FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

Аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг

ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ ПРОГРАМУУДЫН АЮУЛГҮЙ БАЙДЛЫН АУДИТ

АЮУЛГҮЙ БАЙДЛЫН АЖЛЫН ХЭСГИЙН ТАЙЛАН

Аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг

ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ ПРОГРАМУУДЫН АЮУЛГҮЙ БАЙДЛЫН АУДИТ

АНХААРУУЛГА

Санхүүгийн хүртээмжийн дэлхийн санаачилга (FIGI), Дэлхийн Банкны Групп (ДБГ), Төлбөр ба зах зээлийн дэд бүтцийн хороо (CPMI), Олон Улсын Цахилгаан Холбооны Холбоо (ITU) хамтран хэрэгжүүлдэг үндэсний санхүүгийн хүртээмжийн зорилтууд, дэлхийн 'Санхүүгийн бүх нийтийн хүртээмж 2020' зорилгод хүрэх зорилт бүхий 3 жилийн хөтөлбөр бөгөөд улс орны хэмжээнд шинэчлэлийг хэрэгжүүлэхэд дэмжлэг үзүүлэх зорилготой. Түс хөтөлбөр Билл & Мелинда Гейтсийн сан (BMGF)-ийн дэмжлэгтэй хэрэгждэг.

Хамтын ажиллагаа болон ерөнхий зохион байгуулалтын хувьд (1) Цахим төлбөр тооцоог нүтагшуулах ажлын хэсэг (ДБАА удирдлагаар), (2) Дижитал санхүүгийн үйлчилгээн дэх танилт бүртгэл, хаяг ID -н ажлын хэсэг (ДБАА удирдлагаар), (3) Дэд бүтэц аюулгүй бадлыг бэхжүүлэх ажлын хэсэг (ОУЦХБ удирдлагаар) үүд ажиллаж тухайн улсын бодлого, зохицуулалтын байгууллага болон хувийн хэвшил, олон нийтийн санаа, санаачлагыг тусган уялдуулж хамтран ажиллаж байна.

Санхүүгийн хүртээмжийн дэлхийн санаачилга (FIGI)-ын хүрээнд үндэсний эрх баригчид хувийн хэвшил болон бусад холбогдох талуудыг оролцуулан тулгамдаж буй асуудал, шинээр гарч ирж буй ойлголтуудыг хуваалцах арга хэмжээг жил бүр 3 удаа зохион байгуулдаг.

Энэхүү тайлан нь Олон улсын цахилгаан холбооны байгууллагаар ахлуулсан аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсгийн бүтээгдэхүүн юм. Энэхүү ажилд илэрхийлсэн дүгнэлт, тайлбар, дүгнэлтүүд нь Төлбөр ба зах зээлийн дэд бүтцийн хороо, Билл ба Мелинда Гейтсийн сан, Олон улсын цахилгаан холбооны байгууллага, Дэлхийн банк, Санхүүгийн хүртээмжийн дэлхийн санаачилгын түншүүдийн үзэл баримтлал биш бөгөөд шууд дагаж мөрдөх албагүй.

Тодорхой компаниуд эсвэл тодорхой үйлдвэрлэгчдийн бүтээгдэхүүнийг дурьдсан нь тэдгээрийг дурдаагүй бусад ижил төстэй шинж чанартай бүтээгдэхүүнээс илүүд зөвшөөрч, санал болгосон гэсэн үг биш юм. Алдаа, орхигдуулсан зүйлсийг эс тооцвол өмчийн бүтээгдэхүүний нэрсийг эхний том үсгээр ялгана. FIGI-ийн түншүүд энэ ажилд орсон мэдээллийн үнэн зөвийг баталгаажуулахгүй. Энэхүү бүтээлийн газрын зураг дээрх хил хязгаар, өнгө, нэр томъёо болон бусад мэдээлэл нь аливаа улс орон, нутаг дэвсгэр, хот, бүс нутгийн эрх зүйн байдлын талаарх FIGI-ийн түншүүдийн дүгнэлт, түүний эрх бүхий байгууллагуудын дүгнэлтийг илэрхийлэхгүй.

Энэ тайлангийн талаар

Энэхүү илтгэлийг Себастьян Матью, Филипп Охслин нар бичсэн. Мөн FIGI Аюулгүй байдлын дэд бүтэц, итгэлцлийн ажлын хэсгийн гишүүдэд оруулсан хувь нэмэр, санал хүсэлтэд талархал илэрхийлье.

Хэрэв та нэмэлт мэдээлэл өгөхийг хүсвэл Vijay Mauree-тэй tsbfigisit@ itu .int хаягаар холбогдоно уу.

Агуулга

Ерөнхий зүйл

Энэхүү тайлангийн гол зорилго нь гар утсанд зориулагдсан дижитал санхүүгийн үйлчилгээний (DFS) Андройд үйлдлийн систем дээр ажилладаг цөөн хэдэн аппликейший аюулгүй байдлын аудитын үр дүнг танилцуулж, аюулгүй байдлын аудит хийх системчилсэн аргачлалыг боловсруулахад оршино.

Аюулгүй байдлын аудитын аргачлал нь 18 тест дээр суурилж, OWASP Mobile-ийн аюулгүй байдлын шилдэг эрсдэлийн 10 ангилалын долоон ангилалын хүрээнд авч үзсэн.

Бид ДСҮ-ний гурван програмыг туршиж үзсэн: Африкт үйлчилгээ үзүүлэгчдээс хоёр, Европоос нэг апп сонгосон програмын аюулгүй байдлын аудитын үр дүнг тайланд нууцалсан бөгөөд АПП1, АПП2, АПП3 гэж нэрлэсэн.

Тайлан дахь аюулгүй байдлын аудитын арга зүйд тодорхойлсон аюулгүй байдлын 18 туршилтыг мөн DFS Аюулгүй байдлын баталгааны хүрээний тайлангийн аюулгүй байдлын шилдэг туршлагуудтай харьцуулан харуулсан бөгөөд аюулгүй байдлын туршилтууд нь туршиж буй програмын шилдэг туршлагыг дагаж мөрдөж буй эсэхийг хэрхэн шалгаж болохыг харуулсан болно. (тайлангийн 4-р бүлгийг үзнэ үү). Энэхүү аргачлалыг ДСҮ-ний аюулгүй байдлын лабораторид Android платформ дээр суурилсан ДСҮ-ний програмуудын аюулгүй байдлыг хангах зорилгоор ашиглах болно. ДСҮ-ний аюулгүй байдлын лабораторийг ОУЦХБ-аас Санхүүгийн хүртээмжийн дэлхийн санаачилгын (FIGI) хүрээнд Аюулгүй байдал, дэд бүтэц, итгэлцлийн (SIT) ажлын хэсгийн үйл ажиллагааны хүрээнд гаргасан.

OWASP гар утасны шилдэг 10	Туршилт	App1	App2	App3
M1: Платформын зохисгүй хэрэглээ	T1.1 Android: нөөцлөхийг зөвшөөрөх	?	?	?
	T1.2 Android: дибаг хийх боломжтой	?	?	?
	T1.3 Android: суулгах байршил тодорхойлох	?	?	?
	T1.4 Аюултай зөвшөөрөл агуулга зөвшөөрөл өгөх байдал	?	?	?
M2: Өгөгдөл аюулгүй хадгалах	T2.1 Android.зөвшөөрөл. WRITE_EXTERNAL_STORAGE хадгалах байршилд зөвшөөрөл өгөх	?	?	?
	T2.2 Дэлгэцийн зураг авах(screenshot), идэвхгүй байна	?	?	?
M3: Найдвартүй харилцаа холбоо	T3.1 Програм нь зөвхөн HTTPS холболтыг ашиглах ёстой	?	?	?
	T3.2 Аппликешн нь итгэжлээгүй гэрчилгээ бүхий “ Machine-in-the-Middle” халдлагыг илрүүлэх ёстой	?	?	?
	T3.3 Аппликешн нь итгэмжлэгдсэн гэрчилгээ болон “ Machine-in-the-Middle” халдлагыг илрүүлэх ёстой	?	?	?
	T3.4 Апп манифест нь тодорхой текстийн урсгалыг зөвшөөрөх ёсгүй	?	?	?
M4: Аюулгүй баталгаажуулалт	T4.1 Нууц мэдээлэлд хандахын өмнө баталгаажуулалт шаардлагатай	?	?	?
	T4.2 Аппликешн идэвхгүй болгох хугацаатай байх ёстой	?	?	?
	T4.3 Хэрэв хурууны хээ нэмсэн бол одоо байгаа хурууны хээгээр баталгаажуулалтыг идэвхгүй болгох шаардлагатай	?	?	?
	T4.4 Эмзэг хүсэлтийг дахин эхлүүлэх боломжгүй байлгах	?	?	?
M5: Криптограф хангалтгүй	T5.1 Апп нь аюултай, хамгаалалтгүй крипто командыг ашиглах ёсгүй	?	?	?
	T5.2 HTTPS холболтыг шилдэг туршлагын дагуу тохируулах хэрэгтэй	?	?	?
	T5.3 Аппликешн нь HTTPS-ээр илгээгдсэн нууц мэдээллийг шифрлэх ёстой	?	?	?
M8: Кодыг өөрчлөх	T8.1 Програм нь үндэстэй төхөөрөмж дээр ажиллагаа хийдэггүй байх ёстой	?	?	?
M9: Урвуу инженерчлэл	T9.1 Програмын кодыг бүдэгрүүлсэн байх ёстой	?	?	?

