Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάλυση της ασφάλειας εφαρμογών γνωριμιών σε κινητά τηλέφωνα** **Analysis of Security in Mobile Dating Applications**
Ονοματεπώνυμο Φοιτητή	**Τσιρώνης Βασίλειος - Μαντούζας**
Πατρώνυμο	**Χαράλαμπος**
Αριθμός Μητρώου	**ΜΠΣΠ/13116**
Επιβλέπων	**Πατσάκης Κωνσταντίνος, Λέκτορας**

Ημερομηνία Παράδοσης **Απρίλιος 2016**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πατσάκης Κωνσταντίνος Λέκτορας	Αλέπης Ευθύμιος Λέκτορας	Τσιχριντζής Γεώργιος Καθηγητής

Περίληψη

Η ραγδαία ανάπτυξη του Διαδικτύου τα τελευταία χρόνια είναι γεγονός. Νέες ιστοσελίδες, υπηρεσίες και εφαρμογές που χρησιμοποιούν το Διαδίκτυο δημιουργούνται καθημερινά. Ακόμα και η πρόσβαση σε αυτό είναι πια πολύ εύκολη μέσω των κινητών συσκευών (κινητά τηλέφωνα/tablets κ.α.) που παρέχουν αυτήν την πρόσβαση.

Μία διαδεδομένη κατηγορία εφαρμογών που κάνουν χρήση του Διαδικτύου, έχει ως σκοπό την γνωριμία ανθρώπων. Με στοιχεία που προτείνουν στον κάθε χρήστη άλλα άτομα με βάση προσωπικά ενδιαφέροντα, ηλικία, εθνικότητα, την πραγματική τοποθεσία του κάθε χρήστη και πολλά άλλα, οι εφαρμογές γίνονται ελκυστικές και χρησιμοποιούνται από έναν τεράστιο αριθμό ανθρώπων.

Τέτοιες εφαρμογές μπορεί να αποθηκεύουν σημαντικές πληροφορίες από τους χρήστες, που περιλαμβάνουν προσωπικά στοιχεία (όπως όνομα ή διεύθυνση), φωτογραφίες τους και τις σεξουαλικές τους προτιμήσεις. Είναι αμφίβολο όμως το αν οι εφαρμογές αυτές είναι υλοποιημένες έτσι ώστε να παρέχουν την ασφάλεια που θα έπρεπε να παρέχουν στους χρήστες τους.

Στην εργασία αυτή μελετάται η ασφάλεια εφαρμογών σε κινητές συσκευές, οι οποίες είναι σχετικές με γνωριμίες (dating). Οι συγκεκριμένες εφαρμογές που εξετάστηκαν είναι κυρίως ευρέως γνωστές στο είδος τους. Χρησιμοποιώντας τέτοιες εφαρμογές είναι πιθανό να μην φαίνονται κίνδυνοι σε θέματα ασφάλειας και ευαίσθητων δεδομένων, αλλά αν κοιτάξουμε τα πακέτα δεδομένων που διακινούνται από και προς αυτές, βλέπουμε και τι κινδύνους μπορεί να κρύβει πραγματικά κάποια εφαρμογή.

Μελετήθηκε ένας συγκεκριμένος αριθμός τέτοιων εφαρμογών και σαν αποτέλεσμα της εργασίας έχουμε την αρίθμηση όλων των προβλημάτων/κινδύνων που βρεθήκαν σε αυτές. Βλέπουμε συγκεκριμένα τι προβλήματα υπάρχουν με τα δεδομένα που μεταφέρει η κάθε εφαρμογή, και πώς αυτά μπορεί να αποτελέσουν κάποια τρωτότητα σε θέματα ασφαλείας. Έπειτα από την ανάλυση αυτών των προβλημάτων θα κατανοήσουμε σαν σύνολο το πόσο ασφαλείς είναι αυτές οι εφαρμογές.

Abstract

The growth of the Internet within the last years is a fact. On a daily basis, new Internet-based websites, services and application are created. In addition, the access to the Internet has become way easier through smart mobile devices (such as mobile phones/tablets etc.).

A widely known category of applications that do use the Internet has a purpose of connecting people in a way similar of a date. Most of these applications are implemented in a way that a user can search people that fit in a specific category regarding age, nationality, personal interests, the real location of a user, etc. With attractive features like that, these applications are growing more and more in popularity.

The information that these application get from their users varies and can contain personal information (like real names and addresses), photos of themselves, and their sexual preferences. It is doubtful though that they provide the necessary security to their users and that their information is protected.

In this work we study the security of dating applications used in mobile devices. Most of the applications used in this study are the currently most known in their category. By simply using dating applications, they may not seem to be dangerous in revealing information that they should not, but if we study the actual packets that are transmitted through them, we can clearly find out potential issues in terms of their security.

A specific number of dating applications is studied in this work and as a result we provide a list of all security issues that were found. We analyze specifically what are those issues and how each one of them can result in a risk of the security of a user. After an extended analysis of those issues we will get an idea of whether dating applications are really safe to use or not.

Περιεχόμενα

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΕΣ

Κεφάλαιο 1ο

1 Εισαγωγή

Η χρήση των ηλεκτρονικών υπολογιστών τα τελευταία χρόνια γινόταν και συνεχίζει να γίνεται όλο και πιο διαδεδομένη. Σε αυτό έχει συμβάλει και το Διαδίκτυο, το οποίο μέσα σε όλα τα πλεονεκτήματα του που μπορεί να προσφέρει, παρέχει πρόσβαση σε έναν αμέτρητο αριθμό πληροφοριών, σε διάφορες χρήσιμες υπηρεσίες αλλά και σε ιστότοπους ή εφαρμογές που προορίζονται για διασκέδαση και ψυχαγωγικούς σκοπούς. Με την ανάπτυξη της τεχνολογίας σε πολλούς τομείς που αφορούν ακόμα και τις κινητές συσκευές, η πρόσβαση στο Διαδίκτυο έχει γίνει πολύ πιο εύκολη από οπουδήποτε βρίσκεται κάποιος με μία απλή συσκευή (tablet, κινητά τηλέφωνα, κ.α.).

Σαν συνέχεια, οι παροχές και τα δεδομένα του Διαδικτύου έπρεπε με διάφορους τρόπους να προσαρμοστούν σε αυτές τις συσκευές, και σε αυτό έχουν βοηθήσει τα σχετικά πρόσφατα λειτουργικά συστήματα που χρησιμοποιούν οι κινητές συσκευές που αναφέρθηκαν πιο πάνω (android, iOS, κ.α.). Κάτι που παρέχουν αυτά τα λειτουργικά συστήματα είναι ένας τεράστιος αριθμός εφαρμογών, οι οποίες πιθανώς να συνδέονται ακόμα και με το Διαδίκτυο ώστε να προσφέρουν τα πλεονεκτήματα του Διαδικτύου με έναν πιο εύκολο και άμεσο τρόπο. Η συγκεκριμένη εργασία ασχολείται αποκλειστικά με έναν τύπο τέτοιων εφαρμογών, και συγκεκριμένα με εφαρμογές γνωριμιών.

Η προσέγγιση της εργασίας σε αυτές τις εφαρμογές είναι τέτοιος έτσι ώστε να βρεθούν ‘αρνητικά’ στοιχεία αυτών των εφαρμογών, για να εξετάσουμε έτσι το πόσο ασφαλείς είναι γενικά, συγκεκριμένα τι θέματα ασφαλείας υπάρχουν σε αυτές και συμπερασματικά να δούμε τι πρέπει να προσέχουμε όταν χρησιμοποιούμε τέτοιου είδους εφαρμογές. Πριν την απότομη διάδοση των κινητών συσκευών, αντίστοιχοι ιστότοποι και διαδικτυακές υπηρεσίες παρείχαν την δυνατότητα γνωριμίας μεταξύ ανθρώπων.

Η εφαρμογές που εξετάστηκαν είναι συγκεκριμένα από κινητές συσκευές διότι μέσα από αυτές προκύπτουν θέματα ασφαλείας που μπορεί να μην προέκυπταν από έναν ηλεκτρονικό υπολογιστή. Ας σκεφτούμε για τώρα το ότι για παράδειγμα εφαρμογές των κινητών τηλεφώνων μπορούν να εντοπίσουν εύκολα την τοποθεσία του χρήστη τους μέσω GPS, ή ακόμα και ότι κάθε εφαρμογή κατά την εγκατάσταση της ζητάει κάποια δικαιώματα που θα έχει στο κινητό που εγκαθίσταται.

Συγκεκριμένα σε αυτή την εργασία υπάρχει πρακτική μελέτη εφόσον έγινε χρήση εφαρμογών γνωριμιών, και χρησιμοποιήθηκαν τα παρακάτω εργαλεία/ιστότοποι για να βοηθήσουν στο να βρεθούν τρωτά τους σημεία σε θέματα ασφαλείας, τα οποία θα αναφερθούν αναλυτικά σε επόμενο κεφάλαιο.

- Fiddler [1]
- SSL Server Test [2]
- Mobile Security Framework (MobSF) [3]

1.1 Περιγραφή του υπό μελέτη προβλήματος

Η τεχνολογία στις κινητές συσκευές τα τελευταία χρόνια έχει τεράστια άνοδο μιας και όλο και περισσότερος κόσμος ανταποκρίνεται σε αυτές τις εξελίξεις και έχει βάλει στη ζωή του τις

τεχνολογίες αυτές. Νέες υπηρεσίες και εφαρμογές δημιουργούνται συνεχώς για τις κινητές συσκευές που πολλές φορές έχουν σκοπό να υποκαταστήσουν ενέργειες και καταστάσεις της πραγματικής ζωής.

Ένα τέτοιο χαρακτηριστικό παράδειγμα είναι οι εφαρμογές γνωριμιών, που δημιουργούν έναν εντελώς διαφορετικό τρόπο για γνωριμίες από τον συνηθισμένο. Οι εφαρμογές αυτές έχουν μεγάλη απήχηση, είναι πάρα πολλές σε αριθμό, και οι πιο πολλές είναι αρκετά ελκυστικές στην χρήση τους και τον τρόπο που λειτουργούν.

Υπάρχουν όμως θέματα στην ασφάλεια αυτών των εφαρμογών, που αφορούν το τι προσωπικά δεδομένα μπορούν να διαρρεύσουν, μέχρι ακόμα και την διαρροή της επακριβούς τοποθεσίας μας σε κάποια χρονική στιγμή. Ίσως αυτές οι πληροφορίες να μην γίνονται γνωστές σε όλους όσους χρησιμοποιούν την ίδια εφαρμογή με εμάς, ή ίσως να μην είναι τόσο ‘σημαντικό’ για κάποιους το να φανούν κάποια βασικά τους προσωπικά δεδομένα, το σίγουρο όμως είναι πως οποιαδήποτε πληροφορία μας όταν μπορεί να διαρρεύσει, ειδικά χωρίς να το γνωρίζουμε εμπιστευόμενοι την κάθε εφαρμογή που χρησιμοποιούμε, μπορεί να μας θέσει ακόμα και σε σοβαρό κίνδυνο.

1.2 Σκοπός και στόχοι της εργασίας

Έχοντας αναφέρει γενικά ότι οι εφαρμογές γνωριμιών στις κινητές συσκευές μπορούν να αποτελέσουν σοβαρό κίνδυνο για τους χρήστες τους, μπορούμε να πούμε ότι οι στόχοι της εργασίας περιλαμβάνουν τα ακόλουθα:

1. Η χρήση ενός συγκεκριμένου αριθμού εφαρμογών σχετικές με γνωριμίες με σκοπό την εύρεση στοιχείων που θεωρούνται μη ασφαλή με τον οποιονδήποτε τρόπο για τους χρήστες της κάθε μιας από αυτές
2. Η αναλυτική καταγραφή των σφαλμάτων που βρέθηκαν χρησιμοποιώντας αυτές, και το πώς προκύπτουν αυτά τα σφάλματα
3. Η σύγκριση αυτών των σφαλμάτων μεταξύ των εφαρμογών που εξετάστηκαν, με ιδανικό σκοπό την προσοχή στον προγραμματισμό τέτοιων μελλοντικών και τωρινών εφαρμογών
4. Η παρουσίαση των σφαλμάτων που βρέθηκαν με τρόπο ώστε οι χρήστες των εφαρμογών να καταλάβουν πώς μπορούν να μειώσουν τον κίνδυνο που μπορεί να τους προκληθεί

1.3 Εργαλεία που χρησιμοποιήθηκαν (αναφορικά)

Τα εργαλεία που χρησιμοποιήθηκαν στην υλοποίηση της εργασίας που αναφέρονται εδώ και θα αναλυθούν σε επόμενο κεφάλαιο είναι τα εξής:

1.3.1 Fiddler

Είναι το εργαλείο με το οποίο ελέγχουμε το περιεχόμενο των πακέτων που διακινούνται από και προς την κάθε εφαρμογή, μεταξύ αυτής και του Διαδικτύου.

1.3.2 SSL Server Test

Είναι ιστότοπος που δίνοντας του ένα domain name (που χρησιμοποιείται για ανταλλαγή δεδομένων μέσω κάποιας εφαρμογής), ελέγχει το πόσο ασφαλής είναι.

1.3.3 Mobile Security Framework (MobSF)

Είναι εργαλείο που ελέγχει θέματα ασφαλείας ενός αρχείου apk μιας εφαρμογής, παράγοντας στην συνέχεια μία αναφορά κυρίως προγραμματιστικών σφαλμάτων.

1.3.4 DROWN Attack Test

Ένας ιστότοπος που δίνοντας του ένα domain name, μας ενημερώνει αν αυτός ο domain είναι ευάλωτος σε επιθέσεις DROWN.

1.4 Βασικές έννοιες

Στην ενότητα αυτή θα αναφερθούν περιγραφικά μερικές έννοιες που πιθανώς να μην είναι προφανές το τι σημαίνουν.

1.4.1 Λειτουργικό σύστημα Android

Είναι ένα από τα πιο γνωστά λειτουργικά συστήματα που χρησιμοποιεί ένας τεράστιος αριθμός κινητών συσκευών. Οι εφαρμογές που έχουν εξεταστεί σε αυτή την εργασία, είναι εφαρμογές φτιαγμένες για το συγκεκριμένο λειτουργικό σύστημα.

1.4.2 Εφαρμογές γνωριμιών

Αναφέρονται στον συγκεκριμένο τύπο εφαρμογών που εξετάζει η εργασία, και σκοπός τους είναι οι γνωριμίες ατόμων με την χρήση αυτών των εφαρμογών. Μπορεί η χρήση τους να είναι απλή (όπως για παράδειγμα εφαρμογές που δείχνουν σε έναν χρήστη άλλους πιθανούς χρήστες που είναι όλοι σε κοντινή απόσταση μεταξύ τους) ή και πιο περίπλοκη (έχοντας εφαρμογές που μοιάζουν αρκετά με social media, που ο κάθε χρήστης έχει ένα προφίλ που παρουσιάζει τον εαυτό του).

1.4.3 Ευαίσθητα (και μη) προσωπικά δεδομένα

Οι δύο κατηγορίες μαζί αναφέρονται γενικά σε δεδομένα ενός ατόμου που τον διαχωρίζουν από τους υπόλοιπους, και πιθανώς να μην πρέπει να είναι δημόσια. Συγκεκριμένα τα προσωπικά δεδομένα περιγράφουν ένα άτομο (πχ όνομα – επώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση, ενδιαφέροντα). Τα ευαίσθητα προσωπικά δεδομένα αναφέρονται κυρίως σε φυλετική προέλευση ενός ατόμου, θρησκευτικές πεποιθήσεις, θέματα υγείας, ακόμα και σε ζητήματα της ερωτικής του ζωής.

1.4.4 Πακέτα Δεδομένων

Η επικοινωνία μεταξύ μίας εφαρμογής και του Διαδικτύου γίνεται με τα πακέτα δεδομένων. Όλες οι πληροφορίες που ανταλλάσσονται είναι δομημένες σε συγκεκριμένη μορφή ώστε να είναι εφικτή η επικοινωνία μεταξύ των εφαρμογών και του Διαδικτύου. Αυτή η δομημένη μορφή των δεδομένων είναι συγκεκριμένα τα πακέτα δεδομένων.

1.4.5 Http/Https

Αυτά τα δύο είναι πρωτόκολλα επικοινωνίας με το Διαδίκτυο (HyperText Transfer Protocol, και HyperText Transfer Protocol Secure). Η διαφορά τους είναι ότι το Https θεωρείται πιο ασφαλές, μιας και τα δεδομένα που ανταλλάσσονται με το Διαδίκτυο είναι κρυπτογραφημένα. Άρα είναι πολύ βασικό το να ανταλλάσσονται δεδομένα μίας εφαρμογής που διακινεί με κάποιον τρόπο πραγματικά δεδομένα ενός ανθρώπου με το πρωτόκολλο Https, ώστε αν κάποιος τρίτος καταφέρει να έχει πρόσβαση στα πακέτα που ανταλλάσσονται, να μην μπορεί να αναλύσει το περιεχόμενο τους.

1.4.6 SSL

Το SSL (Secure Sockets Layer) είναι κάποιο πιστοποιητικό που σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση δεδομένων στο Διαδίκτυο. Είναι αυτό που στην ουσία καθιστά ασφαλή την σύνδεση μεταξύ ενός browser και ενός web server που χρειάζεται η ανταλλαγή των δεδομένων να γίνει με κρυπτογράφηση.

1.4.7 Permission (μιας εφαρμογής σε μια κινητή συσκευή)

Οι εφαρμογές που είναι φτιαγμένες σε λειτουργικά συστήματα android, κατά την εγκατάσταση τους ζητούν από αυτόν που εγκαθιστά την εφαρμογή στην εκάστοτε κινητή συσκευή να μπορούν να έχουν κάποιου είδους πρόσβαση στην συσκευή. Αυτό το είδος πρόσβασης μπορεί να αφορά την ανάγνωση των επαφών που βρίσκονται στη συσκευή που εγκαθίσταται η εφαρμογή, την πρόσβαση στα αρχεία της συσκευής, την επεξεργασία αρχείων της συσκευής, και πολλά άλλα. Ανάλογα όμως με το επίπεδο πρόσβασης που έχει η κάθε εφαρμογή μπορούν να προκύψουν διάφορα θέματα ασφαλείας.

1.5 Παραδοτέα της εργασίας

Τα στοιχεία και τα παραδοτέα που συμπεριλαμβάνονται στο σύνολο αυτής της εργασίας είναι τα εξής:

1. Το παρόν έντυπο κείμενο της πτυχιακής εργασίας
2. Τα αποτελέσματα διακίνησης δεδομένων από το λογισμικό Fiddler που βοήθησε στην ανάλυση των πακέτων που μεταφέρει η κάθε εφαρμογή από και προς το Διαδίκτυο
3. Τα αρχεία apk της κάθε εφαρμογής που αναλύθηκε στην εκάστοτε έκδοση τους
4. Τα reports από τα SSL Server Tests που χρησιμοποιήθηκαν για τις εφαρμογές που χρησιμοποιούν το πρωτόκολλο επικοινωνίας Https και συγκεκριμένα για τον έλεγχο του domain name που απευθύνεται η κάθε εφαρμογή, από τον ιστότοπο www.ssllabs.com/ssltest/ .
5. Τα reports από το εργαλείο Mobile Security Framework (MobSF) που ελέγχουν θέματα ασφαλείας σε αρχεία apk. Το αρχείο αυτό παρέχεται δωρεάν στον ιστότοπο www.github.com/ajinabraham/Mobile-Security-Framework-MobSF .

1.6 Δομή της εργασίας

Στη συνέχεια τα κεφάλαια που θα ακολουθήσουν θα αφορούν τα εξής:

- Επισκόπηση χώρου της εργασίας, όπου περιγράφεται το πώς επικοινωνεί μία εφαρμογή με έναν server, και πώς αυτό χρησιμοποιήθηκε για αυτή την εργασία
- Εφαρμογές που εξετάστηκαν, όπου αναλύονται όλες οι εφαρμογές που εξετάστηκαν και θα αναφερθούν τα σφάλματα ασφάλειας που βρέθηκαν στην κάθε μία
- Συγκεντρωτικά στοιχεία για όλες τις εφαρμογές, όπου είναι συγκεντρωμένα τα στοιχεία όλων των εφαρμογών που εξετάστηκαν
- Χρήση των εργαλείων που χρησιμοποιήθηκαν, όπου αναλύονται τα βασικότερα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση της εργασίας
- Συμπεράσματα, όπου αναφέρονται τα συμπεράσματα της εργασίας
- Βιβλιογραφικές πηγές

1.7 Σχετική Δουλειά

Έχουν γίνει παρόμοιες δουλειές πάνω σε θέματα ασφαλείας εφαρμογών κινητών συσκευών. Το άρθρο ‘’Privacy and Security for Multimedia Content shared on OSNs’’ [1] εξετάζει διαδικτυακά κοινωνικά δίκτυα. Σε τέτοια δίκτυα διακινείται συνήθως ένας τεράστιος αριθμός πολυμέσων (κυρίως εικόνες και βίντεο χρηστών) από έναν μεγάλο αριθμό χρηστών. Είναι λογικό να παρέχεται κάποιο είδος ασφάλειας σε τέτοια προσωπικά δεδομένα, αυτό όμως το άρθρο αναγνωρίζει σφάλματα ασφαλείας σε τέτοια δίκτυα που αφορούν την έκθεση των πολυμέσων που χρησιμοποιούν, και αναφέρει πιθανές λύσεις σε αυτά τα σφάλματα.

Το άρθρο ‘’Playing Hide and Seek with Mobile Dating Applications’’ [2] αναφέρεται σε εφαρμογές γνωριμιών σε κινητές συσκευές οι οποίες χρησιμοποιούν την πραγματική τοποθεσία του κάθε χρήστη. Με βάση αυτή τη τοποθεσία, η εφαρμογή παρουσιάζει σε έναν χρήστη άλλους ανθρώπους που βρίσκονται κοντά του, και πολλές φορές του δίνεται και η μεταξύ τους απόσταση αλλά όχι η ακριβής τοποθεσία κάποιου χρήστη. Σε κάποιες συγκεκριμένες εφαρμογές που εξετάστηκαν για το σκοπό του άρθρου, εντοπίζεται τρόπος όπου η πραγματική τοποθεσία χρηστών των εφαρμογών μπορεί να διαρρεύσει.

