

BANK KALTENG - Bug #3348

Update Attendance Menu Menggunakan Foto + Package Fixing Pantest

01/16/2025 03:28 PM - shofwan shiddiq

Status:	Closed	Start date:	01/16/2025
Priority:	Normal	Due date:	
Assignee:	shofwan shiddiq	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:		Spent time:	0.00 hour

Description

Dear All

1. Untuk BKT Dev sudah di deploy menu attendance terbaru (yg bisa menggunakan foto) dan tidak menggunakan async
2. Update Package Untuk Fixing beberapa poin Pantest pada aplikasi mobile

No	Deskripsi	Lokasi	HRIS Mobile App Android	HRIS Mobile App IOS	BKT Mobile Apps Android
Black Box 1					
1	Attacker menemukan celah keamanan SQL Injection pada API menu Login (parameter Username) Aplikasi Mobile HRIS (Android) https://hris-api.bankkalteng.co.id:65132/api/Auth/Login/	api mobile			
2	Attacker menemukan celah keamanan pada saat input kode activation, data user ID dan password tercantum secara terbuka pada URL: https://api.minovaiscloud.com/token/	api all			
3	Attacker mengidentifikasi Aplikasi Mobile HRIS (Android) masih bisa berjalan pada perangkat handphone/mobile device	apk mobile			
4	Attacker menemukan celah keamanan SSL Certificate Pinning belum diterapkan pada Aplikasi Mobile HRIS (Android).	api mobile			
5	Attacker mengidentifikasi terdapat atribut android:usesCleartextTraffic=true pada file AndroidManifest.xml.	apk mobile	Done		Done
6	Pentester menemukan celah keamanan Task Hijacking pada Aplikasi Mobile HRIS (Android).	apk mobile	Done		Done
7	Pentester menemukan celah keamanan Task Hijacking pada Aplikasi Mobile HRIS (Android).	apk mobile	Done		Done
8	Attacker mengidentifikasi HTTP Header API Aplikasi Mobile HRIS (Android) berisi informasi sensitif mengenai sistem.	api mobile			
9	Attacker menemukan celah keamanan Attribute hasFragileUserData tidak di aktifkan/set pada Aplikasi Mobile HRIS (Android).	apk mobile	Done		Done
Black Box 2					
1	Attacker menemukan celah keamanan data sensitif (image & pdf), seperti surat cuti, payslip, dll, dapat diakses secara terbuka pada URL: https://hris-api.bankkalteng.co.id:65132/image/	api mobile			
2	Attacker menemukan celah keamanan beberapa folder sensitif dapat diakses secara terbuka pada URL: https://hris-api.bankkalteng.co.id/backup/	api mobile			
White Box					
1	Attacker menemukan celah keamanan SQL Injection pada API menu History (URL path) Aplikasi Mobile HRIS (Android).	api mobile			
2	Attacker menemukan celah keamanan password pengguna tercantum secara terbuka pada URL API Change Password: https://hris-api.bankkalteng.co.id:65132/api/role/changepassword/Jakarta@123	api mobile			
3	Attacker menemukan celah keamanan Authorization ID API Mobile HRIS (Android) masih tetap aktif di server walaupun aplikasi sudah di uninstall.	api mobile			
4	Attacker menemukan celah keamanan bypass duration pada API menu Leave (Cut) Aplikasi Mobile HRIS (Android) saat di akses.	api mobile			
5	Attacker menemukan celah keamanan bypass time clockout pada API menu Absence Aplikasi Mobile HRIS (Android) saat di akses.	apk mobile	Done		Done
6	Attacker menemukan celah keamanan belum ada pembatasan (rate limit) absence clockin pada API menu Absence Aplikasi Mobile HRIS (Android).	api mobile			

- Untuk testing BKT Prod menggunakan apk bkt, kalau bkt dev menggunakan apk mobile product

Package Pantest terdapat di apk mobile

Package Menu Attendance New

UPDATE API

API: Minovals.Mobile.API

Controller > WorkflowController = [Route("api/wf/submitAttendanceNew")]

Contract > EndpointContract = public class AttendanceNewRequest, public class AttendanceNewResponse

UPDATE DATABASE

1. Pastikan PHRPA0019 memiliki kolom AuditorFlag
2. Create Table PHRPA0068
3. Stored Procedure = Mobile_GetValidasiBeforeSubmit, Mobile_InsertAttendanceClockIn, Mobile_InsertAttendanceClockOut

NOTES

1. Validasi Clock In Clock Out ada di SP Mobile_GetValidasiBeforeSubmit
2. Data Absen masuk ke PHRPA0019
3. Foto Absen masuk ke PHRPA0068 dengan id = AuditorFlag.PHRPA0019

History

#1 - 01/17/2025 03:28 PM - Muhammad Bintar

- Status changed from User Test to Closed
- Assignee changed from Muhammad Bintar to shofwan shiddiq

okeh sudah di deploy ke client.

Files

clipboard-202501161524-6dcc9.png	102 KB	01/16/2025	shofwan shiddiq
----------------------------------	--------	------------	-----------------