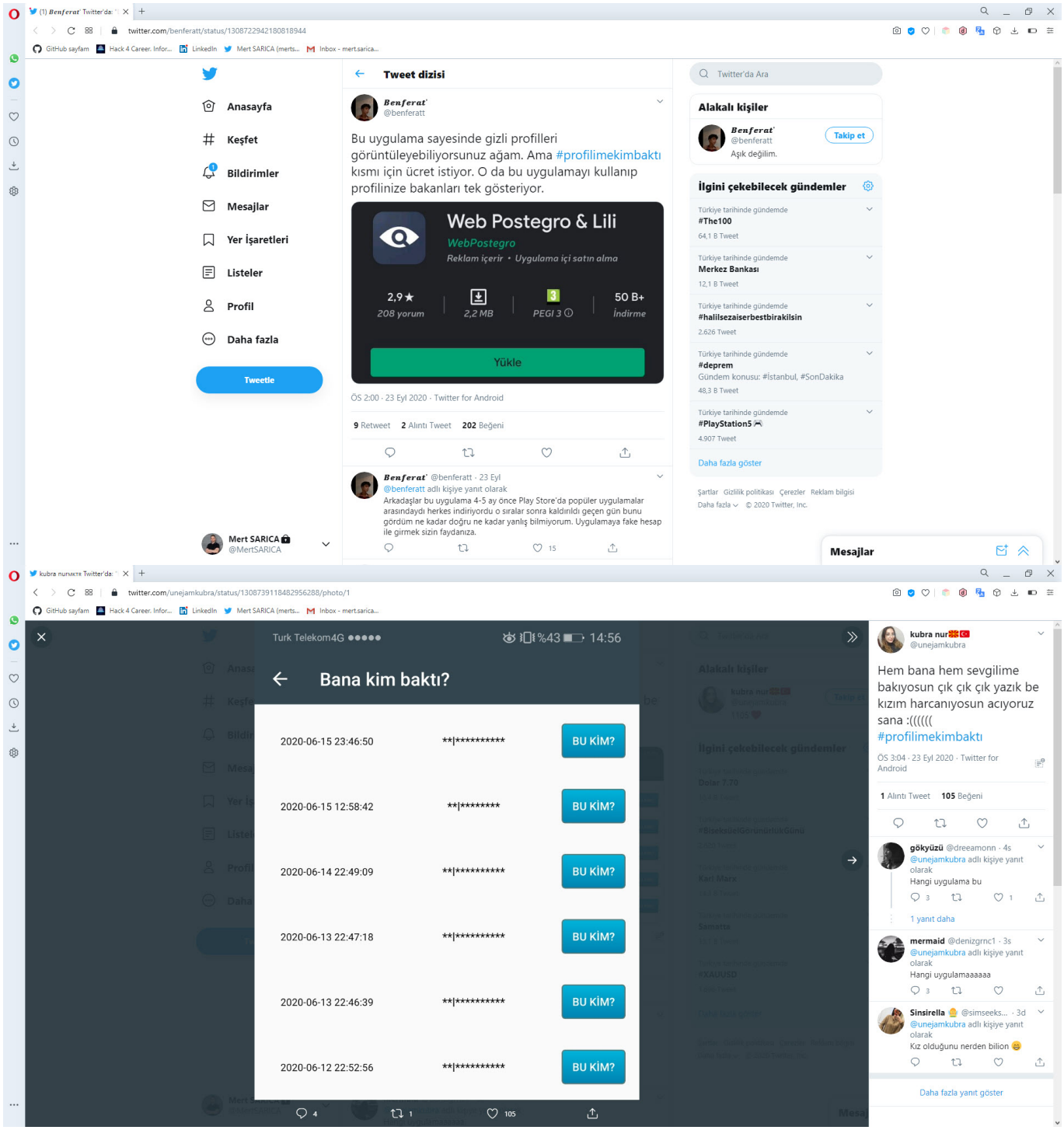
Profilime Kim Baktı?

written by Mert SARICA | 1 October 2020

If you are looking for an English version of this article, please visit here.

