



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	2
2. Informazioni sull'azienda	2
3. Scopo dello stage	3
3.1. Strumenti e metodologia di lavoro	3
3.2. Date di inizio e fine	3
4. Pianificazione del lavoro	4
5. Obiettivi	5
6. Approvazione	6



1. Contatti

Studente:

- Soranzo Mendez Andrea Jesus 2075539
soranzoandrea.mj@gmail.com
andreajesus.soranzomendez@studenti.unipd.it
+39 328 447 7297

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. Strumenti e metodologia di lavoro

- **Linguaggio:** Python, HTML
- **IDE:** Visual Studio Code
- **Tecnologie:** Burp Suite, firewall, log analysis, F5, cloud (opzionale).

3.2. 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 <ul style="list-style-type: none">• Studio approfondito delle applicazioni web esistenti per identificare le vulnerabilità• Definizione dei requisiti specifici per la protezione delle applicazioni
130	Progettazione e Implementazione <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Implementazione di sistemi di monitoraggio per rilevare e rispondere agli attacchi in tempo reale
16	Revisione della documentazione
Totale ore	
300	



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:

A handwritten signature in blue ink, reading "Stefano Marchetti", positioned above a horizontal line.

Stefano Marchetti - Tutor aziendale

Zanella Marco - Tutor interno