Товчлол

CA Certificate Authority

DES Data Encryption Standard

DFS Digital Financial Services

ECB Electronic Code Book

HTTPS Hyper Text Transfer Protocol

MD Message Digest

MITM Man in the Middle

OWASP Open Web Application Security Project

PIN Personal Identification Number

PUK Personal Unlock Key

RC Rivest Cipher

SHA Secure Hash Algorithm

SSL Secure Sockets Layer

TLS Transport Layer Security

Android DFS програмуудын аюулгүй байдлын аудит

1. АПП- ЫН ТУХАЙ

Шинжилгээнд Африк тивээс хоёр, Европ тивээс нэг дижитал санхүүгийн үйлчилгээ эрхлэгчийн дижитал санхүүгийн үйлчилгээний програмыг сонгосон, сонгогдсон програмын аюулгүй байдлын аудитын үр дүнг тайланд нэрийг нь нууцалсан бөгөөд гурван програмыг цаашид судалгааны тайланд АПП1, АПП2, АПП3 гэж нэрлэнэ.

1.1. Програм 1

АПП1 нь Европт хэрэглэгчийн кредит карт болон банкны дансыг холбон үйлчилгээ үзүүлдэг гар утасны програм юм. Үүнийг мөнгө илгээх, хүсэлт гаргах, хүлээн авахад ашиглаж болно. Энэхүү программ нь QR кодыг уншуулж онлайн төлбөр тооцоо хийх боломжтой бөгөөд дэлгүүр, ресторанд бэлэн бус төлбөр тооцоо хийх, QR код эсвэл худалдааны дохио ашиглан зогсоолын тасалбарыг төлөхөд ашиглагдана. Хэрэглэгч бүртгүүлэхийн тулд гар утасны дугаар, зээлийн карт эсвэл банкны дансны дэлгэрэнгүй мэдээллийг шаарддаг.

1.2. Програм 2

АПП2 нь Африк даяар үйл ажиллагаа явуулж бүй бүс нутагт дижитал санхүүгийн үйлчилгээ үзүүлдэг гар утасны сүлжээний оператор хангадаг. Мобайл санхүүгийн үйлчилгээний шинэлэг аппликейшн нь хэрэглэгчдэд дотоод болон гадаадад мөнгө илгээх, бараа, үйлчилгээний төлбөр төлөх, дэлхийн хаанаас ч гүйлгээ хийх, гар утасны хэтэвч болон хэрэглэгчийн банкны данс хооронд шилжүүлэг хийх боломжтой болсон. Хэрэглэгч бүртгүүлэхийн тулд операторын гар утасны дугаар шаардлагатай. Аппликейшн хэрэглэгчид банкны данстай байх шаардлагагүй.

1.3. Програм 3

АПП3 нь Африк, Азийн хэд хэдэн оронд үүрэн холбооны операторoор хангадаг. Энэхүү програм нь хэрэглэгчдэд харилцагчид руу мөнгө илгээх, бараа, үйлчилгээний төлбөрийг төлөх, мөн гар утасны хэтэвч болон банкны данс хооронд шилжүүлэх боломжийг олгодог. Програмыг бүртгүүлэхийн тулд операторын гар утасны дугаар шаардлагатай. Аппликейшн хэрэглэгчид банкны данстай байх шаардлагагүй.

2. ТУРШИЛТЫН АРГА

Эдгээр туршилтын зорилго нь Дижитал санхүүгийн үйлчилгээнд зориулсан ухаалаг гар утасны програмуудын аюулгүй байдлын стандартчилсан оноог өгөх явдал юм. Энэ нь програмыг туршилтын утсан дээр суулгаж, аюулгүй байдлын шинж чанаруудыг тестийн хэрэгслээр шинжлэх замаар хийгддэг. Туршилтуудыг нээлттэй эхийн хэрэгслээр, боломжийн хүчин чармайлтаар хийх боломжтойгоор сонгосон. Туршилтыг OWASP гар утасны шилдэг 10 жагсаалтын дагуу зохион байгуулдаг. Open Web Application Security Project [1] (OWASP) нь програм хангамжийн аюулгүй байдлыг сайжруулах зорилготой ашгийн бус сан юм. Тэдний төслүүдийн нэг нь OWASP гар утасны шилдэг 10^2 бөгөөд дараах эрсдэлүүдийг хамгийн чухал гэж жагсаасан байна.

a) M1 платформын зохисгүй хэрэглээ
b) M2 өгөдөл аюулгүй хадгалах
c) M3 Найдваргүй харилцаа холбоо
d) M4 Аюулгүй баталгаажуулалт
e) M5 Криптограф хангалтгүй
f) M6 Аюулгүй зөвшөөрөл
g) M7 Хэрэглэгчийн кодын чанар
h) M8 кодыг өөрчлөх
i) M9 урвуу инженерчлэл
j) M10 Гадны функциональ байдал

M6, M7, M10 ангилалууд нь програмын эх код руу нэвтрэх эсвэл програмын логикийг урвуу инженерчлэх шаардлагатай тул бидний туршилтын хамрах хүрээнээс гадуур байна.
Дараахь 18 тестийн багцыг тэдгээрийн хамаарал болон туршилтын боломжит байдалд үндэслэн сонгосон.

2.1. M1 платформын зохисгүй хэрэглээ

Эдгээр туршилтыг програмын манифестийг шинжлэх замаар хийдэг. Дараахь асуудлуудыг баталгаажуулсан болно.

a) **T1.1 Android: allowBackup** [3] :
   Энэ тохиргоог худал гэж тохируулах ёстой бөгөөд энэ нь өгөгдмөл утга биш юм.
   Хэрэв энэ атрибутыг худал гэж тохируулсан бол програмын бүх өгөгдлийг хадгалахад хүргэдэг бүрэн системийн нөөцлөлтөөс ч гэсэн програмыг нөөцлөх, сэргээх ажлыг хэзээ ч хийхгүй.
b) **T1.2 Android: дибаг хийх боломжтой** [4] :
   Энэ тохиргоог худал гэж тохируулах ёстой бөгөөд энэ нь өгөгдмөл утга юм.
   Хэрэв програмыг дибаг хийх боломжтой гэж тэмдэглэсэн бол халдагчид эмзэг програмын үйл явцын хүрээнд үүнийг гүйцэтгэхийн тулд өөрийн кодыг оруулж болно.
c) **T1.3 Android: суулгах Байршил** [5] :
   Үүнийг internalOnly гэж тохируулах эсвэл өгөгдмөл утга нь тохируулаагүй байх ёстой.
   Хэрэв энэ параметрийг auto эсвэл preferExternal гэж тохируулсан бол уг програмыг зөөврийн санах ойн картанд суулгаж болно.
   Халдагчид санах ойн карт руу нэвтрэх эрх авснаар программыг өөрчлөх эсвэл нууц мэдээллийг задлах боломжтой.
   Аппликейшн энэ шалгалтанд тэнцээгүй байсан ч энэ нь уг програмыг зөөврийн картанд суулгана гэсэн үг биш гэдгийг анхаарна уу.
d) **T1.4 Аюултай зөвшөөрөл :**
   Аппликешн нь ямар ч үндэслэлгүйгээр аюултай зөвшөөрөл шаардах ёсгүй.
   Андройд аппликейшн нь олон төрлийн үйлдлүүдэд зөвшөөрөл хүсдэг. Эдгээр зөвшөөрлүүдийн заримыг Android-д ''аюултай'' гэж тэмдэглэсэн байдаг. Апп нь харилцах цонхоор хэрэглэгчээс аюултай зөвшөөрөл олгохыг тодорхой хүсэх ёстой (жишээ нь: Апп-д утсаар ярихыг зөвшөөрөх үү?). Аюултай зөвшөөрөл хүсэх үндэслэлтэй шалтгаан байж болно. Жишээлбэл, төлбөр хийхдээ QR кодыг сканнердах шаардлагатай DFS програмд камер ашиглах зөвшөөрөл шаардлагатай болно гэх мэт.
   Мэдээлэл хадгалах зөвшөөрлийг дараагийн хэсэгт авч үзнэ гэдгийг анхаарна уу.
   Аюултай зөвшөөрөл шаарддаг програм нь хэрэглэгч үүг халдах зөвшөөрлийг урвуулан ашиглаж болзошгүй. Жишээлбэл, хэрэв залгах зөвшөөрөл олгосон хувийн хадгалсан утасны жагсаалт болон өндөр зэрэглэлтэй дугаар руу залгах боломжтой.