Το άρθρο ‘’Analysis of Privacy and Security Exposure in Mobile Dating Applications’’ [3] όπως και το προηγούμενο άρθρο που αναφέρθηκε εξετάζει εφαρμογές γνωριμιών από κινητές συσκευές, και αναφέρει τρωτά σημεία ασφαλείας που βρέθηκαν, και που μπορεί να εντοπίσει και έναν κακόβουλος χρήστης που θέλει να υποκλέψει προσωπικά δεδομένα άλλων χρηστών.

Αντίστοιχα στο άρθρο ‘’Privacy Risks in Mobile Dating Apps’’ [4] εξετάζονται 9 εφαρμογές και εντοπίζονται αδύναμα σημεία στην ασφάλεια τους. Παραδείγματα από τέτοια τρωτά σημεία είναι πως ένας κακόβουλος χρήστης μπορούσε να ανακτήσει συνομιλίες από άλλους χρήστες, αλλά και διάφορα στοιχεία από χρήστες που βρισκόντουσαν κοντά στον κακόβουλο μπορούσαν να ανακτηθούν.

Το άρθρο ‘’Where’s Wally? Precise User Discovery Attacks in Location Proximity Services’’ [5] εξετάζει όπως και τα υπόλοιπα εφαρμογές γνωριμιών από κινητές συσκευές, εντοπίζοντας όμως σφάλματα που αφορούν συγκεκριμένα τον εντοπισμό της ακριβής τοποθεσίας ενός χρήστη.

Κεφάλαιο 2ο

2 Επισκόπηση του χώρου

Σε αυτό το κεφάλαιο θα αναλυθούν κάποιες έννοιες για την κατανόηση του πώς λειτουργούν οι εφαρμογές στις κινητές συσκευές. Συγκεκριμένα θα περιγραφούν τουλάχιστον θέματα όπως το πώς γίνεται η επικοινωνία μίας εφαρμογής με το Διαδίκτυο και το τι εργαλεία χρησιμοποιήθηκαν για την υλοποίηση της εργασίας, έτσι ώστε να είναι κατανοητή η μέθοδος που ακολουθήθηκε για τον έλεγχο εφαρμογών σχετικά με την ασφάλεια τους.

2.1 Επικοινωνία μεταξύ εφαρμογών και Διαδικτύου

Πολλές από τις εφαρμογές που υπάρχουν για κινητές συσκευές χρησιμοποιούν το Διαδίκτυο για να κάνουν κάποιες προηγμένες λειτουργίες που δεν θα μπορούσαν προφανώς να κάνουν χωρίς τη βοήθεια του Διαδικτύου. Εφόσον η εκάστοτε κινητή συσκευή είναι συνδεδεμένη στο Διαδίκτυο, τότε η κάθε αντίστοιχη εφαρμογή μπορεί εύκολα να κάνει τις καθορισμένες λειτουργίες της.

Οι εφαρμογές αυτές είναι δεδομένο πως θα απευθύνονται σε κάποιους καθορισμένους από αυτές ιστότοπους, που οι τελευταίοι θα εκτελούν τις διαδικασίες όπου απαιτείται η χρήση του Διαδικτύου από την εκάστοτε εφαρμογή. Αυτοί οι ιστότοποι μπορούν εύκολα να παρομοιαστούν με τουςServers, που έχουν και αυτοί συγκεκριμένα κομμάτια κώδικα που εκτελούν, και μεταφέρουν πληροφορίες προς την κάθε εφαρμογή όταν τους ζητηθεί.

2.1.1 Πρωτόκολλα Http και Https

Τα Http [6] και Https [7] είναι δύο πολύ διαδεδομένα πρωτόκολλα επικοινωνίας που χρησιμεύουν στις επικοινωνίες μέσω του Διαδικτύου. Στους φυλλομετρητές κάθε φορά που επισκεπτόμαστε έναν ιστότοπο, είναι σχεδόν σίγουρο ότι στον σύνδεσμο που προσπαθούμε να επισκεφτούμε θα φαίνεται και ένα από αυτά τα δύο πρωτόκολλα επικοινωνίας.

Χαρακτηρίζονται για το ότι λειτουργούν με ‘αιτήματα και απαντήσεις’. Δηλαδή αν μία εφαρμογή επικοινωνεί με έναν server, τότε για κάθε αίτημα που στέλνεται από την εφαρμογή στον server, ο τελευταίος θα δίνει και μία κατάλληλη απάντηση (μοντέλο client – server).

Τα αιτήματα που αναφέρθηκαν, πραγματοποιούν έγκυρες και συγκεκριμένου είδους επικοινωνίες χρησιμοποιώντας ορισμένες μεθόδους. Αυτή τη στιγμή υπάρχουν αρκετές τέτοιες μέθοδοι αλλά όσον αφορά τις πιο βασικές και συνηθισμένες, αλλά και αυτές που βρέθηκαν ακόμα και ως πιο χρήσιμες στην υλοποίηση αυτής της εργασίας, είναι οι εξής:

- GET

Η συγκεκριμένη μέθοδος θέλει και ζητά από έναν server να ανακτήσει, και μόνο να ανακτήσει ορισμένα δεδομένα.

- POST

Η μέθοδος αυτή συνδυάζεται με δεδομένα, για τα οποία μία εφαρμογή μπορεί να ζητά από τον server της να τα αποδεχτεί και ίσως να τα αποθηκεύσει. Τα δεδομένα αυτά μπορεί να είναι για παράδειγμα ένα απλό μήνυμα σε κείμενο, ή ένα σύνολο πληροφορίας που περιέχει πληροφορίες μία φόρμας ενός ιστότοπου, ή ακόμα και ένα αντικείμενο που προορίζεται για να μπει σε μία βάση δεδομένων.

- CONNECT

Αυτή η μέθοδος έχει ως σκοπό την αλλαγή με κάποιο τρόπο της ήδη υπάρχουσας σύνδεσης μεταξύ ενός client και ενός server. Μπορεί για παράδειγμα να δημιουργήσει κανάλια (tunnels) για

την διευκόλυνση της χρήσης του πρωτοκόλλου Https, διαμέσου ενός proxy που χρησιμοποιεί Http.

Ένα παράδειγμα χρήσης της μεθόδου GET είναι το παρακάτω:

GET
/zz_pg_redirect_url.php?mobile_app_webservice=TRUE&web_service_request=zz_pg_searc
h_user_list.php&sess_uid=167268&page_size=10&appVersionName=28&platform_id=1&m
obTimestamp=2015-10-
0318:24:17.731&searchFor=online_now&currentPageNo=1&key=Female HTTP/1.1

το οποίο είναι από μία εφαρμογή γνωριμιών και έχει ως σκοπό την αναζήτηση και την ανάκτηση πληροφοριών από άτομα που χρησιμοποιούν την ίδια εφαρμογή,

και η απάντηση στο παραπάνω αίτημα μπορεί να είναι αυτή:

HTTP/1.1 200 OK

όπου η απάντηση είναι στη ουσία ότι το παραπάνω αίτημα που ζητήθηκε από τον server ολοκληρώθηκε με επιτυχία.

Οι μέθοδοι που αναφέρθηκαν είναι πράγματι πολύ συχνές στην λειτουργία εφαρμογών γνωριμιών, μιας και μια βασική λειτουργία είναι η αναζήτηση υπόλοιπων χρηστών μιας εφαρμογής με βάση κάποια κριτήρια που θα επιθυμεί κάποιος.

Κάποιες ακόμα μέθοδοι που υπάρχουν, αναφέρονται ονομαστικά και είναι οι

- HEAD
- PUT
- DELETE
- TRACE
- OPTIONS
- PATCH

Σχετικά με τις διαφορές των 2 πρωτοκόλλων. Γενικά τα δύο πρωτόκολλα χρησιμοποιούν διαφορετικό port, και τα URL που τα χρησιμοποιούν περιέχουν τις λέξεις ‘http’ ή ‘https’ ανάλογα με το ποιο πρωτόκολλο χρησιμοποιείται για την κάθε επικοινωνία.

Η πρακτική διαφορά τους όμως είναι πως το πρωτόκολλο Http δεν χρησιμοποιεί κρυπτογράφηση στις πληροφορίες που μεταφέρει, και έτσι αυτές οι πληροφορίες μπορούν πανεύκολα να υποκλαπούν σε περίπτωση που κάποιος ‘κρυφακούσει’ κάποια επικοινωνία σε Http. Το πρωτόκολλο Https αντίθετα, θεωρείται ότι προστατεύει από τέτοιες επιθέσεις για υποκλοπή στοιχείων, αφού κρυπτογραφεί τις πληροφορίες που μεταφέρονται.

Οι πληροφορίες που μεταφέρονται συγκεκριμένα στις εφαρμογές γνωριμιών, είναι λογικό ότι μπορεί να είναι ιδιαίτερα προσωπικές, από άποψη προσωπικών στοιχείων ενός ατόμου (όνομα, διεύθυνση κτλ.), στοιχείων της τοποθεσίας του, και φυσικά λεπτομερειών σε θέματα σεξουαλικής φύσης ενός ατόμου. Σε αυτές τις περιπτώσεις είναι προφανές ότι η χρήση του πρωτοκόλλου Https που παρέχει κρυπτογράφηση των δεδομένων και παρέχει μια παραπάνω ασφάλεια στις πληροφορίες που μεταδίδονται, είναι καθοριστική για να θεωρείται ότι μια εφαρμογή παρέχει μία ασφάλεια στο απόρρητο του κάθε χρήστη της. Στις περιπτώσεις που δεν γίνει χρήση του πρωτοκόλλου Https, ευαίσθητα προσωπικά είναι εύκολο να υποκλαπούν.

2.1.2 Proxy Server

Ένας proxy server [8] είναι στην ουσία ένας server που λειτουργεί ως ενδιάμεσος στην επικοινωνία μεταξύ ενός client και ενός server. Μία εφαρμογή γνωριμιών για παράδειγμα, μπορεί να συνδεθεί σε έναν proxy server και να ζητήσει από αυτόν οποιαδήποτε πληροφορία, εικόνα κτλ., και στη συνέχεια ο proxy server θα αναλάβει να ζητήσει αυτό που του ζητήθηκε, από τον server που στοχεύει ο client. Η λογική είναι ότι μειώνεται η πολυπλοκότητα στις επικοινωνίες, και αυτές απλοποιούνται.

Στην συγκεκριμένη εργασία χρησιμοποιήθηκε ένας proxy, ανάμεσα στην επικοινωνία των εφαρμογών γνωριμιών και του κάθε server που απευθυνόντουσαν. Κάνοντας το αυτό έγινε εφικτό το να φαίνονται εύκολα όλες οι μέθοδοι επικοινωνίας που χρησιμοποιήθηκαν από τις εφαρμογές, οι πληροφορίες που ζητούνται και μεταφέρονται από και προς τις εφαρμογές, εικόνες χρηστών, και γενικότερα όλα τα πακέτα επικοινωνίας ήταν προσβάσιμα.

2.2 Εργαλεία που χρησιμοποιήθηκαν

2.2.1 Fiddler

Το fiddler [9], είναι ένα εργαλείο γνωστό ως web debugging proxy. Μέσω αυτού μπορούμε να ελέγξουμε τα πακέτα που διακινούνται μεταξύ μίας εφαρμογής και του Διαδικτύου. Άρα τα περισσότερα δεδομένα και τα στοιχεία που θεωρήθηκαν ως αρνητικά σε θέματα ασφαλείας για τις εφαρμογές που εξετάστηκαν, βρέθηκαν μέσω αυτού του εργαλείου.

2.2.2 SSL Server Test

SSL Server Test [10], από το τον ιστότοπο ssllabs.com/ssltest/ . Αυτός ο ιστότοπος βοηθά στον έλεγχο του πόσο ασφαλής είναι ένας domain που θα του δοθεί για έλεγχο. Μέσω του εργαλείου Fiddler μπορούμε να δούμε τις επικοινωνίες μιας εφαρμογής με το Διαδίκτυο. Έτσι μπορούμε να βρούμε και τα βασικά domains της κάθε εφαρμογής που χρησιμοποιεί για την ανταλλαγή δεδομένων. Δίνοντας το κάθε domain name που μας ενδιαφέρει στον παραπάνω ιστότοπο που αναφέρθηκε, αυτός θα κάνει έναν αναλυτικό έλεγχο στον domain και θα μας παράξει ένα αναλυτικό report με όλα τα τρωτά σημεία στην ασφάλεια του domain, βαθμολογώντας τον παράλληλα (σε μορφή A, B, C κτλ). Μερικά χαρακτηριστικά παραδείγματα θεμάτων ασφαλείας που βρέθηκαν είναι ότι ένας domain server:

- Μπορεί να χρησιμοποιεί πιστοποιητικό που για κάποιο λόγο δεν είναι ασφαλές (This server's certificate is not trusted)
- Μπορεί να είναι τρωτός σε Poodle attack (This server is vulnerable to the POODLE attack)
- Μπορεί να έχει θέματα ασφαλείας σε συνδέσεις που πραγματοποιούνται μέσω SSL (This server supports anonymous (insecure) suites)

2.2.3 Mobile Security Framework (MobSF)

Mobile Security Framework (MobSF) [11]. Το συγκεκριμένο εργαλείο έχει ως σκοπό τον αναλυτικό έλεγχο ενός αρχείου apk, δηλαδή στην ουσία, μίας εφαρμογής. Μετά το πέρας του ελέγχου που θα κάνει σε ένα τέτοιο αρχείο, θα παράξει ένα αναλυτικό report που θα περιέχει πληροφορίες σχετικά με την εφαρμογή (πχ. αριθμό έκδοσης της εφαρμογής, τον χώρο που καταναλώνει στο κινητό, και πολλά άλλα). Το βασικότερο όμως είναι το ότι παρέχει πληροφορίες για το τι δεν έχει υλοποιηθεί σωστά προγραμματιστικά και μπορεί να υπάρξει τρωτότητα ασφαλείας. Οι πιο βασικές αλλά όχι οι μοναδικές τέτοιες πληροφορίες που αντλούμε είναι:

- Σχετικές με τα permissions που ζητά μία εφαρμογή. Πιθανώς όλες οι εφαρμογές χρειάζονται permissions για να πραγματοποιήσουν τον σκοπό τους, όμως δεν σημαίνει ότι όλα αυτά τα permissions είναι ασφαλές να τα έχει κάποια εφαρμογή. Έχουμε λοιπόν αναλυτικά αυτά τα permissions μαζί με έναν βαθμό επικινδυνότητας τους, όπως και το τι ακριβώς προκαλούν. Παράδειγμα ανάλυσης ενός permission - *permission: android.permission.WAKE_LOCK, Status: dangerous, Info: prevent phone from sleeping, Description: allows an application to prevent the phone from going to sleep.*
- Σχετικές με το manifest μιας εφαρμογής. Αντίστοιχα με πριν μας παρουσιάζεται το πρόβλημα, ένας βαθμός σοβαρότητας, και μία ανάλυση του πώς ακριβώς δημιουργήθηκε το κάθε πρόβλημα. Παράδειγμα πληροφορίας σε αυτόν τον τομέα – *Issue: Activity (com.plugin.gcm.PushHandlerActivity) is not Protected. [android:exported=true] , Severity: High, Description: An Activity was found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.*
- Σχετικές με την ανάλυση του κώδικα της εφαρμογής. Ακριβώς όπως πριν μας παρουσιάζεται το πρόβλημα, ένας βαθμός σοβαρότητας, και τα αρχεία στα οποία ακριβώς υπάρχει το κάθε πρόβλημα. Και παρόμοια λαμβάνουμε πληροφορίες στην εξής μορφή – *Issue: App can read/write to External Storage. Any App can read data written to External Storage, Severity: High, Files: DirectoryManager.java CameraLauncher.java .*

2.2.4 DROWN Attack Test

Το DROWN (**D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption) αντιπροσωπεύει μία σημαντική τρωτότητα πρωτόκολλων κρυπτογράφησης που χρησιμοποιούνται στο Διαδίκτυο (όπως το Https). Ιστότοποι που χρησιμοποιούν πρωτόκολλα κρυπτογράφησης συνήθως μεταφέρουν πληροφορία που δεν πρέπει κάποιος να υποκλέψει, όπως credentials, αριθμούς πιστωτικών καρτών και πολλά άλλα. Μία επίθεση DROWN σε έναν τέτοιο τρωτό ιστότοπο μπορεί να εκθέσει σημαντικά δεδομένα μιας και ο επιτιθέμενος αποκρυπτογραφεί στην ουσία όλη την κρυπτογραφημένη πληροφορία που διακινείται στον ιστότοπο.

Το DROWN Attack Test [12] μας βοηθά στο να εντοπίσουμε τρωτούς ιστότοπους σε αυτό το είδος επίθεσης.

Κεφάλαιο 3ο

3 Εφαρμογές που εξετάστηκαν

Παρακάτω θα αναλυθούν μια προς μια οι εφαρμογές που εξετάστηκαν, μαζί με τα σφάλματα που βρέθηκαν σχετικά με την ασφάλεια τους.

3.1 Black Dating for Free

Αριθμός έκδοσης: 4.0

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 100.000

Περιγραφή εφαρμογής:

Η Black Dating for Free είναι μία εφαρμογή που αποσκοπεί στην γνωριμία με άτομα από τις Αφρικανικές χώρες και γενικότερα με μελαμψούς ανθρώπους. Κάθε χρήστης δημιουργεί το προφίλ του εισάγοντας γενικές πληροφορίες για αυτόν. Η αναζήτηση χρηστών γίνεται ανά χώρα/περιοχή.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Είναι εμφανές το username που ένας χρήστης κάνει login
- Είναι εμφανές το password που ένας χρήστης κάνει login
- Φαίνεται το email του κάθε χρήστη
- Φαίνεται η ημερομηνία γέννησης των χρηστών
- Φαίνεται η ip μέσω της οποίας συνδέθηκε ένας χρήστης
- Φαίνονται στοιχεία ερωτικής προτίμησης των χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Η εφαρμογή δεν παρέχει καμία ασφάλεια στην μεταφορά δεδομένων αφού χρησιμοποιεί το πρωτόκολλο Http. Σε πακέτα δεδομένων φαίνονται αρκετά προσωπικά στοιχεία, με βασικότερο ίσως όλων τα στοιχεία username, password που κάνει login στην εφαρμογή κάποιος χρήστης. Τα στοιχεία ερωτικής προτίμησης ενός χρήστη φαίνονται μιας και μπορούμε να δούμε στοιχεία όπως τα όρια ηλικίας που έχει μπλοκάρει αυτός, και άλλα είδη χρηστών που έχει μπλοκάρει (πχ καπνιστές κτλ.). Σε περίπτωση επίσκεψης ενός συγκεκριμένου προφίλ ή και σε αποστολή μηνύματος σε ένα συγκεκριμένο προφίλ, το userid αυτού του προφίλ είναι εμφανές στο url που καλείται από την συσκευή μας.

3.2 BoyAhoy

Αριθμός έκδοσης: 4.14.4

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Η Boyahoy είναι μία εφαρμογή που απευθύνεται σε ομοφυλόφιλους άντρες. Δημιουργεί ο κάθε χρήστης ένα προφίλ με τα προσωπικά του στοιχεία, και η αναζήτηση υπόλοιπων χρηστών μπορεί να γίνει βάσει πραγματικής τοποθεσίας.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνεται η χιλιομετρική απόσταση από τους υπόλοιπους χρήστες
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν παρέχεται καμία ασφάλεια στα δεδομένα των χρηστών με την χρήση του πρωτοκόλλου Http. Η χιλιομετρική απόσταση μεταξύ των χρηστών είναι αρκετά ακριβής (πχ 99.8 km). Στα url, σε περιπτώσεις όπως επίσκεψης ενός προφίλ ενός χρήστη, ή ακόμα και σε αποστολή μηνύματος σε αυτόν, είναι εμφανές το userid αυτού του χρήστη.

3.3 Choice of Love

Αριθμός έκδοσης: 2.8

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Η Choice of Love χρησιμοποιεί τα στοιχεία ενός προφίλ (όπως τα ενδιαφέροντα ενός ανθρώπου) ώστε να βρει αντίστοιχα άτομα που τα προτείνει για γνωριμίες. Επίσης μπορεί να δώσει αποτελέσματα χρηστών με βάση την τοποθεσία του κάθε χρήστη.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνεται η ημερομηνία γέννησης των χρηστών
- Φαίνεται η ακριβής τοποθεσία χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Σε αυτή την εφαρμογή τα περισσότερα δεδομένα μεταφέρονται με το πρωτόκολλο Https. Παρόλα αυτά οι εικόνες χρηστών μεταφέρονται με το πρωτόκολλο Http, και τα links αυτών είναι στατικά. Από προσωπικά στοιχεία φαίνεται η ημερομηνία γέννησης χρηστών που δεν είναι κάποιο εμφανές στοιχείο κατά την χρήση της εφαρμογής. Τέλος είναι εμφανής η τοποθεσία χρηστών, εφόσον μπορούμε να δούμε το ακριβές τους γεωγραφικό μήκος και πλάτος πάνω στον χάρτη.

