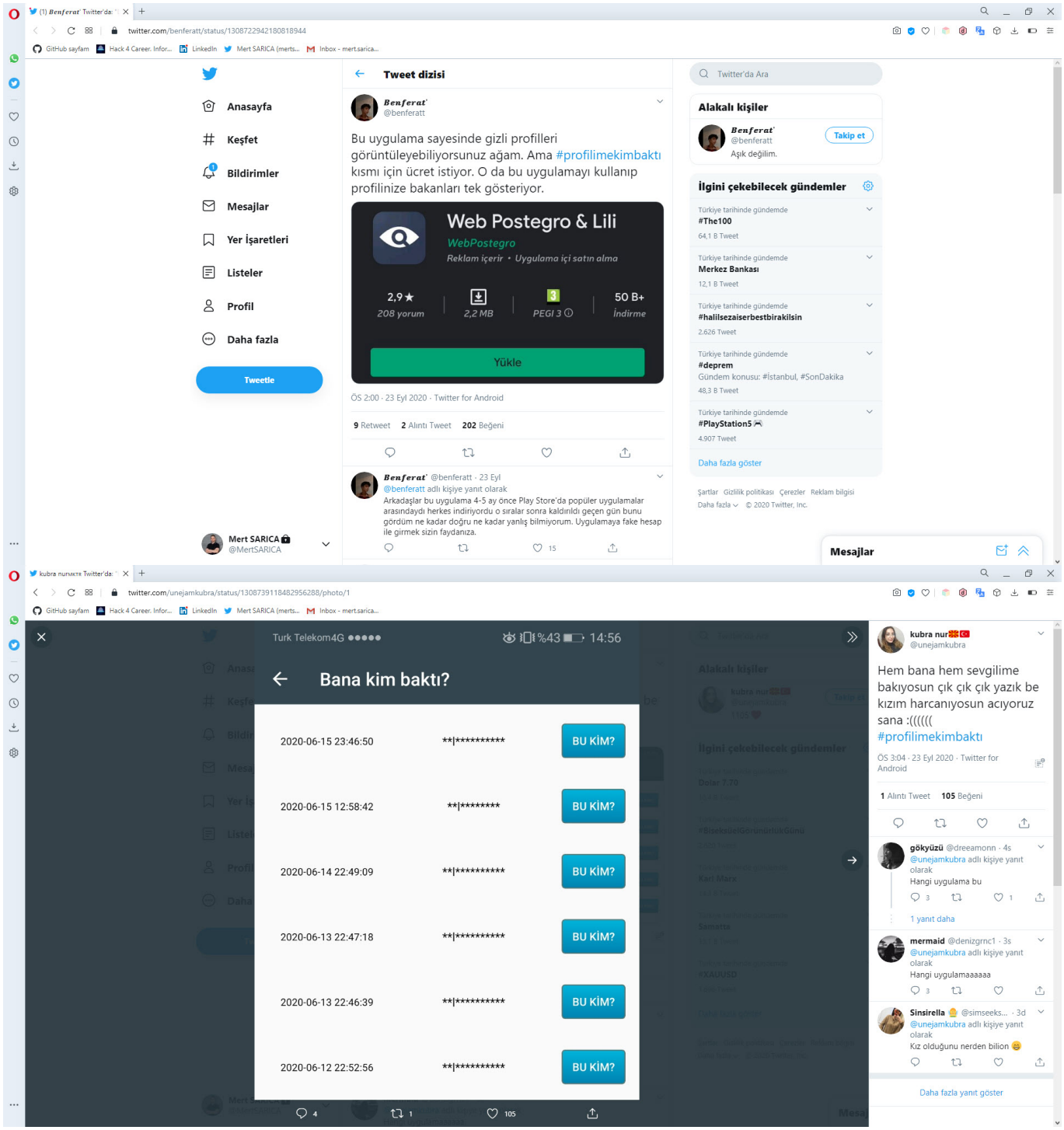
Who Viewed My Profile?

written by Mert SARICA | 1 October 2020

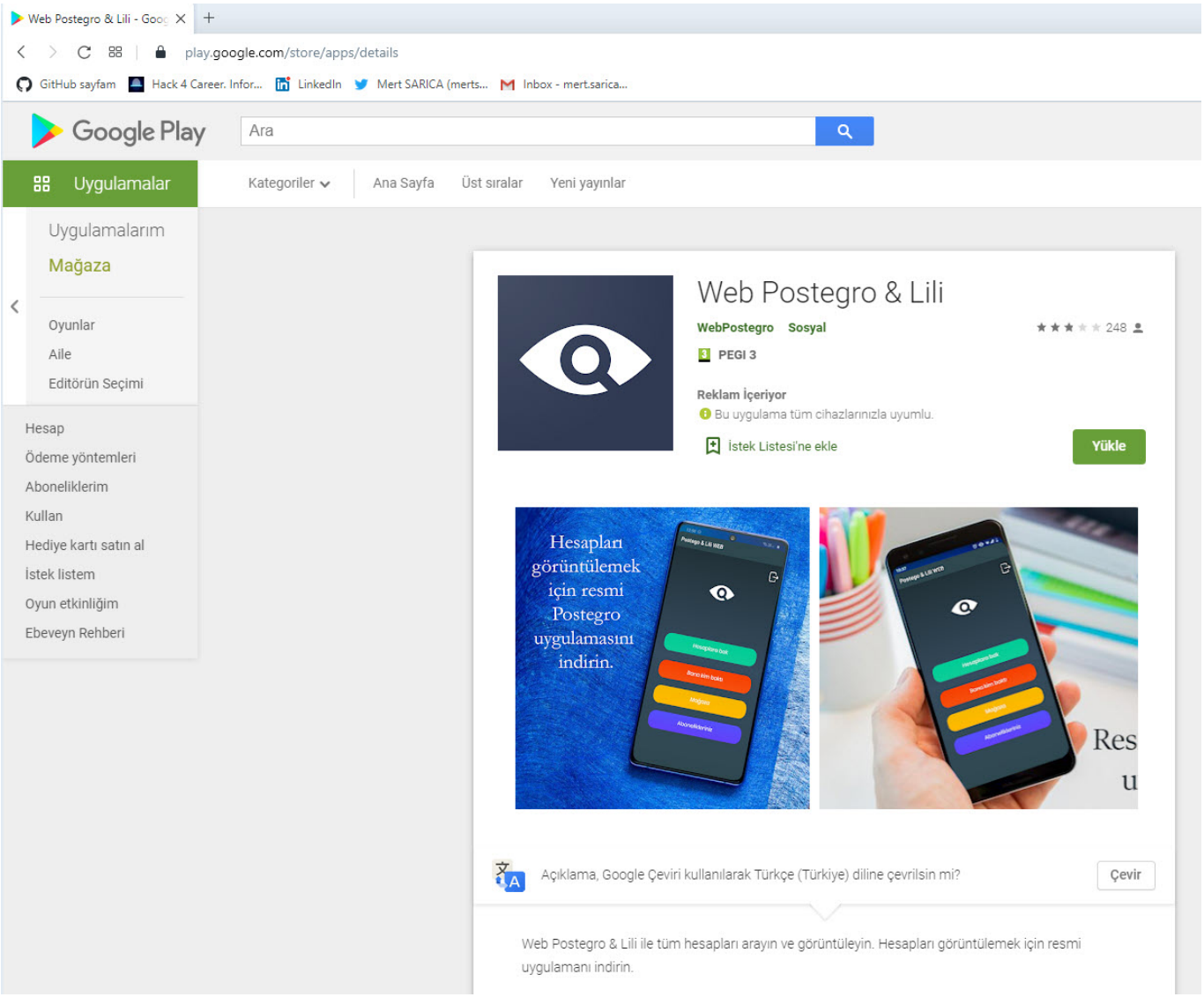
On September 23, 2020, while browsing cybersecurity-related news on Twitter, I noticed the hashtag #profilimekimbaktı in the trending topics. I decided to check the accounts sharing this hashtag as it raised suspicion. One of the accounts had written in their message that the Android app Web Postegro & Lili showed who viewed their profile.

