

Cybersecurity, Bug Hunting & Android Skills Reference

Anthropic Cybersecurity Skills (mukul975), Bug Hunting (m4vic), and Official Google Android Skills (android/skills) • සිංහල සහ ඉංග්‍රීසි විධාන නාමාවලිය

Part 1: Bug Bounty Hunting & Penetration Testing Framework (m4vic/bug-hunting)

/bug-hunting

FRAMEWORK

Bug Bounty Hunting & Penetration Testing Framework Router

Bug Bounty සහ Penetration Testing මඟපෙන්වීම් රාමුව

Systematic penetration testing methodology across 7 security domains: Web endpoints, APIs (REST/GraphQL), iOS/Android mobile apps, Cloud/IAM identity, AI/LLM security, and Recon.

Web, REST/GraphQL APIs, Mobile Apps, Cloud Identity සහ AI/LLM ආරක්ෂාව විධිමත්ව පරීක්ෂා කර vulnerabilities සෙවීමේ සම්පූර්ණ bug hunting රාමුව.

/bug-hunting web recon and business logic flaw discovery on target scope

Part 2: Anthropic Cybersecurity Skills Library (mukul975) - Core Suite

/performing-csrf-attack-simulation

OWASP

CSRF Attack Simulation & Verification

Cross-Site Request Forgery (CSRF) පරීක්ෂාව

Test web applications for Cross-Site Request Forgery vulnerabilities by crafting forged requests that exploit authenticated user sessions.

Web app එකක form submissions සහ cookies වල anti-CSRF tokens සහ SameSite ආරක්ෂාව පරීක්ෂා කිරීම.

/performing-csrf-attack-simulation analyze password change endpoint for missing anti-CSRF tokens

/performing-memory-forensics-with-volatility3

FORENSICS

Memory Forensics with Volatility 3

Volatility 3 මගින් Memory Forensics විශ්ලේෂණය

Analyze volatile memory dumps (RAM) using Volatility 3 plugins to detect rootkits, injected code, hidden processes, and active network connections.

පරිගණකයක RAM memory dump එකක් Volatility 3 හරහා පරීක්ෂා කර සැඟවුණු malware, injected code සහ අස්වාභාවික processes හඳුනාගැනීම.

```
/performing-memory-forensics-with-volatility3 analyze memory.dmp for hidden injected threads
```

/performing-kerberoasting-attack

AD-SECURITY

Active Directory Kerberoasting Audit

Active Directory Kerberos ආරක්ෂක විගණනය

Audit Active Directory service principal names (SPNs) for weak encryption and vulnerable service accounts susceptible to Kerberoasting ticket cracking.

Active Directory ජාලයක Service Principal Names (SPN) පරීක්ෂා කර දුර්වල මුරපද සහිත service accounts වල Kerberos ප්‍රවේශ පත්‍ර ආරක්ෂාව තහවුරු කිරීම.

```
/performing-kerberoasting-attack audit domain SPNs for RC4 ticket encryption and weak passwords
```

/performing-kubernetes-penetration-testing

CLOUD-SEC

Kubernetes Cluster Penetration Testing

Kubernetes Cluster Penetration Testing

Assess Kubernetes clusters for misconfigurations, overly permissive RBAC roles, exposed kubelet/API server endpoints, and insecure pod policies.

Kubernetes clusters වල RBAC අවසර, Kubelet endpoints, pod security standards සහ container breakout අවදානම් පරීක්ෂා කිරීම.

```
/performing-kubernetes-penetration-testing evaluate cluster RBAC permissions and pod security admission
```

/performing-dynamic-analysis-of-android-app

MOBILE-SEC

Android App Dynamic Security Analysis

Android App Dynamic Security විශ්ලේෂණය

Conduct runtime dynamic security analysis of Android APKs: intercept network traffic, hook functions with Frida, bypass SSL pinning, and inspect local storage.

Android App එකක් ධාවනය වන අතරතුර එහි network traffic, SSL pinning, Frida hooks සහ SQLite data storage වල ආරක්ෂාව පරීක්ෂා කිරීම.

`/performing-dynamic-analysis-of-android-app inspect package com.example.app for token leaks in shared_prefs`

/performing-graphql-security-assessment

API-SEC

GraphQL API Security Assessment

GraphQL API ආරක්ෂණ තක්සේරුව

Assess GraphQL endpoints for schema introspection leakage, query depth/complexity denial of service, object-level authorization (BOLA), and batching attacks.

GraphQL APIs වල introspection leaks, query depth DoS, BOLA/IDOR අවදානම් සහ field-level authorization ආරක්ෂාව පරීක්ෂා කිරීම.