2.2. M2 Аюулгүй мэдээлэл хадгалах

Эдгээр туршилтыг мөн програмын манифестийг шинжлэх, утсан дээр програм ажиллуулах замаар хийдэг. Дараах асуудлуудыг баталгаажуулсан болно.

a) **T2.1 Android зөвшөөрөл WRITE_EXTERNAL_ STORAGE** :

Аппликешн нь ямарч шалтгаангүйгээр энэ зөвшөөрлийг шаардах ёсгүй.

Энэхүү зөвшөөрөл нь апп-д утсанд суулгасан санах ойн карт дээрх өгөгдлийг унших, бичих боломжийг олгоно. Хэрэв аппликейшн нь их хэмжээний эмзэг бүс мэдээллийг хадгалах шаардлагатай бол энэ нь гадаад санах ой руу бичих үндэслэл болно.

Халдагчид санах ойн карт руу нэвтрэх эрх авснаар программыг өөрчлөх эсвэл нууц мэдээллийг задлах боломжтой.

Аппликешн энэ шалгалтанд тэнцээгүй байсан ч энэ нь тухайн аппликешн нь гадаад санах ойд эмзэг өгөгдлийг бичнэ гэсэн үг биш гэдгийг анхаарна уу.

б) **T2.2 Дэлгэцийн зураг дарах боломжийг идэвхгүй болгож байна(Screenshot)** :

Аппликешн ажиллаж байх үед дэлгэцийн зураг дарах боломжийг идэвхгүй болгох ёстой бөгөөд зөвхөн шаардлагатай үед хоосон зураг харуулах болно.

Энэ нь аюулгүй программуудад зориулсан стандарт үйлдэл бөгөөд үүнийг FLAG_SECURE[6] нэртэй програмын параметрээр хийж болно. Үүнийг програмыг ажиллуулж, а) дэлгэцийн зураг дарах оролдлого, б) програм хооронд сэлгэх, програмын өнгөц зургийг ажиглах замаар шалгаж болно. Энэ тохиргоо байхгүй бол хортой програм нь програмын дэлгэцээс нууц мэдээллийг хулгайлж болзошгүй.

2.3. M3 Найдваргүй харилцаа холбоо

a) **T3.1 Аппликешн нь зөвхөн HTTPS холболтыг ашиглах ёстой** :

Аппликейшний траффикийг аудитын шалгагчаар ажиглахдаа зөвхөн HTTPS урсгалыг ажиглах хэрэгтэй.

HTTPS траффик шифрлэгдсэн байна. Эдгээр нь траффикийг шифрлэх өөр аргууд байх боловч HTTPS нь програмууд болон серверүүдийн хоорондын харилцааны стандарт арга юм. Хэрэв өгөгдлийг HTTP эсвэл бусад шифрлэгдээгүй протоколоор дамжуулдаг бол халдагчид амархан нөлөөлж эсвэл бүр өөрчлөх боломжтой.

b) **T3.2 Аппликейшн нь итгэмжгүй гэрчилгээ бүхий халдлагыг илрүүлэх ёстой :**

Програмын серверийн итгэмжлэгдсэн гэрчилгээг эзэмшдэггүй machine-in the-middle (MITM) прокси-ээр дамжуулан траффик ажиллуулах үед програм нь холболтоос татгалзах ёстой.

MITM прокси нь HTTPS урсгалыг таслан зогсоох, шалгах, өөрчлөх зорилгоор шифрийг тайлж, зориулалтын сервер рүү илгээхийн өмнө дахин шифрлэхэд ашиглагдаж болно.

Ердийн халдагчид очих серверт хүчинтэй гэрчилгээ эзэмшдэггүй; Тиймээс програм нь итгэмжлэгдсэн эрх бүхий байгууллага проксины гэрчилгээнд зөвшөөрөл олгоогүй болохыг илрүүлэх ёстой. Хэрэв програм нь гэрчилгээний хүчинтэй эсэхийг шалгахгүй бол халдагчид урсгалыг таслан зогсоож, өөрчлөх боломжтой.

c) **T3.3 програм нь итгэмжлэгдсэн гэрчилгээгээр дотоод халдлагыг илрүүлэх ёстой :**

Ухаалаг утсанд итгэмжлэгдсэн “certificate signed” CA-ийн зөвшөөрөл бүхий гэрчилгээг ашигладаг machinein-the-middle (MITM) проксигоор дамжуулан траффикийг ажиллуулах үед програм нь холболтоос татгалзах ёстой.

Проксины оператор утсаар итгэмжлэгдсэн гэрчилгээг үүсгэх боломжтой бол өөр нөхцөл байдал үүсч болно. Оператор нь CA оператор (жишээ нь, засгийн газар), оператор нь компанийн утсанд эх гэрчилгээгээ суулгасан компани байж болно, эсвэл үндсэн гэрчилгээг хэрэглэгч эсвэл халдагч гараар суулгасан байж болно. Уг програм нь “root pinning” хийснээр ийм төрлийн халдлагаас өөрийгөө хамгаалж чадна.

Энэ нь програм үндсэн тохиргоогоороо серверийн гэрчилгээнд аль CA батаглаажсан байхыг тодорхойлж чаддаг бөгөөд эдгээр CA-д итгэмжлэгдсэн байсан ч бусад CA-уудыг баталгаажуулах эсхүл татгалзах чадамжтай гэсэн үг юм. Энэ тестийг гүйцэтгэхийн тулд үндсэн гэрчилгээг суулгахын тулд утасны үндсэн тохиргоог үндэслэх шаардлагатай болдог.

Хэрэв аппликешн нь гэрчилгээ тогтоохыг ашиглахгүй бол итгэмжлэгдсэн эх CA-н аль нэгийг нь хакердаж чадсан халдагчид траффикийг саатуулж болзошгүй.

d) **T3.4 Апп манифест нь тодорхой текст урсгалыг зөвшөөрөх ёсгүй :**

Тодорхой текстийн урсгалыг ашиглах нь Android 8.1 эсвэл түүнээс дээш хувилбар дээр анхдагчаар идэвхгүй болсон. Апп манифест нь энэ өгөгдмөл тохиргоонд дарах тохиргоог агуулж болохгүй.

Эдгээр нь програмын android:u sesCleartextTraffic тохиргоо эсвэл сүлжээний аюулгүй байдлын тохиргоон дахь clear textTrafficPermitted байж болно.

Тодорхой текстийн урсгалыг идэвхгүй болгосон тохиолдолд програм болон түүний ашигладаг бусад бүрэлдэхүүн хэсгүүд (жишээ нь, медиа тоглуулагч) тодорхой текстийн урсгалыг ашиглахаас татгалзах болно.

Тодорхой текстийн урсгалыг халдагчид амархан чагнаж, удирдаж болно.

