europass

Ana Vidal

Data de nascimento: 24/06/1999 | **Nacionalidade:** Portuguesa | **Sexo:** Feminino |

Número de telemóvel: (+351) 928113593 (Telemóvel) | **Endereço de email:** rvidal@outlook.pt |

Sítio Web: https://v1dal9.github.io/ | **LinkedIn:**

https://www.linkedin.com/in/ana-vidal-48b3b7230/ | **Github:** https://github.com/V1dal9 |

Endereço: Aveiro, aveiro, Portugal (Casa)

SOBRE MIM

Sou uma profissional dedicada e apaixonada pela área de Tecnologia da Informação, com uma sólida formação académica em Engenharia Informática. Concluí minha licenciatura no IPG e atualmente, frequento o mestrado em Cibersegurança na Universidade de Aveiro.

EDUCAÇÃO E FORMAÇÃO

02/07/2023 – ATUAL Aveiro, Portugal

MESTRADO EM CIBERSEGURANÇA Universidade de Aveiro

Sítio Web https://www.ua.pt/

12/09/2020 – 31/07/2023 Guarda, Portugal

LICENCIATURA EM ENGENHARIA INFORMÁTICA Instituto Politécnico da Guarda

Sítio Web https://politecnicoguarda.pt/

COMPETÊNCIAS LINGUÍSTICAS

Língua(s) materna(s): **PORTUGUÊS**

Outra(s) língua(s):

	COMPREENDER		FALAR		ESCRITA
	Compreensão oral	Leitura	Produção oral	Interação oral	
INGLÊS	B2	B2	B1	B1	B1

Níveis: A1 e A2: Utilizador de base; B1 e B2: Utilizador independente; C1 e C2: Utilizador avançado

COMPETÊNCIAS DIGITAIS

Python | C, C++ Programming | Java | Assembly | ASP .NET | JavaScript | HTML | CSS | Bootstrap | PL/SQL | Flask | SALESFORCE

EXPERIÊNCIA PROFISSIONAL

04/02/2024 – 04/08/2024 Aveiro, Portugal

ESTÁGIO DE PROGRAMADORA WEB TEKA

- Desenvolvi uma aplicação web CRM para Teka, utilizando a framework Vue.js e a base de dados MySQL;
- Implementei medidas de segurança em conformidade dado os CWE mais comuns, incluindo:
  - Controlo de Acesso Baseado em Funções (RBAC) para garantir a segurança e a privacidade dos dados do cliente;
  - Aplicação de soluções criptográficas na base de dados para proteger os dados contra acesso não autorizado;
  - Utilização de tokens JWT para autenticação e autorização de utilizadores, garantindo uma comunicação segura e fiável;

    - Entre outros.
- Realizei uma base de dados de raiz através do MySQL, onde implementei:
    - Implementei triggers BEFORE e AFTER no MySQL para automatizar processos específicos e garantir a integridade dos dados;
    - Procedures de inserção de dados para teste;
    - Entre outros;
- Colaborei com a equipa para garantir que todas as práticas de segurança fossem seguidas de acordo com os padrões mais recentes;
- Desenvolvi funcionalidades de fácil utilização e uma interface intuitiva para maximizar a eficiência e a usabilidade da aplicação.

PROJETOS

03/04/2024 – 19/06/2024

IdP (Identity Provider) para aplicação CRM

Autenticação e autorização são tópicos de extrema relevância a nível de cibersegurança, permitindo que o acesso é concedido à entidade certa. Neste projeto foi desenvolvido um IdP que suporta serviços, neste caso acesso a informação e a funcionalidades de um CRM, com diferentes graus de criticidade e aplica métodos de autenticação multifator, de forma dinâmica, de acordo com o perfil de risco.

Foram aprofundados o seguintes conceitos:
- Projeção arquitetural do projeto;
- Criação de perfis de utilização;
- Abordagem de autenticação com base no risco;
- Implementação do protocolo de autorização OAuth 2.0;
- Segurança a nível de desenvolvimento web;
- Integração de um único método de autenticação para três serviços distintos.

13/04/2024 – 05/06/2024

Análise de Ficheiro Debian Malicioso (Engenharia Reversa)

Realizei uma análise detalhada de um ficheiro Debian suspeito, utilizando técnicas de engenharia reversa para determinar se o ficheiro representava uma ameaça de malware.

Tecnologias Utilizadas:
- **Ferramentas de Análise:** Utilizei ferramentas especializadas como Ghidra, Strace, Ltrace, Veles e Binwalk para realizar a análise estática e dinâmica do ficheiro.;
- **Análise Estática:** Realizei verificações de integridade, comparação de assinaturas e análise de discrepâncias em ficheiros Debian utilizando comandos como *diff* e *hash;*
- **Análise Dinâmica**: Utilizei o Ghidra para analisar o ficheiro e entender o fluxo de dados e operações maliciosas, como a manipulação de buffers e operações XOR;
- **Análise Binária:** Com a ferramenta Veles, investiguei anomalias em ficheiros PDF, identificando *headers* suspeitos e conteúdo comprimido indicativo de manipulação ou dados maliciosos;
- **Script em C:** Desenvolvi scripts em C para descodificar conteúdos maliciosos embutidos no ficheiro PDF e obter bibliotecas partilhadas (.so) usadas pelo malware;
- **Identificação de Indicadores de Comprometimento:** Identifiquei várias atividades suspeitas, incluindo manipulação de memória, execução de código dinâmico e exploração de servidores Telnet para possíveis ataques DDoS.