3.4 Christian Dating for Free

Αριθμός έκδοσης: 4.0

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 100.000

Περιγραφή εφαρμογής:

Η Christian Dating for Free είναι μία εφαρμογή που αποσκοπεί στην γνωριμία με άτομα που ακολουθούν την Χριστιανική θρησκεία. Κάθε χρήστης δημιουργεί το προφίλ του εισάγοντας γενικές πληροφορίες για αυτόν. Η αναζήτηση χρηστών γίνεται ανά χώρα/περιοχή. Η εφαρμογή αυτή έχει φτιαχτεί από την ίδια εταιρία με αυτή που δημιουργήθηκε η εφαρμογή Black Dating for Free, και έχουμε πολλά όμοια σφάλματα που θα αναφερθούν αμέσως.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http

- Τα links των εικόνων χρηστών είναι στατικά
- Είναι εμφανές το username που ένας χρήστης κάνει login
- Είναι εμφανές το password που ένας χρήστης κάνει login
- Φαίνεται το email του κάθε χρήστη
- Φαίνεται η ημερομηνία γέννησης των χρηστών
- Φαίνεται η ip που συνδέθηκε ένας χρήστης
- Φαίνονται στοιχεία ερωτικής προτίμησης των χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Τα δεδομένα που μεταφέρονται μέσω της εφαρμογής, μεταφέρονται αποκλειστικά με το πρωτόκολλο Http. Στα πακέτα δεδομένων φαίνονται προσωπικά στοιχεία, με κυριότερα τα στοιχεία username, password που κάνει login στην εφαρμογή κάποιος χρήστης. Τα στοιχεία ερωτικής προτίμησης ενός χρήστη φαίνονται μιας και μπορούμε να δούμε στοιχεία όπως τα όρια ηλικίας που έχει μπλοκάρει αυτός, και άλλα είδη χρηστών που έχει μπλοκάρει (πχ καπνιστές κτλ.). Σε περίπτωση επίσκεψης ενός συγκεκριμένου προφίλ ή και σε αποστολή μηνύματος σε ένα συγκεκριμένο προφίλ, το userid αυτού του προφίλ είναι εμφανές στο url που καλείται από την συσκευή μας.

3.5 Daddyhunt

Αριθμός έκδοσης: 1.0.4

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 100.000

Περιγραφή εφαρμογής:

Η Daddyhunt είναι μία εφαρμογή που απευθύνεται σε ομοφυλόφιλους άντρες που αναζητούν κυρίως άντρες προχωρημένης ηλικίας. Και εδώ υπάρχει η δυνατότητα εύρεσης ατόμων με βάση το πόσο κοντά βρίσκονται οι χρήστες, και παρέχεται και η δυνατότητα ανεβάσματος ‘προσωπικών φωτογραφιών’, με τη λογική πως αυτές δεν είναι εμφανείς σε όλους τους χρήστες.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνεται η ακριβής τοποθεσία χρηστών
- Φαίνονται (κωδικοποιημένα) προσωπικά στοιχεία των χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Η ασφάλεια των δεδομένων είναι ισχνή αφού χρησιμοποιείται στην μεταφορά δεδομένων και εικόνων το πρωτόκολλο Http. Τα links των εικόνων των χρηστών που μπορούμε να βρούμε, είναι στατικά. Η τοποθεσία χρηστών φαίνεται με μεγάλη ακρίβεια βλέποντας το γεωγραφικό μήκος και πλάτος τους πάνω τον χάρτη. Σε ορισμένους χρήστες, μέσω του Fiddler εντοπίστηκαν links ‘προσωπικών εικόνων’ χρηστών, οι οποίες κανονικά θα έπρεπε να φαίνονται μόνο μετά από άδεια που θα έδινε ο χρήστης που κατέχει αυτές τις προσωπικές φωτογραφίες. Τέλος από προσωπικά στοιχεία βλέπουμε την ημερομηνία γέννησης χρηστών, η οποία βέβαια είναι σε κωδικοποιημένη μορφή (πχ μία ημερομηνία γέννησης μπορεί να φαίνεται ως ‘513633600’, κάτι που ίσως δεν θεωρείται σφάλμα αφού δεν είναι ένα προφανές προσωπικό στοιχείο).

3.6 Date me

Αριθμός έκδοσης: 1.5.0.8

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή που μπορεί κάποιος να αναζητήσει χρήστες που βρίσκονται σε μία συγκεκριμένη πόλη/χώρα.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία των χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει χρήση του πρωτοκόλλου Https στην μεταφορά εικόνων ή γενικών δεδομένων, άρα η εφαρμογή δεν μπορεί να θεωρηθεί ασφαλής. Η ημερομηνία γέννησης χρηστών μπορεί να εντοπιστεί εύκολα από τα πακέτα δεδομένων. Επίσης στα url, τουλάχιστον στις περιπτώσεις επίσκεψης ενός προφίλ και σε αποστολή μηνύματος σε έναν χρήστη, φαίνεται το userid του χρήστη αυτού.

3.7 Eharmony

Αριθμός έκδοσης: 2.4.3.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνεται η ακριβής τοποθεσία χρηστών
- Φαίνονται προσωπικά στοιχεία των χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Στην εφαρμογή αυτή χρησιμοποιείται το πρωτόκολλο Https. Στην περίπτωση των εικόνων χρηστών, τα links είναι στατικά. Παρόλο που στην εφαρμογή δεν βλέπουμε ακριβή στοιχεία για την τοποθεσία κάποιου χρήστη, στα πακέτα δεδομένων βλέπουμε την απόσταση μας με κάποιον άλλον χρήστη, όπως και το ακριβές του γεωγραφικό μήκος και πλάτος πάνω στον χάρτη. Στην εφαρμογή ένας χρήστης μπορεί να ανεβάσει φωτογραφίες που να μην είναι εμφανείς στους υπόλοιπους χρήστες, εκτός αν ο πρώτος δώσει την άδεια του για αυτό. Από το Fiddler βρέθηκαν links τέτοιων εικόνων (χωρίς να έχουμε την αντίστοιχη άδεια). Τέλος σε url που καλούνται τουλάχιστον στην περίπτωση επίσκεψης κάποιου χρήστη, το user id αυτού του χρήστη φαίνεται καθαρά.

3.8 Eskimi

Αριθμός έκδοσης: 5.6.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Μία ακόμα εφαρμογή που χρησιμοποιεί μόνο το πρωτόκολλο Http. Σε url που καλούνται τουλάχιστον στην περίπτωση επίσκεψης κάποιου χρήστη, το user id αυτού του χρήστη φαίνεται καθαρά.

3.9 Flirtxchange

Αριθμός έκδοσης: 1.6.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνεται η ακριβής τοποθεσία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Μία ακόμα μη ασφαλής εφαρμογή που δεν χρησιμοποιεί το πρωτόκολλο Https. Το γεωγραφικό μήκος και πλάτος άλλων χρηστών είναι εμφανές στα πακέτα δεδομένων. Τέλος σε url που καλούνται τουλάχιστον στις περιπτώσεις επίσκεψης κάποιου χρήστη και αποστολής μηνύματος, το user id αυτού του χρήστη φαίνεται καθαρά.

3.10 Grindr

Αριθμός έκδοσης: 2.2.4

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 5.000.000

Περιγραφή εφαρμογής:

Μία εφαρμογή που απευθύνεται σε ομοφυλόφιλους άντρες. Είναι μία από τις πιο γνωστές εφαρμογές στο είδος της με έναν μεγάλο αριθμό ανθρώπων που έχουν εγκαταστήσει την εφαρμογή.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά

- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Τα πιο πολλά δεδομένα στην εφαρμογή αυτή μεταφέρονται με την χρήση του πρωτοκόλλου Https, όχι όμως και οι εικόνες χρηστών. Είναι επίσης μέσω url εμφανής η ακριβής τοποθεσία μας, δείχνοντας καθαρά το γεωγραφικό μας μήκος και πλάτος.

3.11 Guyspy

Αριθμός έκδοσης: 4.3.2

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Η Guyspy απευθύνεται αποκλειστικά σε ομοφυλόφιλους άντρες. Η πραγματική τοποθεσία είναι κριτήριο για να προτείνει χρήστες που είναι σε κοντινή απόσταση, και παρέχει και την αποστολή βιντεομηνυμάτων.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται προσωπικά στοιχεία των χρηστών σεξουαλικής φύσης
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Οι εικόνες των χρηστών μεταφέρονται με χρήση του πρωτοκόλλου Http. Το γεωγραφικό μήκος και πλάτος χρηστών φαίνονται εύκολα στα πακέτα δεδομένων. Στα πακέτα φαίνονται επίσης λεπτομέρειες για το τι συγκεκριμένα ψάχνουν οι χρήστες της εφαρμογής (πχ φαίνεται εύκολα ο ‘ρόλος’ της σεξουαλικής τους προτίμησης). Επίσης στα url που καλούνται όταν επισκεπτόμαστε ένα προφίλ, παρόλο που οι πληροφορίες είναι σε Https, το url δείχνει ξεκάθαρα το user id του χρήστη που επισκεφτήκαμε.

3.12 Hawaya

Αριθμός έκδοσης: 1.0.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000

Περιγραφή εφαρμογής:

Μία ακόμα εφαρμογή χωρίς κάποια ιδιαιτερότητα στο είδος γνωριμιών που απευθύνεται. Από τις εφαρμογές που εξετάστηκαν σε αυτή την εργασία, είναι μία από τις εφαρμογές με τους λιγότερους χρήστες.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία για την τοποθεσία χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει ασφάλεια στην μεταφορά των δεδομένων με την χρήση του πρωτοκόλλου Http. Σε χρήστες που πιθανότατα έχουν ενεργοποιήσει το GPS τους και η εφαρμογή είχε πρόσβαση στην

τοποθεσία τους, βλέπουμε την ακριβή τους τοποθεσία (το γεωγραφικό τους μήκος και πλάτος). Υπάρχει μάλιστα και πεδίο ‘accuracy’ στους χρήστες που φαίνεται να απευθύνεται στην τοποθεσία τους που βλέπουμε, και αν είναι ακριβής (με χρήση GPS) ή όχι.

3.13 Hi5

Αριθμός έκδοσης: 6.2.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Κλασική και γνωστή εφαρμογή που δεν είναι περιορισμένη σε κάποιο συγκεκριμένο είδος γνωριμίας.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία σχετικά με την τοποθεσία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Οι εικόνες των χρηστών μεταφέρονται με το πρωτόκολλο Http. Μπορούμε από τα πακέτα δεδομένων να δούμε την ημερομηνία γέννησης χρηστών. Μπορούμε επίσης να δούμε την απόσταση μας από τους άλλους χρήστες, κάτι που δεν βλέπουμε εντός της εφαρμογής, η οποία μεν απόσταση δεν είναι ακριβής, αλλά υπάρχει. Η απόσταση αυτή είναι πάντα ακέραιος αριθμός, άρα όχι απόλυτα ακριβής. Στα url φαίνονται αρκετές προσωπικές πληροφορίες. Όταν επισκεφτούμε ένα προφίλ, στο url που καλείται τότε φαίνεται το user id του χρήστη που επισκεπτόμαστε. Επιπλέον, όταν κάνουμε αναζήτηση χρηστών με κριτήρια που έχουμε ορίσει, τα κριτήρια αυτά (οι προτιμήσεις μας δηλαδή), είναι εμφανή στα αντίστοιχα url, χάνοντας έτσι αρκετά το νόημα της ύπαρξης του πρωτοκόλλου Https.

3.14 Hornet

Αριθμός έκδοσης: 2.0.33

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Η Hornet είναι μία εφαρμογή που απευθύνεται σε ομοφυλόφιλους άντρες.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Το πρωτόκολλο Http χρησιμοποιείται, αλλά μόνο στην μεταφορά εικόνων. Στην περίπτωση επίσκεψης προφίλ κάποιου χρήστη, στο url που καλείται εκείνη τη στιγμή φαίνεται το user id του χρήστη αυτού.

3.15 Hot or Not

Αριθμός έκδοσης: 4.6.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Μία πολύ γνωστή εφαρμογή γνωριμιών, που η κύρια λειτουργικότητα της είναι να προτείνει χρήστες με βάση την απόσταση τους. Για να συνδεθούν δύο χρήστες, πρέπει και οι δύο πρώτα να δηλώσουν ότι ενδιαφέρονται ο ένας για τον άλλον.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http

Ανάλυση σφαλμάτων που βρέθηκαν:

Η Hot or Not ίσως είναι η πιο ασφαλής από αυτές που εξετάστηκαν στην εργασία. Παρόλο που χρησιμοποιείται το πρωτόκολλο Http, τα links των εικόνων που μεταφέρονται είναι δυναμικά. Επίσης τα δεδομένα των χρηστών που μεταφέρονται φαίνονται να είναι κωδικοποιημένα, και δεν φαίνεται να μπορεί να διαρρεύσει οποιαδήποτε πληροφορία κάποιου χρήστη.

3.16 I-am

Αριθμός έκδοσης: 2.54

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία που δεν βλέπουμε στην εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Το πρωτόκολλο Http υπάρχει μόνο για την μεταφορά εικόνων χρηστών. Στην εφαρμογή αυτή οι χρήστες μπορούν να δηλώσουν ότι τους αρέσει ένα προφίλ κάποιου άλλου χρήστη. Σε ένα προφίλ φαίνεται ένας μικρός αριθμός ονομάτων χρηστών που έχουν δηλώσει ότι τους αρέσει το συγκεκριμένο προφίλ. Μέσω των πακέτων δεδομένων φαίνονται όλα τα ονόματα από αυτούς τους χρήστες που έχουν δηλώσει πως τους αρέσει ένα συγκεκριμένο προφίλ. Μπορεί να μην φανερώνεται κάποια ευαίσθητη πληροφορία, αλλά είναι κάτι που δεν φαίνεται στην εφαρμογή και βλέπουμε συγκεκριμένους χρήστες που δηλώνουν κάποια προτίμηση.

3.17 Jaumo

Αριθμός έκδοσης: 3.5.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 5.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Το κριτήριο της απόστασης μεταξύ των χρηστών παίζει ρόλο στην λειτουργία της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Η Jaumo είναι από τις εφαρμογές που χρησιμοποιούν το πρωτόκολλο Https και στην μεταφορά εικόνων αλλά και στην μεταφορά των υπόλοιπων δεδομένων. Το μόνο σφάλμα σε αυτό είναι ότι τα links των εικόνων των χρηστών είναι στατικά. Εκτός αυτού, στοιχεία τοποθεσίας είναι εμφανή βλέποντας το γεωγραφικό μήκος και πλάτος των χρηστών, αλλά και την απόσταση μεταξύ χρηστών. Αυτά τα στοιχεία τοποθεσίας πολλές φορές φαίνονται ως ίδια για πολλούς χρήστες, άρα είναι πιθανό να φαίνονται με βάση την πόλη που βρίσκεται κάποιος. Η εφαρμογή πάντως κάνει προαιρετική χρήση του GPS, άρα και στοιχεία τοποθεσίας πολλών χρηστών είναι ακριβή και αληθή. Όσον αφορά τα url, όταν επισκεπτόμαστε κάποιον χρήστη, το user id αυτού φαίνεται στο url που καλείται εκείνη τη στιγμή.

3.18 Loveplanet.ru

Αριθμός έκδοσης: 2.7.6

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Μία απλή εφαρμογή γνωριμιών, που παρόλο που είναι στην Ρώσικη γλώσσα, έχει αρκετούς χρήστες που την χρησιμοποιούν.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Το θέμα ασφαλείας της χρήσης μόνο του πρωτόκολλο Http υπάρχει και στην εφαρμογή Loveplanet.ru . Τα url είναι το επόμενο πρόβλημα ασφαλείας για την εφαρμογή, μιας και φαίνονται πολλές πληροφορίες από αυτά. Σε περιπτώσεις αποστολής μηνύματος σε κάποιον συγκεκριμένο χρήστη ή ακόμα και αποστολής μηνύματος σε αυτόν, στο url φαίνεται το user id του. Συγκεκριμένα στην περίπτωση αποστολής μηνύματος σε κάποιον χρήστη, το μήνυμα μας φαίνεται ολόκληρο στο αντίστοιχο url.

3.19 Lovoo

Αριθμός έκδοσης: 2.5.5

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Το κριτήριο της απόστασης μεταξύ των χρηστών παίζει ρόλο στην λειτουργία της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή
- Φαίνεται η ακριβής τοποθεσία χρηστών
- Φαίνονται προσωπικά στοιχεία των χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Το πρωτόκολλο Https χρησιμοποιείται μόνο στις εικόνες χρηστών. Η απόσταση από τους υπόλοιπους χρήστες φαίνεται πολύ εύκολα από πεδία που ονομάζονται ‘relativeXposition’ και ‘relativeYposition’ που δείχνουν την σχετική μας απόσταση από κάποιον άλλον χρήστη. Για ορισμένους χρήστες που έχουν κάνει λογαριασμό μέσω του λογαριασμού τους στο facebook, το facebook id τους ήταν εμφανές σε πακέτα δεδομένων. Πολλές πληροφορίες φαίνονται και στα url. Τουλάχιστον στην περίπτωση που βλέπουμε τις εικόνες ενός χρήστη, το αντίστοιχο url δείχνει το id του χρήστη αυτού. Σε περίπτωση επίσης που αναζητούμε χρήστες για γνωριμία, το url που καλείται δείχνει το γεωγραφικό μας μήκος και πλάτος, όπως και το τι φύλο ανθρώπου ψάχνουμε για γνωριμία, αλλά και το όριο ηλικίας που έχουμε δώσει για την προτίμηση μας αυτή.

3.20 Matchup

Αριθμός έκδοσης: 1.1.9.7

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται προσωπικά στοιχεία των χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Η εφαρμογή είναι πιο ασφαλής από πολλές υπόλοιπες αφού το πρωτόκολλο Https χρησιμοποιείται και για τα γενικά δεδομένα χρηστών, άλλα και για τις εικόνες. Η θέση χρηστών φαίνεται από πεδία γεωγραφικού μήκους και πλάτους που βλέπουμε στα πακέτα δεδομένων. Τέλος μπορούμε να δούμε και την ημερομηνία γέννησης χρηστών, κάτι που δεν γίνεται εντός της εφαρμογής.

3.21 Meet 4u

Αριθμός έκδοσης: 1.23.5

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία για την τοποθεσία χρηστών
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία σεξουαλικής φύσης χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Η ασφάλεια στην μεταφορά των δεδομένων χρηστών άλλα και των εικόνων είναι μικρή αφού χρησιμοποιείται το πρωτόκολλο Http. Από προσωπικά στοιχεία βλέπουμε την ημερομηνία γέννησης χρηστών, κάτι που δεν φαίνεται στην εφαρμογή. Η χιλιομετρική απόσταση με άλλους

χρήστες είναι εμφανής στην εφαρμογή, άλλα μέσα από τα πακέτα δεδομένων είναι πιο ακριβής (πχ στην εφαρμογή μία απόσταση που φαίνεται ως 17km, στα πακέτα δεδομένων φαίνεται ως 16802). Στα πακέτα βλέπουμε επίσης πεδίο ‘interestedIn’, που αναφέρεται στο φύλο που ενδιαφέρεται ο κάθε χρήστης.

3.22 Meet24

Αριθμός έκδοσης: 1.23.5

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Είναι υλοποιημένη από την ίδια εταιρία που υλοποιήθηκε και η Meet 4u.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία για την τοποθεσία χρηστών
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία σεξουαλικής φύσης χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Η ασφάλεια στην μεταφορά των δεδομένων χρηστών άλλα και των εικόνων είναι μικρή αφού χρησιμοποιείται το πρωτόκολλο Http. Από προσωπικά στοιχεία βλέπουμε την ημερομηνία γέννησης χρηστών, κάτι που δεν φαίνεται στην εφαρμογή. Η χιλιομετρική απόσταση με άλλους χρήστες είναι εμφανής στην εφαρμογή, άλλα μέσα από τα πακέτα δεδομένων είναι πιο ακριβής (πχ στην εφαρμογή μία απόσταση που φαίνεται ως 66km, στα πακέτα δεδομένων φαίνεται ως 65917). Στα πακέτα βλέπουμε επίσης πεδίο ‘interestedIn’, που αναφέρεται στο φύλο/φύλα που ενδιαφέρεται ο κάθε χρήστης.

3.23 Mico

Αριθμός έκδοσης: 3.5.7

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Η Mico είναι μία εφαρμογή που έχει αρκετά στοιχεία κοινωνικών δικτύων. Για παράδειγμα σε μία φωτογραφία ενός προφίλ, φαίνεται ο αριθμός άλλων χρηστών που έχουν δηλώσει πως τους αρέσει η κάθε φωτογραφία (likes). Υπάρχει η δυνατότητα ανταλλαγής μηνυμάτων σε μορφή κειμένου ή βίντεο. Επίσης υπάρχει και εδώ η χρήση του GPS για τον εντοπισμό χρηστών που βρίσκονται σε κοντινή απόσταση μεταξύ τους.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει ασφάλεια στην μεταφορά των δεδομένων/εικόνων με το πρωτόκολλο Http. Στοιχεία που δεν βλέπουμε στην εφαρμογή αλλά βλέπουμε στα πακέτα δεδομένων, είναι αρχικά οι γεωγραφικές συντεταγμένες (τοποθεσία) χρηστών. Βλέπουμε επίσης την ημερομηνία γέννησης τους, η οποία όμως φαίνεται σαν κωδικοποιημένη και δεν είναι προφανής (πχ ημερομηνίας γέννησης: 672008400000). Στα url φαίνονται επίσης αρκετά στοιχεία. Σε επίσκεψη προφίλ κάποιου χρήστη, το user id του είναι εμφανές στο αντίστοιχο url. Επίσης σε δική μας αναζήτηση για χρήστες κοντινούς σε εμάς, στο αντίστοιχο url φαίνονται στοιχεία όπως η τοποθεσία μας (συντεταγμένες), το φύλο που προτιμάμε, και η προτίμηση μας στην ηλικία των ατόμων που ψάχνουμε.

3.24 Miumeet

Αριθμός έκδοσης: 2.18

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Η Miumeet είναι μια εφαρμογή με σκοπό την ανάπτυξη οποιασδήποτε είδους σχέσης μεταξύ των χρηστών της. Απευθύνεται επίσης σε ανθρώπους οποιασδήποτε σεξουαλικής ταυτότητας.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά

Ανάλυση σφαλμάτων που βρέθηκαν:

Παρόλο που δεν βρέθηκαν ‘πολλά’ σφάλματα ασφαλείας, το ότι δεν χρησιμοποιείται καθόλου το πρωτόκολλο Https είναι πολύ βασικό σφάλμα. Επίσης στα πακέτα δεδομένων φαίνονται προσωπικά στοιχεία χρηστών όπως το εύρος ηλικίας ατόμου που αναζητούν, και το φύλο που αναζητούν, αλλά είναι στοιχεία που φαίνονται και εντός της εφαρμογής, άρα δεν τα θεωρούμε ως σφάλματα.