`/performing-graphql-security-assessment audit https://api.target.com/graphql for depth limit enforcement`

Part 3: Official Google Android Skills (android/skills)

/jetpack-compose-performance

OFFICIAL

Jetpack Compose Performance & Recomposition

Jetpack Compose Performance ප්‍රශස්තකරණය

Diagnose and optimize Android Jetpack Compose UI code. Minimize recomposition overhead, resolve state derivation issues, and eliminate UI lag and dropped frames.

Android Jetpack Compose UI වල අනවශ්‍ය recomposition අවම කිරීම, derivedStateOf නිවැරදිව භාවිතය සහ UI lag/dropped frames වළක්වා ගැනීම.

`/jetpack-compose-performance optimize LazyColumn feed screen with heavy state updates`

/agp-9-upgrade**OFFICIAL****Android Gradle Plugin 9.0 Upgrade**

Android Gradle Plugin 9.0 යාවත්කාලීන කිරීම

Automate migration to Android Gradle Plugin 9.0, resolving deprecated APIs, buildSrc changes, Gradle configuration cache compatibility, and Kotlin DSL updates.

Android ව්‍යාපෘතියක් Android Gradle Plugin 9.0 (AGP) වෙත පහසුවෙන් upgrade කිරීම සහ deprecated build APIs නිවැරදි කිරීම.

`/agp-9-upgrade migrate app build configuration to AGP 9.0`

/adaptive**OFFICIAL****Adaptive Compose Layouts (Foldables & Tablets)**

Adaptive Layouts (Foldables සහ Tablets සඳහා)

Build adaptive Jetpack Compose layouts for Android that seamlessly scale across phones, foldables, tablets, and desktop ChromeOS with window size classes.

Smartphones, Foldables, Tablets සහ ChromeOS සඳහා එකසේ ගැළපෙන Adaptive Compose Layouts (List-Detail, Supporting Pane) සකස් කිරීම.

`/adaptive implement list-detail pane layout for tablet and phone form factors`

/camerax**OFFICIAL****Modern Android CameraX Integration**

Android CameraX කැමරා ඒකාබද්ධකර

Integrate Android CameraX for high-reliability photo capture, video recording, image analysis (ML Kit), and lifecycle-aware camera management.

Android යෙදුමකට photo capture, video recording සහ QR/Barcode image analysis සඳහා CameraX පහසුවෙන් එක් කිරීම.

`/camerax build a lifecycle-aware camera preview screen with photo capture`

/litert-runtime**OFFICIAL****LiteRT (TFLite) On-Device AI Runtime**

LiteRT On-Device AI ධාවක පද්ධතිය

Deploy and optimize machine learning models on Android using Google LiteRT (formerly TensorFlow Lite) with NPU, GPU, and CPU hardware acceleration.

Android උපාංගය මතම (On-Device) ක්‍රියාත්මක වන AI/ML models, LiteRT සහ GPU/NPU acceleration මඟින් වේගවත්ව ධාවනය කිරීම.

`/litert-runtime integrate quantized object detection model with GPU delegate`

[/ml-kit-genai-prompt-api](#)

OFFICIAL

On-Device GenAI Prompt API (Gemini Nano)

On-Device Gemini Nano Prompt API

Harness on-device Generative AI with Google's Prompt API backed by Gemini Nano: summarize text, smart reply, and extract entities with zero latency and complete privacy.

Android දුරකථනයේම ඇති Gemini Nano AI model එක Prompt API හරහා භාවිත කරමින් text summarization සහ smart replies සකස් කිරීම.

[/ml-kit-genai-prompt-api build on-device note summarization using Gemini Nano](#)[/android-intent-security](#)

OFFICIAL

Android Intent & Deep Link Security

Android Intent සහ Deep Link ආරක්ෂණ විගණනය

Audit Android components for Intent redirection, unauthorized component exposure, implicit intent hijacking, and unvalidated deep link vulnerabilities.

Android App එකේ Activities, Broadcast Receivers සහ Deep Links අනවශ්‍ය ලෙස පිටතට නිරාවරණය වීම (Exported components) සහ Intent hijacking වැළැක්වීම.

[/android-intent-security audit exported activities and custom URI scheme deep links](#)[/testing-setup](#)

OFFICIAL

Android Testing Setup & Best Practices

Android Automated Testing පද්ධතිය සැකසීම

Establish a modern, robust Android automated testing suite: Compose UI tests, ViewModel unit tests, Coroutines/Turbine testing, and Mockito/MockK mocking.

Jetpack Compose UI tests, Coroutines Turbine tests සහ ViewModel unit tests සඳහා සම්පූර්ණ Android automated testing setup එක සකස් කිරීම.

[/testing-setup configure Compose test rule and MockK test suite for ViewModel](#)