Resultados Importantes:
- Identificação de um ficheiro Debian manipulado, com diferenças substanciais no conteúdo, assinatura e tamanho;
- Descoberta de operações suspeitas através de análise estática e dinâmica, sugerindo atividade maliciosa;
- Compreensão do funcionamento de uma botnet, incluindo inicialização de números aleatórios, manipulação de ficheiros do sistema, e comunicação via socket;
- A análise do ficheiro revelou funcionalidades típicas de malware, como operações de ofuscação e técnicas para evitar detecção por sistemas de segurança.

A análise demonstrou que o ficheiro Debian suspeito continha malware com capacidades de botnet e potencial para realizar ataques coordenados, comprometendo a segurança e integridade da rede.

15/01/2024 – 10/04/2024

Análise de uma aplicação Android - Engenharia Reversa

Foi realizado uma análise detalhada da aplicação Android "OLB", da **Câmara Municipal de Oliveira do Bairro**, utilizando técnicas de engenharia reversa para compreender sua estrutura, identificar vulnerabilidades e avaliar práticas de segurança.

Tecnologias Utilizadas:
- **JADX:** Para descompilação do código-fonte para análise estática;
- **Ghidra:** Para a análise do código fonte.

Metodologia:
- Revisão de documentação para compreensão da arquitetura e funcionalidades;
- Identificação e análise de elementos de segurança como autenticação, comunicação e persistência de dados.

Resultados Importantes:
1. **Permissões e Configurações**: Verificação das permissões requeridas e configurações do SDK no manifesto do Android;
2. **Estrutura da Aplicação:** Análise das atividades principais (*MainActivity*, *NotificationsActivity*, *SplashActivity*) e suas funcionalidades;
3. **Potenciais Vulnerabilidades:** Identificação de riscos como Injeção de Intenção, *Cross-Site Scripting* (XSS) e SQL *Injection;*
4. **Serviço de Mensagens *Firebase*:** Avaliação de métodos de *logging* e validação de dados de entrada;
5. **Base de Dados**: Análise da classe *GridDatabase* para gestão da informação.

10/10/2023 – 18/12/2023

Monitorização de Vulnerabilidades em Ambientes IoT

No âmbito da cadeira de Software Robusto, foi desenvolvido uma análise para uma aplicação de monitorização de dispositivos IoT, com base na metodologia ciclo de vida do desenvolvimento seguro (SDL).

Deste modo, foi abordado os seguintes tópicos:
- Treino e Consciencialização;
- Concepção do Projeto;
- Análise e Requisitos;
- Conceção Arquitetônica Detalhada;
- Implementação e Testes (análise estática e dinâmica);
- Lançamento, Distribuição e Suporte;

16/10/2023 – 08/12/2023

Sistema de deteção de intrusão usando Machine Learning

Neste projeto foi desenvolvido um **sistema de deteção de intrusão**, que consiste numa aplicação que exerce o papel de monitorizar tráfego de rede e procura por ameaças conhecidas ou atividade anómala, alertando as equipas de possíveis ameaças e riscos.

Nele foram aprofundados os seguintes conceitos:
- Tratamento de dados com fins de extrair informação relevante da rede a avaliar;
- Aplicação de abordagens de classificação binária (é ou não anómolo);
- Estudo de qual o melhor modelo de ML a utilizar usando "*Grid-Search*";
- Aplicação de abordagens de classificação multiclasse (categorização de ameaças);
- Conhecimento de ferramentas usadas no âmbito da inteligência artificial (pandas, numpy, sklearn, keras).

15/09/2023 – 28/11/2023

Modificação do algoritmo de geração de chaves RSA

Os pares de chaves RSA são geralmente gerados aleatoriamente, dificultando a reprodução do processo para descobrir a chave privada. Essas chaves precisam de proteção adequada, incluindo confidencialidade e controle de acesso. Alternativamente, a geração determinística de pares de chaves sempre gera o mesmo par a partir de um conjunto de parâmetros.

Neste projeto é feita esta abordagem, chamada **D-RSA**, utilizada em dispositivos TPM, que recriam chaves **RSA** a partir de um segredo fornecido pelo utilizador. Nele foram aprofundados os seguintes conceitos:
- Aprendizagem do processo de geração de chaves RSA;
- Implementação prática de geradores pseudoaleatórios para fins criptográficos;
- Implementação do problema usando bibliotecas criptográficas conhecidas (*openssl*, *biginteger*);
- Aquisição de conhecimento de vulnerabilidades presentes face à má implementação de algoritmos de geração de chaves e segredos criptográficos.