3.25 Mocospace

Αριθμός έκδοσης: 2.6.62

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Το κριτήριο της απόστασης μεταξύ των χρηστών παίζει ρόλο στην λειτουργία της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Λείπει και από αυτή την εφαρμογή η ασφάλεια στην μεταφορά δεδομένων/εικόνων μιας και υπάρχει χρήση μόνο του πρωτοκόλλου Http. Σε επίσκεψη ενός προφίλ κάποιου χρήστη, το user id αυτού φαίνεται στο url που καλείται εκείνη τη στιγμή.

3.26 On.com

Αριθμός έκδοσης: 1.2.16

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Η On είναι μία εφαρμογή που έχει αρκετά στοιχεία κοινωνικών δικτύων. Για παράδειγμα σε μία φωτογραφία ενός προφίλ, φαίνεται ο αριθμός άλλων χρηστών που έχουν δηλώσει πως τους αρέσει η κάθε φωτογραφία (likes) και μπορούν να γίνουν σχόλια.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Γίνεται η χρήση μόνο του πρωτοκόλλου Http έχοντας ήδη έτσι ισχνή ασφάλεια στην εφαρμογή. Στα url που καλούνται όταν δηλώνουμε ότι ένα προφίλ μας αρέσει, το id του χρήστη αυτού είναι εμφανές.

3.27 Sam (Singles Around Me)

Αριθμός έκδοσης: 1.1.2

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Το κριτήριο της απόστασης μεταξύ των χρηστών παίζει ρόλο στην λειτουργία της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Σε αυτή την εφαρμογή έχουμε χρήση του πρωτοκόλλου Https στη μεταφορά γενικών δεδομένων χρηστών, αλλά έχουμε χρήση του πρωτοκόλλου Http στην μεταφορά εικόνων χρηστών. Τα links των εικόνων αυτών είναι δυναμικά. Η τοποθεσία του κάθε χρήστη και συγκεκριμένα οι γεωγραφικές του συντεταγμένες φαίνονται στα πακέτα δεδομένων. Επίσης φαίνονται στοιχεία όπως το email χρηστών, η ακριβής τους ημερομηνία γέννησης, αλλά και το πότε ήταν συνδεδεμένοι την τελευταία φορά στην εφαρμογή. Σε περίπτωση επίσκεψης ενός συγκεκριμένου προφίλ, το userid αυτού του προφίλ είναι εμφανές στο url που καλείται από την συσκευή μας.

3.28 SayHi

Αριθμός έκδοσης: 5.35

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει, και απευθύνεται σε άντρες και γυναίκες.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Στην μεταφορά των δεδομένων/εικόνων χρησιμοποιείται μόνο το πρωτόκολλο Http. Οι γεωγραφικές συντεταγμένες χρηστών φαίνονται στα πακέτα δεδομένων. Σε url επίσης που καλείται από τη συσκευή μας, βρέθηκαν να φαίνονται καθαρά οι δικές μας γεωγραφικές συντεταγμένες.

3.29 Single Searcher

Αριθμός έκδοσης: 6.0.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 100.000

Περιγραφή εφαρμογής:

Η Single Searcher είναι μία απλή εφαρμογή για γνωριμίες χωρίς κάποια ιδιαιτερότητα.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά

Ανάλυση σφαλμάτων που βρέθηκαν:

Η εφαρμογή είναι πολύ απλή και φαινόταν να είχε προβλήματα στην λειτουργία της. Ίσως για αυτό το μόνο σφάλμα που βρέθηκε να είναι ότι τα links εικόνων χρηστών είναι στατικά.

3.30 Skout

Αριθμός έκδοσης: 4.14.4

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Η Skout είναι μία ακόμα εφαρμογή γνωριμιών χωρίς κάποια ιδιαιτερότητα στα άτομα και προτιμήσεις που απευθύνεται. Η χρήση του GPS όπως και η εισαγωγή προσωπικών δεδομένων είναι προαιρετική.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει η χρήση του ασφαλούς πρωτοκόλλου επικοινωνίας Https ούτε στις εικόνες ούτε στα γενικότερα δεδομένα των χρηστών της εφαρμογής. Στην περίπτωση επίσκεψης προφίλ κάποιου χρήστη, στο url που καλείται εκείνη τη στιγμή φαίνεται το user id του χρήστη αυτού. Στα πακέτα δεδομένων βλέπουμε επίσης χιλιομετρική απόσταση από άλλους χρήστες, αλλά από ότι φάνηκε

δεν είναι ακριβής, μιας και εμφανιζόταν απόσταση από άλλους χρήστες μη έχοντας κάνει χρήση του GPS, αλλά έχοντας εισάγει απλά την πόλη που μένουμε.

3.31 Tagged

Αριθμός έκδοσης: 6.1.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει και στο είδος ατόμων που απευθύνεται.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικές πληροφορίες χρηστών
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Το πρωτόκολλο Http χρησιμοποιείται μόνο στην μεταφορά εικόνων χρηστών, ενώ στα υπόλοιπα δεδομένα χρησιμοποιείται το πρωτόκολλο Https. Φαίνεται η απόσταση από άλλους χρήστες, η οποία δεν είναι ακριβής (είναι ακέραιος αριθμός). Από προσωπικά στοιχεία βλέπουμε την ακριβή ημερομηνία γέννησης χρηστών. Στα url διαρρέουν αρκετές πληροφορίες. Συγκεκριμένα σε δική μας αναζήτηση για άλλους χρήστες, όλα τα κριτήρια και οι προτιμήσεις που έχουμε ορίσει για την αναζήτηση αυτή, φαίνονται στο αντίστοιχο url που καλείται. Σε επίσκεψη επίσης ενός συγκεκριμένου προφίλ κάποιου χρήστη, το user id αυτού είναι εμφανές στο url που καλείται εκείνη τη στιγμή.

3.32 Twoo

Αριθμός έκδοσης: 6.4.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 5.000.000

Περιγραφή εφαρμογής:

Μία κλασική και γνωστή εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία για την τοποθεσία χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Με την χρήση του πρωτοκόλλου Http δεν υπάρχει ασφάλεια στην μεταφορά των εικόνων χρηστών. Στα υπόλοιπα δεδομένα των χρηστών που μεταφέρει η εφαρμογή, χρησιμοποιείται το πρωτόκολλο Https. Σε χρήστες που πιθανότατα έχουν ενεργοποιήσει το GPS τους και η εφαρμογή είχε πρόσβαση στην τοποθεσία τους, βλέπουμε την ακριβή τους τοποθεσία (το γεωγραφικό τους μήκος και πλάτος). Υπάρχει μάλιστα και πεδίο ‘accuracy’ στους χρήστες που φαίνεται να απευθύνεται στην τοποθεσία τους που βλέπουμε, και αν είναι ακριβής (με χρήση GPS) ή όχι.

3.33 Voo

Αριθμός έκδοσης: 2.0.1

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Στην εφαρμογή υπάρχει χρήση του πρωτοκόλλου Https μόνο για την μεταφορά γενικών δεδομένων των χρηστών. Στην μεταφορά εικόνων έχουμε χρήση του πρωτοκόλλου Http. Σχετικά με τα προσωπικά στοιχεία, βλέπουμε στα πακέτα δεδομένων ένα πεδίο ‘genderLooking’, που προφανώς αναφέρεται στο φύλο που ενδιαφέρεται να γνωρίσει κάποιος χρήστης. Στα url της εφαρμογής, στην επίσκεψη κάποιου συγκεκριμένου προφίλ ενός χρήστη, είναι εμφανές το user id αυτού του χρήστη, όπως και ίσως μερικές ακόμα λεπτομέρειες (όπως για παράδειγμα στο άνοιγμα των φωτογραφιών ενός συγκεκριμένου χρήστη, στο url βλέπουμε το user id αυτού του χρήστη και τη λέξη pictures στο url). Επίσης σε αναζήτηση χρηστών με βάση κάποια κριτήρια, τα κριτήρια σεξουαλικής προτίμησης και επιθυμητά όρια ηλικίας φαίνονται ξεκάθαρα στο αντίστοιχο url που καλείται.

3.34 Voxle

Αριθμός έκδοσης: 2.0.19

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 100.000

Περιγραφή εφαρμογής:

Μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Η πραγματική τοποθεσία των χρηστών παίζει ρόλο στην λειτουργία της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται στοιχεία τοποθεσίας
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Στην εφαρμογή δεν υπάρχει καμία ασφάλεια στην μεταφορά των δεδομένων χρηστών και των εικόνων τους, αφού χρησιμοποιείται μόνο το πρωτόκολλο Http. Οι γεωγραφικές συντεταγμένες των χρηστών φαίνονται καθαρά στα πακέτα δεδομένων, όπως και η χιλιομετρική μας απόσταση από αυτούς. Σχετικά με τα url, στην επίσκεψη ενός προφίλ κάποιου χρήστη, μπορούμε και εδώ να δούμε εύκολα το user id του, και το ότι το url απευθύνεται στο αρχείο showProfile.php .

3.35 Waplog

Αριθμός έκδοσης: 2.3.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Η Waplog είναι μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Έχει μορφή κοινωνικού δικτύου με αιτήματα φιλίας, σχόλια σε φωτογραφίες, και άλλα.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει η χρήση του πρωτοκόλλου Https στην μεταφορά εικόνων και γενικότερων δεδομένων των χρηστών. Τα προσωπικά στοιχεία χρηστών που βλέπουμε είναι συγκεκριμένα η διεύθυνση του ηλεκτρονικού τους ταχυδρομείου, αλλά και η ακριβής ημερομηνία γέννησης τους. Επίσης σε επίσκεψη του προφίλ ενός άλλου χρήστη, στο url που καλεί η εφαρμογή βλέπουμε το user id του χρήστη αυτού.

3.36 Waplog Match

Αριθμός έκδοσης: 1.4.3

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 1.000.000

Περιγραφή εφαρμογής:

Από την ίδια εταιρία που υλοποιήθηκε η Waplog, η Waplog Match λειτουργεί διαφορετικά βρίσκοντας άτομα που ενδιαφέρονται ο ένας για τον άλλον (matches). Δηλαδή μόνο όταν δύο χρήστες δηλώσουν ότι ενδιαφέρονται ο ένας για τον άλλον θα συνδεθούν μέσω της εφαρμογής.

Σφάλματα που βρέθηκαν:

- Όλα τα δεδομένα μεταφέρονται με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών μεταφέρονται επίσης με το πρωτόκολλο Http
- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία χρηστών
- Φαίνονται στοιχεία στα url που καλεί η εφαρμογή

Ανάλυση σφαλμάτων που βρέθηκαν:

Δεν υπάρχει ούτε εδώ η χρήση του πρωτοκόλλου Https στην μεταφορά εικόνων και γενικότερων δεδομένων των χρηστών. Τα προσωπικά στοιχεία χρηστών που βλέπουμε είναι συγκεκριμένα η διεύθυνση του ηλεκτρονικού τους ταχυδρομείου, αλλά και η ακριβής ημερομηνία γέννησης τους. Τέλος στην περίπτωση επίσκεψης του προφίλ κάποιου άλλου χρήστη, στο αντίστοιχο url που καλείται βλέπουμε το user id του χρήστη αυτού.

3.37 Znakomstva

Αριθμός έκδοσης: 1.1.8

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 500.000

Περιγραφή εφαρμογής:

Η Znakomstva είναι μία κλασική εφαρμογή γνωριμιών χωρίς συγκεκριμένη ιδιαιτερότητα στο είδος γνωριμιών που παρέχει. Είναι υλοποιημένη στην Ρωσία, και για αυτό οι περισσότεροι χρήστες της εφαρμογής είναι από εκεί.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται προσωπικά στοιχεία των χρηστών
- Φαίνονται ορισμένα στοιχεία του λογαριασμού των χρηστών
- Φαίνονται πληροφορίες για την τοποθεσία χρηστών

Ανάλυση σφαλμάτων που βρέθηκαν:

Η συγκεκριμένη εφαρμογή είναι από τις λίγες που χρησιμοποιούν το πρωτόκολλο Https για την μεταφορά των δεδομένων και των εικόνων των χρηστών της. Το username που κάθε χρήστης login είναι εμφανές στα πακέτα δεδομένων, και το να φαίνεται είναι κάτι που σίγουρα δεν μπορεί να θεωρείται ασφαλές. Έπειτα μπορούμε να δούμε την ακριβή ημερομηνία γέννησης των χρηστών, και αν έχουν εγγραφεί στην εφαρμογή χρησιμοποιώντας το GPS, μπορούμε να δούμε τις ακριβείς γεωγραφικές τους συντεταγμένες.

3.38 Zoosk

Αριθμός έκδοσης: 3.5.11

Αριθμός χρηστών της εφαρμογής (τουλάχιστον): 10.000.000

Περιγραφή εφαρμογής:

Η τελευταία εφαρμογή που εξετάστηκε, η Zoosk, μία ακόμα εφαρμογή που δεν απευθύνεται σε συγκεκριμένο κοινό. Δεν διαφέρει πολύ από τις υπόλοιπες, πέρα από το ότι από την υλοποίηση της προσπαθεί να βρει από μόνη της άτομα που ταιριάζουν μεταξύ τους, με βάση ορισμένα κριτήρια.

Σφάλματα που βρέθηκαν:

- Τα links των εικόνων χρηστών είναι στατικά
- Φαίνονται πληροφορίες τοποθεσίας

Ανάλυση σφαλμάτων που βρέθηκαν:

Η Zoosk παρέχει και αυτή μία ασφάλεια μόνο και μόνο αφού χρησιμοποιεί το πρωτόκολλο Https. Η χιλιομετρική απόσταση μεταξύ των χρηστών φαίνεται στα πακέτα δεδομένων ως ακέραιος αριθμός, αλλά φαίνεται επίσης και στην εφαρμογή, για αυτό και δεν το θεωρούμε τόσο αρνητικό σε θέμα ασφάλειας. Μπορούμε όμως σε ορισμένους χρήστες να δούμε τον ταχυδρομικό κώδικα της περιοχής που μένουν, το οποίο πιθανότατα αποθηκεύτηκε από την εφαρμογή κατά την εγγραφή του κάθε χρήστη που εισήγαγε την πόλη που διαμένει.

Κεφάλαιο 4ο

4 Συγκεντρωτικά στοιχεία για όλες τις εφαρμογές

4.1 Σημαντικότερα σφάλματα ασφαλείας που βρέθηκαν

Σε προηγούμενο κεφάλαιο είδαμε αναλυτικά τα σφάλματα ασφαλείας που βρέθηκαν στις εφαρμογές εξετάσαμε. Εδώ θα πούμε τα πιο σημαντικά συγκεντρωτικά σαν σφάλματα μαζί με μία επεξήγηση για αυτά.

- Μετάδοση δεδομένων των χρηστών κάποιας εφαρμογής με την χρήση του πρωτοκόλλου Http. Τα Urls που καλεί η ίδια εφαρμογή για να πραγματοποιήσει τις λειτουργίες της είναι εκτεθειμένα σε οποιονδήποτε που μπορεί να 'κρυφακούσει' την επικοινωνία που έχει η κάθε εφαρμογή με τον server της. Άρα η χρήση και μόνο του πρωτοκόλλου Http δείχνει ότι υπάρχει ένα μεγάλο κενό στην ασφάλεια της εφαρμογής.
- Μετάδοση εικόνων των χρηστών κάποιας εφαρμογής με την χρήση του πρωτοκόλλου Http. Πάλι η χρήση του πρωτοκόλλου Http αμέσως δείχνει το κενό της ασφάλειας που υπάρχει.
- Εικόνες χρηστών που είναι προσβάσιμες μέσω στατικών links. Τέτοια links δεν παρέχουν κάποια ασφάλεια, μόνο και μόνο αν σκεφτούμε ότι εικόνες χρηστών μπορούν εύκολα να αποσταλούν και να αποθηκευτούν από τον οποιονδήποτε.
- Γενικά δεδομένα που φαίνονται ξεκάθαρα σε Urls που καλεί κάποια εφαρμογή. Ακόμα και σε εφαρμογές που χρησιμοποιούν το πρωτόκολλο Https για την μεταφορά δεδομένων, έχουν εντοπιστεί διάφορα δεδομένα να φαίνονται καθαρά σε Urls που καλούν οι εφαρμογές αυτές, τα οποία Urls προφανώς και δεν κωδικοποιούνται κατά την μεταφορά τους. Συνήθη δεδομένα που φαίνονται είναι το όνομα ή το μοναδικό id χρηστών σε περίπτωση που επισκεφτούμε το προφίλ τους εντός της εφαρμογής, μαζί με κάποια λέξη κλειδί που υποδηλώνει ότι επισκεφτήκαμε κάποιο προφίλ (πχ η λέξη visit). Αντίστοιχα μπορεί να φανεί πάλι το όνομα ή το id ενός χρήστη όταν του στείλουμε κάποιο μήνυμα.
- Διαρροή προσωπικών στοιχείων, είτε στα πακέτα δεδομένων, είτε στα Urls που καλεί κάποια εφαρμογή. Τα προσωπικά δεδομένα αυτά περιλαμβάνουν κυρίως κάποιο από τα επόμενα: πραγματικό όνομα, ηλικία, ημερομηνία γέννησης, σεξουαλικά ενδιαφέροντα.
- Διαρροή στοιχείων τοποθεσίας ενός χρήστη. Τέτοια διαρροή μπορεί να γίνει αν μπορέσουμε να ανακτήσουμε κάποια πληροφορία όπως την ακριβή (ή έστω κοντινή) πραγματική απόσταση μας από κάποιον συγκεκριμένο χρήστη. Επίσης σε πολλές εφαρμογές ήταν εύκολο να ανακτηθούν οι πραγματικές γεωγραφικές συντεταγμένες ενός χρήστη, μιας και οι περισσότερες εφαρμογές κάνουν χρήση του GPS για να προτείνουν στους χρήστες άλλους χρήστες που είναι κοντά ο ένας με τον άλλον. Η διαρροή της διεύθυνσης Ip ενός χρήστη θεωρούμε ότι ανήκει σε αυτή τη κατηγορία.
- Διαρροή credentials, δηλαδή το να μπορούμε να βρούμε τα στοιχεία σύνδεσης ενός χρήστη για μία εφαρμογή.
- Οτιδήποτε άλλο που είναι 'ίσως' ελαφρώς λιγότερης σημασίας

4.2 Εκδόσεις των εφαρμογών που εξετάστηκαν

Ο παρακάτω πίνακας δείχνει τις εκδόσεις των εφαρμογών που εξετάστηκαν.

Application Name	**Application Version**
Black Dating for Free	4.0
BoyAhoy	4.14.4
Choice of Love	2.8
Christian Dating for Free	4.0
Daddyhunt	1.0.4

Date Me	1.5.0.8
Eharmony	2.4.3.1
Eskimi	5.6.3
FlirtXchange	1.6.1
Grindr	2.2.4
GuySpy	4.3.2
Hawaya	1.0.1
Hi5	6.2.3
Hornet	2.0.33
Hot Or Not	4.6.3
I-am	2.54
Jaumo	3.5.1
Loveplanet.ru	2.7.6
Lovoo	2.5.5
Matchup	1.1.9.7
Meet 4u	1.23.5
Meet24	1.23.5
Mico	3.5.7
Miumeet	2.18
Mocospace	2.6.62
On.com	1.2.16
Singles Around me	1.1.2
SayHi	5.35
Single Searcher	6.0.1
Skout	4.14.4
Tagged	6.1.1
Twoo	6.4.3
Voo	2.0.1
Voxle	2.0.19
Waplog	2.3.3
Waplog Match	1.4.3
Znakomstva	1.1.8
Zoosk	3.5.11

Table 1 Εκδόσεις των εφαρμογών

4.3 Ελάχιστος αριθμός χρηστών των εφαρμογών

Ο παρακάτω πίνακας δείχνει τον ελάχιστο αριθμό χρηστών που εγκατέστησαν την κάθε εφαρμογή.

Application Name	**Number of Downloads (minimum)**
Black Dating for Free	100.000

BoyAhoy	1.000.000
Choice of Love	1.000.000
Christian Dating for Free	100.000
Daddyhunt	100.000
Date Me	500.000
Eharmony	1.000.000
Eskimi	500.000
FlirtXchange	500.000
Grindr	5.000.000
GuySpy	1.000.000
Hawaya	10.000
Hi5	1.000.000
Hornet	1.000.000
Hot Or Not	10.000.000
I-am	500.000
Jaumo	5.000.000
Loveplanet.ru	1.000.000
Lovoo	10.000.000
Matchup	500.000
Meet 4u	500.000
Meet24	1.000.000
Mico	10.000.000
Miumeet	1.000.000
Mocospace	10.000.000
On.com	500.000
Singles Around me	1.000.000
SayHi	10.000.000
Single Searcher	100.000
Skout	10.000.000
Tagged	10.000.000
Twoo	5.000.000
Voo	1.000.000
Voxle	100.000
Waplog	10.000.000
Waplog Match	1.000.000
Znakomstva	500.000
Zoosk	10.000.000

Table 2 Αριθμός χρηστών των εφαρμογών

Ο παραπάνω αριθμός των λήψεων κάθε εφαρμογής θεωρείται ο ελάχιστος αριθμός λήψεων. Σύμφωνα με το Google Play Store αυτοί οι ελάχιστοι αριθμοί σε πραγματικό αριθμό λήψεων ανήκουν σε ένα εύρος που φαίνεται στον παρακάτω πίνακα

Minimum number of downloads (according to google store)	**Range of actual number of downloads**
100.000	100.000 – 500.000
500.000	500.000 – 1.000.000
1.000.000	1.000.000 – 5.000.000
5.000.000	5.000.000 – 10.000.000
10.000.000	10.000.000 – 50.000.000

Table 3 Αντιστοίχηση ελάχιστου αριθμού λήψεων κάθε εφαρμογής στο πραγματικό πιθανό εύρος

4.4 Συγκεντρωτικά γραφήματα για τα σφάλματα που βρέθηκαν

Παρακάτω υπάρχουν μερικοί πίνακες και γραφήματα που δείχνουν συγκεντρωτικά στοιχεία για τις εφαρμογές που εξετάστηκαν για αυτή την εργασία και τα σφάλματα σε θέματα ασφαλείας που βρέθηκαν σε αυτές.