Аппликешн энэ шалгалтанд тэнцээгүй байсан ч энэ нь тухайн программ нь тодорхой текстийн урсгалыг илгээх эсвэл хүлээн авах гэсэн үг биш гэдгийг анхаарна уу.

2.4. M4 Аюулгүй баталгаажуулалт

Уг программыг утсан дээр ажиллуулж, түүний үйлдлийг ажигласнаар дараах туршилтуудыг хийдэг.

a) **T4.1 Нууц мэдээлэлд хандахын өмнө баталгаажуулалт шаардлагатай** :

Апп нь нууц мэдээлэл эсвэл функцэд (жишээ нь, үлдэгдэл, төлбөр) хандахын өмнө нууц үг, ПИН код эсвэл хурууны хээ хүсэх ёстой.

Үүнийг утсан дээрх программыг ашиглан шалгаж болно. Хэрэглэгчийг баталгаажуулахгүй байхын үр дагавар нь хэрэв утсаа хулгайд алдсан эсвэл түгжээг нь тайлсан үед зүй бусаар утас эзэмшиж буй болон халдагч нууц мэдээлэл эсвэл функцэд нэвтэрч болзошгүй.

b) **T4.2 Аппликешн идэвхгүй байх хугацаатай байх ёстой** :

Аппликешныг хэсэг хугацаанд нээлттэй орхиж, автоматаар түгжигдэх эсэхийг ажигласнаар үүнийг шалгаж болно.

Хэрэв хугацаа хэтрээгүй эсвэл хэтэрхий удаан байвал утсыг хулгайд алдсан эсвэл түгжээг нь тайлсан үед зүй бусаар утас эзэмшиж буй этгээд болон халдагчид нууц мэдээлэл эсвэл функцэд хандах эрсдэлтэй.

b) **T4.3 Хэрэв хурууны хээ нэмсэн бол хурууны хээгээр баталгаажуулалтыг идэвхгүй болгох шаардлагатай** :

Утсанд шинэ хурууны хээ бүртгүүлсэн тохиолдолд хэрэглэгч програмын ПИН код эсвэл нууц үгээ оруулах хүртэл хурууны хээгээр өмнөх баталгаажуулалтыг идэвхгүй болгох ёстой.

Халдагчид гар утсан дээрээ хурууны хээгээ бүртгүүлж, хурууны хээгээр хамгаалагдсан программ руу нэвтэрч орох эрсдэлтэй.

c) **T4.4 Тасалсан хүсэлтийг дахин эхлүүлэх боломжгүй** :

Хэрэв хүсэлт дундаас дундын этгээд, хүн, прокси авсан хүсэлтийг (жишээ нь, мөнгө шилжүүлэх) дахин эхлүүлэх нь нэг хүсэлтийг хоёр удаа илгээхэд хүргэж болохгүй.

Эрсдэл нь халдагчид мөнгө шилжүүлэх хүсэлтийг таслан зогсоож, хохирогчоос мөнгө хулгайлахын тулд үүнийг давтаж болно.

2.5. M5 Криптограф хангалтгүй

a) **T5.1 Аппликешн нь аюултай крипто командыг ашиглах ёсгүй:**

MD5, SHA-1, RC4, DES, 3DES, Blowfish, блок шифрт зориулсан ECB горим, криптографийн бус санамсаргүй генератор зэрэг алгоритмууд сул байдаг тул программ ашиглах ёсгүй [7] .

Аппликешн нь эдгээр аюултай алгоритмууд руу залгаж байгаа эсэхийг шалгахын тулд програмын хоёртын файлд дүн шинжилгээ хийх замаар үүнийг шалгаж болно.

Хэрэв нууц мэдээллийг эдгээр алгоритмаас хамаарсан эсвэл зохицуулсан бол халдагчид үг мэдээллийг чагнаж, удирдах эрсдэлтэй. Эдгээр алгоритмуудыг ашиглаж байгаа нь тэдгээрийг эмзэг үйлдлүүдэд ашигладаг гэсэн үг биш юм. Гэсэн хэдий ч эргэлзээ төрүүлэхийн тулд эдгээр алгоритмыг ашиглахгүй байх нь хамгийн сайн арга юм.

Аппликешн энэ шалгалтанд тэнцээгүй байсан ч энэ нь тухайн аппликейшн эмзэг өгөгдөлд аюултай крипто командыг ашигладаг гэсэн үг биш гэдгийг анхаарна уу.

b) **T5.2 HTTPS холболтыг хамгийн сайн туршлагын дагуу тохируулах ёстой** :

Програмын сүлжээний урсгалыг ажигласнаар түүний холбгдож буй серверүүдийг тодорхойлж болно. Эдгээр серверүүдийн HTTPS тохиргоог Qualys SSL Labs [8] гэх мэт хэрэгслээр шалгаж болно . Нийт үнэлгээ нь B ба түүнээс дээш байх ёстой. Хэрэв HTTPS-г зөв тохируулаагүй бол зарим нэг чагнах, залилан хийх халдлага хийх боломжтой.

c) **T5.3 Апп нь HTTPS-ээр илгээгдсэн нууц мэдээллийг шифрлэх ёстой** :

Үүнийг MITM прокси ашиглан траффикийг таслан шалгах замаар шалгаж болно (M3 дээрх туршилтуудыг үзнэ үү). Хэрэв програм нь гэрчилгээ тогтоохыг ашигладаг бол ачааллыг таслахын тулд энэ хамгаалалтыг идэвхгүй болгох шаардлагатайг анхаарна уу. Энэ нь үргэлж боломжтой байдаггүй.

Хэрэв өгөгдөл нь програмаар шифрлэгдээгүй бол MITM нь мэдээллийг чагнаж эсвэл өөрчлөх боломжтой.

2.6. M8 кодыг өөрчлөх

T8.1 Төхөөрөмж код өөрчилхөөс татгалзах ёстой :

Үндсэн тохиргоотой Android утсан дээр суулгасан тохиолдолд програмыг ажиллуулахаас татгалзах ёстой.

Үндсэн тохиргоотой утсан дээр аюулгүй байдлын хэд хэдэн механизмыг идэвхгүй болгож болно. Энэ нь халдагчид програмын код эсвэл өгөгдлийг өөрчлөх залиллан мэхлэх боломжийг олгоно.

Хэрэв програм нь үндсэн тохиргоотой төхөөрөмж дээр ажиллахыг зөвшөөрвөл хамгийн багадаа дараах гурван аюулгүй байдлын хяналтыг хэрэгжүүлэх ёстой: Кодыг нуун дарагдуулах (T9.1), итгэмжлэгдсэн гэрчилгээтэй харилцахад саад

учруулахаас сэргийлэхийн тулд гэрчилгээ тогтоох (T3.3) болон нууц мэдээллийг HTTPS (T5.3)-ээр дамжуулсан ч гэсэн програмаар шифрлэсэн байх ёстой.

2.7. M9 Урвуу инженерчлэл

T9.1 Програмын кодыг бүдгэрүүлсэн байх ёстой :

Хэд хэдэн хэрэгслийг ашиглан програмын хоёртын файлд дүн шинжилгээ хийж, түүнийг бүдгэрүүлсэн эсэхийг илрүүлэх боломжтой. Эсвэл кодыг decompiler ашиглан урьдчилсан байдлаар задалж болно. Хэрэв энэ нь амжилттай болбол задалсан код нь ойлгомжтой эсэхийг шинжлэх боломжтой.

Кодыг бүдгэрүүлэх нь түүний логик, алгоритмыг ойлгох, шинжлэхэд илүү төвөгтэй болгодог.

3. YP ДҮН

3.1. Програм 1

АПП1-ийг хэрэглэгчид хооронд мөнгө илгээх эсвэл дэлгүүр эсвэл автомат дээр бэлэн мөнгөгүйгээр төлбөр төлөхөд ашиглаж болно. Хэрэглэгчдийг утасны дугаараар нь тодорхойлдог. Өөр хэрэглэгчрүү мөнгө илгээхэд утасны дугаар л шаардлагатай. Дансуудыг ихэвчлэн банкны дансаар баталгаажуулдаг. Мөн банкны данснаас хамааралгүй урьдчилсан төлбөрт данстай байх боломжтой.

