ambienti virtuali
- **Application Security, Traffic Management, Network Security:** F5
- **Versionamento:** git, GitHub
- **Frontend:** HTML
- **Backend:** Python

3.2. Strumenti e metodologia di lavoro

- **Linguaggi:** Python, HTML
- **IDE:** Visual Studio Code

- **Tecnologie:** Burp Suite, firewall, log analysis, F5, cloud (opzionale).
- **Modalità di svolgimento tirocinio:** Ibrida (presenza e smart working)
- **Modalità di interazione col tutor aziendale:** su richiesta dello studente o del tutor

3.3. Date di inizio e fine

- **Data inizio:** 19-05-2025
- **Data fine:** 10-07-2025

4. Pianificazione del lavoro

La pianificazione, in termini di quantità di ore di lavoro, sarà così distribuita:

Durata in ore	**Descrizione attività**
50	Analisi delle Esigenze • Studio approfondito delle applicazioni web esistenti per identificare le vulnerabilità • Definizione dei requisiti specifici per la protezione delle applicazioni
130	Progettazione e Implementazione • Esaminazione delle soluzioni disponibili (F5) e adattamento in modo che soddisfi le necessità dell'organizzazione. • Implementazione del WAF assicurandosi che non interferisca con il normale funzionamento delle applicazioni web. • Ricerca librerie e asset esistenti
50	Testing e Ottimizzazione • Testing e simulazioni di attacchi per verificare l'efficienza del WAF • Miglioramento delle regole di sicurezza per ridurre i falsi positivi e ottimizzare le performance
54	Monitoraggio e Manutenzione • Implementazione di sistemi di monitoraggio per rilevare e rispondere agli attacchi in tempo reale
16	Revisione della documentazione
Totale ore	
300	

4.1. Ripartizione delle attività suddivise per settimane

4.1.1. Prima Settimana

Durata in ore	Descrizione attività
20	• Incontro con il tutor aziendale e analisi dei requisiti del progetto • Configurazione degli strumenti di lavoro e formazione iniziale

4.1.2. Seconda Settimana

Durata in ore	Descrizione attività
40	• Analisi delle applicazione web e identificazione delle vulnerabilità principali • Studio delle funzionalità del Web Application Firewall • Inizio redazione del documento «analisi dei requisiti»

4.1.3. Terza Settimana

Durata in ore	Descrizione attività
40	• Progettazione e configurazione iniziale del Web Application Firewall • Personalizzazione delle regole di sicurezza • Inizio redazione del documento «specifica tecnica»

4.1.4. Quarta Settimana

Durata in ore	Descrizione attività
40	• Implementazione del Web Application Firewall e test di compatibilità con le applicazioni • Ottimizzazione delle regole

4.1.5. Quinta Settimana

Durata in ore	Descrizione attività
40	• Simulazione di attacchi per testare l'efficacia del Web Application Firewall • Analisi dei risultati e ottimizzazione delle configurazioni

4.1.6. Sesta Settimana

Durata in ore	Descrizione attività
40	• Configurazione di sistemi di monitoraggio per rilevare attacchi • Verifica della conformità agli standard di sicurezza

4.1.7. Settima Settimana

Durata in ore	Descrizione attività
40	• Manutenzione o ottimizzazione del Web Application Firewall • Fine redazione della documentazione

4.1.8. Ottava Settimana

Durata in ore	Descrizione attività
40	• Revisione finale e presentazione dei risultati • Consegna della documentazione e chiusura del progetto

5. Obiettivi

Si farà riferimento ai requisiti secondo le seguenti notazioni:

- **O** per i requisiti obbligatori, vincolanti in quanto obiettivo primario richiesto dal committente.
- **D** per i requisiti desiderabili, non vincolanti o strettamente necessari ma dal riconoscibile valore aggiunto.
- **F** per i requisiti facoltativi, rappresentanti valore aggiunto non strettamente competitivo.

Le sigle precedentemente indicate saranno seguite da un numero, identificativo univoco del requisito.

Si prevede lo svolgimento dei seguenti obiettivi:

Obbligatori	
O1	Studio e analisi delle vulnerabilità
O2	Studio delle possibili soluzioni adottabili
O3	Studio e ricerca di librerie e assets esistenti per l'implementazione
O4	Implementazione del WAF
O5	Testing e simulazioni di attacchi
O6	Miglioramento delle regole per ridurre i falsi positivi
O7	Redazione di una documentazione tecnica e metodologica per il progetto
Desiderabili	
D1	Valutare il monitoraggio del progresso formativo.
Facoltativi	
F1	Implementazione, gestione ed erogazione del WAF attraverso piattaforme cloud

6. Approvazione

Il presente piano di lavoro è stato approvato dai seguenti:

_____

Stefano Marchetti - Tutor aziendale