**NOTA DINAS**

|  |  |  |
| --- | --- | --- |
| Yth. | : |  |
| Dari | : | Direktur Pemantauan, Evaluasi, dan Pengendalian Pembangunan Daerah |
| Perihal | : | Penyampaian Laporan Evaluasi Sistem Keamanan Aplikasi |
| Tanggal | : | 25 Maret 2024 |

Sehubungan dengan telah dilaksanakannya *assessment* terhadap keamanan sistem aplikasi oleh Pusdatinrenbang pada hari pada Selasa, 19 maret 2024, bersama ini kami sampaikan poin-poin laporan sebagai berikut:

1. Pertemuan dibuka oleh Bapak Dr. Agung Indrajit, ST, M.Sc selaku kepala Pusat Data dan Informasi Perencanaan Pembangunan yang menyampaikan tujuan pertemuan yaitu guna melakukan koordinasi dan bimbingan teknis aplikasi sebagai upaya dalam meningkatkan keamanan informasi.
2. Paparan disampaikan oleh Bapak Mirza, S.Kom, MAIR, MPA diantaranya menyampaikan beberapa poin sebagai berikut:
   1. Adapun beberapa dasar hukum dalam keamanan pengembangan aplikasi meliputi PP Nomor 95 tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik, Peraturan Menteri PPN/Kepala Badan Perencanaan Pembangunan Nasional Republik Indonesia Nomor 11 Tahun 2023 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik, Surat Edaran Sesmen/Sestama Kementerian PPN/Bappenas Nomor 02 Tahun 2022 Tentang Pembangunan Aplikasi Dan Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, Kebijakan Keamanan Informasi Kementerian PPN/Bappenas.
   2. Merujuk pada teknik – teknik dalam pengembangan perangkat lunak yang dirancang untuk menghasilkan aplikasi yang tahan terhadap berbagai jenis serangan keamanan, maka di perlukan setidaknya 3 teknik yang digunakan yaitu *input validation*, *authentication and authorization*, dan *data encryption.*
   3. *Input validation* bertujuan untuk memastikan input yang diterima oleh aplikasi diuji dan divalidasi dengan benar untuk mencegah serangan seperti SQL injection, Cross-Site Scripting (XSS), dan sejenisnya.
   4. *authentication and authorization* bertujuan untuk memastikan bahwa proses otentikasi (verifikasi identitas) dan otorisasi (pengendalian hak akses) diimplementasikan dengan benar dan kuat.
   5. *data encryption* bertujuan untuk mengamankan data selama transmisi dan penyimpanan data.
   6. Untuk meningkatkan keamanan data pribadi, hal yang harus diperhatikan jika aplikasi menggunakan kata sandi yaitu jumlah karakter kata sandi minimal 8 (delapan karakter), tidak berasal dari karakter yang mudah ditebak, dan menggunakan kombinasi huruf besar, huruf kecil, angka, dan sedapat mungkin menggunakan tanda baca dan karakter khusus.
   7. Adapun alur pengujian keamanan aplikasi (VA) yang dilakukan sebagai berikut:
      * **Internal/ External Request** (Unit Kerja melakukan permintaan berupa ND atau melalui arahan dari Koordinator tim Keamanan Informasi seperti VA rutin)
      * **Data Collection/Backup Apps** (Dilakukan pendataan aplikasi yang akan diuji dan menyiapkan kebutuhan pengujian serta meminta pemilik aplikasi untuk melakukan backup jika diperlukan)
      * **Testing** (Melakukan pengujian keamanan (VA) pada aplikasi yang diminta menggunakan scanning tools)
      * **Analysis** (Melakukan analisis dan hasil pengujian keamanan (VA) pada aplikasi menggunakan scanning tools)
      * **Reporting** (Membuat laporan analisis dari hasil pengujian keamanan aplikasi menggunakan scanning tools)
      * **Coordination** (Koordinasi dengan pemilik aplikasi terkait hasil pengujian keamanan (VA) pada aplikasi yang sudah di analisis)
      * **Assistance** (Pendampingan perbaikan hasil pengujian keamanan)
      * **Re-Testing** (Melakukan pengujian ulang setelah aplikasi dilakukan perbaikan dari hasil pengujian sebelumnya)
      * **Final Report** (Membuat laporan akhir dari hasil perbaikan keamanan aplikasi)
3. Saat ini alur pengujian keamanan aplikasi (VA) sudah pada tahap *Assistance.* Pusdatinrenbang menyediakan asistensi dalam keamanan aplikasi di Gedung Bappenas Lantai 3A Jl. H.R. Rasuna Said Kuningan
4. Pusdatinrenbang bekerjasama dengan BSSN untuk melakukan pentest pada beberapa aplikasi kementerian PPN/Bappenas
5. Jika tidak ada perbaikan selama 1 minggu setelah asistensi, maka Pusdatinrenbang akan menjalankan prosedur perlindungan keamanan aplikasi dengan menonaktifkan domain.
6. Direktorat PEPPD dijadwalkan asistensi pada minggu ke 4 bulan maret.
7. Beberapa catatan penting dalam diskusi sebagai berikut:
   1. Pengujian aplikasi dapat melalui *repository* GIT yang disediakan bappenas atau melalui URL.
   2. Aplikasi yang dikembangkan diusahakan tidak diletakan pada subfolder aplikasi. Disarankan menggunakan subdomain untuk memudahkan pengujian.
   3. Pusdatinrenbang sedang mengkaji terkait pengembangan aplikasi yang menggunakan sistematika devops (CI/CD)
   4. Aplikasi dihimbau untuk bermigrasi dari arsitektur *monolithic* ke arsitektur *microservices*.

Demikian kami sampaikan, atas perhatiannya kami ucapkan terima kasih.