Figure 1 Οι εφαρμογές που εξετάστηκαν και η αντιστοιχία τους σε κουτάκια

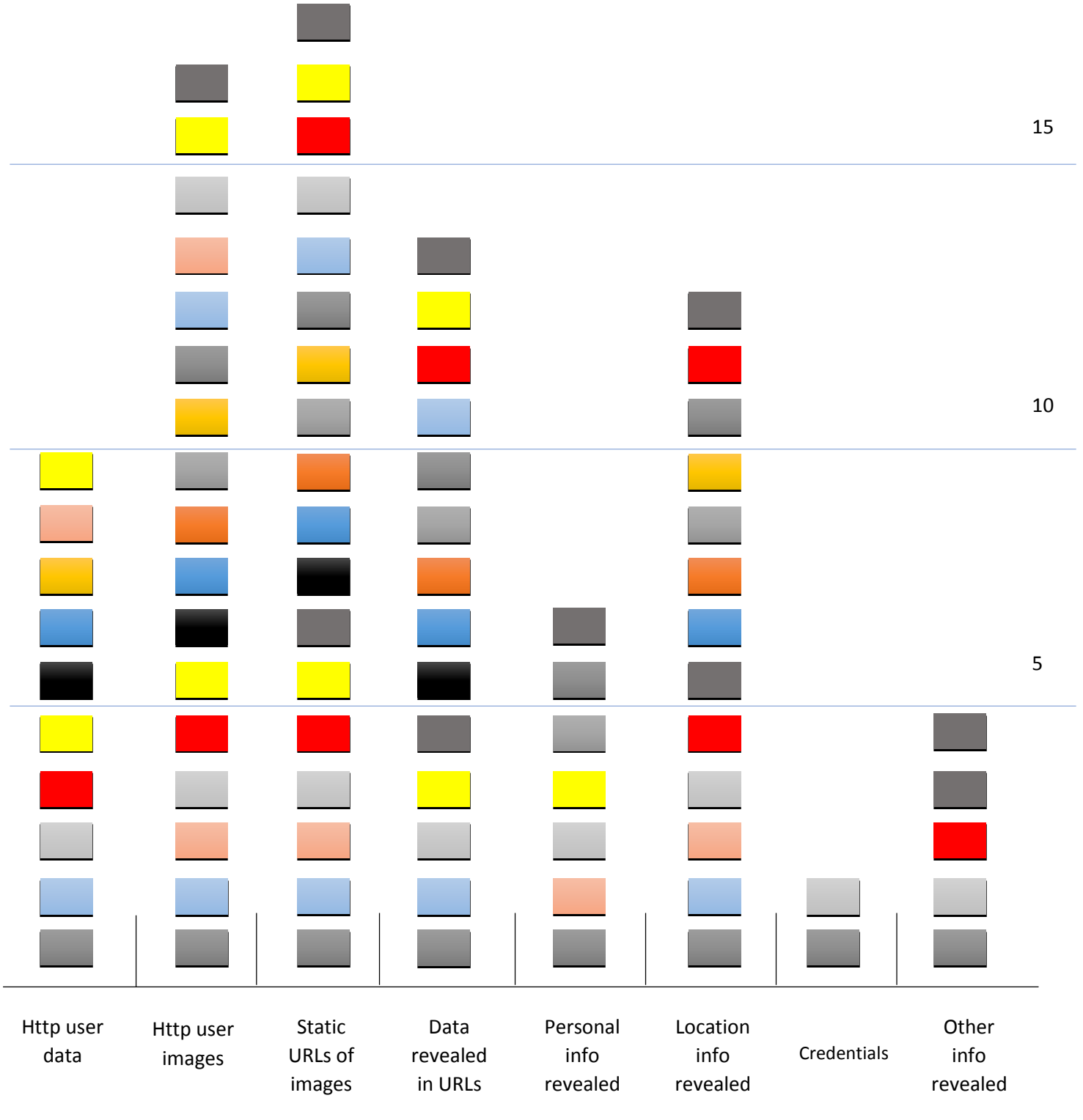

Figure 2 Οι 19 πρώτες εφαρμογές που εξετάστηκαν, με τα λάθη που βρέθηκαν σε αυτές

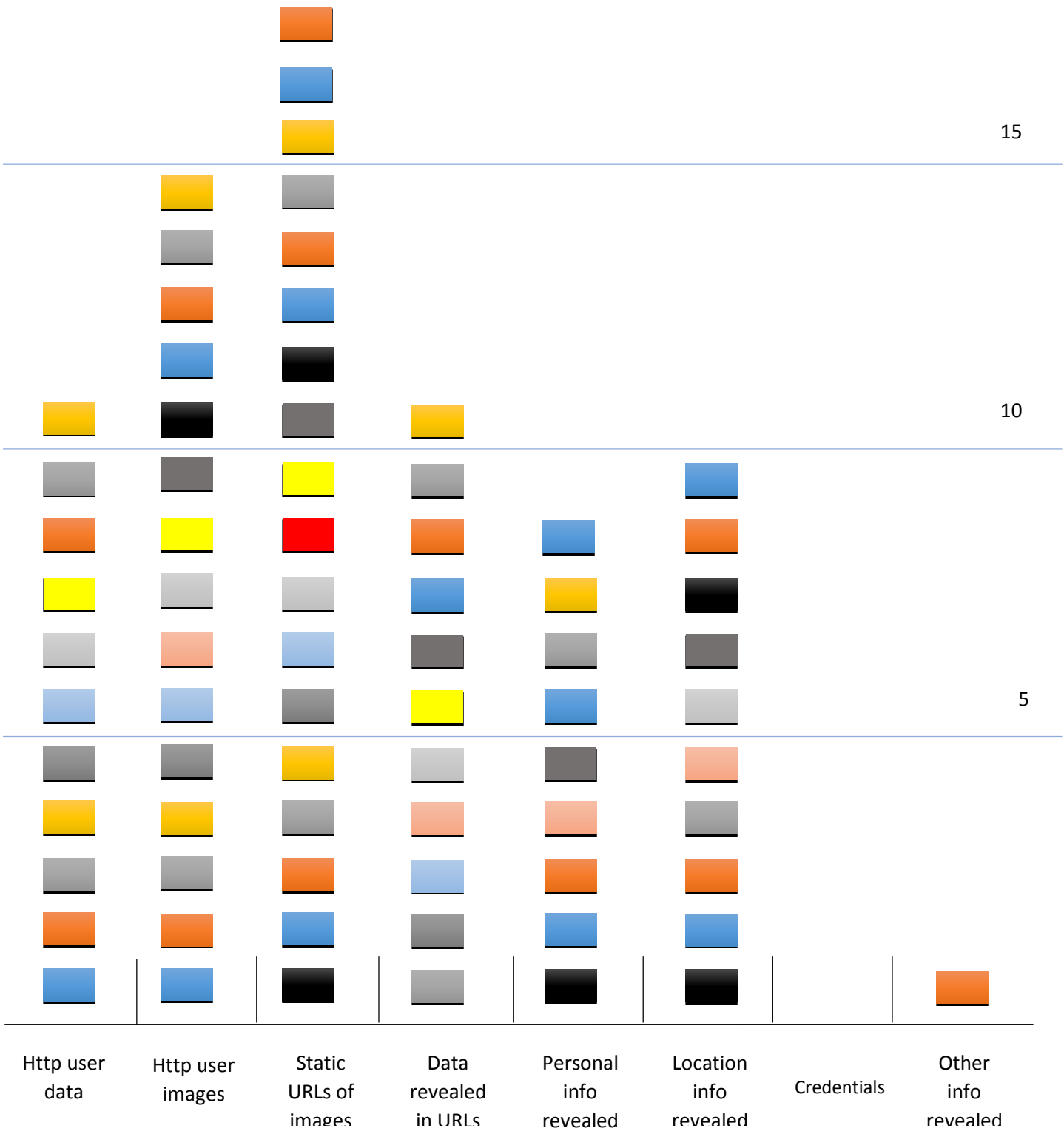

Figure 3 Οι 19 τελευταίες εφαρμογές που εξετάστηκαν, και τα λάθη που βρέθηκαν σε αυτές

App/Flaw	Http user data	Http user images	Static image URLs	Data in URLs	Personal info revealed	Location info revealed	Credentials	Other
Black Dating for Free	■	■	■	■	■	■	■	■
BoyAhoy	■	■	■	■		■		
Choice of Love		■	■		■	■		
Christian Dating for Free	■	■	■	■	■	■	■	■
Daddyhunt	■	■	■			■		■
Date Me	■	■	■	■	■			
Eharmony			■	■		■		■
Eskimi	■	■	■	■				
FlirtXchange	■	■	■	■		■		
Grindr		■	■	■		■		
GuySpy		■	■	■	■	■		
Hawaya	■	■	■			■		
Hi5		■	■	■	■	■		
Hornet		■	■	■				
Hot Or Not	■	■						
I-am		■	■					
Jaumo			■	■		■		
Loveplanet.ru	■	■	■	■				
Lovoo		■	■	■	■	■		■
Matchup			■		■	■		
Meet 4u	■	■	■		■	■		
Meet24	■	■	■		■	■		
Mico	■	■	■	■		■		
Miumeet	■	■	■					
Mocospace	■	■	■	■				
On.com	■	■	■	■				
Singles Around me		■		■	■	■		
SayHi	■	■	■	■		■		
Single Searcher			■					
Skout	■	■	■	■				
Tagged		■	■	■	■	■		
Twoo		■	■			■		
Voo		■	■	■	■			
Voxle	■	■	■	■		■		
Waplog	■	■	■	■	■			

Waplog Match								
Znakomstva								
Zoosk								

Table 4 Συγκεντρωτικός πίνακας με τις εφαρμογές και τα σφάλματα ασφαλείας που έχουν

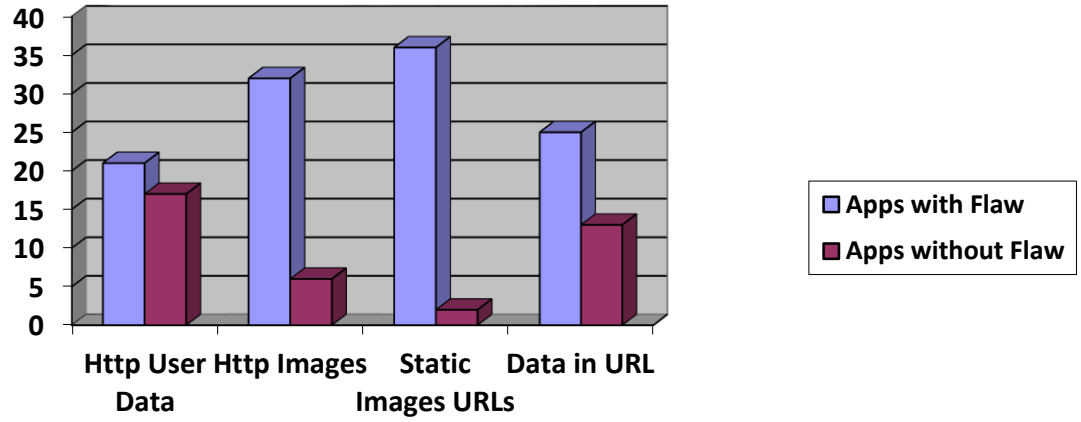

Figure 4 Γράφημα αναφερόμενο στις εφαρμογές που εξετάστηκαν και πόσες έχουν τα αναφερόμενα σφάλματα

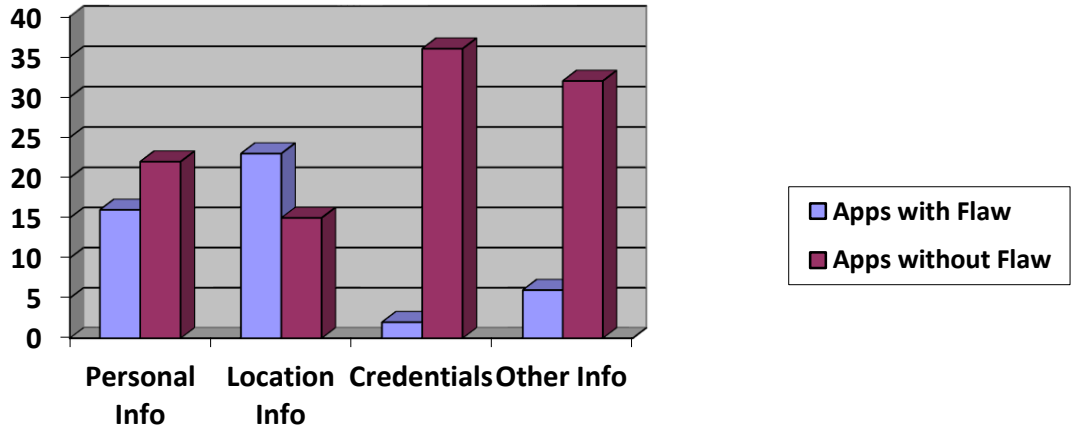

Figure 5 Γράφημα αναφερόμενο στις εφαρμογές που εξετάστηκαν και πόσες έχουν τα αναφερόμενα σφάλματα

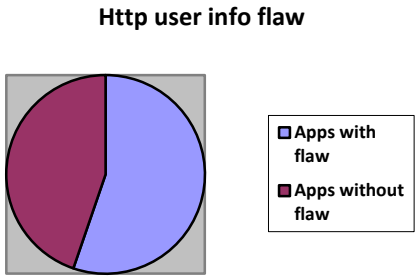

Figure 6 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα χρήσης του πρωτοκόλλου Http στην μεταφορά δεδομένων χρηστών τους

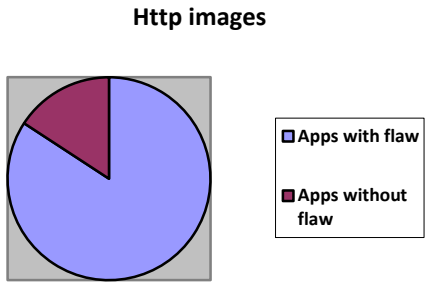

Figure 7 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα χρήσης του πρωτοκόλλου Http στην μεταφορά εικόνων χρηστών τους

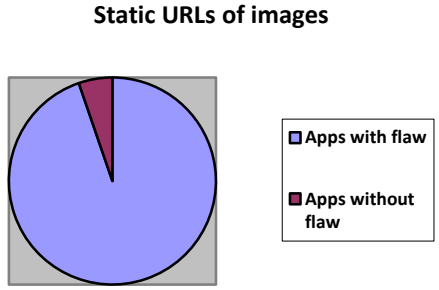

Figure 8 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα στατικών links εικόνων χρηστών τους

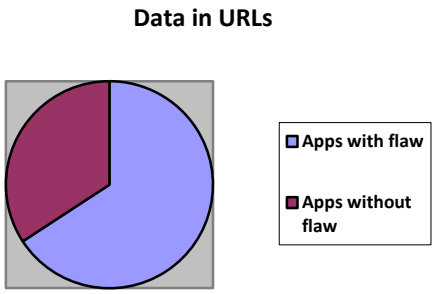

Figure 9 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα εμφάνισης προσωπικών δεδομένων στα url τους

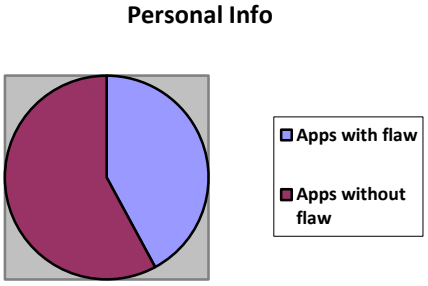

Figure 10 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα διαρροής προσωπικών στοιχείων των χρηστών τους

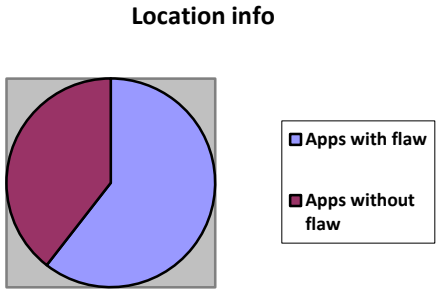

Figure 11 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα διαρροής πληροφοριών στοιχείων της τοποθεσίας των χρηστών τους

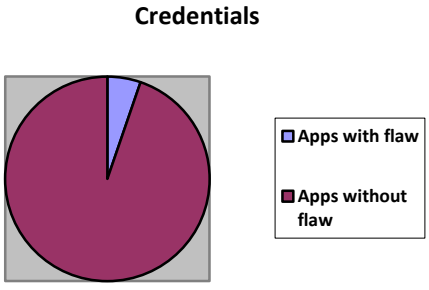

Figure 12 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα διαρροής στοιχείων σύνδεσης λογαριασμού

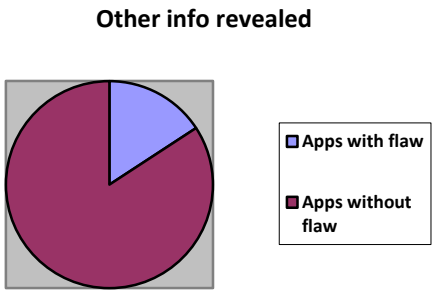

Figure 13 Πίτα σχετικά με τις εφαρμογές που περιέχουν το σφάλμα διαρροής άλλου είδους πληροφορίας από ότι έχει αναφερθεί

4.5 Κυριότερα λάθη που εντοπίστηκαν

4.5.1 Credentials για την είσοδο σε λογαριασμό ενός χρήστη

Το συγκεκριμένο σφάλμα βρέθηκε πρώτα στην εφαρμογή Black Dating for Free. Στα πακέτα δεδομένων που βλέπουμε διάφορα στοιχεία χρηστών, βλέπουμε και το username και το password που έχουν ορίσει για να συνδέονται στο προφίλ τους.

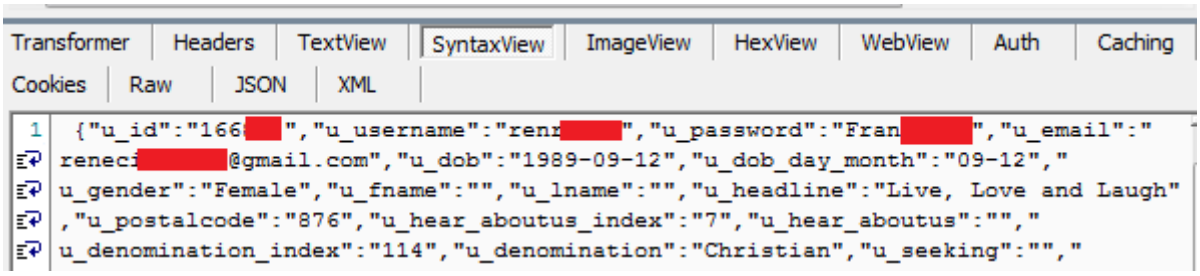

Figure 14 Στοιχεία εισόδου σε λογαριασμό χρήστη

4.5.2 Πληροφορίες σεξουαλικού προσανατολισμού

Το σφάλμα της εικόνας είναι από την εφαρμογή Guyspy, μία εφαρμογή που απευθύνεται κυρίως σε ομοφυλόφιλα άτομα. Στην συγκεκριμένη εικόνα βλέπουμε πολύ συγκεκριμένες πληροφορίες σεξουαλικής φύσης ενός χρήστη.

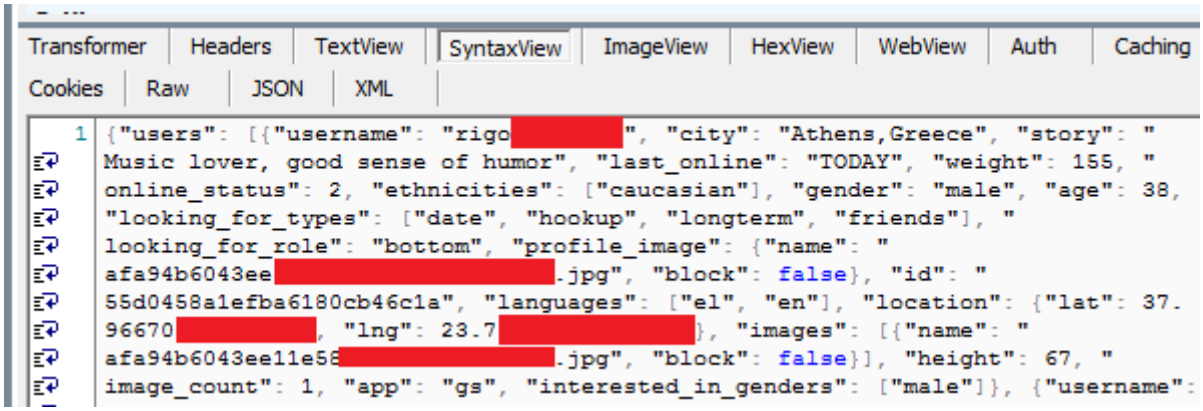

Figure 15 Προσωπικές πληροφορίες σχετικές με τον σεξουαλικό προσανατολισμό χρήστη

4.5.3 Σχετική γεωγραφική θέση ενός χρήστη

Στην εφαρμογή Lovoo βρέθηκε σε πακέτα δεδομένων η πληροφορία που δείχνει ακριβώς την σχετική μας γεωγραφική θέση σε σχέση με κάποιον άλλον χρήστη.