3.1.1. M1: Платформын зохисгүй хэрэглээ

√ T1.1 Android: кодчлол дотор allowBackup-г худал гэж тохируулсан.

√ T1.2 Android: дибаг хийх нь эх код дотор тодорхойлогдоогүй байна.

√ T1.3 Android: кодын суулгалтын байршлыг тодорхойлоогүй байна.

√ T1.4 Бид эх кодоос Android-ийн зохисгүй зөвшөөрлийг олоогүй.

3.1.2. M2: Аюулгүй өгөгдөл хадгалах

x T2.1 Аппликешн нь "android.permission.WRITE_EXTERNAL_STORAGE" зөвшөөрөл шаарддаг. Энэ нь програм нь гадаад санах ойд өгөгдөл бичдэг гэсэн үг биш гэдгийг анхаарна уу, хэрэв бичсэн бол энэ өгөгдөл нь өндөр эсдэлтэй байна.

√ T2.2 Аппликешн ажиллаж байх үед дэлгэцийн агшин(Screenshot)-г идэвхгүй болгосон.

3.1.3. M3: Найдваргүй харилцаа холбоо

√ T3.1 Зөвхөн HTTPS холболтуудыг ашигладаг.

√ T3.2 Апп нь итгэмжгүй гэрчилгээ бүхий прокситэй HTTPS холболт үүсгэхээс татгалзсан.

√ T3.3 Апп нь итгэмжлэгдсэн сертификат бүхий прокситэй HTTPS холболт үүсгэхээс татгалзсан. Энэ нь гэрчилгээний бэхэлгээг ашиглаж байгааг харуулж байна.

√ T3.4 Аппликешн нь өөрийн эх кодын баримт бичиг дэх түсгай сүлжээний аюулгүй байдлын тохиргоог тодорхойлдог. Энэ тохиргоо нь тодорхой текст урсгалыг идэвхгүй болгодог:

```
<network-security-config>
<base-config clear textTrafficPermitted="false"> ...
        </base-config>
        </network-security-config>
```

3.1.4. M4: Аюулгүй баталгаажуулалт

√ T4.1 Аппликешныг эхлүүлэх бүрд уг програмыг баталгаажуулахын тулд PIN код эсвэл хурууны хээ шаардлагатай.

√ T4.2 Аппликейшн нь идэвхгүй байдлын хугацааг хэрэгжүүлдэг. Хэсэг хугацаанд идэвхгүй болсны дараа програмаас гарна.

√ T4.3 Хурууны хээ нэмсэн тохиолдолд програм нь өмнөх хурууны хээгээр баталгаажуулалтыг идэвхгүй болгоно.

√ T4.4 Мөнгө илгээх хүсэлтийг амжилттай дахин тоглуулах боломжгүй. Сервер нь "409 Conflict" алдааны мессежээр хариу өгөх бөгөөд мөнгө илгээх хүсэлтийг боловсруулахгүй.

3.1.5. M5: Криптограф хангалтгүй

x T5.1 Аппликейшн нь сул MD5 болон SHA-1 хэшлэх алгоритмууд болон ECB-ийн сул шифрлэлтийн горимыг ашигладаг. com/appdynamics/eumagent/runtime/p000private/ae.java файл дахь MD5:

MessageDigest instance = MessageDigest.getInstance("MD5");
com/App1/android/Security/SecCore/b/a.java файл дахь SHA-1:
MessageDigest instance = MessageDigest.getInstance("SHA-1");
com/App1/android/Security/SecCore/b/a.java файл дахь ECB:
Шифрийн жишээ = Cipher.getInstance("AES/ECB/ NoPadding");

√ T5.2 HTTPS хүсэлтийг Burp Proxy-ээр таслан зогсоосноор үйлчлүүлэгчийн холбогдох серверийг тодорхойлох боломжтой. Серверийн TLS тохиргоог Qualys SSL Labs [9] ашиглан үнэлсэн . Нийт үнэлгээ нь A+ байсан.

x T5.3 HTTPS хүсэлтийг Burp Proxy-ээр таслан зогсоосноор үйлчлүүлэгчийн хүсэлтэд гарын үсэг зурсан болно. Харин шилжүүлсэн мөнгөний хэмжээ болон шилжүүлэгт оролцож буй хэрэглэгчдийн нэр, овог, утасны дугаарыг тодорхой бичвэрээр бичсэн байна.

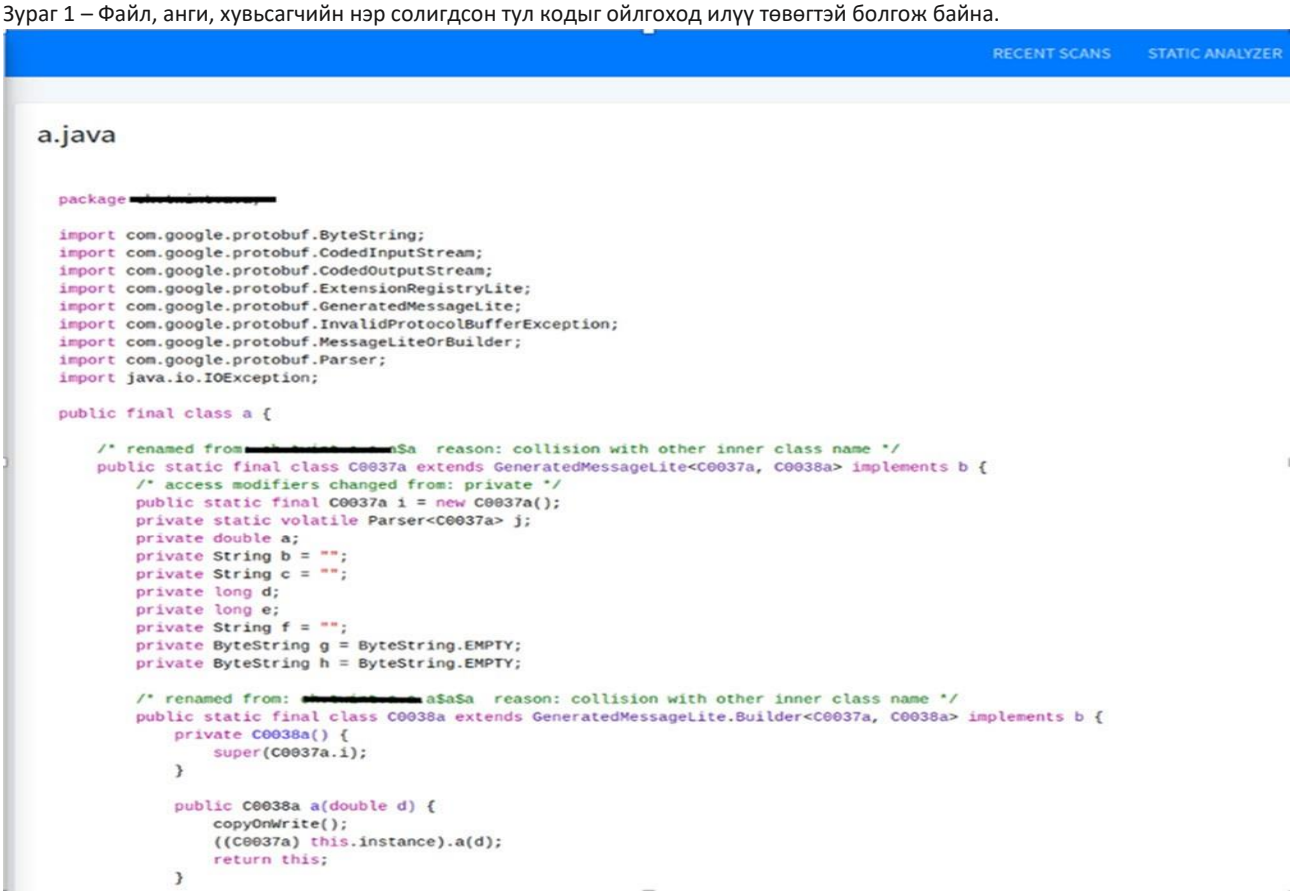
3.1.6. M8: Кодыг өөрчлөх

√ T8.1 Бид програмыг үндсэн тохиргоотой төхөөрөмж дээр суулгаж, ажиллуулж чадсан.

