Dilip Nair

Software Developer

Address Palakkad, Kerala 678551

Phone +91 8136980540

E-mail dilipn6@gmail.com

LinkedIn

https://www.linkedin.com/in/dilip-c-nair/

My main expertise is in Developing softwares using C#. I have more than 2 Years of experience in .NET development, I have developed and deployed a Web Application in ASP.NET MVC (HRMS) and a Cyber security-based desktop application in WPF (Host-based IDS). Being a Post Graduate in Cyber Security I also have 2 years of experience learning and researching in the field of Cyber security independently (mainly in Reverse Engineering Binaries). My experience in Cyber Security makes me a better software engineer.

Skills

- **Languages :** C#,Javascript, C, C++, Java
- **Full Stack Development :** ASP.NET MVC (.NET 8)
- **Front End :** HTML, CSS, Bootstrap, JQuerry, Ajax, Razor, Blazor, API Integration, React
- **Backend :** ASP.NET Web API, REST APIs, JWT, MSSQL, PostgreSQL, Microservices architecture
- **Database Integration :** ADO.NET, Entity Framework
- **Authentication and Authorization :** Identity Framework
- **Cloud :**Azure, Azure App, Azure SQL, Azure Key Vault, Azure CosmosDB, CI/CD Pipeline using Github Actions
- **Testing :** WebAPI Testing using Swagger and Postman, C# Unit testing using NUnit, xUnit
- **Desktop :** XAML, WPF, WINUI3, MVVM
- **Miscellaneous :** Native WinAPI and COM API development, x86, x64, Reverse Engineering Binaries

Experience

Nov 2023 - Current

Full Stack Web Development

Independent, Palakkad

Developed a Web App HRMS (Human Resource Management System) in ASP.NET MVC and Deployed it to Azure using CI/CD Pipeline

Admin Functionalities and Manager Functionalities :

Roles (Create, Read, Update, Delete), Assign roles to users, Remove users from roles, Role based access, Setting department, salary, designation, office location of employees

User Functionalities:

Signup, Signin, Signout, Basic Details (Add, edit, remove), Address (Add, edit, remove), Profile Picture (Add, edit, remove), Notification for any profile

changes, View Profile, Change Password, Reset password using email, Delete Account, Adding experience and summary
Also developed a separate WebAPI version which include the above functionalities

Feb 2021 - Oct 2023

Security Research

Independent (2+ Years), Palakkad

- Procuring and Analyzing Threats, mainly windows malwares.
- Reverse Engineering windows malwares to understand the malicious behavior.
- Linux, Network Security, Cryptography
- Penetration Testing, Cyber security concepts
- Operating Systems
- Native WinAPI programming using Visual C/C++

Sep 2017 - Feb 2018

Programmer Analyst (DR Testing)

Cognizant (5 Months), Chennai, India

I was part of a DR testing team (Disaster recovery testing), where we simulate a disaster and test how an application responds to it. Clients across the world came to us to check how resilient are their applications against any disaster. So we test it and then document the whole process and submit the report to the client.

Jun 2016 - Sep 2017

Cyber Security Software Development (Desktop)

Independent (1+ Years), Ahmedabad

- Developed a Host based Intrusion Detection System, a desktop application for Windows OS in .NET.
- It monitors the processes and files in the background.
  The admin keep restrictions on the processes and files in the system.
- The application will monitor for the violation of these restrictions and will trigger an alert in the system if any violation occurs.
- There are some experimental features like Process Port Mapper, Services Monitoring, User Input Monitoring (Keystroke logger, mouse clicks and coordinates logger), packet
  capturing (both ethernet and wifi) and Alerts mailing.
- Also there is an authentication mechanism with MSSQL server.

Links - Work Portfolio

HRMS - Full Stack Project in ASP.NET MVC (Presentation)
https://www.canva.com/design/DAGF7XeidTg/ZQSxIoWIL9DBgCwtxTqjQA/view

Cyber Security based Desktop Application (Presentation) :
https://www.canva.com/design/DAGJBeEecwg/sy9nFn4hHmFd5esmWP1AZg/view

HRMS - WebAPI Project (Presentation)
https://www.canva.com/design/DAGGIeEJSc0/SeRQVy88N8R6ONK-ddUnvg/view

Source code for Desktop Application (Github repo) :
https://github.com/DilipCNair/RBS

Let me know if you want a live demo for all these projects

Education

Jun 2015 - May 2017 **M.Tech: Information And Network Security**
Nirma University - Ahmedabad, GJ

Jun 2010 - May 2014 **B.Tech: Computer Science And Engineering**
University of Calicut - Kozhikode, KL

Malware Analysis Skills

- Procuring and Analyzing Malware
- Static and Dynamic Analysis of Malware in a Sandboxed Environment (Windows VM and REMNUX)
- PE and ELF File Format, Metadata Analysis, Strings Analysis (ASCII and Unicode strings)
- Analyzing Malicious EXEs as well as DLLs
- Entropy checking in Malware
- Looking for Encoded strings and Cryptographic Signatures
- Unpacking Malware using xdbg,
- Dumping unpacked code from xdbg
- Fixing the dumped code
- Debugging and Monitoring malware execution using IDA
- Signature building using Yara
- Reversing native Win APIs and Crypto APIs
- Operating System Internals and Kali Linux
- Also Familiar with ARM based architecture

Reversing Engineering Skills

- Reversing Malware using IDA,
- Binary patching, binary debugging, reversing jumps
- Looking at the Import table, Export table, Sections, Functions and Strings
- Locating main, renaming functions, variables, labels and adding suitable comments wherever necessary, x86-64 Assembly Language
- Finding Code and Data Xrefs, analyzing the logic flow using Xref graphs from and to a function
- Backtracking from suspicious strings or APIs to the beginning of the Logic (i.e. main)
- Finding dynamically resolved APIs, function calling conventions like Standard Calls and Fast Calls,

- Follow string and register operations,
- Watching a memory location for any change in real time
- Traversing through the API chain to understand the functionalities

Penetration Testing (Skill level - Beginner)

- Network and Open Ports Enumeration
- Looking for Vulnerabilities and finding exploits against vulnerabilities
- Exploiting using public exploits , exploitdb and metasploit
- Web hacking using burpsuite, exploiting vulnerabilities like File Inclusion and Upload, Command Injection etc
- Catching reverse shells using netcat and Socket Programming

Cyber Security Tools

For Reversing Malwares:
File, Trid, DetectItEasy, CFF Explorer, PEiD, PE Studio, PE bear, Resource Hacker, IDA, signsrch, pecli, pehash, peres, xdbg, processhacker, procmon, regshot, Inetsim, fakedns, FakeNet-NG, wireshark, procdot etc...

Penetration Testing Tools:
metasploit, exploitdb, msfvenom, nikto, wpscan, nmap, netcat, burpsuite, nasm, gdb, objdump, strace, ltrace etc...

Miscellaneous

- Configuring CISCO routers and switches
- Setting up Access Lists, Firewall, AAA server, Zone based policy firewalls, DMZ and VLAN
- Cisco Packet Tracer and GNS3, TCP/IP Protocol stack
- Public key and Private Key Cryptography for Confidentiality
- Hashing algorithms for Integrity
- Digital Signature and Digital Certificates for Authentication