23 Eylül 2020 tarihinde Twitter'da siber güvenlik ile ilgili haberlere göz gezdirirken gündem olan başlıklarda #profilimekimbaktı etiketi dikkatimi çekti. Beni oldukça şüphelendiren bu etiketin gündem olmasının arkasında yatan sebebi bulmak için bu etiketi paylaşan hesaplara göz gezdirmeye karar verdim. Paylaşan hesaplardan birinin yazmış olduğu mesajda, Web Postegro & Lili isimli bir Android uygulamasının profil görüntüleyenleri gösterdiğinden bahsediyordu.

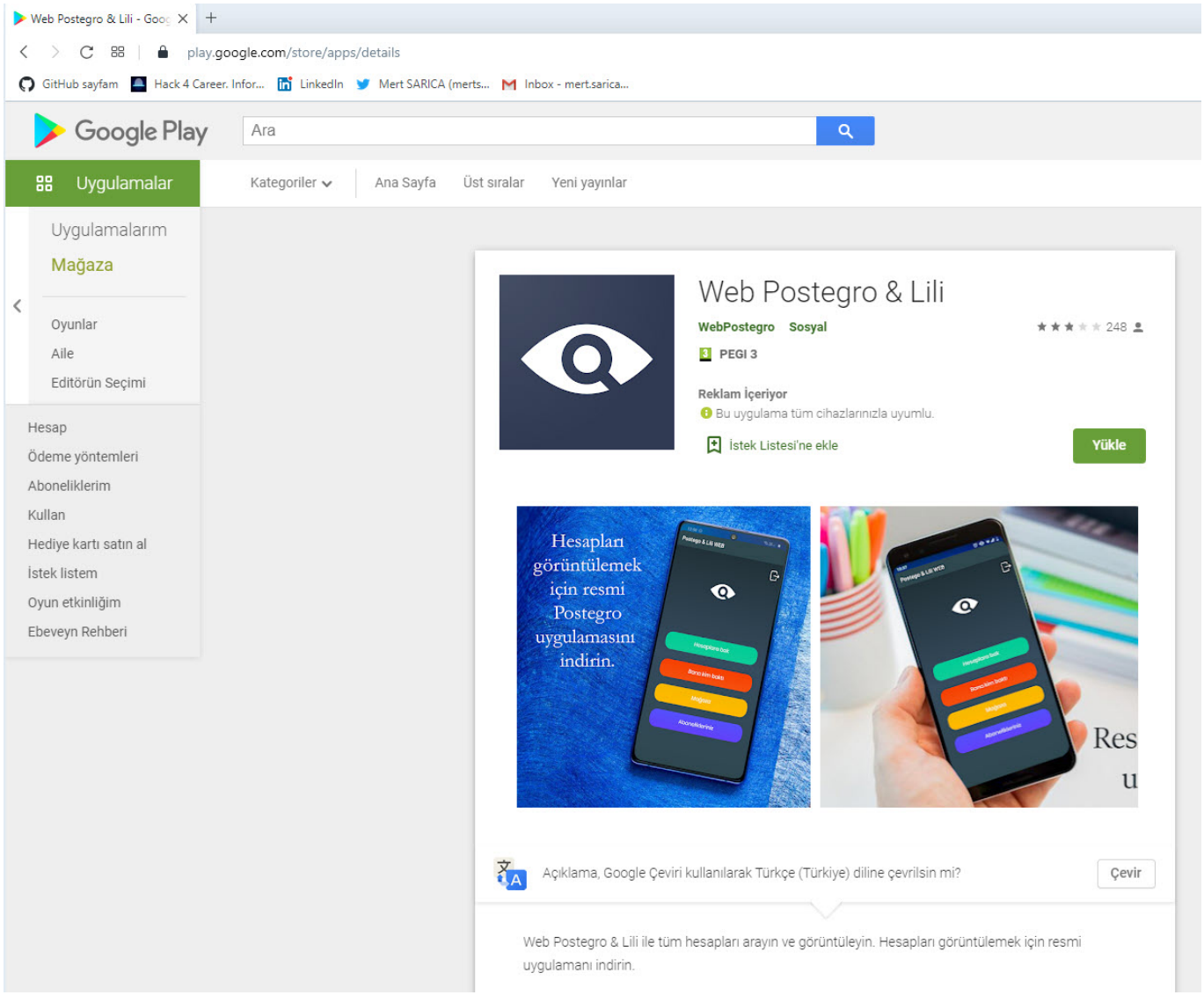


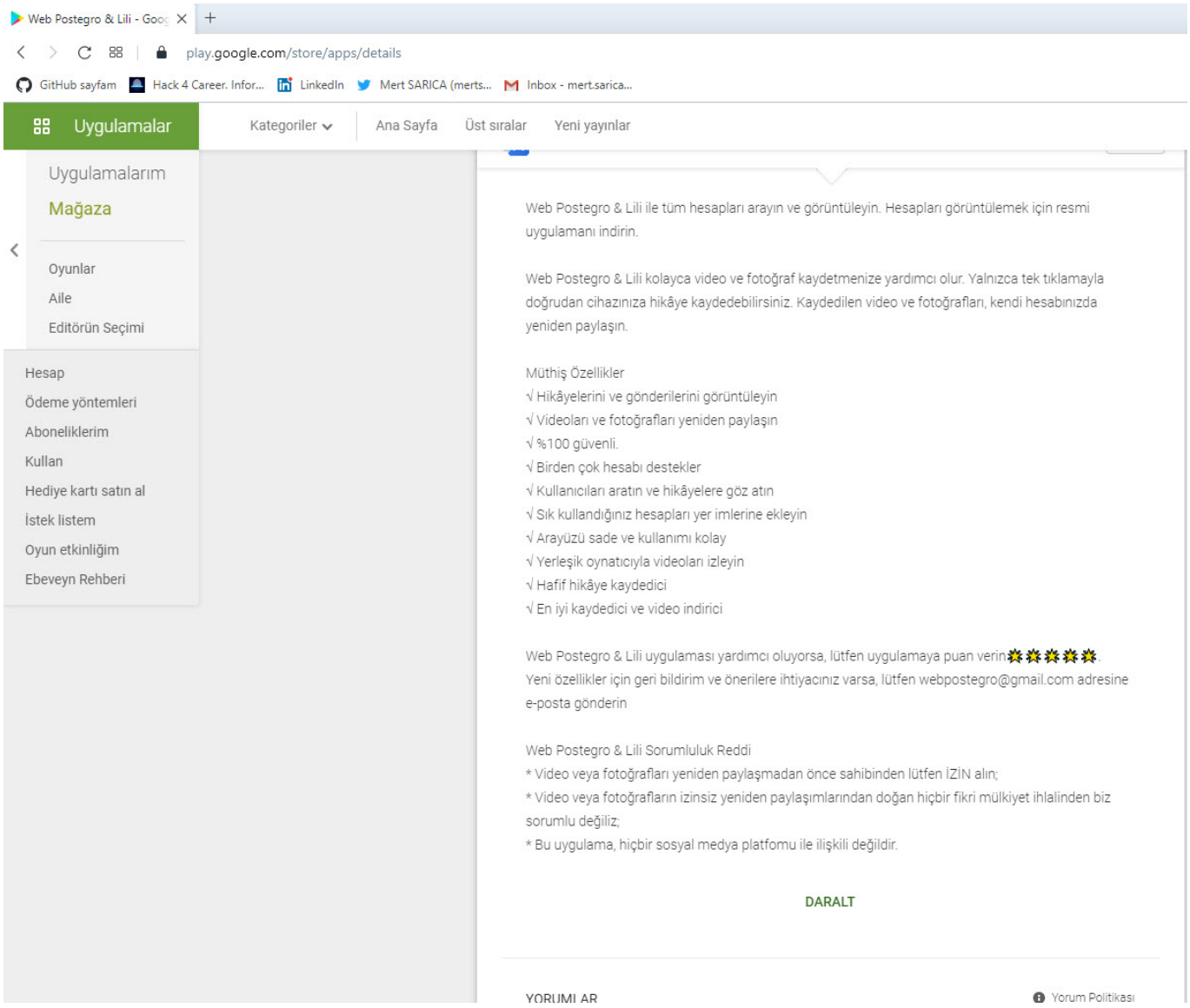


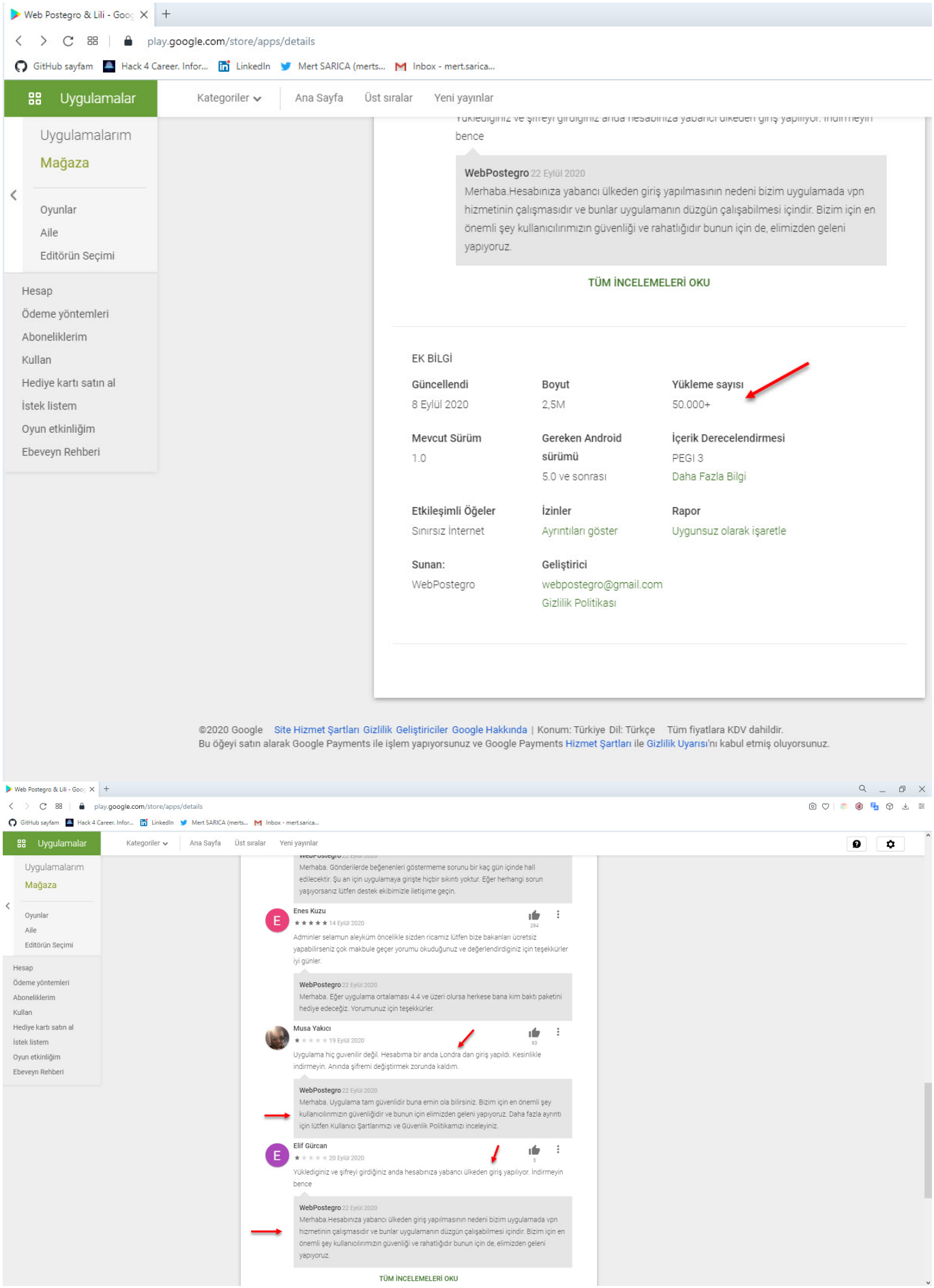
LinkedIn hariç Twitter, Facebook, Instagram gibi sosyal ağların, profil görüntüleyenlerin bilgisini kullanıcıları ile paylaşmadığını bildiğim için bu tür bir uygulamalara her zaman şüpheyle yaklaşmışımdır. Şüphelerim konusunda haklı olup olmadığımı anlamak için bu Android uygulamasını indirip analiz etmeye ve farkındalık adına kaleme almaya karar verdim.