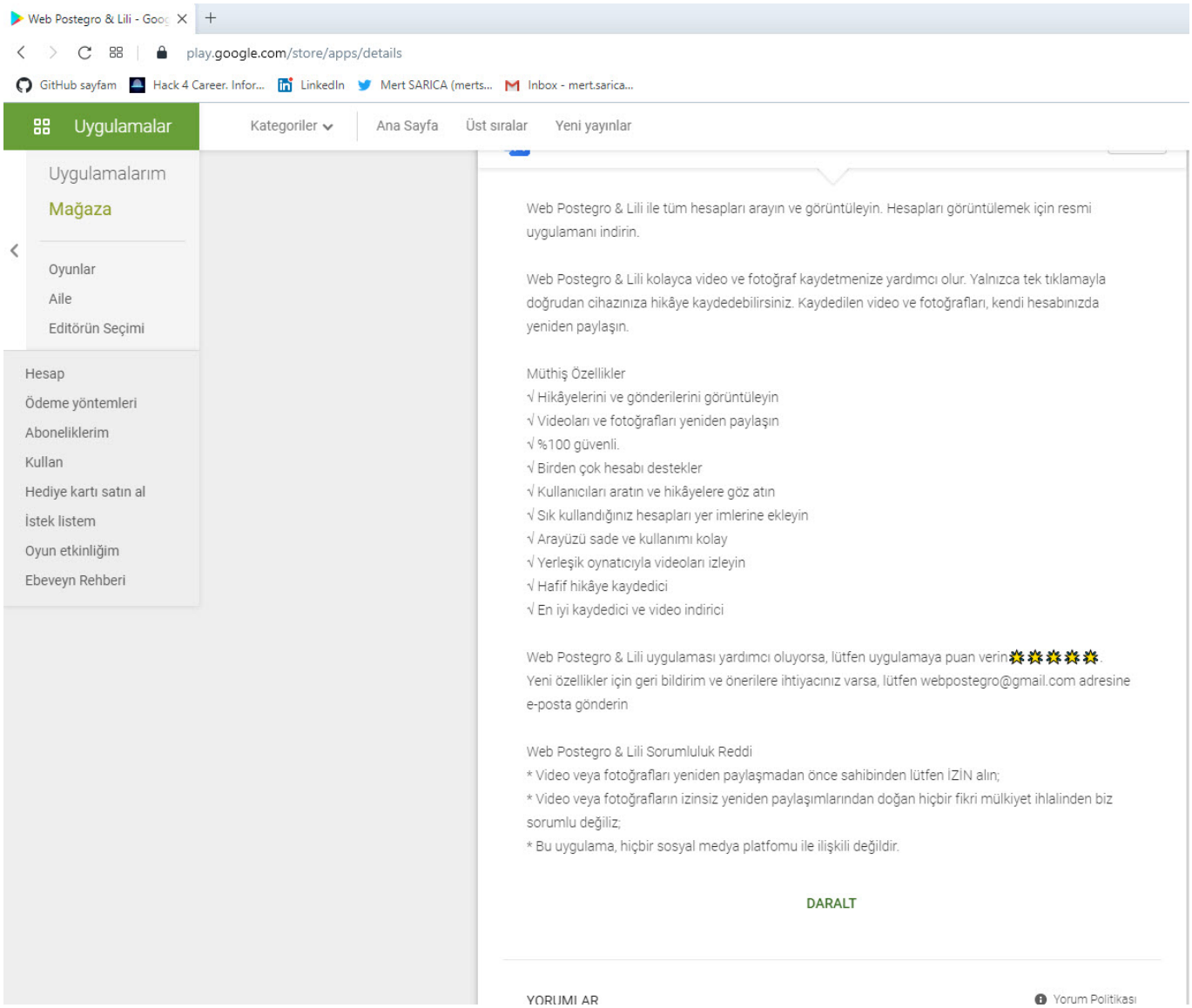


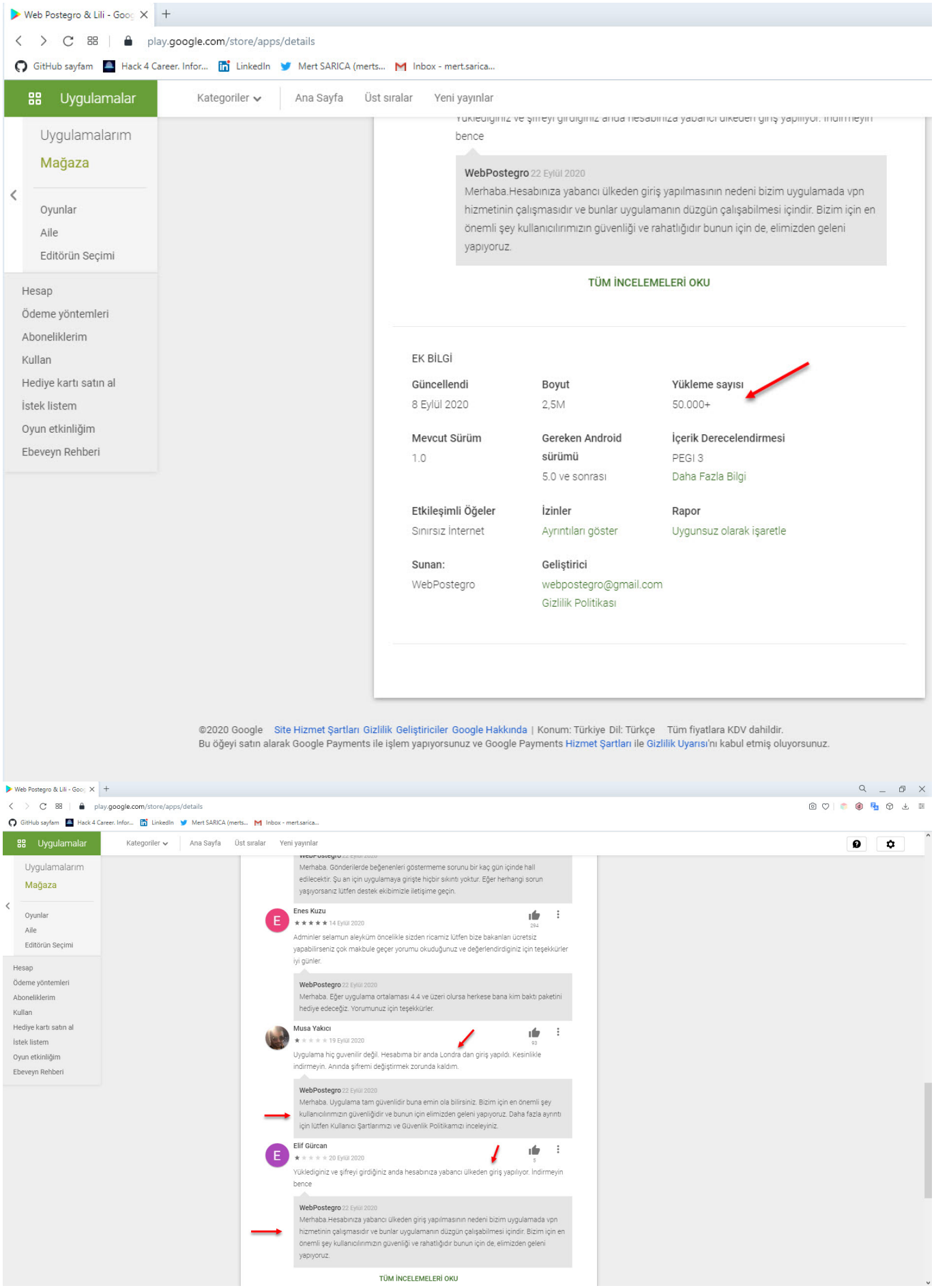
Except for LinkedIn, I have always approached social networks like Twitter, Facebook, and Instagram with skepticism because I know that they do not share the information of profile viewers. I downloaded and analyzed this Android application and wrote about it to understand if my suspicions were justified.

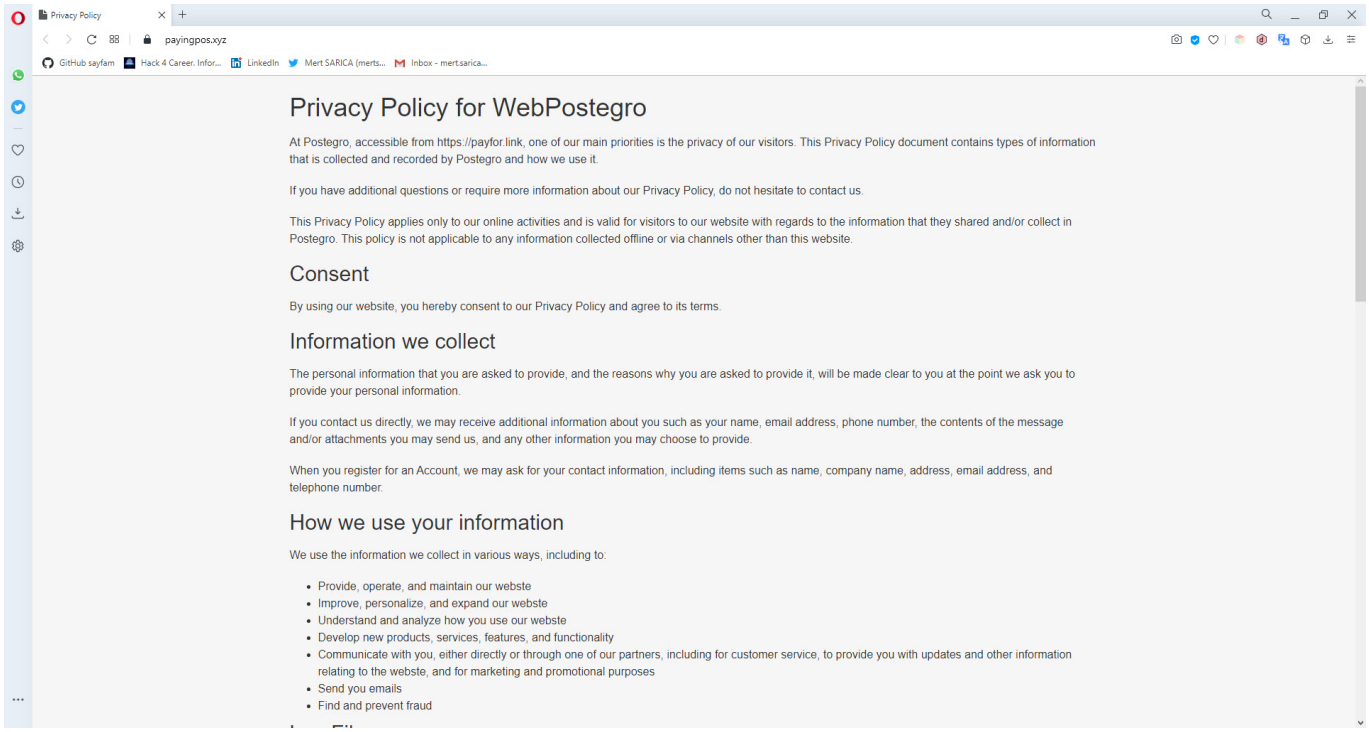
I started by reviewing the page of the Android application Web Postegro & Lili on Google Play. As of September 24, I did not see any permissions that raised any suspicions when I looked at the permissions used by this mobile application, which has been downloaded over 100,000 times. However, when I looked at the comments, I saw some suspicious comments from users claiming

that there were unauthenticated logons to their accounts from unknown sources. Although the developer replied to one of the comments stating that it is stated in their security policy that connections may be made from abroad, I could not find such kind of statement in their policy.



