Monitor de Exposições de Segurança

Orientador: João Paulo Barraca (DETI) jpbarraca@ua.pt

Coorientador: André Zúquete (DETI) andre.zuquete@ua.pt

Colaboradores: Ricardo Martins (GCS) ricardo@ua.pt, Vitor Cunha (IT) vitorcunha@ua.pt

Número de alunos: 4 a 6

Curso: LEI e MIECT

Descrição:

Uma grande entidade como uma Universidade possui uma exposição muito relevante ao mundo exterior, através de páginas e máquinas que exportam serviços. No caso concreto da UA, o número de domínios públicos ultrapassa os 1500, podendo cada um potencialmente divulgar informação ou permitir a exploração de falhas no seu software. O comprometimento de um qualquer destes sistemas, mesmo que não tenha ele só por si muita relevância, pode levar a que o ataque seja escalado lateralmente para outros sistemas, com dados ou criticalidade superior. Existem serviços como este a nível comercial e mesmo open source, mas nem sempre de integração simples e certamente não adequados a um público mais generalista.

Torna-se assim vital a existência de sistemas que consigam monitorizar um conjunto alargado de sistemas, detetando e alertando para potenciais questões de segurança. Este alerta poderá ser realizado para os serviços da UA, mas poderá também contemplar os próprios donos do serviço. A enumeração deverá ser feita de forma automática, através dos registos de DNS e endereços alocados, assim como da utilização de ferramentas que possam identificar potenciais problemas. Devido à natureza de uma ferramenta desta natureza, considera-se que os testes a efetuar serão não destrutivos e focando-se em problemas comuns como os OWASP Top 10 para serviços Web.

Este trabalho foca-se exatamente no desenvolvimento desse sistema. Será composto por um sistema de enumeração, um sistema de análise e uma dashboard que permite avaliar a situação atual, ou interagir de forma mais simples com cada deteção. As questões de segurança serão resolvidas com recurso a ferramentas atuais do estado da arte, estando o trabalho focado na construção da plataforma em si e implementação da lógica funcional.

Embora o projeto aborde aspetos de segurança, em particular a exploração de vulnerabilidades, não são necessários conhecimentos específicos da área.