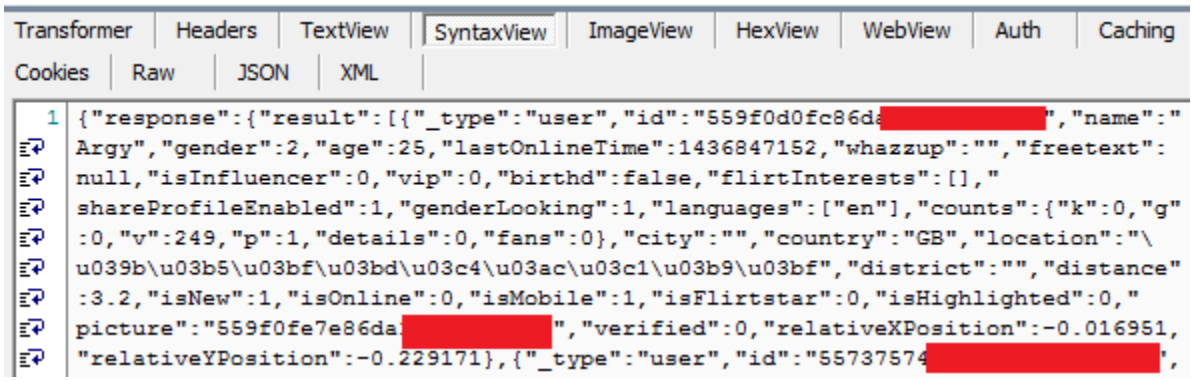

Figure 16 Πληροφορίες τοποθεσίας

4.5.4 Προσωπικό μήνυμα σε URL

Στην εφαρμογή Loveplanet.ru είδαμε ότι σε url που καλεί η εφαρμογή όταν στέλνουμε προσωπικό μήνυμα σε κάποιον χρήστη, το url αυτό δείχνει το μήνυμα που στείλαμε (στην εικόνα στείλαμε το μήνυμα “how are you”).

Figure 17 Προσωπικό μήνυμα σε Url

Κεφάλαιο 5ο

5 Χρήση των εργαλείων που χρησιμοποιήθηκαν

5.1 Fiddler

5.1.1 Ρυθμίσεις πριν την χρήση των εργαλείων

Το Fiddler είναι ένα πολύ βασικό εργαλείο για την υλοποίηση αυτής της εργασίας. Είναι στην ουσία ο proxy server που τοποθετήσαμε ανάμεσα στην επικοινωνία μίας εφαρμογής γνωριμιών και τον server της. Έτσι μπορούσαμε να δούμε τα πακέτα που μεταφέρονται στην επικοινωνία αυτή και να εντοπίσουμε τρωτά σημεία στην ασφάλεια των εφαρμογών.

Το fiddler είναι εύκολο να το κατεβάσουμε και να αρχίσουμε να το χρησιμοποιούμε. Οι ρυθμίσεις που χρειάστηκαν να γίνουν ήταν ελάχιστες. Έχοντας το Fiddler στον υπολογιστή μας, και τον υπολογιστή μας όπως και την κινητή συσκευή μας συνδεδεμένα στο ίδιο δίκτυο του Internet, οι ρυθμίσεις που πρέπει να γίνουν είναι

- Η τροποποίηση του δικτύου στην κινητή μας συσκευή, έτσι ώστε να περνάει τα πακέτα δεδομένων της από και προς το δίκτυο διαμέσου ενός proxy που θα ορίσουμε. Ο proxy αυτός φαίνεται ως μια διεύθυνση ip στον Fiddler και έτσι η σύνδεση με τον proxy γίνεται εύκολα. Ο επίσημος σύνδεσμος για αναλυτικές οδηγίες είναι στην βιβλιογραφία [13].

  Εδώ βλέπουμε την διεύθυνση που θα έχει ο Fiddler για να τον χρησιμοποιήσουμε ως proxy

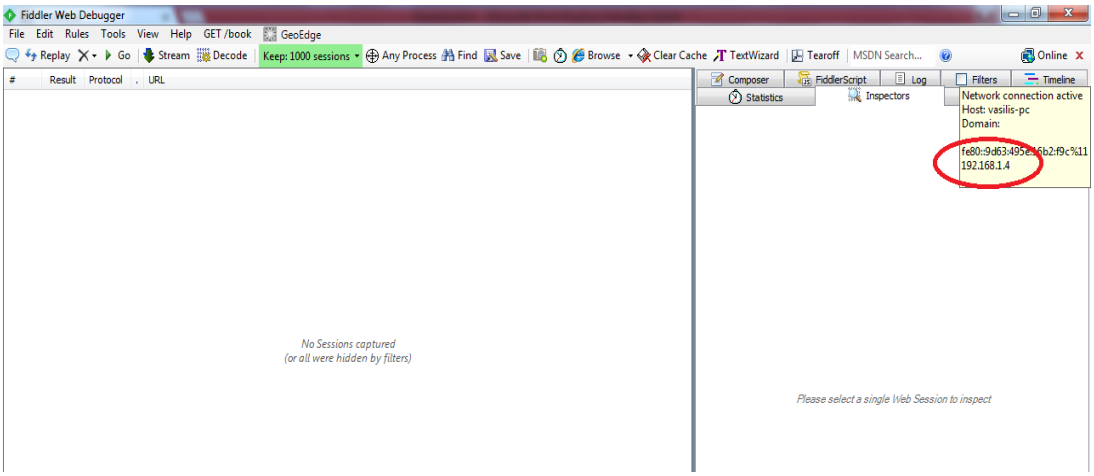

Figure 18 Fiddler Ip

Την ip αυτή θα την βάλουμε στις σύνθετες ρυθμίσεις του δικτύου που θα είμαστε συνδεδεμένοι στην κινητή μας συσκευή. Οι συγκεκριμένες απλές ρυθμίσεις είναι αυτές:

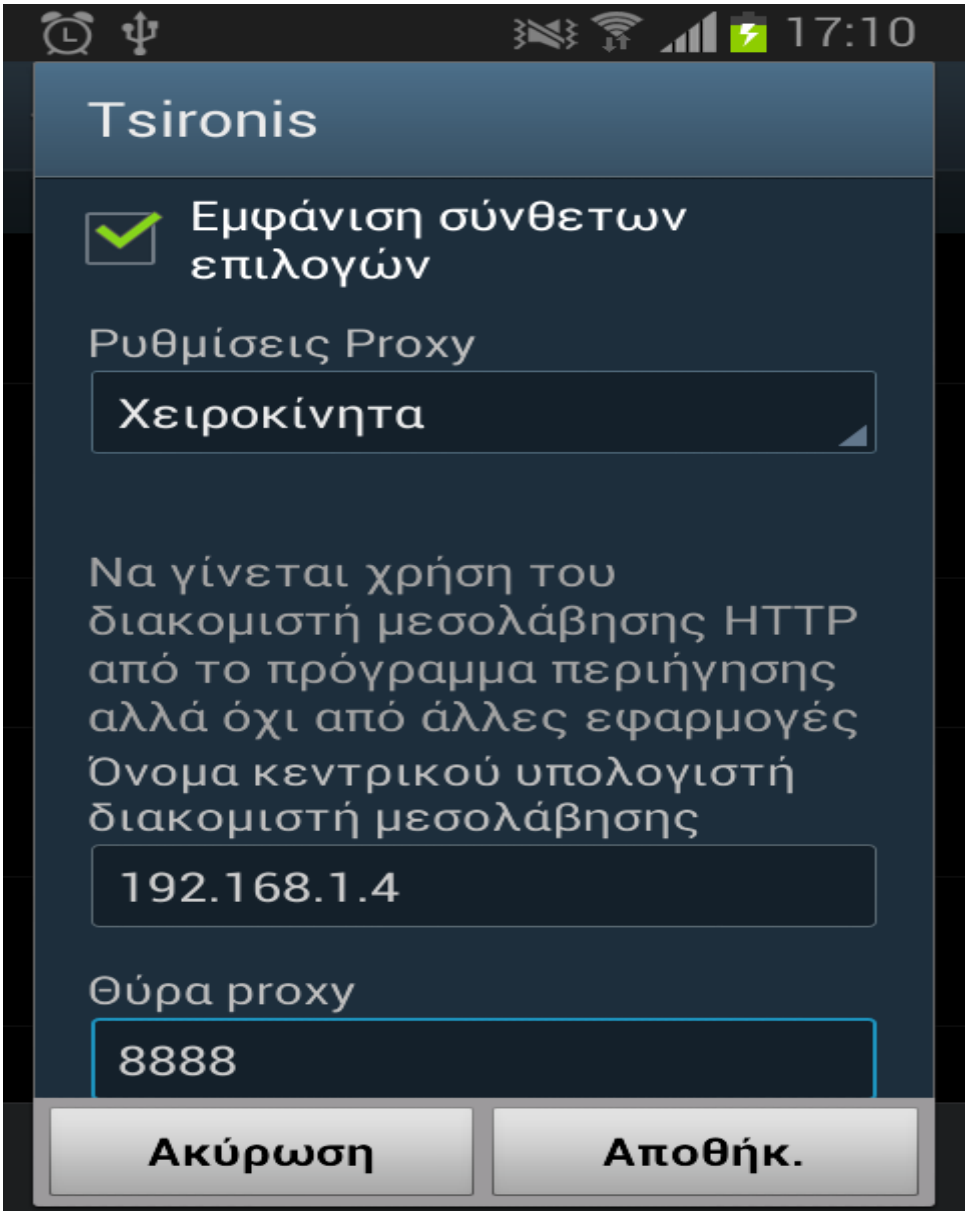

Figure 19 Ρύθμιση Wi-Fi κινητής συσκευής

- Θα χρειαστούν και κάποιες ρυθμίσεις στο Fiddler έτσι ώστε να το εξουσιοδοτήσουμε για να μπορεί να αποκρυπτογραφεί τα δεδομένα που μεταφέρονται με το πρωτόκολλο Https, ώστε να μπορούμε να δούμε και αυτές τις κρυπτογραφημένες πληροφορίες. Ο επίσημος σύνδεσμος είναι και αυτός στην βιβλιογραφία [14].

  Αυτό θα γίνει συγκεκριμένα από το Fiddler ακολουθώντας τις καρτέλες Tools->Fiddler Options->Https και οι ρυθμίσεις που θα πρέπει να γίνουν φαίνονται στην παρακάτω εικόνα:

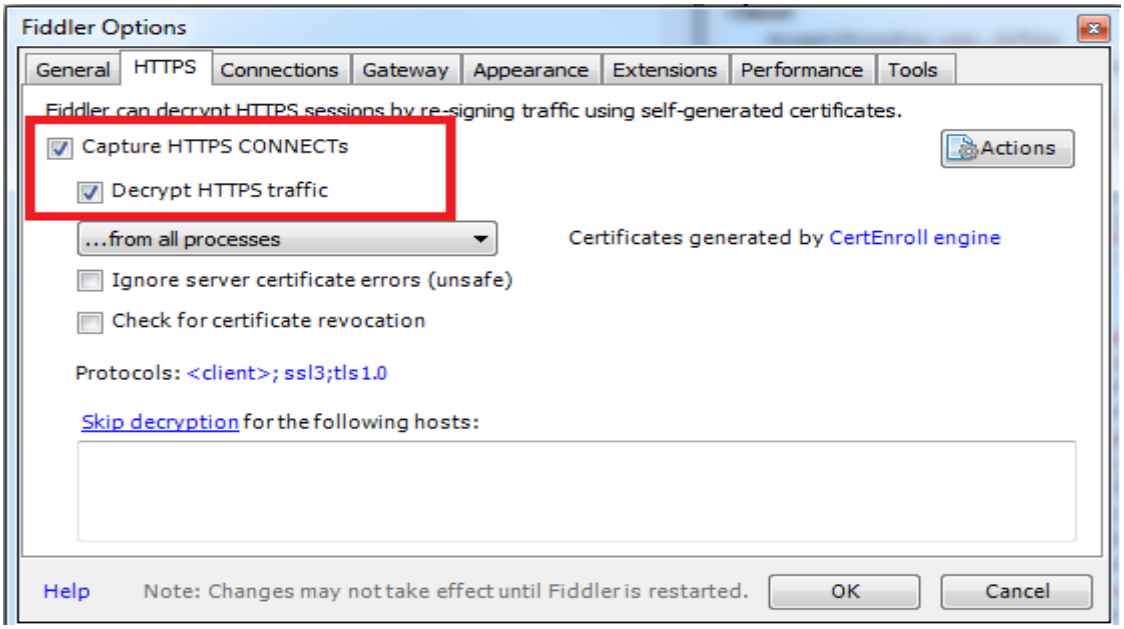

Figure 20 Fiddler Https

5.1.2 Χρήση του Fiddler

Έχοντας κάνει τις παραπάνω ρυθμίσεις, μπορούμε να εξετάσουμε μία εφαρμογή γνωριμιών. Στις περισσότερες εφαρμογές γνωριμιών, η πρώτη οθόνη που βλέπουμε περιέχει μικρογραφίες αρκετών χρηστών που πατώντας επάνω στην εικόνα τους ανοίγει το προφίλ τους. Έχοντας ανοίξει μια εφαρμογή και πατώντας την εικόνα ενός προφίλ κάποιου χρήστη, θα βλέπουμε στην κινητή μας συσκευή και στο Fiddler κάτι αντίστοιχο με τις παρακάτω εικόνες:

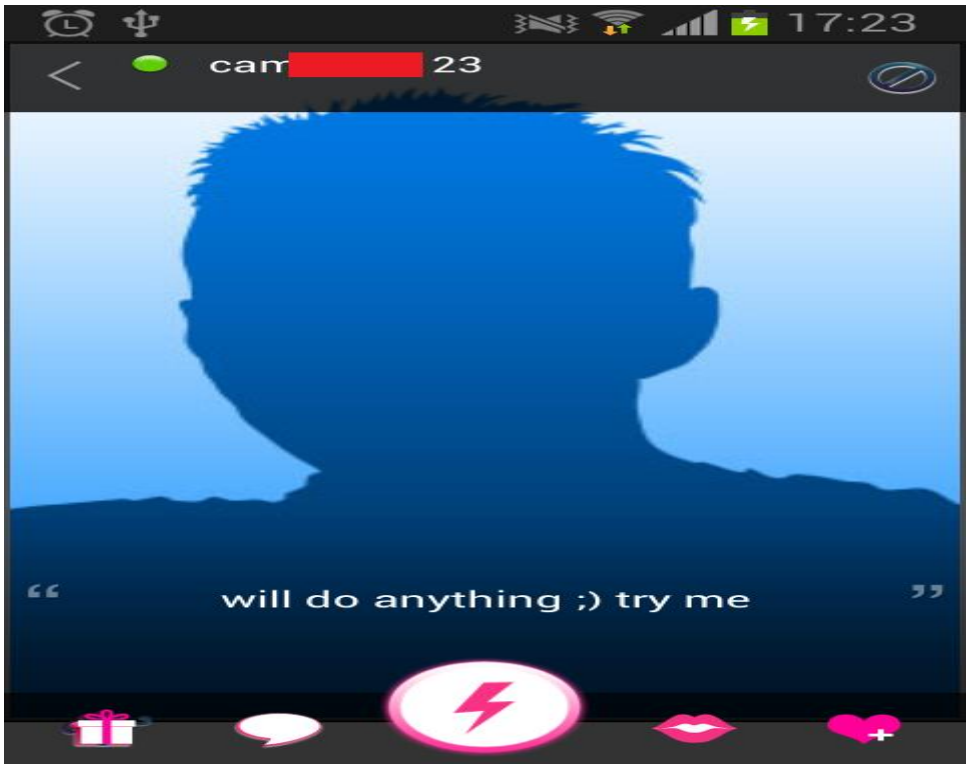

Figure 21 Επίσκεψη προφίλ χρήστη

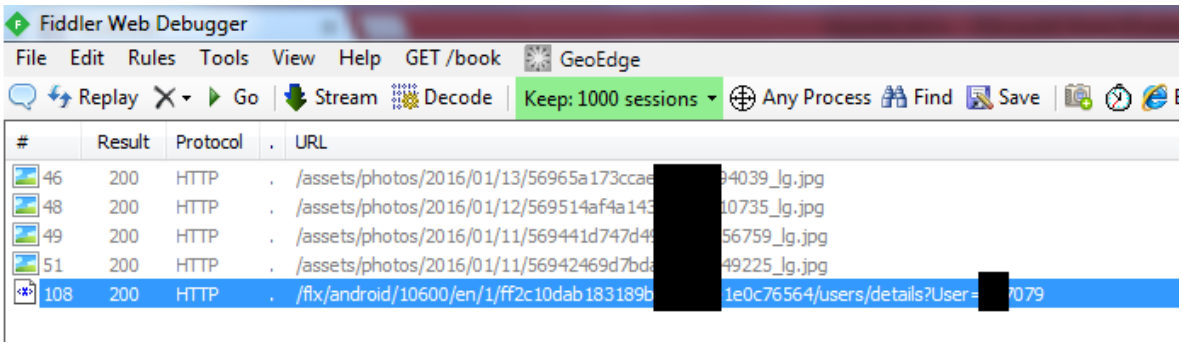

Figure 22 Πακέτα δεδομένων στο Fiddler

Απλά ανοίγοντας το προφίλ ενός χρήστη, βλέπουμε στο Fiddler 5 πακέτα δεδομένων που χρησιμοποιεί η εφαρμογή για την επικοινωνία της με τον server της. Τα 4 πρώτα πακέτων είναι φωτογραφίες χρηστών, και το 5ο πακέτο είναι τα στοιχεία του χρήστη από το προφίλ που ανοίξαμε. Ανοίγοντας το 5ο πακέτο με τα στοιχεία ενός χρήστη, βλέπουμε κάτι αντίστοιχο με την εικόνα:

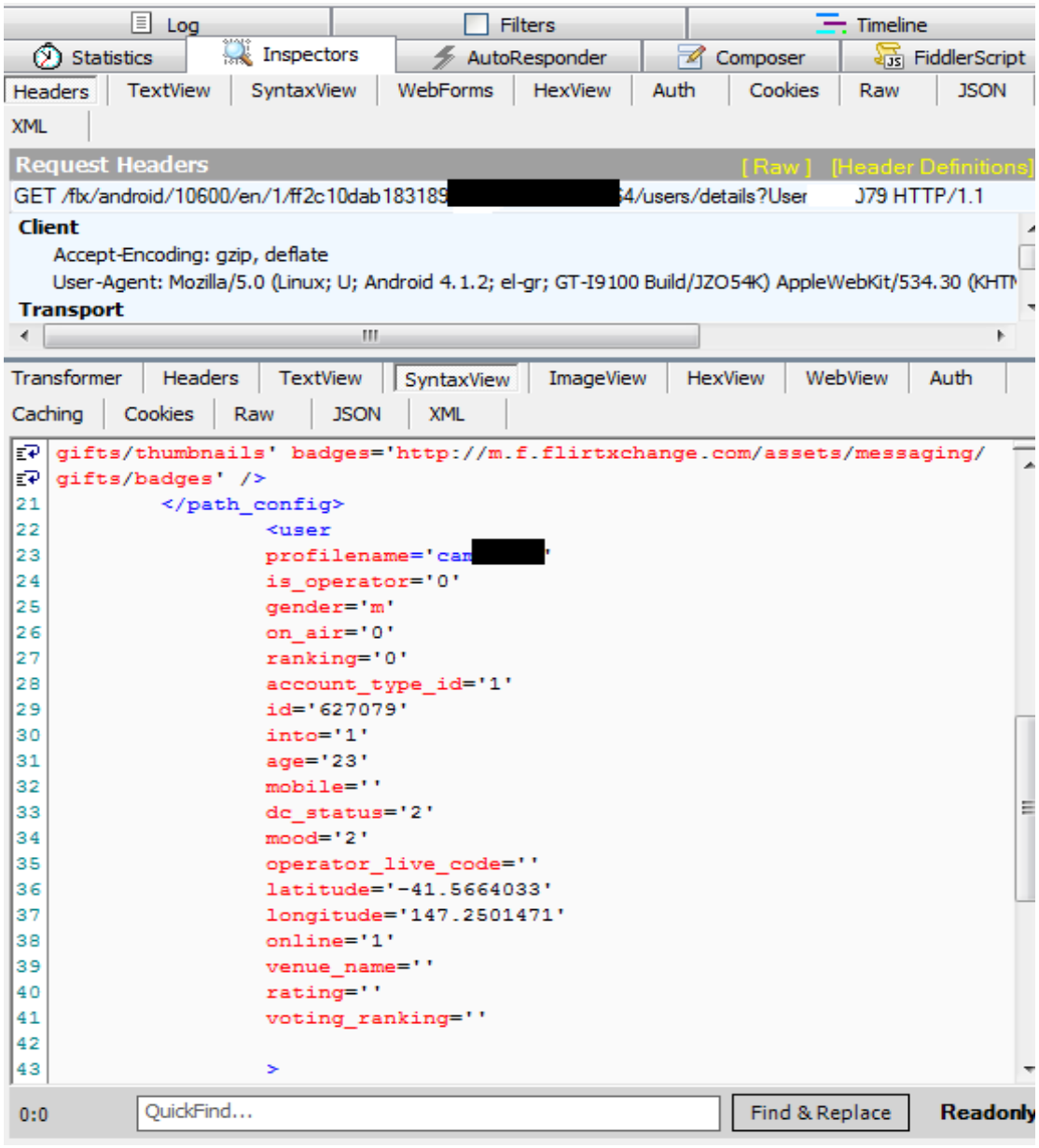

Figure 23 Πληροφορίες σε πακέτο δεδομένων

Από τις παραπάνω εικόνες τα κυριότερα σφάλματα που βλέπουμε είναι ότι:

- Οι εικόνες και τα δεδομένα των χρηστών μεταφέρονται με το πρωτόκολλο Http
- Στο url του 5ου πακέτου φαίνεται το user id του χρήστη που επισκεφτήκαμε
- Στα δεδομένα του χρήστη που επισκεφτήκαμε βλέπουμε ότι υπάρχουν πεδία longitude και latitude που δείχνουν τις ακριβείς γεωγραφικές του συντεταγμένες.

Με αντίστοιχο τρόπο εξετάστηκαν όλες οι εφαρμογές σε αυτή την εργασία.

5.2 SSL Server Test

Στην βιβλιογραφία [10] μπορούμε να βρούμε τον σύνδεσμο για αυτό το εργαλείο που εξετάζει domain names, βρίσκει τρωτά σημεία ασφαλείας, και πολλές φορές προτείνει κατευθείαν την λύση σε αυτά. Ακολουθώντας απλά τον σύνδεσμο για το εργαλείο βλέπουμε αυτή την οθόνη που πρέπει να εισάγουμε ένα domain name. Τα domain names που χρησιμοποιεί κάθε εφαρμογή μπορούμε να τα βρούμε εύκολα από τα πακέτα που βλέπουμε στο Fiddler.