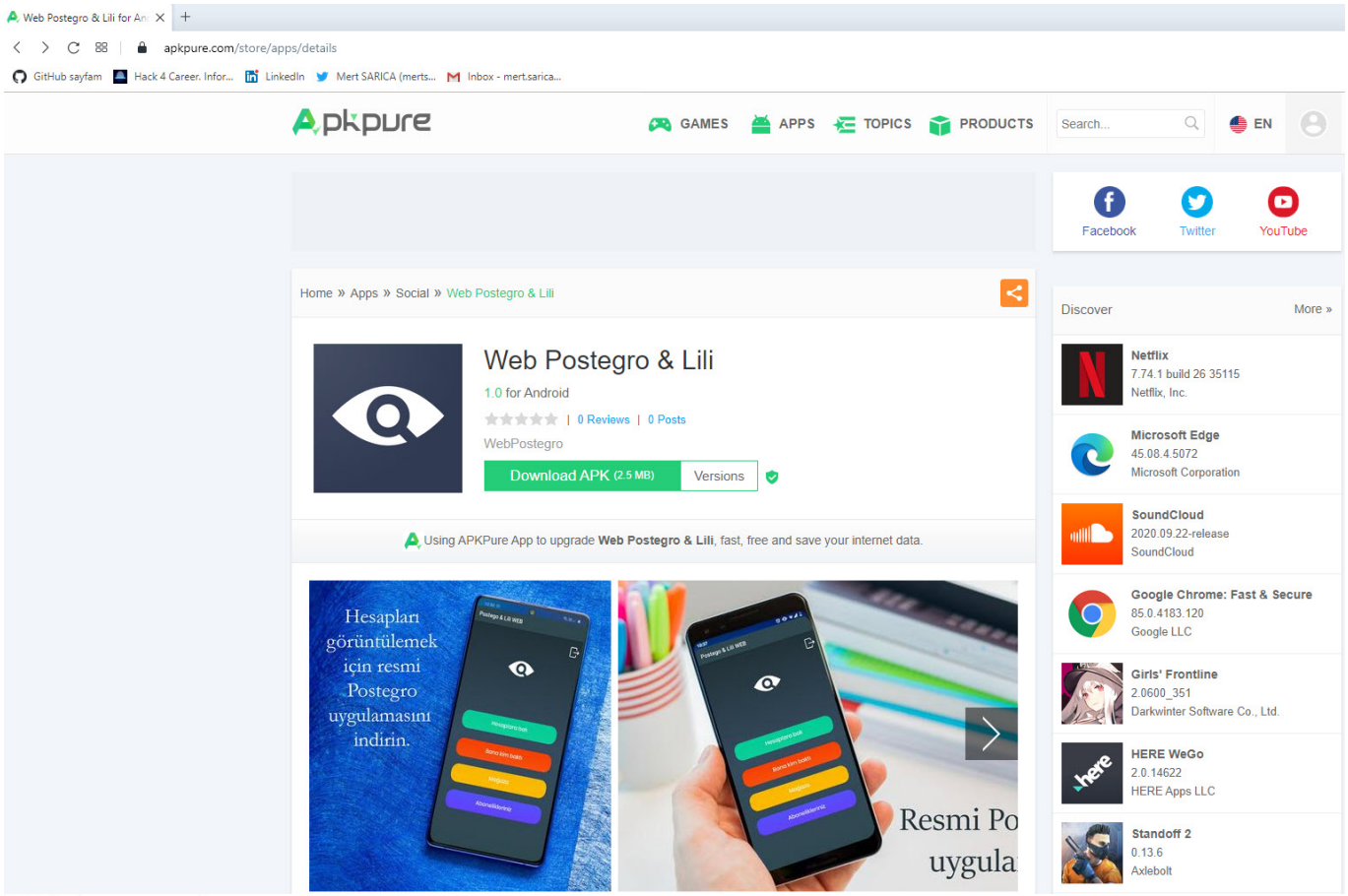

Web Postegro & Lili - Goo
play.google.com/store/apps/details
GitHub sayfam
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Uygulamalar
Kategoriler
Ana Sayfa
Üst sıralar
Yeni yayınlar
Uygulamalarım
Mağaza
Oyunlar
Aile
Editörün Seçimi
Hesap
Ödeme yöntemleri
Aboneliklerim
Kullan
Hediye kartı satın al
İstek listem
Oyun etkinliğim
Ebeveyn Rehberi
Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamanı indirin.
Web Postegro & Lili kolayca video ve fotoğraf kaydetmenize yardımcı olur. Yalnızca tek tıklamayla doğrudan cihazınıza hikâye kaydedebilirsiniz. Kaydedilen video ve fotoğrafları, kendi hesabınızda yeniden paylaşın.
Müthiş Özellikler
√ Hikâyelerini ve gönderilerini görüntüleyin
√ Videoları ve fotoğrafları yeniden paylaşın
√ %100 güvenli.
√ Birden çok hesabı destekler
√ Kullanıcıları aratın ve hikâyelere göz atın
√ Sık kullandığınız hesapları yer imlerine ekleyin
√ Arayüzü sade ve kullanımı kolay
√ Yerleşik oynatıcıyla videoları izleyin
√ Hafif hikâye kaydedici
√ En iyi kaydedici ve video indirici
Web Postegro & Lili uygulaması yardımcı oluyorsa, lütfen uygulamaya puan verin.
Yeni özellikler için geri bildirim ve önerilere ihtiyacınız varsa, lütfen webpostegro@gmail.com adresine e-posta gönderin
Web Postegro & Lili Sorumluluk Reddi
* Video veya fotoğrafları yeniden paylaşmadan önce sahibinden lütfen İZİN alın;
* Video veya fotoğrafların izinsiz yeniden paylaşımlarından doğan hiçbir fikri mülkiyet ihlalinden biz sorumlu değiliz;
* Bu uygulama, hiçbir sosyal medya platformu ile ilişkili değildir.
DARALT
YORUMLAR
Yorum Politikası

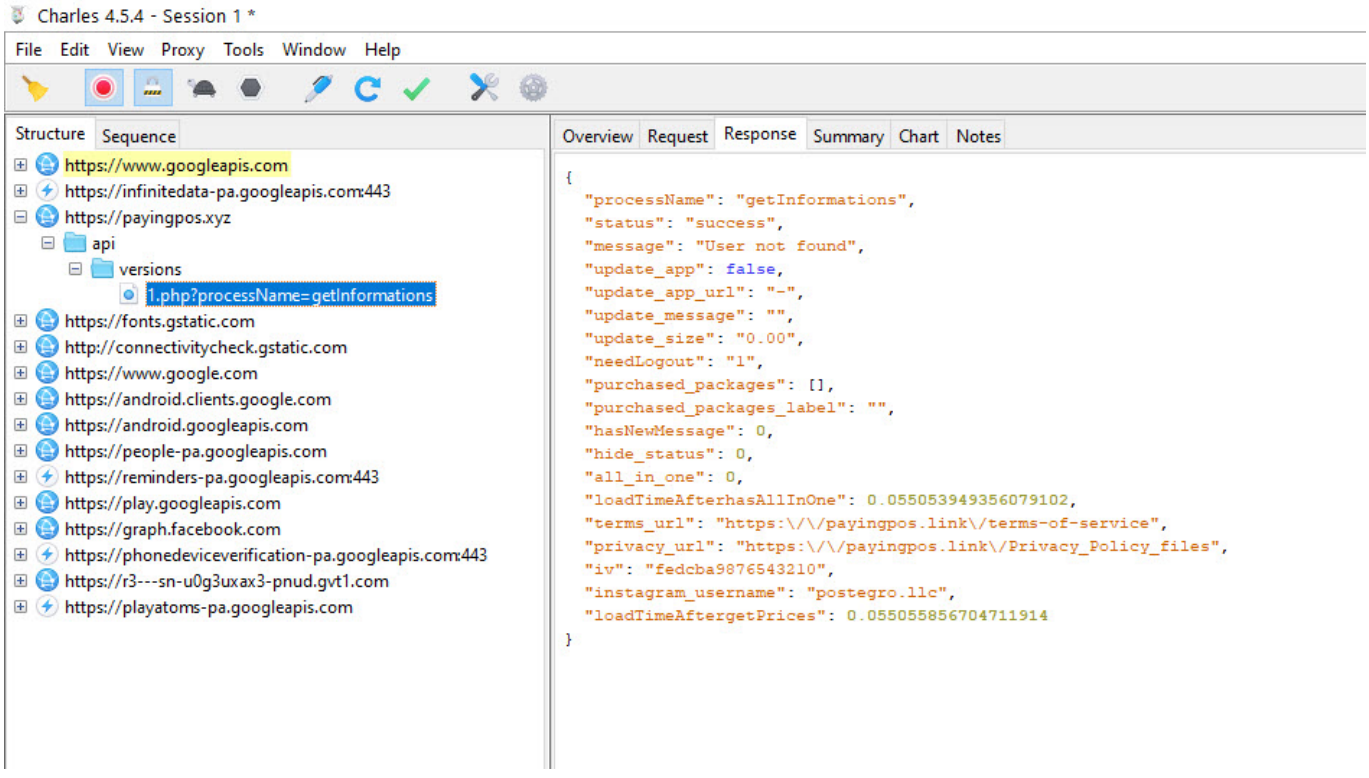

Web Postegro & Lili - Goog
play.google.com/store/apps/details
GitHub sayfam
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Uygulamalar
Kategoriler
Ana Sayfa
Üst sıralar
Yeni yayınlar
Uygulamalarım
Mağaza
Oyunlar
Aile
Editörün Seçimi
Hesap
Ödeme yöntemleri
Aboneliklerim
Kullan
Hediye kartı satın al
İstek listem
Oyun etkinliğim
Ebeveyn Rehberi
bence
WebPostegro 22 Eylül 2020
Merhaba.Hesabınıza yabancı ülkeden giriş yapılmasının nedeni bizim uygulamada vpn hizmetinin çalışmasıdır ve bunlar uygulamanın düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılırımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.
TÜM İNCELEMELERİ OKU
EK BİLGİ
Güncellendi
8 Eylül 2020
Boyut
2,5M
Yükleme sayısı
50.000+
Mevcut Sürüm
1.0
Gereken Android sürümü
5.0 ve sonrası
İçerik Derecelendirmesi
PEGI 3
Daha Fazla Bilgi
Etkileşimli Öğeler
Sınırsız İnternet
İzinler
Ayrıntıları göster
Rapor
Uygunsuz olarak işaretle
Sunan:
WebPostegro
Geliştirici
webpostegro@gmail.com
Gizlilik Politikası
©2020 Google Site Hizmet Şartları Gizlilik Geliştiriciler Google Hakkında | Konum: Türkiye Dil: Türkçe Tüm fiyatlara KDV dahildir.
Bu öğeyi satın alarak Google Payments ile işlem yapıyorsunuz ve Google Payments Hizmet Şartları ile Gizlilik Uyarısı'nı kabul etmiş oluyorsunuz.
Merhaba. Gönderilerde beğenenleri göstermeme sorunu bir kaç gün içinde hall edilecektir. Şu an için uygulamaya girişte hiçbir sıkıntı yoktur. Eğer herhangi sorun yaşıyorsanız lütfen destek ekibimizle iletişime geçin.
Enes Kuzu
14 Eylül 2020
Adminler selamun aleyküm öncelikle sizden ricamız lütfen bize bakanları ücretsiz yapabilirseniz çok makbule geçer yorumu okuduğunuz ve değerlendirdiğiniz için teşekkürler iyi günler.
WebPostegro 22 Eylül 2020
Merhaba. Eğer uygulama ortalaması 4.4 ve üzeri olursa herkese bana kim baktı paketini hediye edeceğiz. Yorumunuz için teşekkürler.
Musa Yakıcı
19 Eylül 2020
Uygulama hiç güvenilir değil. Hesabıma bir anda Londra dan giriş yapıldı. Kesinlikle indirmeyin. Anında şifremi değiştirmek zorunda kaldım.
WebPostegro 22 Eylül 2020
Merhaba. Uygulama tam güvenlidir buna emin ola bilirsiniz. Bizim için en önemli şey kullanıcılırımızın güvenliğidir ve bunun için elimizden geleni yapıyoruz. Daha fazla ayrıntı için lütfen Kullanıcı Şartlarımızı ve Güvenlik Politikamızı inceleyiniz.
Elif Gürcan
20 Eylül 2020
Yüklediginiz ve şifreyi girdiğiniz anda hesabınıza yabancı ülkeden giriş yapılıyor. İndirmeyin bence
WebPostegro 22 Eylül 2020
Merhaba.Hesabınıza yabancı ülkeden giriş yapılmasının nedeni bizim uygulamada vpn hizmetinin çalışmasıdır ve bunlar uygulamanın düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılırımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.
TÜM İNCELEMELERİ OKU