3.1.7. M9: Урвуу инженерчлэл

√ T9.1 Зураг 1-д үзүүлсэн шиг програмын кодыг бүдгэрүүлсэн.

Зураг 1 – Файл, анги, хувьсагчийн нэр солигдсон тул кодыг ойлгоход илүү төвөгтэй болгож байна.



3.2. Програм 2

App2 нь гар утасны мөнгө шилжүүлэх, төлбөр тооцоо, бичил санхүүгийн үйлчилгээнд ашиглагддаг. Банкны дансаар баталгаажаагүй байна. Гэрээт борлуулагч эсвэл жижиглэн худалдааны цэгүүд гэх мэт өөр өөр агентуудаар дамжуулан дансанд мөнгө байршуулж, авах боломжтой.

3.2.1. M1: Платформын зохисгүй хэрэглээ

√ T1.1 Android: эх кодчлолын баримт бичиг дотор allowBackup-г худал гэж тохируулсан.

√ T1.2 Android: дибаг хийх нь эх кодын холбоос баримт бичигт тодорхойлогдоогүй байна.

√ T1.3 Android:i nstallLocation нь эх кодын баримт бичигт тодорхойлогдоогүй байна.

√ T1.4 Бид эх кодын баримт бичигт Android-ийн зохисгүй зөвшөөрлийг олсонгүй.

3.2.2. M2: Аюулгүй өгөгдөл хадгалах

√ T2.1 Аппликейшнүүдэд "android.permission.WRITE_EXTERNAL_STORAGE" зөвшөөрөл шаардлагатай. Энэ нь програм нь гадаад санах ойд өгөгдөл бичдэг гэсэн үг биш гэдгийг анхаарна уу.

√ T2.2 Аппликешн ажиллаж байх үед дэлгэцийн агшин(Screenshot)-г идэвхгүй болгосон.

3.2.3. M3: Найдваргүй харилцаа холбоо

√ T3.1 Зөвхөн HTTPS холболтуудыг ашигладаг.

√ T3.2 Апп нь итгэмжгүй гэрчилгээ бүхий прокситэй HTTPS холболт үүсгэхээс татгалзсан

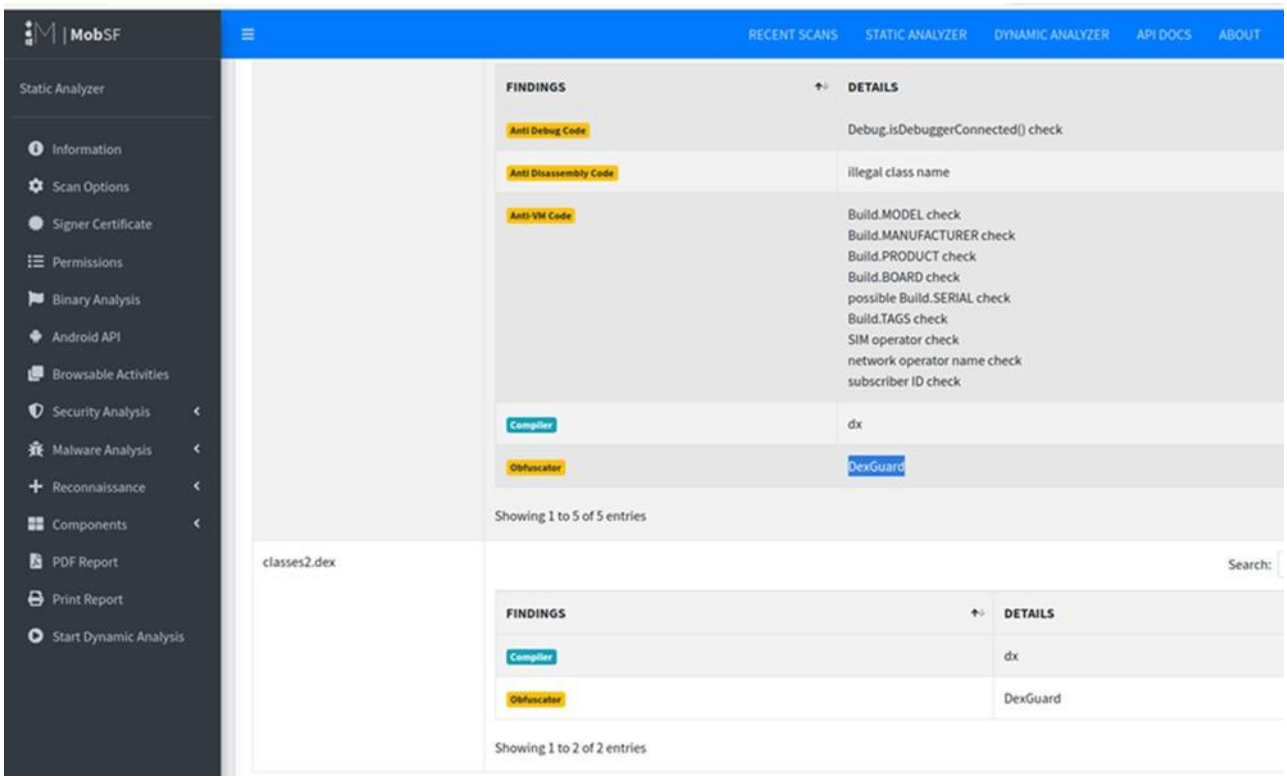
√ T3.3 Апп нь итгэмжлэгдсэн сертификат бүхий прокситэй HTTPS холболт үүсгэхээс татгалзсан. Энэ нь гэрчилгээний бэхэлгээг ашиглаж байгааг харуулж байна.

x T3.4 Android: usesClear textTraffic-г үнэн гэж тохируулсан.

3.2.4. M4: Аюулгүй баталгаажуулалт

x T4.1 Аппликешныг эхлүүлэх бүрдээ PIN код эсвэл хурууны хээ шаардахгүй. Тиймээс түгжээгүй төхөөрөмжийг хулгайлсан халдагч програмыг ажиллуулах боломжтой.

Зураг 2 – App2 нь DexGuard-р хамгаалагдсан



Энэ нь халдагчдад утасны PUK код болон дансны үлдэгдлийг харах боломжийг олгоно. Гэхдээ мөнгөний гүйлгээ хийхэд ПИН код шаардлагатай.

√ T4.2 Мөнгө шилжүүлэх бүрт ПИН код шаардлагатай. Энэ нь хугацаа хэтрүүлэхээс ч илүү аюулгүй юм.

√ T4.3 Хуруугуны хээ нэмсэн тохиолдолд програм нь хуруугуны хээгээр баталгаажуулалтыг идэвхгүй болгоно.

x T4.4 Мөнгө шилжүүлэг гэх мэт эмзэг хүсэлтүүдийг MITM проксигээр дахин тоглуулах боломжтой.

3.2.5. M5: Криптограф хангалтгүй

x T5.1 Аппликешн нь сул SHA-1 хэшлэх алгоритм болон сул анхдагч санамсаргүй тоо үүсгэгчийг ашигладаг.
o/C1668.java файл дахь SHA-1:
MessageDigest instance = MessageDigest.getInstance("SHA-1");

x o/C1783.java файл дахь санамсаргүй генератор:
this(juVar, d, new Random());

√ T5.2 HTTPS хүсэлтийг Burp Proxy-ээр таслан зогсоосноор үг программын холбогдох серверийг тодорхойлсон. Серверийн TLS тохиргоог Qualys SSL Labs [10] ашиглан туршсан . Нийт үнэлгээ нь A+ байна.

3.2.6. M8: Кодыг өөрчлөх

√ T8.1 Програм нь root тохиргоотой Android төхөөрөмж дээр ажилладаггүй.

3.2.7. M9: Урвуу инженерчлэл

√ T9.1 Аппликешны кодыг бүдгэрүүлсэн байна. Зураг 2-т үзүүлсэн шиг програмын кодыг DexGuard [11] бүдгэрүүлсэн.

3.3. Програм 3

App3 нь нийтийн үйлчилгээний төлбөрийг төлөх, мөнгө шилжүүлэх, онлайн дэлгүүрт ашиглагддаг төлбөрийн програм юм. Үүнийг банкны данс эсвэл гэрийн хаягаар бүртгэгдсэн дижитал түрийвчтэй холбож болно.