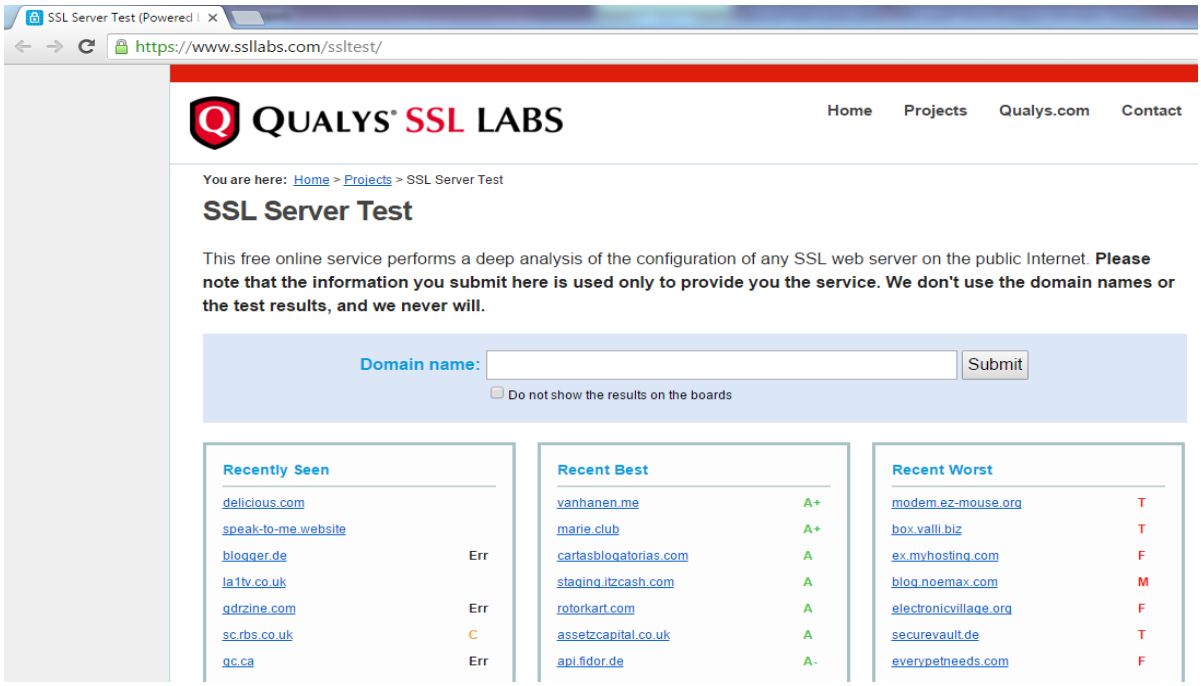

Figure 24 SSL Server Test

Αφού εισάγουμε το domain name που θέλουμε, λίγα δευτερόλεπτα αργότερα θα πάρουμε μία ανάλυση για αυτό το domain name που φαίνεται στην παρακάτω εικόνα.

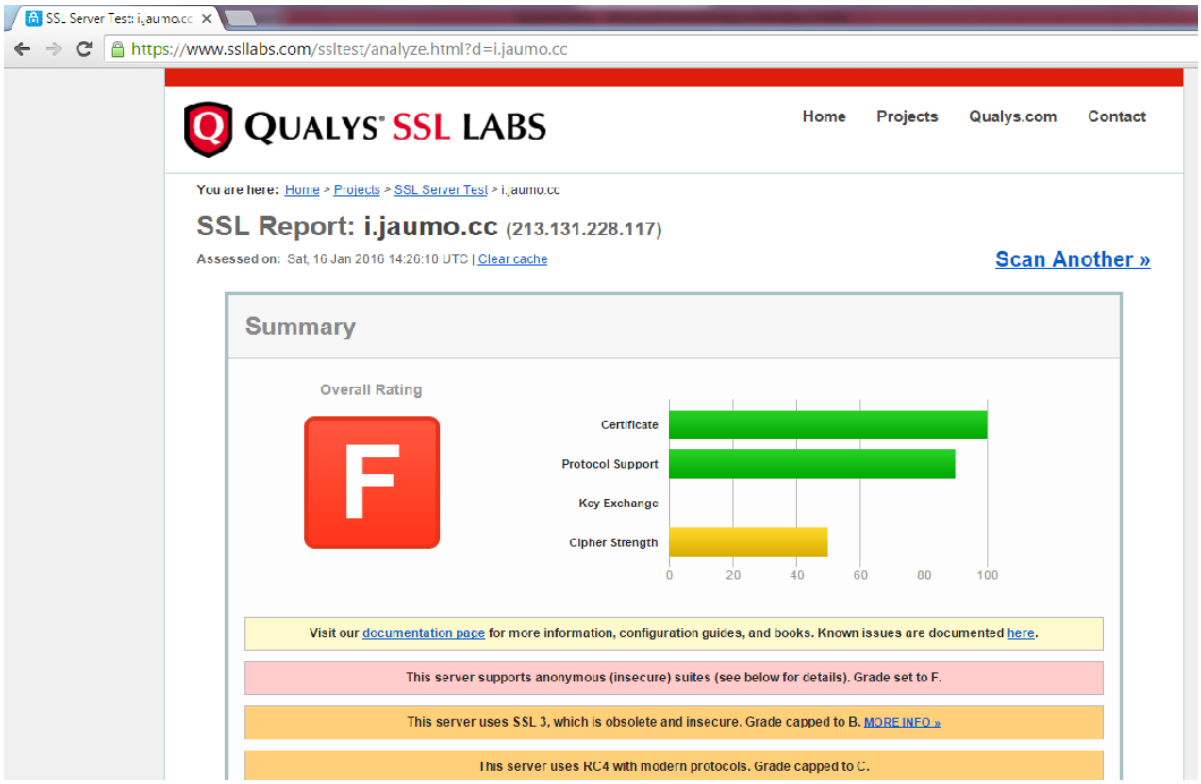

Figure 25 Αποτέλεσμα SSL Test

Μία συνολική βαθμολογία και οι λόγοι που ένας domain δεν θεωρείται ασφαλής φαίνονται στην παραπάνω εικόνα και με μία ματιά καταλαβαίνουμε αμέσως πράγματα για την σημαντικότητα στα σημεία που δεν είναι ασφαλής ένας domain. Με πράσινο χρώμα εμφανίζονται οι domains που δεν έχουν κάποιο σημαντικό πρόβλημα στην ασφάλεια τους, πορτοκαλί αυτοί που έχουν μέτρια προβλήματα ασφαλείας, ενώ σε domains που βλέπουμε το κόκκινο χρώμα υπάρχει κάποιο σημείο στην ασφάλεια του που πρέπει να λυθεί άμεσα.

Παρακάτω φαίνονται μερικά στοιχεία για τις εφαρμογές που εξετάστηκαν, την ‘βαθμολογία’ (grade) που λάβαν από το παραπάνω εργαλείο, τα σημαντικότερα σφάλματα που έχουν βρεθεί, και ποιοι domains τα είχαν.

Application	Domain	Grade for main Domain	Domain for Images	Grade for Image Domain
Choice of Love	choiceoflove.com	B		
Eharmony	eharmony.com	A		
Grindr	primus.grindr.com	A		
GuySpy	api.guyspy.com	B		
Hi5	secure.hi5.com	B		
Hornet	gethornet.com	B		
I-am	node5.citypatrol.ru	T		
Jaumo	api.jaumo.com	F	i.jaumo.cc	F

Lovoo	api.lovoo.net	B		
Matchup	matchupsvc.azurewebsites.net	A		
Singles Around Me	rest.singlesaroundme.com	C		
Single Searcher	fbcdn-profile-a.akamaihd.net	A-		
Tagged	secure.tagged.com	B		
Twoo	jsonapi.twoo.com	B	twoo04-a.akamaihd.net	A-
Voo	api.lovoo.net	B		
Znakomstva	api.mylove.ru	C	f2.mylove.ru	C
Zoosk	api-android.zoosk.com	C	photov3zoosk-a.akamaihd.net	A-

Table 5 SSL Tests για τις εφαρμογές

Από τις 38 εφαρμογές που εξετάστηκαν, οι 17 εφαρμογές χρησιμοποιούσαν Https.
Συνολικά έχουν 16 κύρια domains + 4 domains για εικόνες = 20 domains
Αρίθμηση σφαλμάτων:

Σημαντικά
A) This server's certificate is not trusted, see below for details.
B) This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate.
C) This server supports anonymous (insecure) suites.

Λιγότερο σημαντικά
1) This server supports weak Diffie-Hellman (DH) key exchange parameters.
2) Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings.
3) This server accepts RC4 cipher, but only with older protocol versions.
4) The server does not support Forward Secrecy with the reference browsers.
5) This server's certificate chain is incomplete.
6) This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »
7) This server uses RC4 with modern protocols.
8) Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings.
9) There is no support for secure renegotiation.
10) The server supports only older protocols, but not the current best TLS 1.2.

Και τώρα θα δούμε τους domains που έχουν τα παραπάνω λάθη που αναφέρθηκαν, και σε ποιες εφαρμογές αντιστοιχούν.

Domain/Flaw number	1	2	3	4	5	6	7	8	9	10	A	B	C
choiceoflove.com													
eharmony.com													

primus.grindr.com													
api.guyspy.com													
secure.hi5.com													
gethornet.com													
node5.citypatrol.ru													
api.jaumo.com													
api.lovoo.net													
matchupsvc.azurewebsites.net													
rest.singlesaroundme.com													
fbcdn-profile-a.akamaihd.net													
secure.tagged.com													
jsonapi.twoo.com													
api.mylove.ru													
api-android.zoosk.com													
i.jaumo.cc													
twoo04-a.akamaihd.net													
f2.mylove.ru													
photov3zoosk-a.akamaihd.net													

Table 6 Domains εφαρμογών και SSL Test

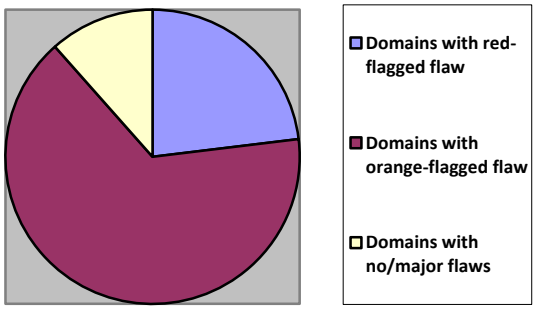

Figure 26 Πίτα αποτελεσμάτων των SLL Tests

5.3 MobSF Mobile Security Framework

Ο σύνδεσμος που υπάρχει στην βιβλιογραφία [11] οδηγεί σε documentation και στη σελίδα που μπορεί κάποιος να αποκτήσει το εργαλείο. Όπως αναλύθηκε και σε άλλο κεφάλαιο το εργαλείο αυτό ελέγχει αρχεία apk και παράγει ένα report σχετικά με την ανάλυση που έκανε, και επισημαίνοντας θέματα ασφαλείας που βρήκε.

Αφού εγκαταστήσουμε το εργαλείο αυτό στον υπολογιστή μας με τον τρόπο που δείχνει το documentation του, ακολουθούμε τα εξής εύκολα βήματα για να αναλύσουμε ένα αρχείο apk.

Σε γραμμή εντολών, εφόσον είμαστε στον κατάλληλο φάκελο που έχουμε κατεβάσει, για να ξεκινήσει να λειτουργεί ένας τοπικός server στον υπολογιστή μας, τρέχουμε την εντολή

python manage.py runserver

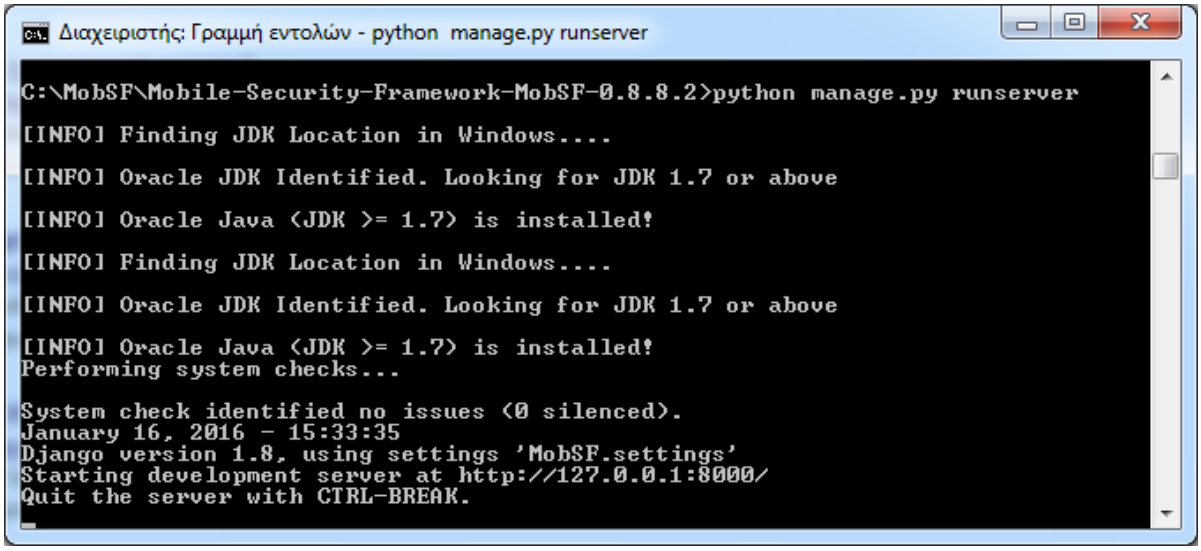

Figure 27 Άνοιγμα MobSF

Έπειτα από έναν browser μπαίνουμε στην διεύθυνση 127.0.0.1:8000 όπου τρέχει αυτός ο server. Η εικόνα που θα δούμε είναι η παρακάτω, και το τι θα πρέπει να κάνουμε για να εξετάσουμε ένα αρχείο apk είναι προφανές

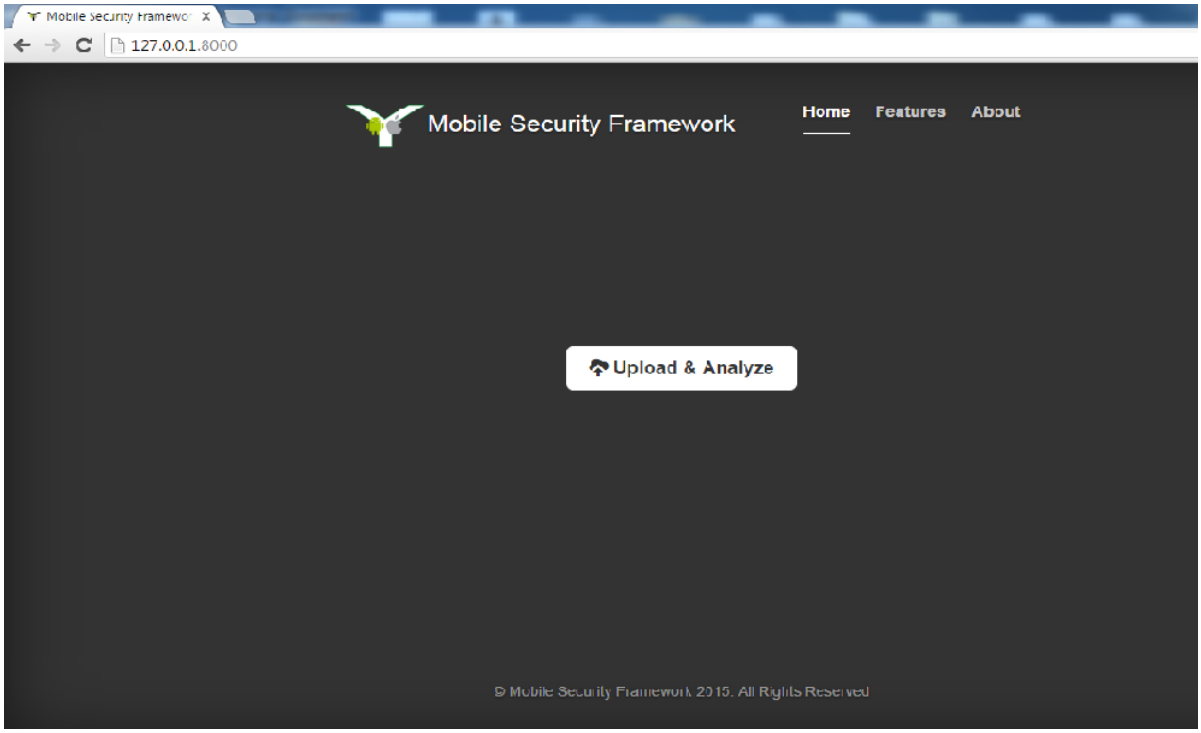

Figure 28 Αρχική Οθόνη MobSF

Αφού πατήσουμε το κουμπί ‘Upload & Analyze’, επιλέγουμε το αρχείο apk που έχουμε στον υπολογιστή μας και αυτό εξετάζεται από το εργαλείο. Το αποτέλεσμα θα είναι αυτό (ένα μέρος του τουλάχιστον)

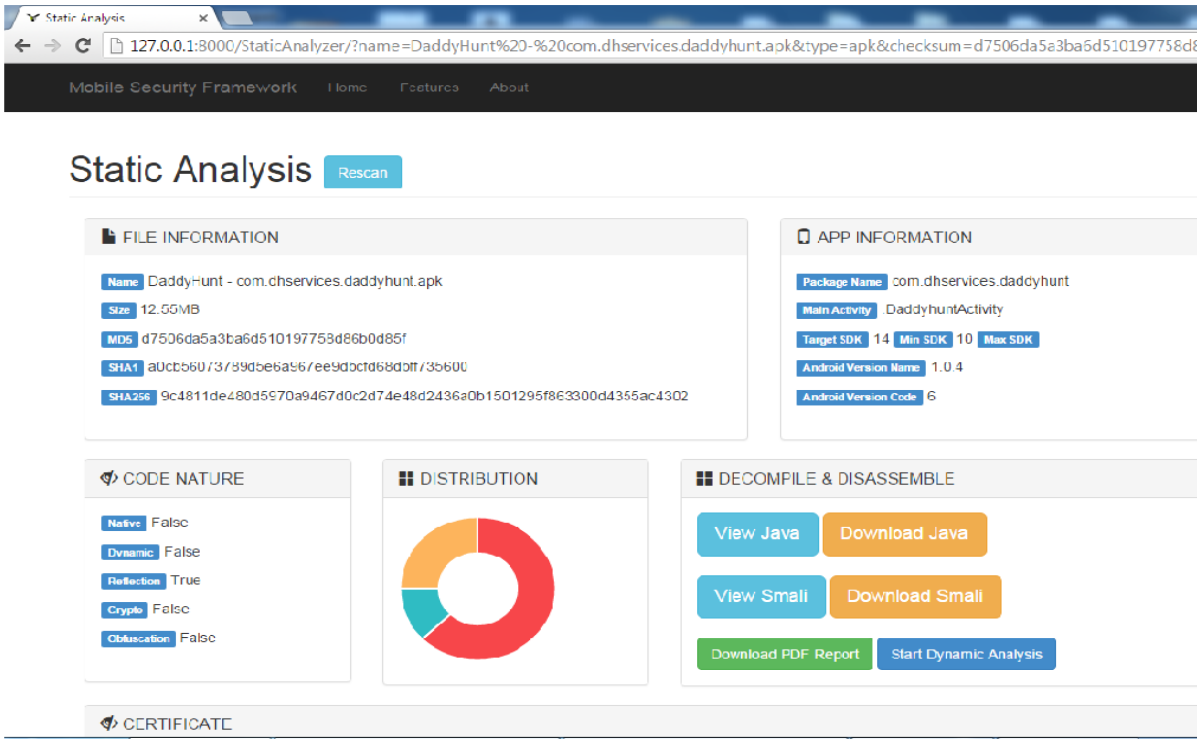

Figure 29 Παράδειγμα αποτελέσματος μίας ανάλυσης με το MobSF

Πατώντας το κουμπί ‘Download PDF Report’, έχουμε ένα αναλυτικό αρχείο σχετικά με την ασφάλεια του αρχείου apk που εξετάσαμε.

Τα reports αυτά είναι πολύ λεπτομερή, παρακάτω όμως έχουμε μερικά συγκεντρωτικά στοιχεία για όλες τις εφαρμογές που εξετάστηκαν σχετικά με τα επικίνδυνα permissions που αποκτούν όταν εγκαθίστανται σε μία κινητή συσκευή. Συγκεκριμένα θα δούμε τα πιο επικίνδυνα permissions που βρέθηκαν, μία περιγραφή για αυτά, και συγκεκριμένα σε ποιες εφαρμογές βρέθηκαν.