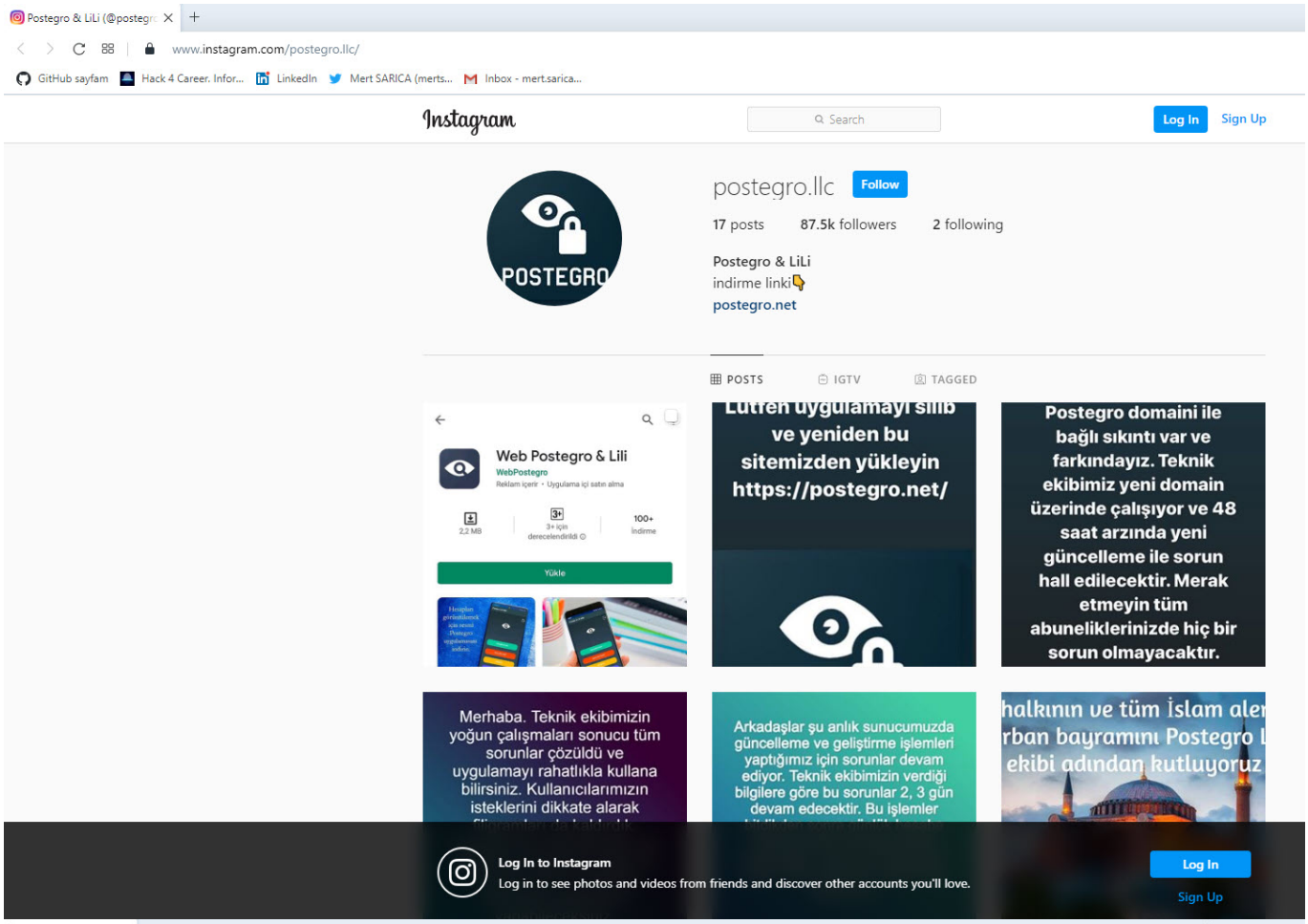


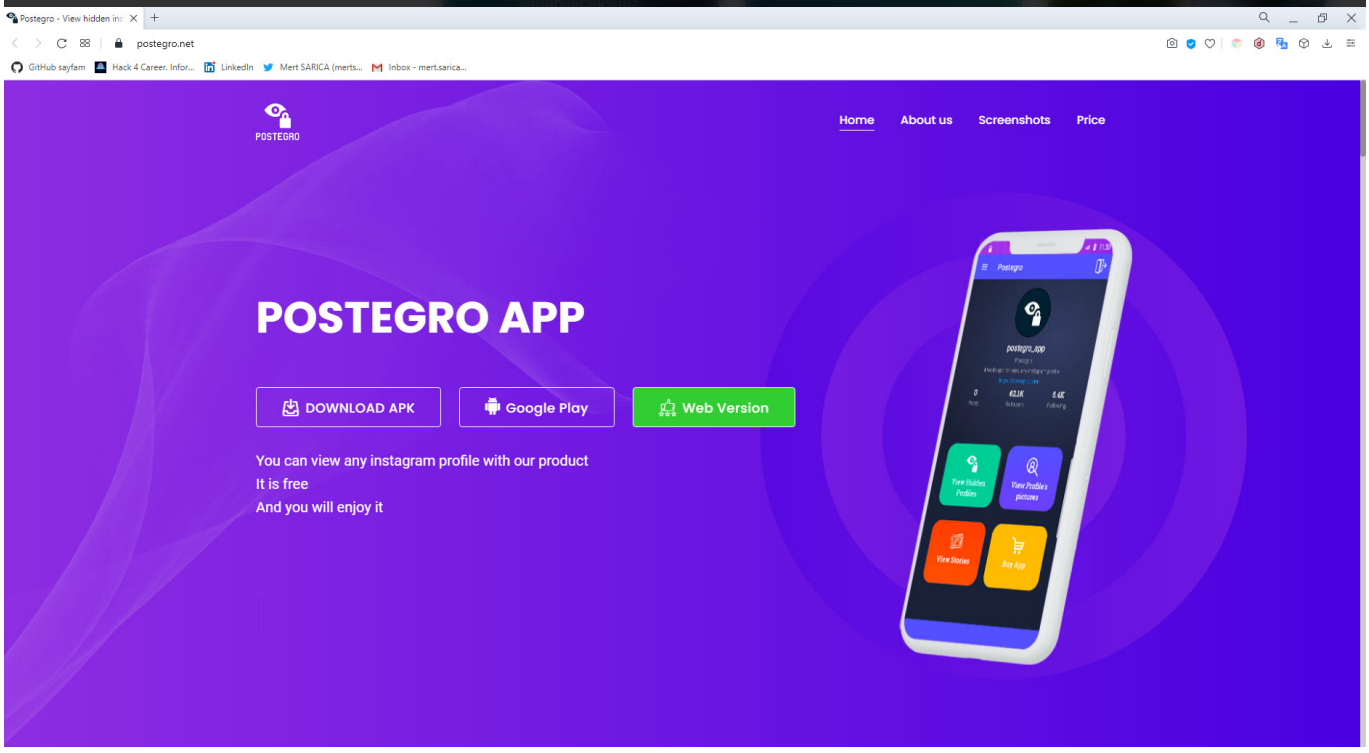
After collecting the preliminary information from the Google Play page, I downloaded the Web Postegro & Lili application from the APKPure website to analyze it. When I uploaded the APK file to VirusTotal, I found no evidence that this application was malicious.

Then, I installed this application on the GenyMotion emulator and began recording the HTTP traffic generated during usage, using Charles Proxy, one of my favorite tools. In the first response from the payingpos[.]xyz web server that the application communicated with, I saw an Instagram account belonging to the application’s developer, postegro.llc. One of the photos shared on the account caught my attention, as it mentioned that the application had been removed from Google Play previously. When I visited the website registered on September 5, which was listed on the Instagram account, I learned that I could directly download the Web Postegro & Lili application (39.apk) from the website.


Web Postegro & Lili for An
apkpure.com/store/apps/details
GitHub sayfam
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Apkpure
GAMES
APPS
TOPICS
PRODUCTS
Search...
EN
Facebook
Twitter
YouTube
Home » Apps » Social » Web Postegro & Lili
Web Postegro & Lili
1.0 for Android
0 Reviews | 0 Posts
WebPostegro
Download APK (2.5 MB)
Versions
Using APKPure App to upgrade Web Postegro & Lili, fast, free and save your internet data.
Hesapları görüntülemek için resmi Postegro uygulamasını indirin.
Resmi Po
uygula
Discover
More »
Netflix
7.74.1 build 26 35115
Netflix, Inc.
Microsoft Edge
45.08.4.5072
Microsoft Corporation
SoundCloud
2020.09.22-release
SoundCloud
Google Chrome: Fast & Secure
85.0.4183.120
Google LLC
Girls' Frontline
2.0600_351
Darkwinter Software Co., Ltd.
HERE WeGo
2.0.14622
HERE Apps LLC
Standoff 2
0.13.6
Axlebolt


Charles 4.5.4 - Session 1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
https://www.googleapis.com
https://infinitedata-pa.googleapis.com:443
https://payingpos.xyz
api
versions
1.php?processName=getInformations
https://fonts.gstatic.com
http://connectivitycheck.gstatic.com
https://www.google.com
https://android.clients.google.com
https://android.googleapis.com
https://people-pa.googleapis.com
https://reminders-pa.googleapis.com:443
https://play.googleapis.com
https://graph.facebook.com
https://phonedeviceverification-pa.googleapis.com:443
https://r3---sn-u0g3uxax3-pnud.gvt1.com
https://playatoms-pa.googleapis.com
Overview
Request
Response
Summary
Chart
Notes
{
"processName": "getInformations",
"status": "success",
"message": "User not found",
"update_app": false,
"update_app_url": "-",
"update_message": "",
"update_size": "0.00",
"needLogout": "1",
"purchased_packages": [],
"purchased_packages_label": "",
"hasNewMessage": 0,
"hide_status": 0,
"all_in_one": 0,
"loadTimeAfterhasAllInOne": 0.055053949356079102,
"terms_url": "https:\/\/payingpos.link\/terms-of-service",
"privacy_url": "https:\/\/payingpos.link\/Privacy_Policy_files",
"iv": "fedcba9876543210",
"instagram_username": "postegro.llc",
"loadTimeAftergetPrices": 0.055055856704711914
}