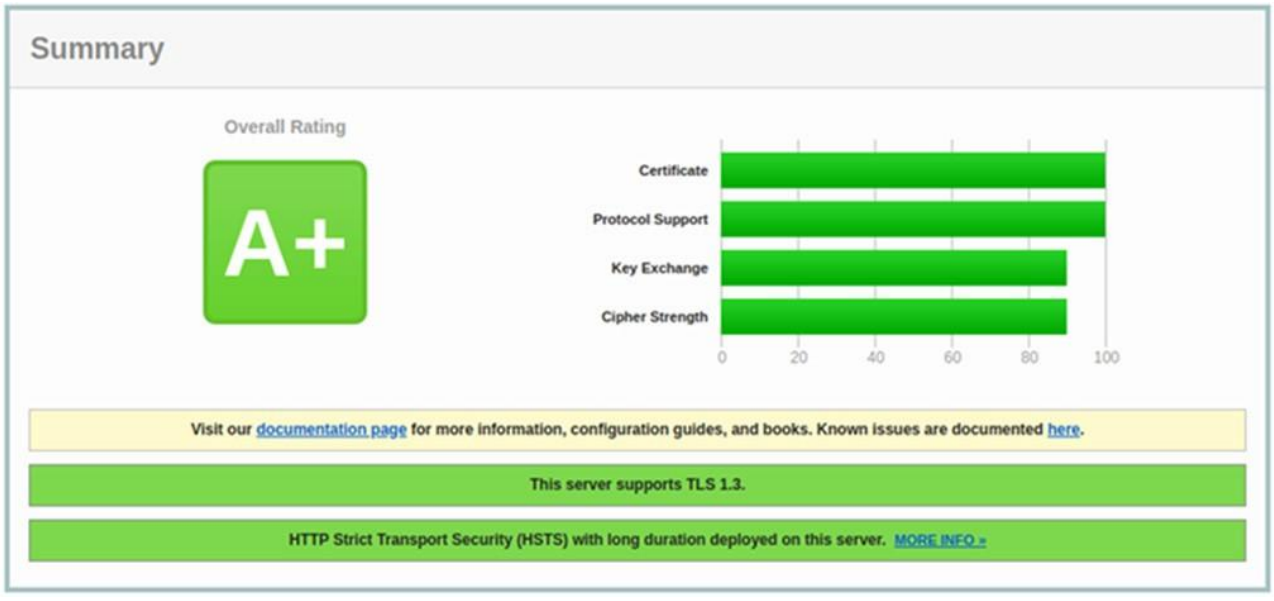
3.3.1. M1: Платформын зохисгүй хэрэглээ

√ T1.1 Android: манифест дотор allowBackup-г худал гэж тохируулсан.

√ T1.2 Android: дибаг хийх нь эх кодын баримт бичигт тодорхойлогдоогүй байна.

√ T1.3 Android:i nstallLocation нь эх кодын тодор тодорхойлогдоогүй байна.

Зураг 3 – app3 серверийн SSL тохиргооны үнэлгээ



√ T1.4 Бид эх кодын баримт бичгээс Android-ийн зохисгүй зөвшөөрлийг олоогүй.

3.3.2. M2: Аюулгүй өгөгдөл хадгалах

√ T2.1 Аппликешн нь "android. зөвшөөрөл. WRITE_EXTERNAL_ STORAGE" зөвшөөрөл шаарддаггүй.

x T2.2 Аппликешн ажиллаж байх үед дэлгэцийн агшин (Screenshot)-г идэвхгүй байна. Түүнчлэн, сүүлийн үеийн даалгаврын түүхээс авсан арын дэлгэцийн агшинг бүдгэрүүлсэнгүй.

3.3.3. M3: Найдваргүй харилцаа холбоо

√ T3.1 Зөвхөн HTTPS холболтуудыг ашигладаг.

√ T3.2 Апп нь итгэмжгүй гэрчилгээ бүхий прокситэй HTTPS холболт үүсгэхээс татгалзсан.

x T3.3 Аппликешн нь итгэмжлэгдсэн сертификат бүхий прокситэй HTTPS холболт үүсгэхийг зөвшөөрнө. Энэ нь гэрчилгээний бэхэлгээг ашиглахгүй байгааг харуулж байна. x T3.4 Android: usesClear textTraffic-г үнэн гэж тохируулсан.

3.3.4. M4: Аюулгүй баталгаажуулалт

x T4.1 Аппликешныг эхлүүлэх бүрдээ PIN код эсвэл хурууны хээ шаардахгүй. Тиймээс түгжээгүй төхөөрөмжийг хулгайлсан халдагч програмыг ажиллуулж болно. Энэ нь халдагчид дансны үлдэгдлийг харах боломжийг олгоно. Гэхдээ мөнгөний гүйлгээ хийхэд ПИН код шаардлагатай.

√ T4.2 Мөнгө шилжүүлэх бүрт ПИН код шаардлагатай. Энэ нь хугацаа хэтрүүлэхээс ч илүү аюулгүй юм.

√ T4.3 Хурууны хээ нэмсэн тохиолдолд програм нь хурууны хээгээр баталгаажуулалтыг идэвхгүй болгоно.

x T4.4 Мөнгө шилжүүлэг гэх мэт эмзэг хүсэлтүүдийг MITM проксигээр дахин тоглуулах боломжтой.

3.3.5. M5: Криптограф хангалтгүй

x T5.1 Аппликейшн нь сул MD5 болон SHA1 хэш алгоритмууд болон анхдагч санамсаргүй тоо үүсгэгчийг ашигладаг.
MD5 in file com/appsflyer/internal/ai.java:
MessageDigest instance = MessageDigest.getInstance("MD5");
SHA-1 in file u/b/a/a/o/b/j.java:
MessageDigest instance = MessageDigest.getInstance("SHA-1");
Random generator in file c/g/a/c/s.java:
Random random = new Random();

√ T5.2 HTTPS хүсэлтийг Burp Proxy-ээр таслан зогсоосноор тухайн аппликешн холбогдож буй серверийг тодорхойлсон. Тодорхойлогдсон серверийн TLS тохиргоог Qualys SSL Labs [12] ашиглан туршсан . Нийт үнэлгээ нь A+ байна.

√ T5.3 Аппликейшний HTTPS хүсэлтийг Burp Proxy-ээр таслан зогсоосноор зарим эмзэг хүсэлтийн хэсэг шифрлэгдсэн болох нь ажиглагдсан.

Гэсэн хэдий ч, одоогийн үлдэгдэл гэх мэт эмзэг өгөгдөлтэй зарим хариултууд шифрлэгдээгүй, баталгаажуулаагүй тул хортой халдлага үйлдэхийн тулд тэдгээрийг өөрчлөх боломжтой байсан. Туршилтын явцад серверийн хариу үйлдэл хийгдсэн бөгөөд хэрэглэгчийн одоогийн үлдэгдэл програм дээр харагдаж байгаа нь өөрчлөгдсөн

3.3.6. M8: Кодыг өөрчлөх

√ T8.1 Програм нь root-той Android төхөөрөмж дээр ажилладаггүй.

3.3.7. M9: Урвуу инженерчлэл

√ T9.1 Аппликешны кодыг бүдгэрүүлсэн байна.

4. ДҮГНЭЛТ

Энэ арга нь хэрэглээний кодын урвуу инженерчлэлийг шаарддаг тул програмын логикийг шинжлэхийг оруулаагүй болно. Туршилтанд хамрагдсан бүх гурван програмууд нь кодын бүдүүвчийг ашигладаг бөгөөд энэ нь урвуу инженерчлэлийг ихээхэн хүндрүүлдэг.

4.1. Үр дүнг үнэлэх

Бид програмын логикийг задлан шинжилдэггүй тул бүтэлгүйтсэн тестийн үр нөлөөг тооцоолоход хэцүү байсан. Жишээлбэл, нууцлалтай криптографийн үйлдлүүд илэрсэн нь нууц мэдээллийг аюулгүйгээр шифрлээгүй гэсэн үг биш юм. Өөр нэг жишээ бол App1 нь HTTPS-ээр дамжуулж буй гүйлгээний дэлгэрэнгүй мэдээллийг (нэр, дүн) шифрлэдэггүй явдал юм. Аппликешн нь гэрчилгээний бэхэлгээг ашигладаг тул мэдээллийг өрсөлдөгчид саатуулах боломж хязгаарлагдмал байдаг.