06/06/2023 – 26/07/2023

Desenvolvimento de uma Aplicação Web em PyCharm (Python)

Desenvolvi uma aplicação web que utiliza técnicas avançadas de análise de solo, incluindo cálculos de resistividade e seleção de geometria do material, para otimizar o planeamento de sistemas de terras. A aplicação web resultante oferece aos profissionais da área uma ferramenta eficaz para tomar decisões informadas sobre aterramentos elétricos.

Tecnologias Utilizadas:

- **Linguagem de Programação:** Python foi a linguagem de programação principal usada para o desenvolvimento do projeto.
- **Framework Web:** Flask, uma micro-framework web em Python, foi empregada para criar a aplicação web.
- **Bibliotecas Python:** Diversas bibliotecas Python foram utilizadas para tarefas como cálculos matemáticos, análise de dados e manipulação de fórmulas (NumPy, SciPy, SymPy e outras).
- **Sistema de Gerenciamento de Banco de Dados (SGBD):** Microsoft SQL Server, juntamente com o SQL Server Management Studio 19, foi usado para gerenciar o banco de dados e executar consultas SQL.
- **Cálculos Matemáticos:** Para realizar cálculos matemáticos e resolver equações, a biblioteca SymPy é mencionada.
- **Ambiente de Desenvolvimento Local:** Um servidor web local, foi utilizado para testar a aplicação durante o desenvolvimento.

22/11/2022 – 06/01/2023

Desenvolvimento de um jogo em Java 3D

No desenvolvimento deste jogo de xadrez, utilizei algumas tecnologias para criar uma experiência tridimensional envolvente e interativa para os jogadores. As principais tecnologias foram:

- **Linguagem de Programação Java:** O projeto foi desenvolvido principalmente em Java, uma linguagem de programação versátil e robusta amplamente usada no desenvolvimento de aplicativos e jogos;
- **Java 3D:** Para criar um ambiente tridimensional realista e renderizar peças de xadrez em um espaço 3D, aproveitei a tecnologia Java 3D.

08/05/2022 – 03/07/2022

Desenvolvimento de uma Aplicação Android em Android Studio (Kotlin)

Desenvolvi uma aplicação de gestão de viagens dedicada a tornar as férias em família uma experiência mais fácil e agradável. Este projeto envolveu a implementação de várias funcionalidades técnicas essenciais, tais como:

- **Linguagem de Programação:** Utilizei Kotlin, uma linguagem moderna e eficiente para o desenvolvimento Android;
- **Framework Android:** Fiz uso do Android Jetpack, um conjunto de bibliotecas e ferramentas recomendadas para o desenvolvimento Android;
- **Gestão de Fragments:** Utilizei Fragmentos Android para criar interfaces de utilizador modulares e reutilizáveis;
- **Android XML:** Para a definição de layouts de ecrã e recursos visuais;

27/11/2021 – 10/02/2022

Desenvolvimento de uma Base de Dados Relacional (PL/SQL)

No âmbito do meu envolvimento num projeto de gestão de residências, desempenhei um papel fundamental na criação e administração de uma base de dados relacional. Utilizei as tecnologias SQL e PL/SQL para desenvolver a estrutura da base de dados, criando tabelas, definindo restrições e garantindo a integridade dos dados.

Esta base de dados foi concebida para armazenar informações detalhadas sobre materiais, requisições, residências, quartos e estudantes, possibilitando uma gestão eficiente e precisa dos recursos e alocações.

05/10/2021 – 04/02/2022

Projeto de um Robô Bombeiro (C++)

Desenvolvi um robô bombeiro capaz de navegar em labirintos em busca de incêndios e, em caso de deteção de uma chama, acionar uma ventoinha para a extinguir. O objetivo principal era criar uma solução automatizada para situações de emergência, aumentando a segurança e a eficácia na resposta a incêndios.

Tecnologias Utilizadas:

- **Arduino:** Utilizei a plataforma Arduino para controlar o hardware do robô, incluindo motores, sensores e atuadores;
- **Sensores de Distância:** Implementei sensores de distância ultrassónicos (sonares) para permitir a navegação autónoma do robô, evitando obstáculos no labirinto;
- **Sensor de Chama:** Utilizei um sensor de chama para detetar a presença de incêndios no ambiente;
- **Motores:** O projeto incorporou motores para a locomoção do robô e uma ventoinha que era ativada automaticamente em resposta à deteção de chamas;

- **Display OLED:** Utilizei um display OLED para exibir informações importantes, como o estado do robô e dados de navegação;
- **Linguagem de Programação C++:** Programei o Arduino usando C++ para implementar a lógica de controlo e as operações de deteção de chamas;

16/10/2021 – 10/12/2021

Projeto Demola - Gender Violation at Work

O projeto teve como tema violação de gênero no trabalho e este irá ser sempre um desafio, não tem fim e será uma luta constante, pois não se resume apenas em alterar mentes atuais, mas também futuras ou até mesmo passadas.