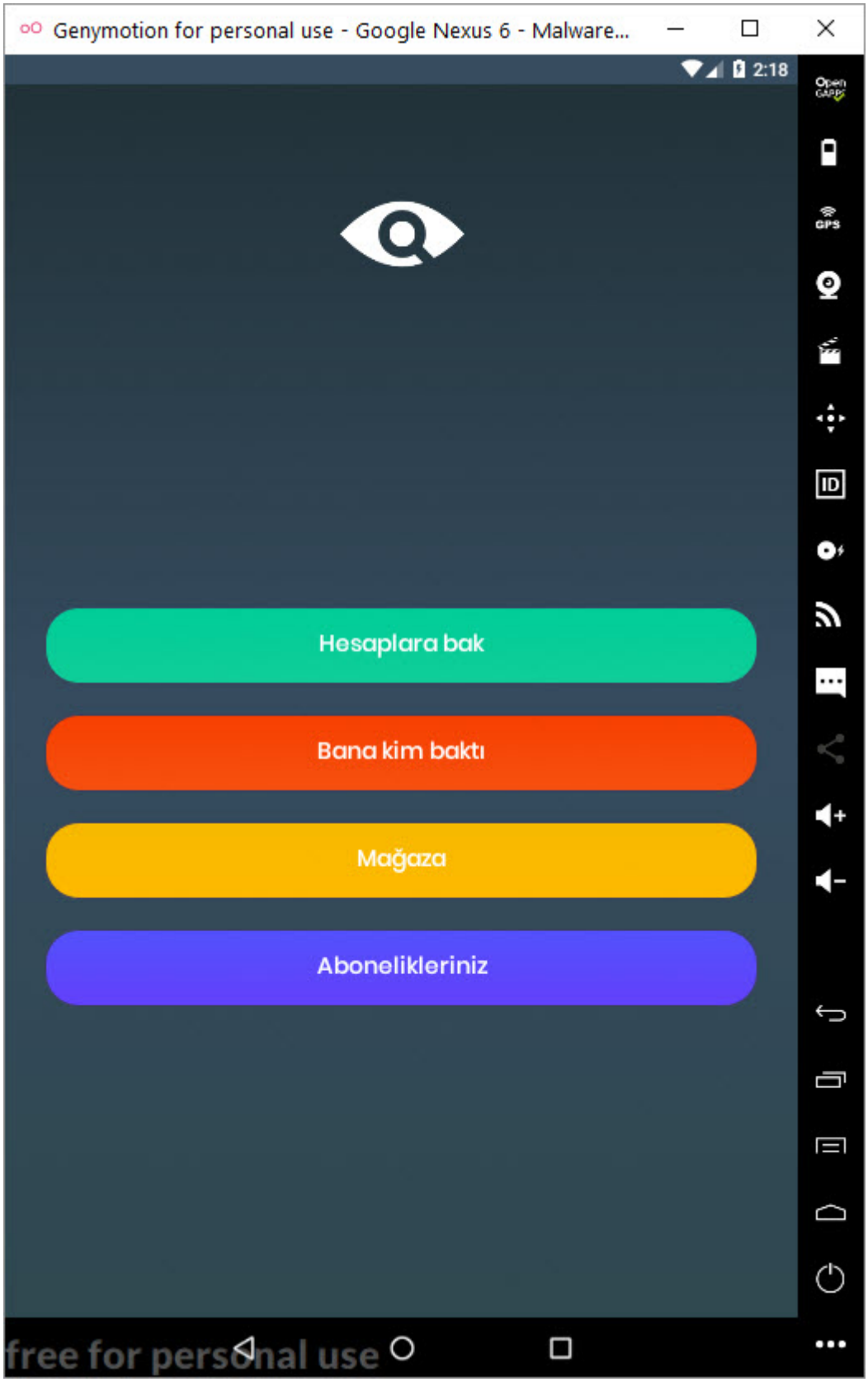


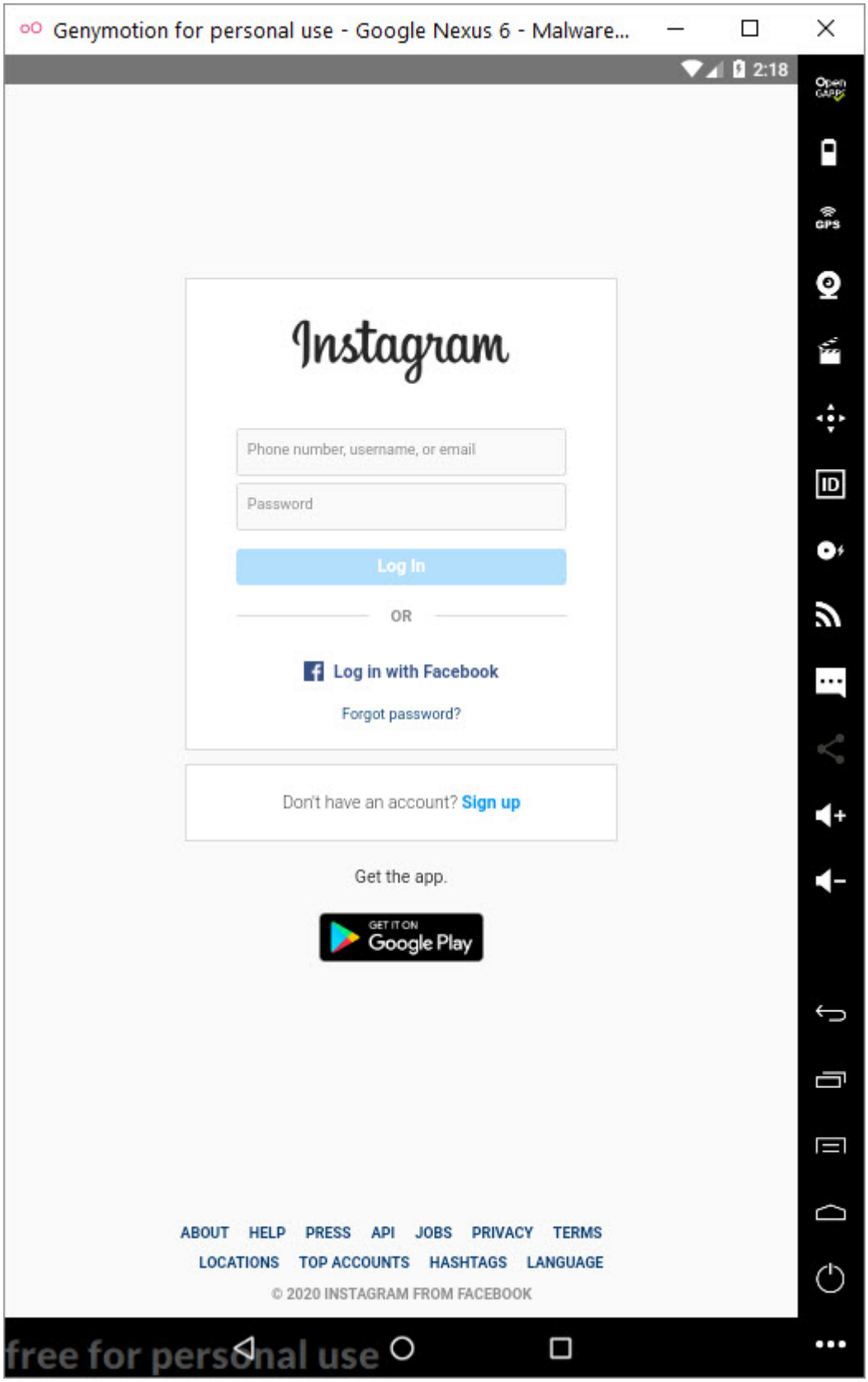


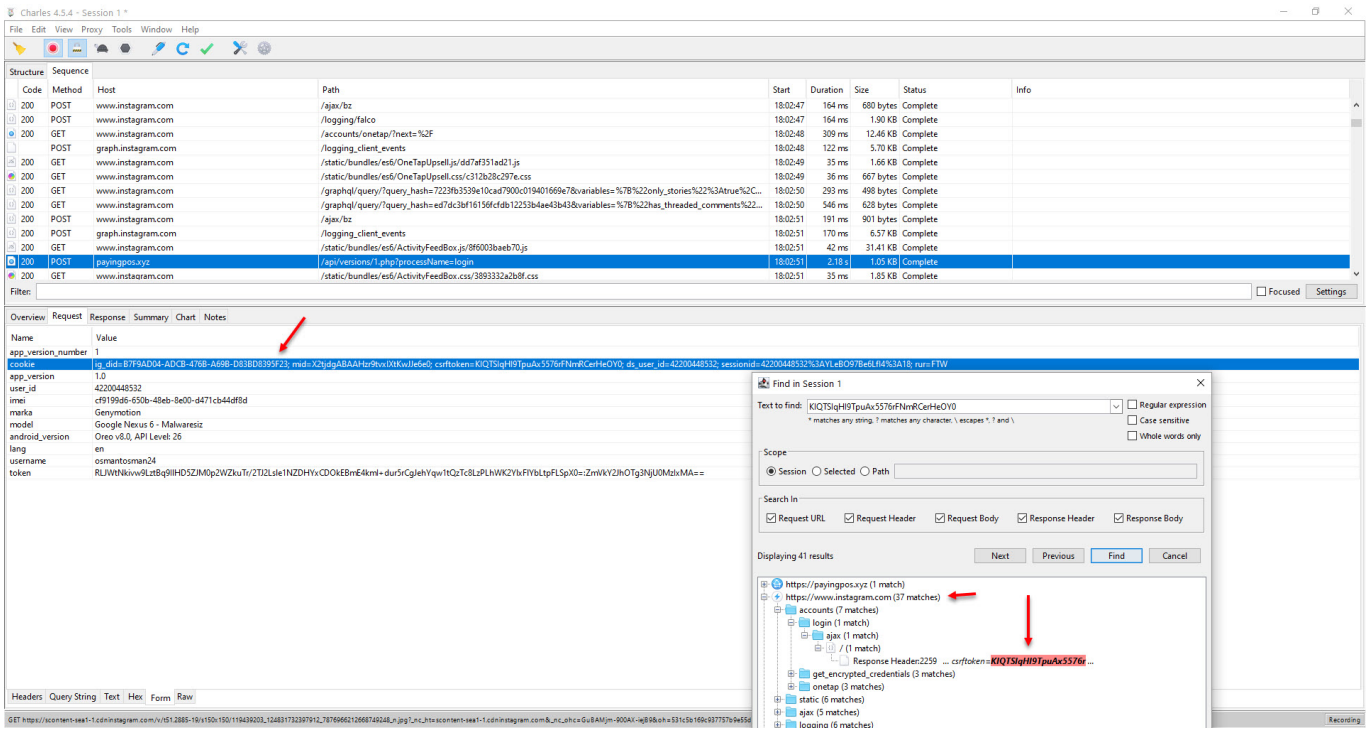
When I examined the traffic recorded with Charles Proxy, I saw that the Web Postegro Lili (Web Postegro Lili_v1.0_apkpure.com.apk) application communicated with the payingpos[.]xyz, webpostegro[.]net, and postegro[.]net servers during use.

When I uploaded the APK file 39.apk to VirusTotal, I did not receive any warning about it being malicious, similar to previous result. When I used the Web Postegro & Lili (39.apk) application, I saw that it communicated with the postegro202039348[.]com, imagecropper2020[.]com, postegro[.]net, and the inactive postegro[.]com servers. Because the postegro[.]com address was not working, and the general functions of the Web Postegro & Lili (39.apk) application, such as viewing profiles that are hidden and viewing profile viewers were not functioning, so I continued my analysis using the Web Postegro & Lili (Web Postegro Lili_v1.0_apkpure.com.apk) application.

