|  |  |
| --- | --- |
| Cuerpo Académico / Individual | Individual |
| Nombre del Proyecto de Investigación / Vinculación / PLADEA-FEI / No registrado | No registrado |
| LGAC que alimenta |  |
| Línea de Investigación |  |
| Duración aproximada | 12 meses |
| Modalidad de Trabajo Recepcional | Monografía |
| Nombre del Trabajo Recepcional | Estado del arte de la seguridad de WebAssembly |
| Requisitos | Seguridad  Pruebas de penetración  Desarrollo de sistemas web |
| **Responsables del Trabajo Recepcional** | |
| Director | Dr. Héctor Xavier Limón Riaño |
| Codirector | M.C.C. Juan Carlos Pérez Arriaga |
| Alumnos participantes | Uno |
| **Descripción del Proyecto de Investigación** | |
| La seguridad en servicios de red es un tema de suma importancia cuyo impacto se ve reflejado en la reciente currícula de la ACM sobre ciberseguridad, destacándose la necesidad de formar a los nuevos profesionistas de esta área, puesto cuya demanda se encuentra y encontrará en creciente aumento en los próximos años.  Desde un punto de vista académico, debe buscarse la investigación y generación de conocimientos referentes a temas de impacto social actual como es el caso de ciberseguridad en todos los aspectos que conlleva, haciendo especial incapié en nuevos desarrollos y tendencias, para mantenerse al ritmo del avance de esta área en creciente y constante expansión. | |
| **Descripción del Trabajo Recepcional** | |
| WebAssembly es una tecnología emergente que está siendo adoptada por los navegadores web más importantes de la actualidad. WebAssembly intenta mejorar el rendimiento de código ejecutado del lado del cliente, al realizar un precompilado del mismo. WebAssembly utiliza el mismo sandbox de ejecución de JavaScript, por lo que cuenta con restricciones de seguridad similares. Dada la novedad de la tecnología, se continúan reforzando aspectos de seguridad, siendo que abre nuevos vectores de ataque a considerar en el futuro.  En este trabajo de investigación se plantea realizar una revisión sistemática multivocal, donde se cubran los siguientes aspectos de seguridad de WebAssembly:   * Arquitectura de seguridad * Posibles vectores de entrega de ataques * Vulnerabilidades y explotaciones conocidas * Prácticas de desarrollo orientadas a la seguridad | |
| **Resultados esperados** | |
| Trabajo escrito con investigación que de fundamento a la revisión sistemática realizada  Artículo con hallazgos | |
| **Bibliografía recomendada** | |
| Disselkoen, C., Renner, J., Watt, C., Garfinkel, T., Levy, A., & Stefan, D. (2019, June). Position Paper: Progressive Memory Safety for WebAssembly. In *Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy* (p. 4). ACM.  Brian McFadden, Tyler Lukasiewicz, Jeff Dileo, Justin Engler (2018, August). Security Chasms of WASM. NCC Group. | |

Xalapa, Ver., a fecha

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Nombre y firma del director del trabajo |  | Nombre y firma del co-director del trabajo |

|  |  |  |
| --- | --- | --- |
| Vo. Bo. |  | Vo. Bo. |
| Nombre y firma del Responsable del CA si aplica, en otro caso nombre y firma del Director de la Facultad |  | Nombre y firma del Coordinador de Academia Servicio Social y Practicas de Redes |