Flaw code	Permission	Description
1	android.permission.ACCESS_COARSE_LOCATION	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

2	android.permission.ACCESS_FINE_LOCATION	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
3	android.permission.ACCESS_GPS	Unknown permission from android reference
4	android.permission.ACCESS_LOCATION	Unknown permission from android reference
5	android.permission.ACCESS_MOCK_LOCATION	Create mock location sources for testing. Malicious applications can use this to override the location and/or status returned by real-location sources such as GPS or Network providers.
6	com.google.android.gms.permission.ACTIVITY_RECOGNITION	Unknown permission from android reference
7	android.permission.AUTHENTICATE_ACCOUNTS	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
8	android.permission.BAIDU_LOCATION_dSaEnRgVeIrCouE	Unknown permission from android reference
9	com.android.vending.BILLING	Unknown permission from android reference

10	android.permission.BLUETOOTH	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
11	com.sonyericsson.home.permission.BROADCAST_BADGE	Unknown permission from android reference
12	android.permission.CALL_PHONE	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
13	android.permission.CAMERA	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
14	android.permission.CHANGE_CONFIGURATION	Allows an application to change the current configuration, such as the locale or overall font size.
15	android.permission.CHANGE_WIFI_STATE	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
16	com.android.vending.CHECK_LICENSE	Unknown permission from android reference

17	android.permission.CLEAR_APP_CACHE	Allows an application to free phone storage by deleting files in application cache directory. Access is usually very restricted to system process.
18	android.permission.DISABLE_KEYGUARD	Allows an application to disable the key lock and any associated password security. A legitimate example of this is the phone disabling the key lock when receiving an incoming phone call, then re-enabling the key lock when the call is finished.
19	com.samsung.wmanager.ENABLE_NOTIFICATION	Unknown permission from android reference
20	com.google.android.gallery3d.permission.GALLERY_PROVIDER	Unknown permission from android reference
21	android.permission.GET_TASKS	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
22	com.android.launcher.permission.INSTALLSHORTCUT	Unknown permission from android reference
23	android.permission.INTERNET	Allows an application to create network sockets.
24	net.lovoo.android.permission.LOVOO com.voo.permission.VOO	Unknown permission from android reference

25	android.permission.MANAGE_ACCOUNTS	Allows an application to perform operations like adding and removing accounts and deleting their password.
26	android.permission.MANAGE_DOCUMENTS	Unknown permission from android reference
27	com.dhservices.daddyhunt.permission.MAPS_RECEIVE com.jaumo.permission.MAPS_RECEIVE com.unearby.sayhi.permission.MAPS_RECEIVE de.bsi.singlecheck.permission.MAPS_RECEIVE	Unknown permission from android reference
28	android.permission.MODIFY_AUDIO_SETTINGS	Allows application to modify global audio settings, such as volume and routing.
29	android.permission.MOUNT_UNMOUNT_FILESYSTEMS	Allows the application to mount and unmount file systems for removable storage.
30	android.permission.NFC	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
31	com.twoo.hawaya.PAYMENT_BROADCAST_PERMISSION	Unknown permission from android reference
32	com.sec.android.provider.badge.permission.READ	Unknown permission from android reference
33	android.permission.READ_CONTACTS	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
34	android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from SD Card.

35	com.google.android.providers.gsf.permission.READ_GSERVICES	Unknown permission from android reference
36	android.permission.READ_LOGS	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
37	android.permission.READ_OWNER_DATA	Unknown permission from android reference
38	android.permission.READ_PHONE_STATE	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
39	android.permission.READ_PROFILE	Allows an application to read the user's personal profile data.
40	com.htc.launcher.permission.READ_SETTINGS	Unknown permission from android reference
41	com.google.android.c2dm.permission.RECEIVE	Unknown permission from android reference
42	android.permission.RECEIVE_SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your

		messages or delete them without showing them to you.
43	android.permission.RECORD_AUDIO	Allows application to access the audio record path.
44	android.permission.SEND_SMS	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
45	android.permission.STORAGE	Unknown permission from android reference
46	android.permission.SYSTEM_ALERT_WINDOW	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
47	com.eharmony.permission.UA_DATA	Unknown permission from android reference
48	com.majeur.launcher.permission.UPDATE_BADGE	Unknown permission from android reference
49	com.anddoes.launcher.permission.UPDATECOUNT	Unknown permission from android reference
50	com.htc.launcher.permission.UPDATE_SHORTCUT	Unknown permission from android reference
51	android.permission.USE_CREDENTIALS	Allows an application to request authentication tokens.
52	android.permission.WAKE_LOCK	Allows an application to prevent the phone from going to sleep.
53	com.sec.android.provider.badge.permission.WRITE	Unknown permission from android

		reference
54	android.permission.WRITE_EXTERNAL_STORAGE	Allows an application to write to the SD card.
55	android.permission.WRITE_OWNER_DATA	Unknown permission from android reference
56	android.permission.WRITE_SETTINGS	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
57	android.permission.WRITE_SMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
58	android.permission.WRITE_SYNC_SETTINGS	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
59	com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	Unknown permission from android reference
60	android.permission.READ_INTERNAL_STORAGE	Unknown permission from android reference
61	com.voo.permission.READ_USER_DATAdangerous	Unknown permission from android reference
62	android.permission.ACCESS_ASSISTED_GPS	Unknown permission from android reference

Table 7 Στοιχεία για τα permissions από το MobSF

Και εδώ θα δούμε σε ποιες εφαρμογές βρέθηκαν τα παραπάνω αριθμημένα permissions

Application	Permission Flaw Codes
Black Dating for Free	23, 41, 52, 54

BoyAhoy	1, 2, 9, 13, 21, 23, 33, 35, 38, 41, 43, 44, 46, 51, 52, 54, 57
Choice of Love	1, 9, 13, 23, 35, 37, 41, 52, 54, 55
Christian Dating for Free	23, 41, 52, 54
Daddyhunt	1, 2, 9, 12, 13, 23, 27, 35, 41, 51, 52, 54
Date Me	2, 9, 13, 23, 41, 51, 52, 54
Eharmony	11, 13, 19, 23, 32, 38, 40, 41, 47, 48, 49, 50, 52, 53, 54, 59
Eskimi	11, 23, 32, 33, 34, 35, 38, 41, 49, 53, 54
FlirtXchange	1, 2, 9, 12, 13,23, 28, 41, 43, 44, 52, 54
Grindr	1, 2, 13, 21, 23, 30, 38, 41, 46, 54
GuySpy	1, 2, 5, 9, 13, 23, 38, 41, 43, 51, 52, 54
Hawaya	1, 2, 9, 15, 23, 31, 33, 38, 41, 42, 44, 52, 54
Hi5	1, 2, 7, 9, 21, 23, 25, 33, 35, 38, 41, 51, 52, 54, 58
Hornet	1, 2, 9, 23, 34, 38, 41, 52, 54, 60
Hot Or Not	-
I-am	1, 2, 15, 21, 23, 30, 36, 41, 43, 51, 52, 54
Jaumo	1, 2, 9, 23, 27, 33, 38, 39, 41, 51, 52, 54
Loveplanet.ru	1, 2, 9, 13, 17, 23, 33, 38, 41, 44, 54
Lovoo	1, 2, 9, 21, 23, 24, 35, 36, 38, 41, 51, 52, 54, 61
Matchup	1, 2, 13, 23, 36, 41, 51, 52, 54
Meet 4u	9, 13, 23, 33, 35, 36, 38, 41, 43, 44, 52, 54
Meet24	9, 13, 23, 33, 35, 36, 38, 41, 43, 44, 52, 54
Mico	1, 2, 3, 8, 9, 13, 14, 15, 21, 23, 26, 29, 34, 35, 36, 38, 39, 43, 45, 46, 54
Miumeet	1, 2, 6, 9, 23, 35, 41, 52, 54
Mocospace	1, 2, 3, 4, 9, 12, 21, 22, 23, 33, 38, 41, 43, 51, 54, 62
On.com	1, 9, 13, 23, 33, 38, 41, 52, 54
Singles Around me	1, 2, 23, 34, 41
SayHi	1, 2, 9, 11, 13, 20, 22, 23, 27, 32, 34, 35, 38, 40, 41, 43, 49, 50, 51, 52,
Single Searcher	1, 2, 9, 23, 27, 35, 54
Skout	1, 2, 9, 13, 21, 23, 33, 35, 38, 41, 43, 44, 46, 51, 52, 54, 57
Tagged	1, 2, 7, 9, 21, 23, 25, 33, 35, 38, 41, 51, 52, 54, 58
Twoo	1, 2, 9, 15, 23, 31, 33, 38, 41, 42, 44, 52, 54
Voo	1, 2, 9, 21, 23, 24, 35, 38, 41, 52, 54, 61
Voxle	1, 2, 7, 9, 10, 16, 18, 21, 23, 25, 34, 35, 36, 38, 41, 43, 52, 54, 56
Waplog	9, 23, 34, 38, 41, 51, 52, 54
Waplog Match	9, 23, 33, 34, 38, 41, 51, 52, 54
Znakomstva	1, 2, 9, 23, 34, 41, 52, 54
Zoosk	1, 2, 13, 23, 33, 38, 39, 41, 51, 52, 54

Table 8 Εφαρμογές με τα permissions που αποκτούν

5.4 DROWN Attack Test

Στην βιβλιογραφία [12] βρίσκουμε τον σύνδεσμο που χρησιμοποιήσαμε για να εξετάσουμε τους domains των εφαρμογών που κάνουν χρήση του πρωτοκόλλου Https. Η εξέταση έγινε συγκεκριμένα ώστε να δούμε αν αυτοί οι domains είναι τρωτοί σε επιθέσεις DROWN. Το εργαλείο είναι πολύ εύκολο στη χρήση του μιας και εισάγουμε σε μία φόρμα το όνομα ενός domain, και το εργαλείο μας ενημερώνει για το αν ή όχι είναι το domain τρωτό στην επίθεση DROWN, και αν είναι μας ενημερώνει την αιτία που είναι τρωτός. Είναι προφανές ότι στις εφαρμογές γνωριμιών που μεταφέρονται προσωπικές πληροφορίες, πρέπει οι domains των εφαρμογών να μην είναι ευάλωτοι σε DROWN επιθέσεις για να μην αποκρυπτογραφούνται τα δεδομένα που διακινούν.

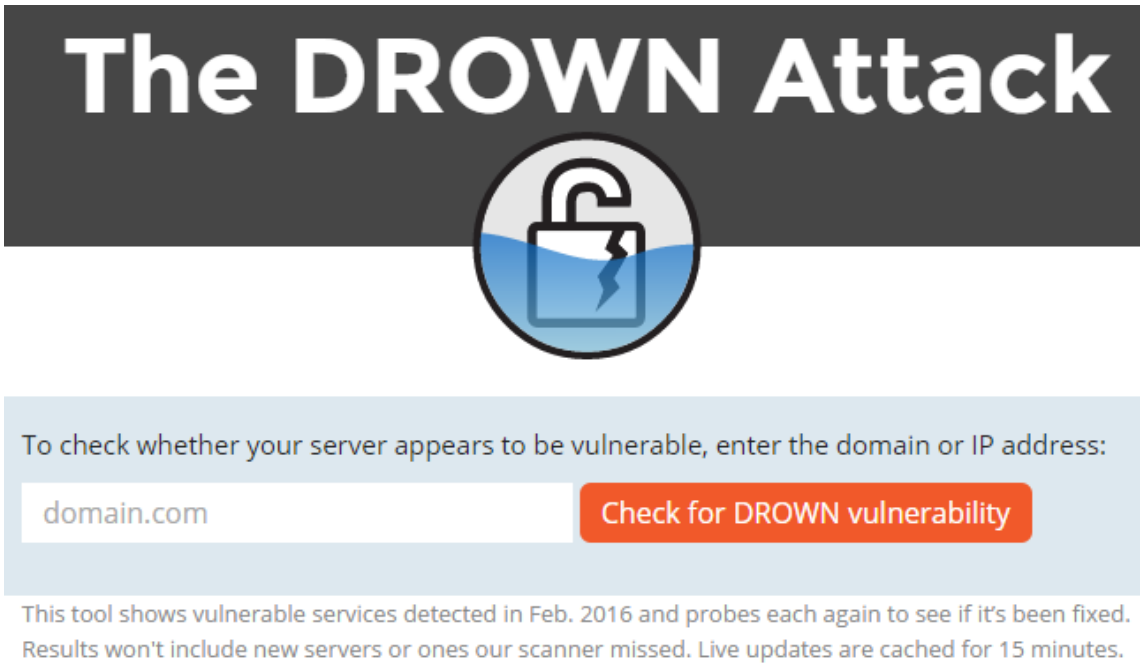

Figure 30 DROWN Attack Test

Στον παρακάτω πίνακα φαίνονται τα αποτελέσματα που πήραμε για τους domains που χρησιμοποιούν το πρωτόκολλο Https από τις εφαρμογές γνωριμιών που εξετάστηκαν.

Domain	Vulnerable to DROWN or not	Vulnerability Because	Vulnerable To
choiceoflove.com	NO		
eharmony.com	YES	supports SSLv2 export ciphers	Eavesdropping
primus.grindr.com	NO		
api.guyspy.com	NO		
secure.hi5.com	NO		
gethornet.com	NO		
node5.citypatrol.ru	NO		
api.jaumo.com	NO		

api.lovoo.net	NO		
matchupsvc.azurewebsites.net	YES	supports SSLv2	Eavesdropping
rest.singlesaroundme.com	NO		
fbcdn-profile-a.akamaihd.net	YES	vulnerable to CVE-2016-0703	Man-in-the-middle-attacks
secure.tagged.com	NO		
jsonapi.twoo.com	NO		
api.mylove.ru	NO		
api-android.zoosk.com	NO		
i.jaumo.cc	NO		
twoo04-a.akamaihd.net	YES	vulnerable to CVE-2016-0703	Man-in-the-middle-attacks
f2.mylove.ru	NO		
photov3zoosk-a.akamaihd.net	YES	vulnerable to CVE-2016-0703	Man-in-the-middle-attacks

Table 9 Αποτελέσματα του DROWN Attack Test

Όπου η επίθεση man-in-the-middle [15] συμβαίνει σε μία επικοινωνία που κάποιος τρίτος (εκτός της επικοινωνίας) μπορεί να ελέγξει την ροή της επικοινωνίας αυτής και να αποσπάσει ή και να αλλάξει πληροφορίες που αποστέλλονται από τα αρχικά μέλη της επικοινωνίας.

Τα eavesdropping [16] συμβαίνει όταν σε μια επικοινωνία κάποιος κακόβουλος τρίτος μπορεί να ‘ακούσει’ τις συνομιλίες σε αυτήν την επικοινωνία, αποσπώντας έτσι τα δεδομένα που διακινούνται.

5.5 Άλλα εργαλεία/εφαρμογές που χρησιμοποιήθηκαν

5.5.1 Fake Gps Location

Πολλές από τις εφαρμογές γνωριμιών χρησιμοποιούν το GPS της κινητής συσκευής για να εντοπίσουν την πραγματική θέση των χρηστών, και στη συνέχεια τους προτείνουν χρήστες που βρίσκονται κοντά τους. Το να δείχνουμε μία διαφορετική τοποθεσία της συσκευής μας από την πραγματική μας, ήταν χρήσιμο διότι μόνο και μόνο αν σκεφτούμε από το από πόσες εφαρμογές μπορεί να διαρρεύσει η τοποθεσία μας, αυτό μας παρείχε μία ασφάλεια. Υπάρχουν πολλές εφαρμογές που βοηθούν σε αυτή τη λειτουργία, του να δείχνουμε δηλαδή μία διαφορετική τοποθεσία μέσω του GPS μας. Συγκεκριμένα για αυτή την εργασία χρησιμοποιήθηκε η εφαρμογή Fake GPS Location [17] που είναι πολύ απλή στη χρήση της.

5.5.2 MyAppSharer

Είδαμε ήδη ότι χρησιμοποιήσαμε ένα εργαλείο για να εξετάσουμε την ασφάλεια των αρχείων apk των εφαρμογών που χρησιμοποιήσαμε. Με την εγκατάσταση μίας εφαρμογής στο κινητό μας, δεν μπορούμε με κάποιον πολύ εύκολο τρόπο να έχουμε και το apk της εφαρμογής. Ο εύκολος τρόπος που χρησιμοποιήθηκε για να αποκτήσουμε πρόσβαση στα αρχεία apk που χρειαζόμασταν, ήταν η χρήση της εφαρμογής MyAppSharer [18] στην κινητή μας συσκευή. Η

εφαρμογή αυτή εντοπίζει τις υπόλοιπες εφαρμογές που έχουμε εγκαταστήσει στην κινητή μας συσκευή, και απλά επιλέγοντας όποια θέλουμε, εξάγεται το αρχείο apk της.

5.5.3 LocalAPK

Η εφαρμογή αυτή [19] χρησιμοποιήθηκε στον υπολογιστή στο λειτουργικό σύστημα Windows. Στην ουσία σκανάρει έναν φάκελο της επιλογής μας με αρχεία apk, και μας παρέχει πληροφορίες για αυτά. Μία χρήση της ήταν πως εύκολα μπορούσαμε να εντοπίσουμε την έκδοση της εφαρμογής που εξετάσαμε, αλλά και την τωρινή έκδοση της κάθε εφαρμογής (πολλές από τις οποίες θα είχαν εκσυγχρονιστεί).

Κεφάλαιο 6ο

6 Συμπεράσματα

Μετά από την χρήση και εξέταση των παραπάνω εφαρμογών γνωριμιών, είδαμε και αναλύσαμε το πόσο ασφαλείς είναι αυτές οι εφαρμογές. Βρέθηκαν πολλά σφάλματα στην ασφάλεια των περισσότερων από αυτών, σφάλματα μέσω των οποίων μπορούν να διαρρεύσουν προσωπικά δεδομένα, άλλα και σφάλματα μέσω των οποίων διαρρέουν πληροφορίες όπως η πραγματική και ακριβή τοποθεσία μας. Αν οποιουδήποτε είδους πληροφορία μας μπορεί να διαρρεύσει, αυτόματα αυτό μπορεί να μας θέσει ακόμα και σε κίνδυνο, ανάλογα με το ποιος μπορεί να δει τις πληροφορίες αυτές.

Η διαδικασία για να μπορέσουμε να ελέγξουμε την ασφάλεια της κάθε εφαρμογής είναι αρκετά απλή και τα εργαλεία που χρησιμοποιήθηκαν είναι λίγα και απλά στην χρήση τους. Έχοντας δει το πόσα σφάλματα ασφαλείας βρέθηκαν στις εφαρμογές που εξετάστηκαν, πρέπει να σκεφτόμαστε το αν είμαστε απόλυτα προστατευμένοι γενικά από τις εφαρμογές που εγκαθιστούμε στις κινητές μας συσκευές. Ο τρόπος να το ελέγξουμε είναι απλός, και είναι μια πολύ καλή λύση το να ελέγχουμε την κάθε εφαρμογή που εγκαθιστούμε στο κινητό μας.

Εκτός αυτού θα πρέπει πάντα να σκεφτόμαστε ότι μέσω των εφαρμογών που χρησιμοποιούμε μπορούμε ακόμα και να θέσουμε τον εαυτό μας σε κίνδυνο, για αυτό πρέπει να σκεφτόμαστε πάντα πράγματα όπως το τι προσωπικά στοιχεία δίνουμε οι ίδιοι στις εφαρμογές που χρησιμοποιούμε ή τι permissions τις επιτρέπουμε να έχουν στη συσκευή μας και να σκεφτόμαστε το πώς μπορούν να μας θέσουν σε κίνδυνο.

Σαν συμπέρασμα λοιπόν βλέπουμε ότι αφού σε εφαρμογές που χρησιμοποιεί ένας τεράστιος αριθμός χρηστών έχουμε τρομερά θέματα στην ασφάλεια των εφαρμογών, πρέπει να ξέρουμε τουλάχιστον το τι κινδύνους μπορεί να αντιμετωπίσουμε οι ίδιοι και το πώς να προστατευτούμε.

Κεφάλαιο 7ο

7 Βιβλιογραφικές Πηγές

[1] C. Patsakis, A. Zigomitros και A. Solanas, «Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures. Comput,» *The Computer Journal,* αρ. (58) 4, pp. 518-535, 2015.

[2] G. Qin, C. Patsakis και M. Bouroch, «Playing Hide and Seek with Mobile Dating Applications,» pp. 185-196, SEC 2014.

[3] C. Patsakis, A. Zigomitros και A. Solanas, «Analysis of Privacy and Security Exposure in Mobile Dating Applications,» pp. 151-162, MSPN 2015.

[4] K.-K. R. Choo, J. Farnden και B. Martini, «Privacy Risks in Mobile Dating Apps,» 2015.

[5] I. Polakis, «Where's Wally?: Precise User Discovery Attacks in Location Proximity Services,» *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,* 2015.

[6] «Hypertext Transfer Protocol - Wikipedia,» [Ηλεκτρονικό]. Available: en.wikipedia.org/wiki/Hypertext_Transfer_Protocol. [Πρόσβαση 1 January 2016].

[7] «HTTPS - Wikipedia,» [Ηλεκτρονικό]. Available: en.wikipedia.org/wiki/HTTPS. [Πρόσβαση 1 January 2016].

[8] «Proxy Server - Wikipedia,» [Ηλεκτρονικό]. Available: en.wikipedia.org/wiki/Proxy_server. [Πρόσβαση 1 January 2016].

[9] «Fiddler free web debugging proxy,» [Ηλεκτρονικό]. Available: http://www.telerik.com/fiddler. [Πρόσβαση 1 January 2016].

[10] «SSL Server Test,» [Ηλεκτρονικό]. Available: www.ssllabs.com/ssltest. [Πρόσβαση 1 January 2016].

[11] «ajinabraham/Mobile-Security-Framework-MobSF,» [Ηλεκτρονικό]. Available: github.com/ajinabraham/Mobile-Security-Framework-MobSF. [Πρόσβαση 1 January 2016].

[12] «DROWN Attack,» [Ηλεκτρονικό]. Available: https://drownattack.com/. [Πρόσβαση 20 March 2016].

[13] «Configure Fiddler for Android,» [Ηλεκτρονικό]. Available: http://docs.telerik.com/fiddler/configure-fiddler/tasks/ConfigureForAndroid. [Πρόσβαση 1 January 2016].

[14] «Configure Fiddler to Decrypt HTTPS Traffic,» [Ηλεκτρονικό]. Available: http://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/DecryptHTTPS. [Πρόσβαση 1 January 2016].

[15] «Man-in-the-middle Attack,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Man-in-the-middle_attack. [Πρόσβαση 1 March 2016].

[16] «Computer Security,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Computer_security#Eavesdropping. [Πρόσβαση 1 March 2016].

[17] «Fake GPS Location,» [Ηλεκτρονικό]. Available: play.google.com/store/apps/details?id=com.lexa.fakegps. [Πρόσβαση 1 January 2016].

[18] «MyAppSharer,» [Ηλεκτρονικό]. Available: play.google.com/store/apps/details?id=com.yschi.MyAppSharer. [Πρόσβαση 1 January 2016].

[19] «LocalAPK,» [Ηλεκτρονικό]. Available: www.breezie.be/dev/localapk. [Πρόσβαση 1 January 2016].