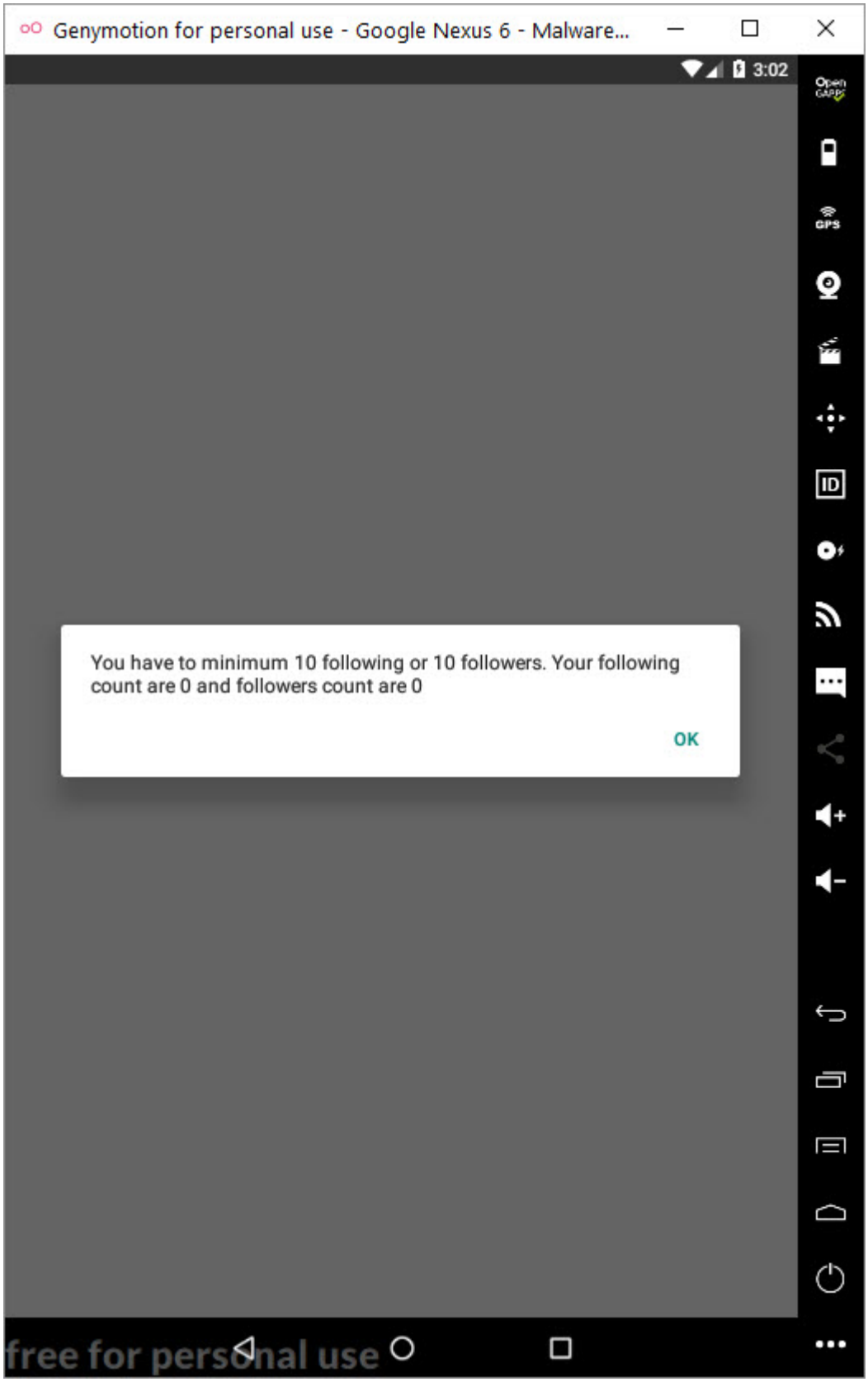
When I ran the Web Postegro & Lili application, I saw menus that allowed me to view profiles set to private (View accounts) and view profile viewers (Who viewed me). When I clicked on the View accounts menu, the application communicated with the instagram.com server through its own interface and brought up the login page where the Instagram username and password were entered. As soon as I logged in with my osmantosman24 Instagram username and password, which I created specifically for this investigation, I noticed that the application sent my session information, which was generated after verification with the instagram.com server, to the payingpos[.]xyz address using the cookie parameter and recorded this and more information in the /data/data/com.web.lilipostego/shared_prefs/com.web.lilipostego_preferences.xml file!

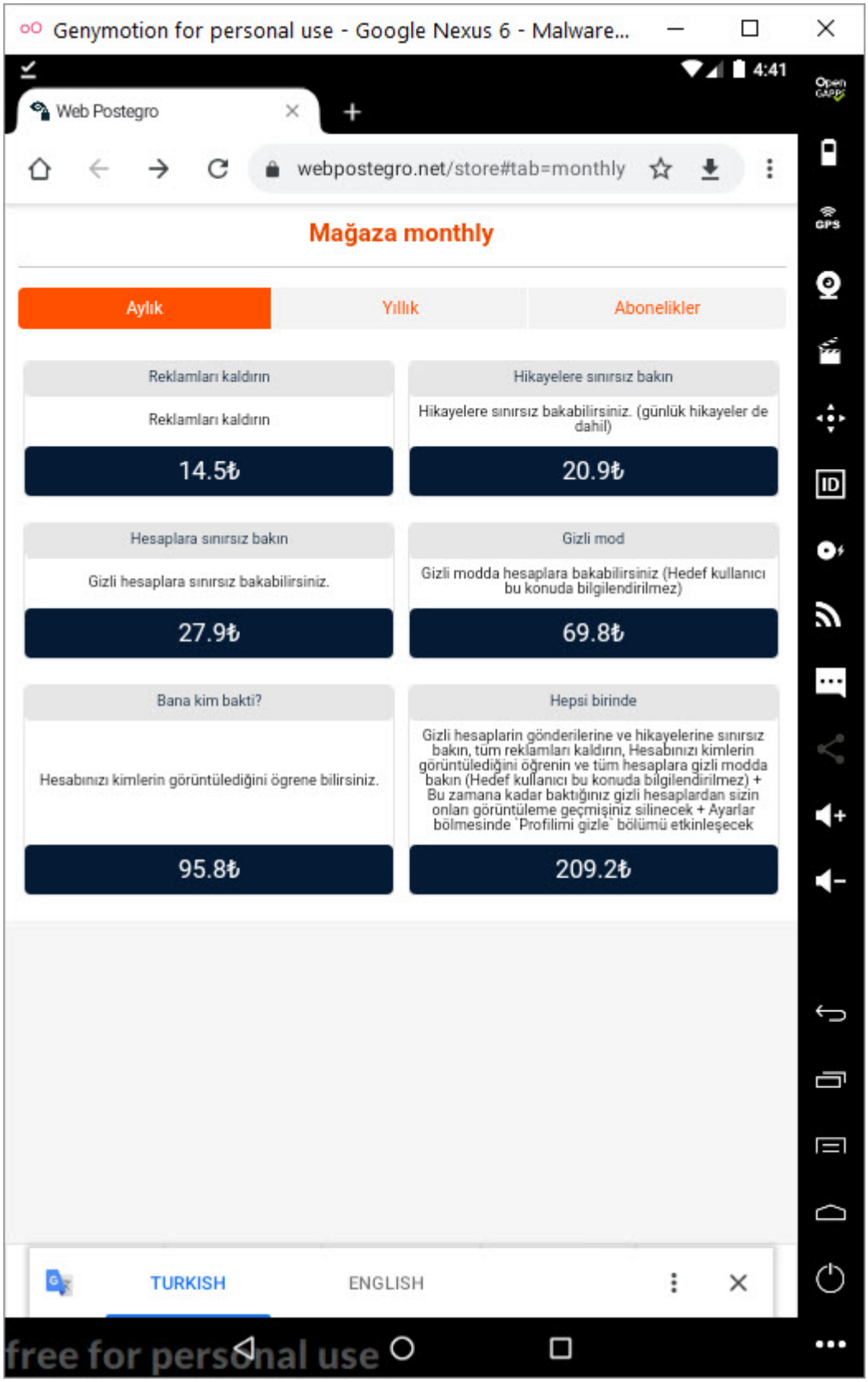

Genymotion for personal use - Google Nexus 6 - Malware...
2:18
Hesaplara bak
Bana kim baktı
Mağaza
Abonelikleriniz
free for personal use

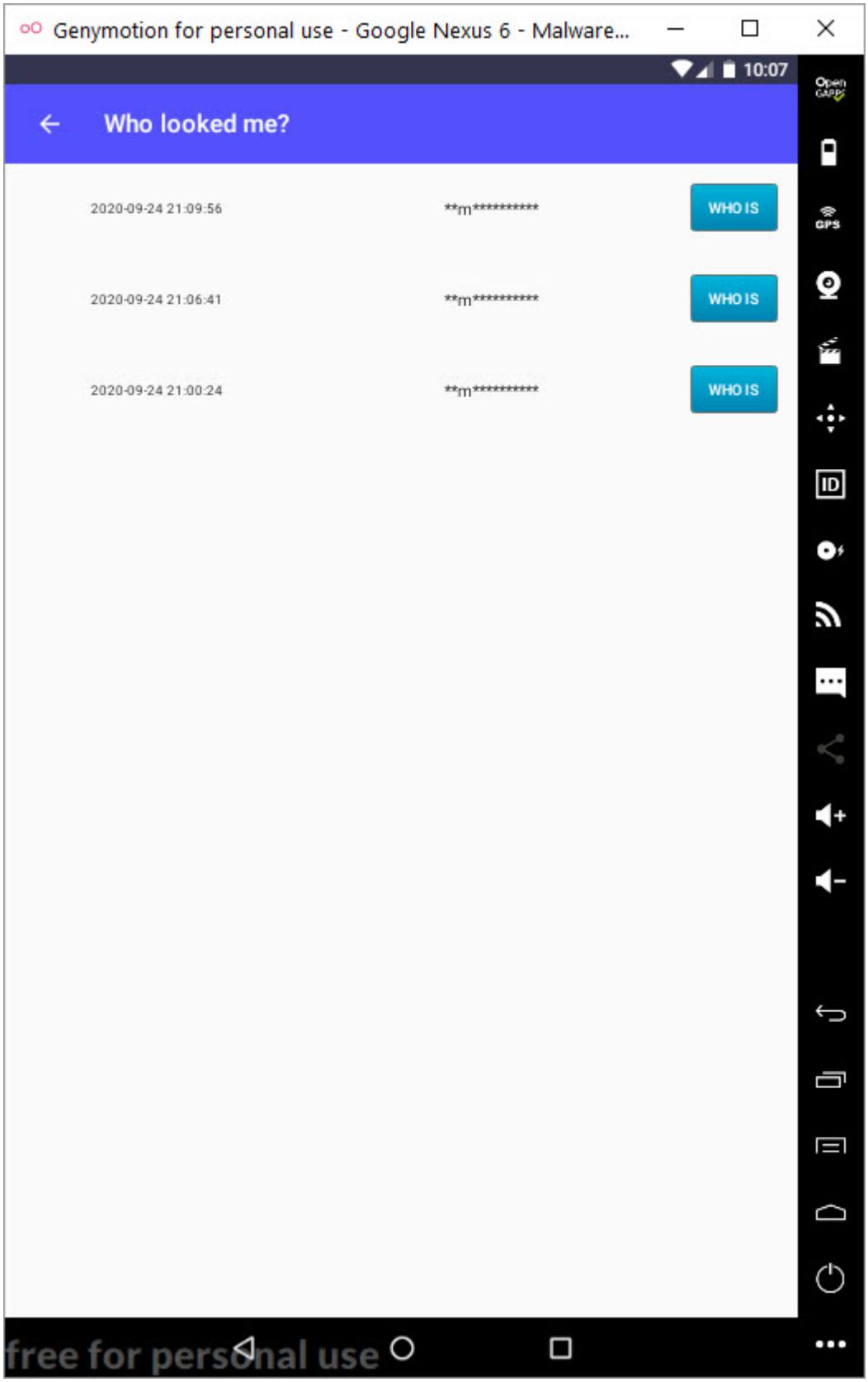

Genymotion for personal use - Google Nexus 6 - Malware...
2:18
Instagram
Phone number, username, or email
Password
Log In
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
GET IT ON Google Play
ABOUT HELP PRESS API JOBS PRIVACY TERMS
LOCATIONS TOP ACCOUNTS HASHTAGS LANGUAGE
© 2020 INSTAGRAM FROM FACEBOOK
free for personal use



To be able to use the application, I had to follow at least 10 people or have 10 people follow me, so I quickly started following Instagram accounts that followed back and made them follow me as well. After increasing my follower count and stopping following all the accounts I was following, I started exploring the menus of the application and could view the content of profiles that were set to private and hidden. This application generates income by charging a certain fee to remove limits on the application (such as removing ads, unlimited viewing of stories, unlimited viewing of accounts, and the uncensored display of names of profile viewers).