Гэсэн хэдий ч бүх туршилтууд нь санхүүгийн хэрэглээнд дагаж мөрдөх шилдэг туршлагуудтай холбоотой. Тиймээс үр дүнг програмууд нь шилдэг туршлагын дагуу бүтээгдсэн эсэхийг стандартчилсан үнэлгээ болгон унших ёстой. Аппликешн нь тодорхой халдлагад өртөмтгий эсэхийг нэмэлт судалгаагүйгээр туршилтын үр дүнгээс дүгнэх боломжгүй.

4.2. FIGI SIT DFS аюулгүй байдлын баталгааны тогтолцоотой харьцуулах

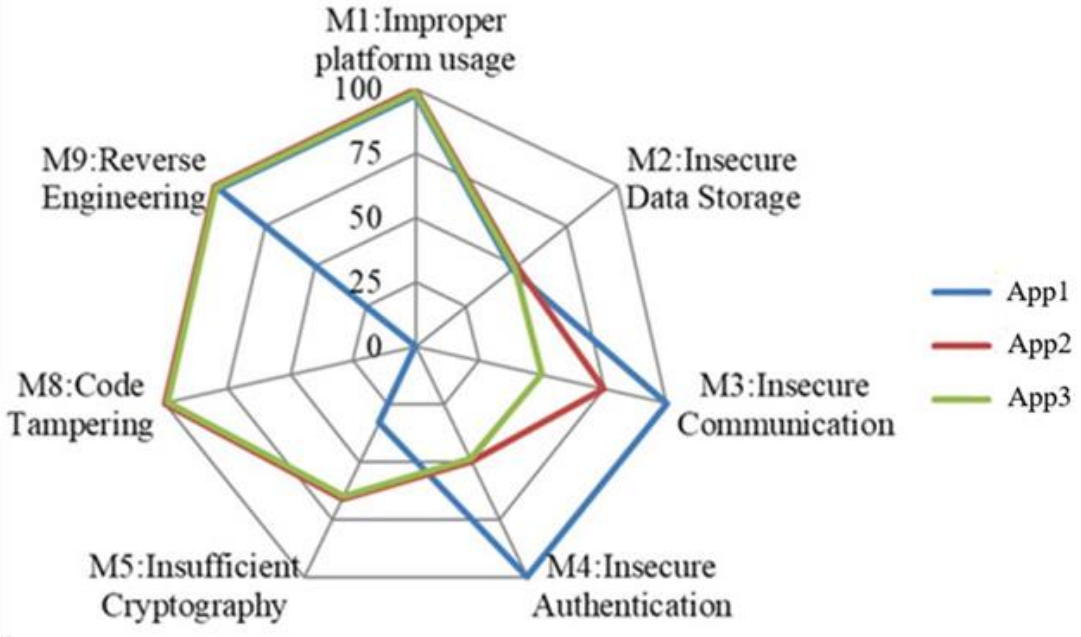
Санхүүгийн хүртээмжийн дэлхийн санаачилга (FIGI)-ын Аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг нь ДСҮ-ний аюулгүй байдлын баталгааны тогтолцоог [13] . ДСҮ-ний аюулгүй байдлын баталгааны хүрээний тайлангийн 9-р бүлэгт аюулгүй байдлын шилдэг туршлагын таван ангиллын загвараар дамжуулан өгсөн. Дараах хүснэгтэд санал болгож буй аргын 18 туршилтыг шилдэг туршлагын таван ангилалд хамааруулж харуулав.

DFS Assurance Framework-ийн шилдэг туршлага	**Холбогдох тестүүд**
9.1 Төхөөрөмжийн бүрэн бүтэн байдал	T1.2 Android: дибаг хийх боломжтой T1.4 Аюултай зөвшөөрөл T8.1 Програм нь үндсэн тохиргоотой төхөөрөмж дээр ажиллахаас татгалзах ёстой
9.2 Харилцаа холбооны аюулгүй байдал, гэрчилгээтэй ажиллах	T3.1 Програм нь зөвхөн HTTPS холболтыг ашиглах ёстой T3.2 Аппликешн нь итгэгдээгүй гэрчилгээ бүхий машин дундах халдлагыг илрүүлэх ёстой T3.3 Аппликешн нь итгэмжлэгдсэн гэрчилгээгээр машин дундах халдлагыг илрүүлэх ёстой T3.4 Апп манифест нь тодорхой текст урсгалыг зөвшөөрөх ёсгүй T5.1 Апп нь аюултай крипто командыг ашиглах ёсгүй T5.2 HTTPS холболтыг шилдэг туршлагын дагуу тохируулах хэрэгтэй T5.3 Аппликешн нь HTTPS-ээр илгээгдсэн нууц мэдээллийг шифрлэх ёстой
9.3 Хэрэглэгчийн баталгаажуулалт	T4.1 Нууц мэдээлэлд хандахын өмнө баталгаажуулалт шаардлагатай T4.2 Аппликешн идэвхгүй байх хугацаатай байх ёстой T4.3 Хуруугы хээ нэмсэн тохиолдолд хуруугы хээгээр баталгаажуулалтыг идэвхгүй болгох шаардлагатай
9.4 Мэдээллийн аюулгүй ажиллагаа	T1.1 Android: зөвшөөрөл нөөцлөх T1.3 Android: суулгах байршил T2.1 Android.зөвшөөрөл.WRITE_EXTERNAL_STORAGE T2.2 Дэлгэцийн агшин(Screenshot)-г идэвхгүй болгож байна
9.5 Аюулгүй програм хөгжүүлэлт	T9.1 Програмын кодыг бүдэгрүүлсэн байх ёстой

4.3. Үр дүнгийн хураангуй

Туршилтын үр дүнг Зураг 4-т нэгтгэн харуулснаар энэхүү тайлангаа дуусгаж байна. Туршилтын явцад ноцтой эмзэг байдал илрээгүй. Гэсэн хэдий ч хоёр үндсэн нөхцөл тогтоогдсон.

Зураг 4 – Туршилтын үр дүнгийн радарын график (радиаль тэнхлэг нь туршсан шилдэг туршлагын хувийг заана)



a) Хувийн түгжээг тайлахад ямар ч ПИН код шаардлагагүй App2 дахь түлхүүр (PUK).

b) App3 нь HTTPS-ээр солилцсон өгөгдлийн нэмэлт шифрлэлтийг ашигладаггүй.

Нэмэлт програмуудыг турших нь харьцуулах илүү том суурийг бий болгож, туршилтыг нарийн тохируулах боломжуудыг олгоно.

Төгсгөлийн тайлбарууд

1 https://owasp .org

2 https:// owasp .org/ www -project -mobile -top -10/

3 https:// хөгжүүлэгч .android .com/ guide/ topics/ manifest/ application -element #allowbackup

4 https:// хөгжүүлэгч .android .com/ guide/ topics/ manifest/ application -element #debug

5 https:// хөгжүүлэгч .android .com/ guide/ topics/ manifest/ manifest -element #install

6 https:// хөгжүүлэгч .android .com/ лавлагаа/ android/ view/ WindowManager .LayoutParams #FLAG _SECURE

7 MD5 ба SHA-1 нь мэдээллийн бүрэн бүтэн байдлыг хамгаалахад, RC4, DES, 3DES, Blowfish болон ECB нь нууцлалыг хамгаалахад ашиглагддаг бол санамсаргүй генераторууд нь бүрэн бүтэн байдал, нууцлал болон бусад шинж чанаруудыг хамгаалах түлхүүрүүдийг үүсгэхэд ашиглагддаг.

8 https:// www .ssllabs .com/ ssltest/ [9] https:// www .ssllabs .com/ ssltest/ [10] https:// www .ssllabs .com/ ssltest/

11 https:// www .guardsquare .com/ en/ products/ dexguard

12 https:// www .ssllabs .com/ ssltest/

13 https:// www .itu .int/ en/ ITU -T/ extcoop/ figisymposium/ Documents/ ITU _SIT _WG _Technical %20report %20on %20Digital %20Санхүү %20Үйлчилгээ %20Аюулгүй байдал %20Баталгаа %20Framework _f .pdf