BAB V
PENUTUP

5.1 Kesimpulan

Secara dasar metode serangan WeVPAM mengkombinasikan website phishing dengan WebView pada aplikasi yang dikembangkan. Website yang telah dikombinasikan dengan system WebView mampu untuk menyembunyikan alamat asli website dan protocol internet yang digunakan sehinga korban tidak akan menyadari website yang sedang diakses merupakan sebuah website phishing. Metode serangan ini terbilang metode baru, hinga memungkinkan para pengguna tidak menyadari potensi bahaya ini.

Selain itu pemanfaatkan kombinasi website dengan system WebView pada aplikasi dapat menjadi hal yang semakin berbahaya apabila threat actor membuat fungsi *fraud all* data dari smartphone korban dengan memanfaatkan akses permisi seperti *Contact, Storage, Log Phone, Internet, Camera, GPS* dan yang lainnya.

Terpaku pada system dan metode yang komplit dan arsitektur yang besar serta inovatif dan komplek mungkin terlihat baik dalam ranah cybersecurity, tetapi sering kali melupakan hal yang sangat simple dan sederhana merupakan hal yang sering dilakukan dan dengan adanya penelitian ini diharap dapat untuk mengedukasi dan berupaya meningatkan bahwa hal-hal yang sederhana dalam ranah cybersecurity dapat berbahaya khususnya untuk para pengguna dan para praktisi professional maupun akademis.

5.2 Saran

Berikut ini adalah saran yang dapat dikemukakan diantaranya:

1. Gunakan aplikasi resmi dan legal serta terdata pada lembaga yang sudah memiliki izin
2. Tidak menggunakan aplikasi bajakan atau cloning.
3. Melakukan screening aplikasi apabila didapat dari sumber tidak dipercaya
4. Memastikan fungsi class website yang ditampilan melalui WebView berada pada satu tema pembahasaan dengan aplikasi.