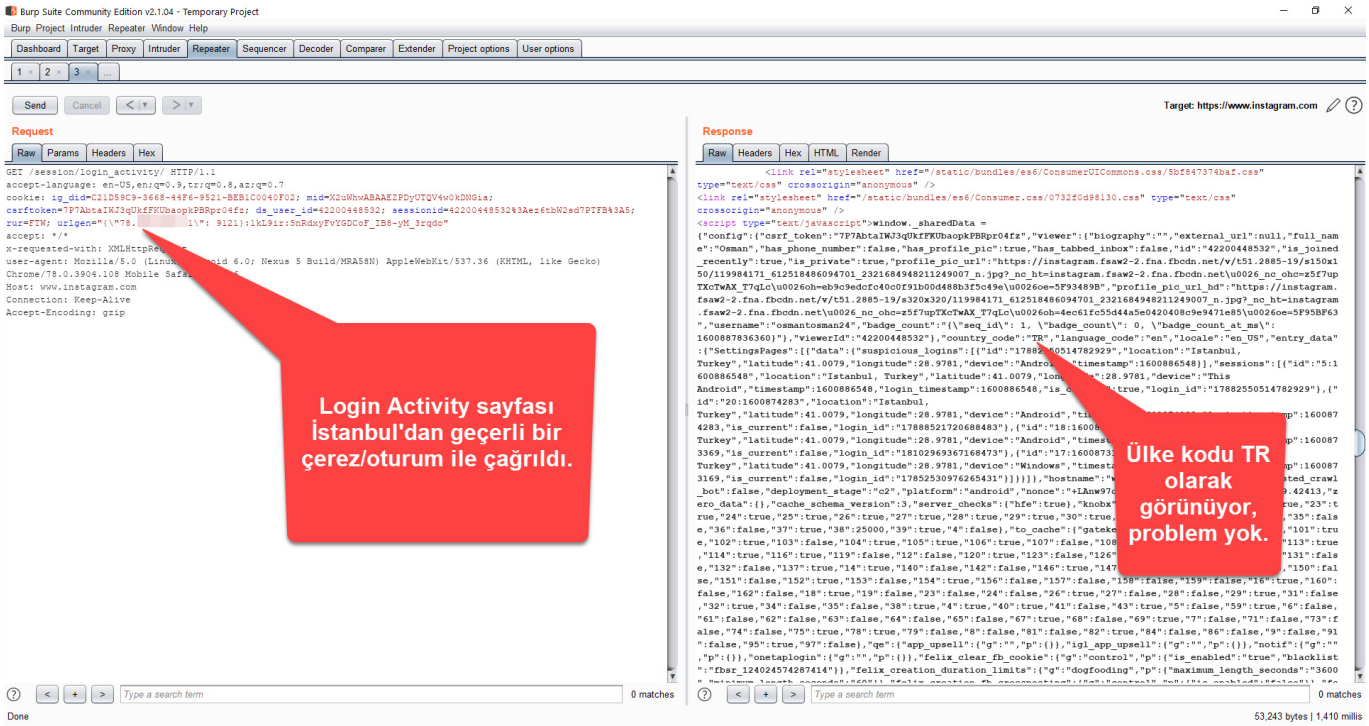

Genymotion for personal use - Google Nexus 6 - Malware...
3:02
You have to minimum 10 following or 10 followers. Your following count are 0 and followers count are 0
OK
free for personal use

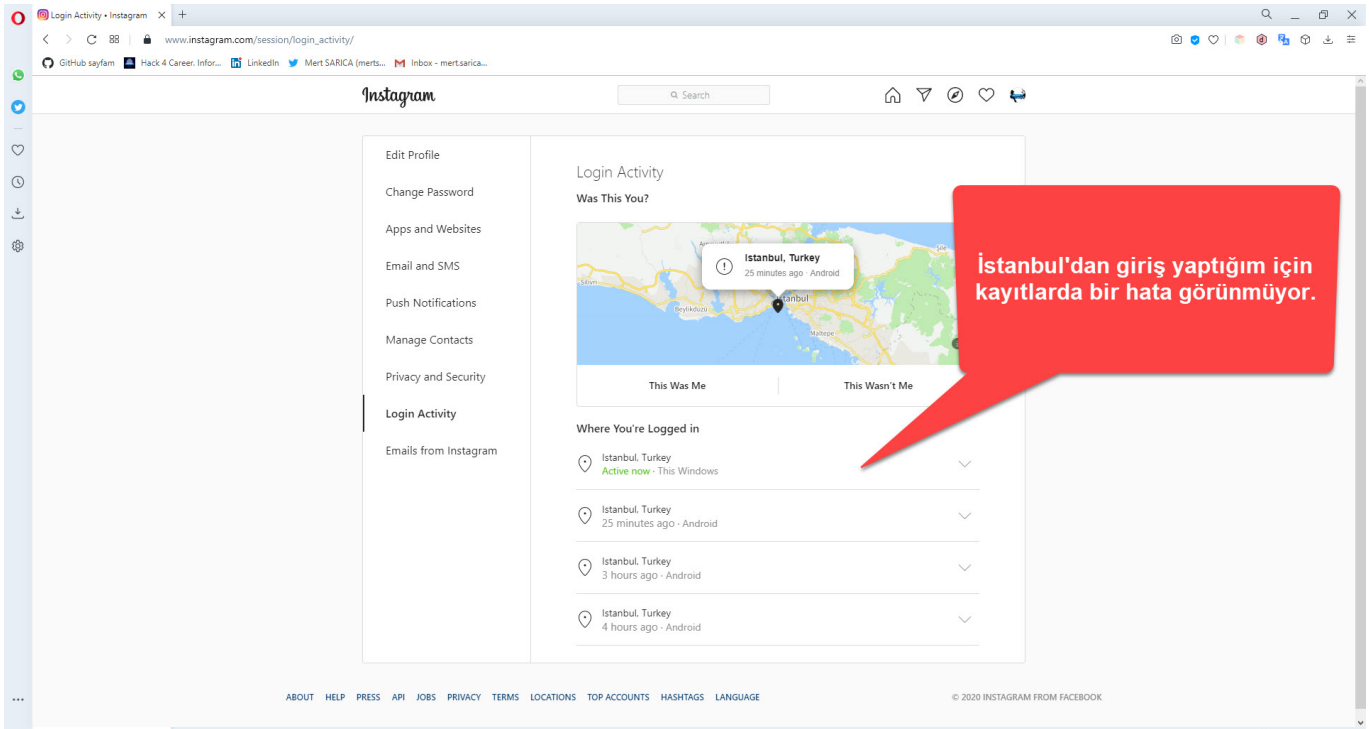

Genymotion for personal use - Google Nexus 6 - Malware...
4:41
Web Postegro
webpostegro.net/store#tab=monthly
Mağaza monthly
Aylık
Yıllık
Abonelikler
Reklamları kaldırın
Reklamları kaldırın
14.5₺
Hikayelere sınırsız bakın
Hikayelere sınırsız bakabilirsiniz. (günlük hikayeler de dahil)
20.9₺
Hesaplara sınırsız bakın
Gizli hesaplara sınırsız bakabilirsiniz.
27.9₺
Gizli mod
Gizli modda hesaplara bakabilirsiniz (Hedef kullanıcı bu konuda bilgilendirilmez)
69.8₺
Bana kim bakti?
Hesabınızı kimlerin görüntülediğini ögrene bilirsiniz.
95.8₺
Hepsi birinde
Gizli hesaplarin gönderilerine ve hikayelerine sınırsız bakın, tüm reklamları kaldırın, Hesabınızı kimlerin görüntülediğini öğrenin ve tüm hesaplara gizli modda bakın (Hedef kullanıcı bu konuda bilgilendirilmez) + Bu zamana kadar baktığınız gizli hesaplardan sizin onları görüntüleme geçmişiniz silinecek + Ayarlar bölmesinde `Profilimi gizle` bölümü etkinleşecek
209.2₺
TURKISH
ENGLISH
free for personal use



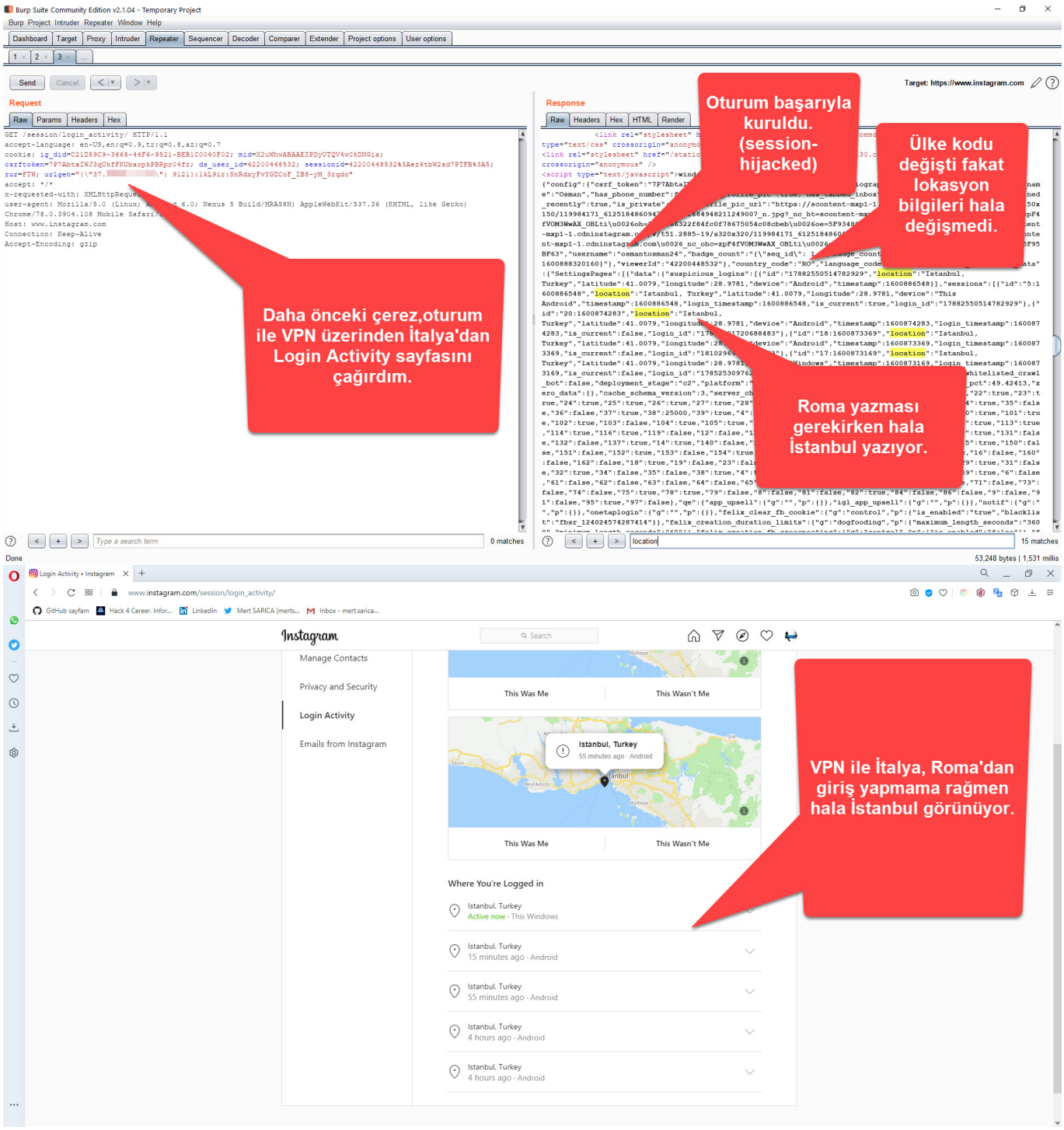
Generally, when an application with a secure architecture wants to access your Instagram information, it uses the Oauth protocol to request authorization from you. However, the Web Postegro & Lili application does not have a section that asks for permission or approval from the user. Therefore, to allow this application to view and list hidden profiles, it must constantly access the information of all accounts belonging to users who log

in through the application by connecting to the Instagram servers with session information belonging to those users. (session hijack) To understand that this method is being used, I conducted a test using Burp Suite over VPN to determine if the session information sent by the Web Postegro & Lili application to the payingpos[.]xyz address with the cookie parameter was sufficient to access my Instagram account. When I logged in to Instagram again through the Web Postegro & Lili application and made a request through Burp Suite to my Instagram account's Login Activity page (https://www.instagram.com/session/login_activity/), I was able to successfully receive a response from the server. When I rechecked the Login Activity page to see if there was a way for Instagram to understand those who accessed the account in this way, unfortunately, my access from abroad using VPN was not shown.




