BIBD 3.9.14 - Enhancement #22196

[CSMS 15993][Android][Device Binding Pentest] Device Binding Login Bypass

13 June 2025 10:27 AM - Feerman Yusoff

Status:	Resolved	**Start date:**	11 June 2025
Priority:	High	**Due date:**	
Assignee:	Feerman Yusoff	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Device Binding Updated flow:
1. Backend generates an RSA key pair (public/private) and pass the public key value to FE through loginInternetPin API response new tag param eg: alias.
2. Frontend retrieves the public key from the backend from loginInternetPin API response.
3. Frontend generates a random AES key (for that session or request).
4. Frontend encrypt device ID|transactionDate (or any other unique values) using AES key.
5. Frontend encrypt AES key using RSA public key.
6. Frontend send encrypted device ID and encrypted AES key to backend.
7. Backend decrypt AES key using RSA private key.
8. Backend decrypt device ID using the decrypted AES key and omit the symbol | and transactionDate values.
9. Backend compare the decrypted and omitted value with MIB DB.

History

#1 - 13 June 2025 11:54 AM - Abdul Halim Baharom

- Status changed from New to Resolved

- Assignee changed from Abdul Halim Baharom to Feerman Yusoff

- % Done changed from 0 to 100

Done