# BAB V
# PENUTUP

## 5.1 Kesimpulan

Kesimpulan yang dapat diambil setelah menyelesaikan penelitian berupa dapat dianalisa serangan phishing yang dikombinasikan dengan aplikasi yang mengunakan WebView sistem didalamnya dengan metode reverse engineering.

Adapun yang didapat dari reverse engineering menggunakan tool d2jar dan Apktool adalah aplikasi dapat diunpackage, didecompile dan dilihat service, string ataupun sumber kode yang digunakan bahkan alamat website yang berada dalam aplikasi yakni website website4061950.nicepage.io.

Teknik serangan ini menjadi teknik baru yang kemudian hari dapat dilakukan dengan masif oleh penyerang untuk mendapatkan kridensial seseorang. Hasil dari reverse engineering yang sudah dilakukan dapat menemukan file manifest yang berisi akses permisi dan sumber code yang digunakan untuk menunjang fungsi aplikasi KredivoReward tersebut. Sumber code yang dapat dianalisa bahkan direka ulang.

## 5.2 Saran

Penulis berharap semoga apa yang penulis sajikan dapat memberikan manfaat bagi penulis dan khususnya untuk para pembaca, serta seluruh pengguna smartphone.

Penulis menyadari masih terdapat banyak kekurangan pada penelitian ini sehingga penulis memberikan saran yang membangun dalam melakukan penelitian selanjutnya sebagai berikut:

1. Menemukan langkah yang lebih efektif dalam menemukan phising yang memanfaatkan class WebView.
2. Meningkatkan maupun menemukan cara baru yang efektifitas dalam melakukan reverse engineering pada phising WebView.

3. Menemukan metode reverse engineering phising WebView pada aplikasi android agar bisa dilakukkan secara otomatis.
4. Menggunakan aplikasi yang resmi dan legal agar terhindar dari serangan phising.