Login Activity • Instagram
www.instagram.com/session/login_activity/
Instagram
Search
Edit Profile
Change Password
Apps and Websites
Email and SMS
Push Notifications
Manage Contacts
Privacy and Security
Login Activity
Emails from Instagram
Login Activity
Was This You?
Istanbul, Turkey
25 minutes ago · Android
This Was Me
This Wasn't Me
Where You're Logged in
Istanbul, Turkey
Active now · This Windows
Istanbul, Turkey
25 minutes ago · Android
Istanbul, Turkey
3 hours ago · Android
Istanbul, Turkey
4 hours ago · Android
İstanbul'dan giriş yaptığım için kayıtlarda bir hata görünmüyor.
ABOUT HELP PRESS API JOBS PRIVACY TERMS LOCATIONS TOP ACCOUNTS HASHTAGS LANGUAGE
© 2020 INSTAGRAM FROM FACEBOOK

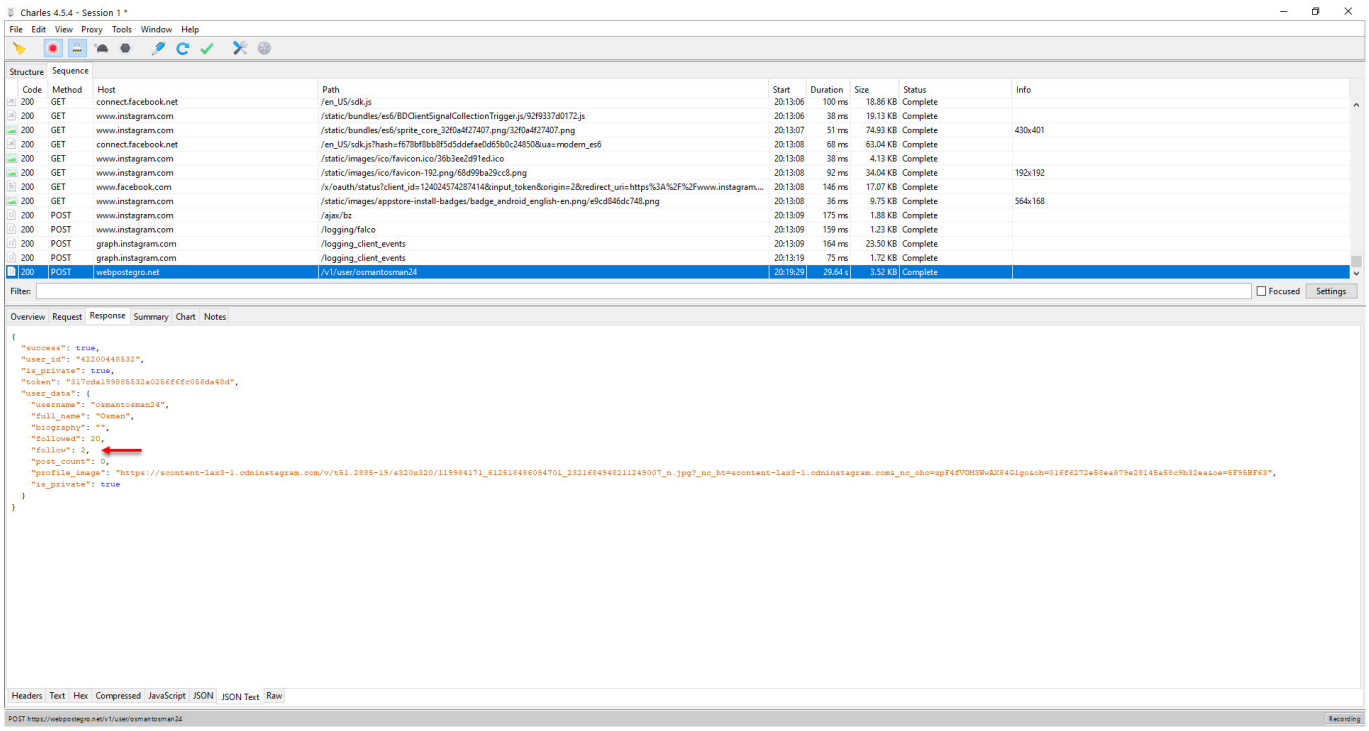
www.whatismyip.com
WhatIsMyIP.com
My IP
Speed Test
IP Lookup
Change IP
Hide IP
Search ...
Sign Up
Login
My Public IPv4 is: 37.1
My Public IPv6 is: Not Detected
Location: Rome, 62 IT
ISP: Secure Data Systems SRL
My IP Information
IP Address Lookup
Recent Articles
Protect Yourself With Two-Factor Authentication
Two-Factor authentication simply adds a second step to the log-in process to verify yourself. This extra verification usually takes the form of a numeric code that is sent to your phone.
Ways to Prevent Hacking
Internet Speed Test
What Is My Public IP?
DNS Lookup
IP Whois Lookup
Email Header Analyzer
Port Scanner
İtalya, Roma'ya VPN yapıldı.
What Is My IP?
WhatIsMyIP.com® is the industry leader in providing REAL IP address information. We provide IP address tools that show users how to perform an Internet Speed Test, IP address lookup, proxy detection, IP Whois Lookup, and more. We have extensive tutorials that show users how to trace an email address, how to change IP addresses, and how to hide their IP information. Knowing your IP address is crucial for online gaming, tech support, using remote desktop connections, connecting to a security camera DVR, anonymity or even running an email server. If you've got questions about IP addresses and can't find the answer on our site, feel free to post your question in our IP Address Q & A section.
What Is An IP Address?
This number is an exclusive number on all information technology devices (printers, routers, modems, etc) use which identifies and allows them the ability to communicate with each other on a computer network. [Read more...]
What Is IPv6?
IPv6 or Internet Protocol version 6 is the replacement for IPv4. An IPv6 address looks like this 2600:1005:b062:61e4:74d7:f292:802c:fbfd and an IPv4



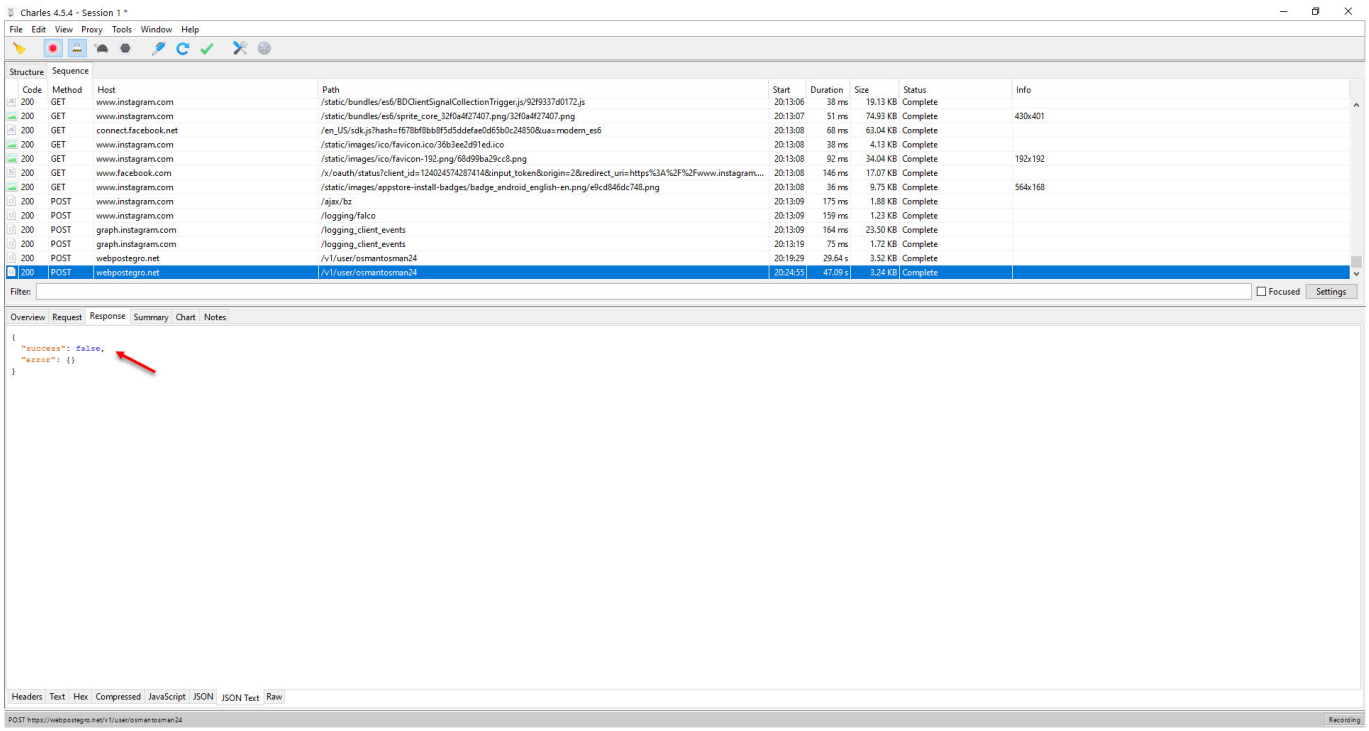
Despite repeatedly explaining the situation to Facebook's security team with screenshots, they were unable to understand what they needed to do in the face of even the most basic fraudulent scenario (if an Instagram account is accessed from two different countries within 5 minutes, the user will be warned and the Login Activity page will show which country the connection was made from).

In order to regain control of my account and find out whether the Web Postegro & Lili app developer was still able to access my account after logging out, I accessed my Instagram account from a Windows device and

increased the number of people I followed by 1. Then, when I asked the webpostegro[.]net server to bring me the current information belonging to the user, it could also get me the information of the person I had most recently started following, meaning that access was still continuing.



While I was thinking about how to prevent the Web Postegro & Lili application and its developer from accessing my Instagram account and session, I decided to see if changing my Instagram password would work and, whether or not I changed it, I confirmed that they couldn’t access my account through webpostegro[.]net and ended my research here.



Brief summary of my research is:

1. The Web Postegro Lili Android app, which is used to see who views your profile, has access to your entire Instagram account by taking your session information when accessing your Instagram account.
2. Even if you log out or delete the Web Postegro Lili app, the developer's access to your Instagram account will continue. To prevent this, you will need to change your Instagram password.

As a personal recommendation, if you come across a person, application, website, etc., that promises to show you who views your profile, be aware that this feature does not exist among the features of the social media applications.

Hope to see you in the following articles.