



Tirocinio in ambito Application Security per sviluppo progetto di tesi

1. Chi stiamo cercando:

Laureando con skill acquisite (es. progetti universitari, progetti personali, ...) in programmazione orientata agli oggetti e conoscenza dei principali pattern architetturali (es: MVC), Linguaggi di programmazione (Java, Python), conoscenze base di software security. Obbligatorio un buon inglese. Gradita la pregressa conoscenza di OWASP e di concetti di Software Development Life Cycle.

2. Che cosa farai durante questo percorso e che contributo potrai dare:

Sarai coinvolto in un progetto di ricerca e sviluppo nell'ambito dell'automazione di test di sicurezza applicativa, tipicamente svolti in maniera manuale da un hacker. Il contributo sarà in particolare nella fase di coding degli automatismi.

3. Le competenze che acquisirai al termine del tirocinio:

Svilupperai una profonda conoscenza tecnica delle minacce OWASP e ad alcuni protocolli e standard di sicurezza, sia dal punto di vista di attacco che di verifica delle debolezze.

4. Perché scegliere noi?

Soft Strategy è una realtà quasi unica nel panorama italiano ed internazionale per l'automazione delle attività di ethical hacking, tipicamente appannaggio esclusivo di vendor di grande prestigio come Qualys, Tenable, Rapid7, ecc.

Chi siamo?

Azienda 100% italiana, **Soft Strategy** è specializzata nel settore del **management consulting e dei servizi Digital**, per la fornitura di servizi professionali alle imprese di medie e grandi dimensioni nei mercati di Telecomunicazioni, Energia, Trasporti e Pubblica Amministrazione.

Nata nel 2006, Soft Strategy è caratterizzata da un ambiente lavorativo giovane seppur con un elevato grado di seniority professionale.

Se interessato invia il tuo cv aggiornato a mmagagna@softstrategy.it indicando come oggetto "Tirocinio in ambito Application Security per sviluppo progetto di tesi – Università Tor Vergata"