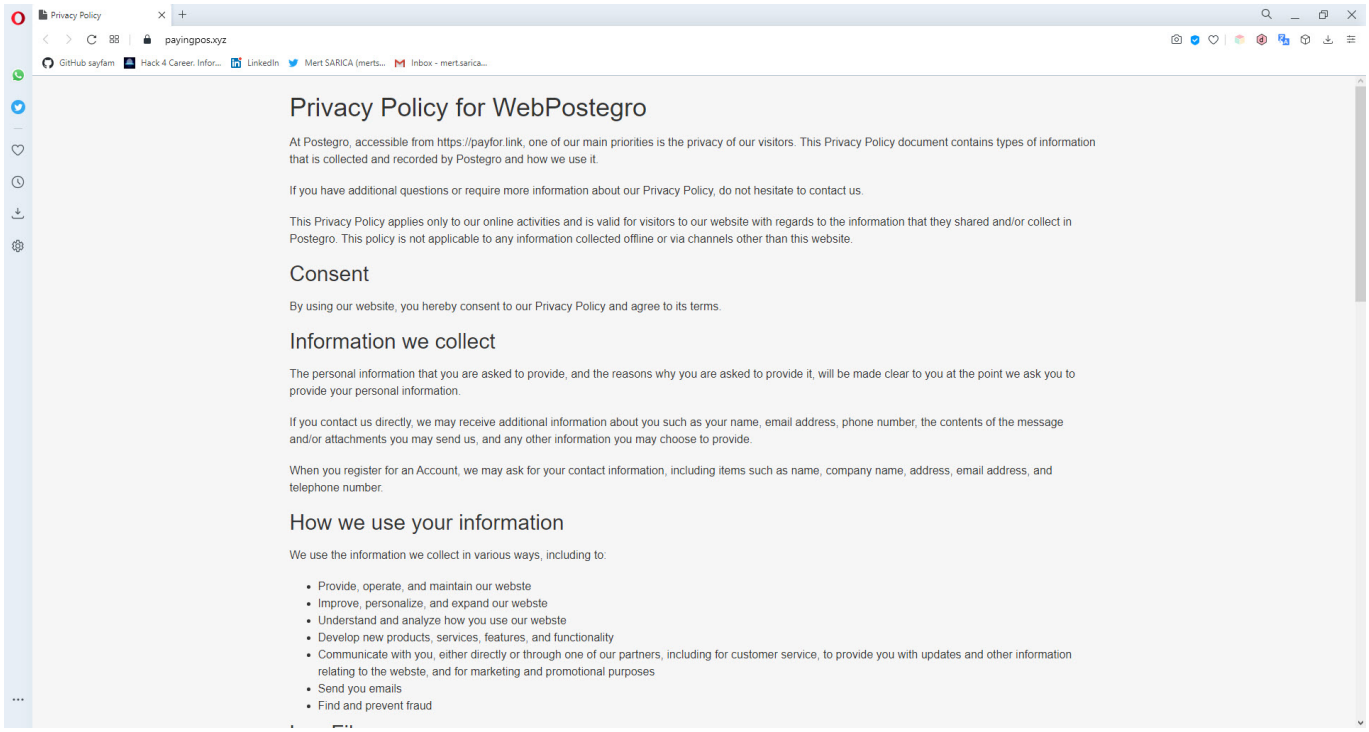
İlk olarak Web Postegro & Lili Android uygulamasının Google Play'deki sayfasını incelemekle işe başladım. 24 Eylül itibariyle 100.000'den fazla yüklenen bu mobil uygulamanın kullandığı izinlere baktığımda beni şüphelendiren bir izin ile karşılaşmadım. Yorumlara göz attığımda ise bazı

kullanıcıların hesaplarına yurtdışından giriş yapıldığına dair şüpheli yorumlar gördüm. Geliştiricinin yanıtladığı yorumlardan birinde güvenlik politikasında yurt dışından bağlantı yapıldığının ifade edildiğini belirtmesine rağmen buna dair politikada herhangi bir kısım göremedim.



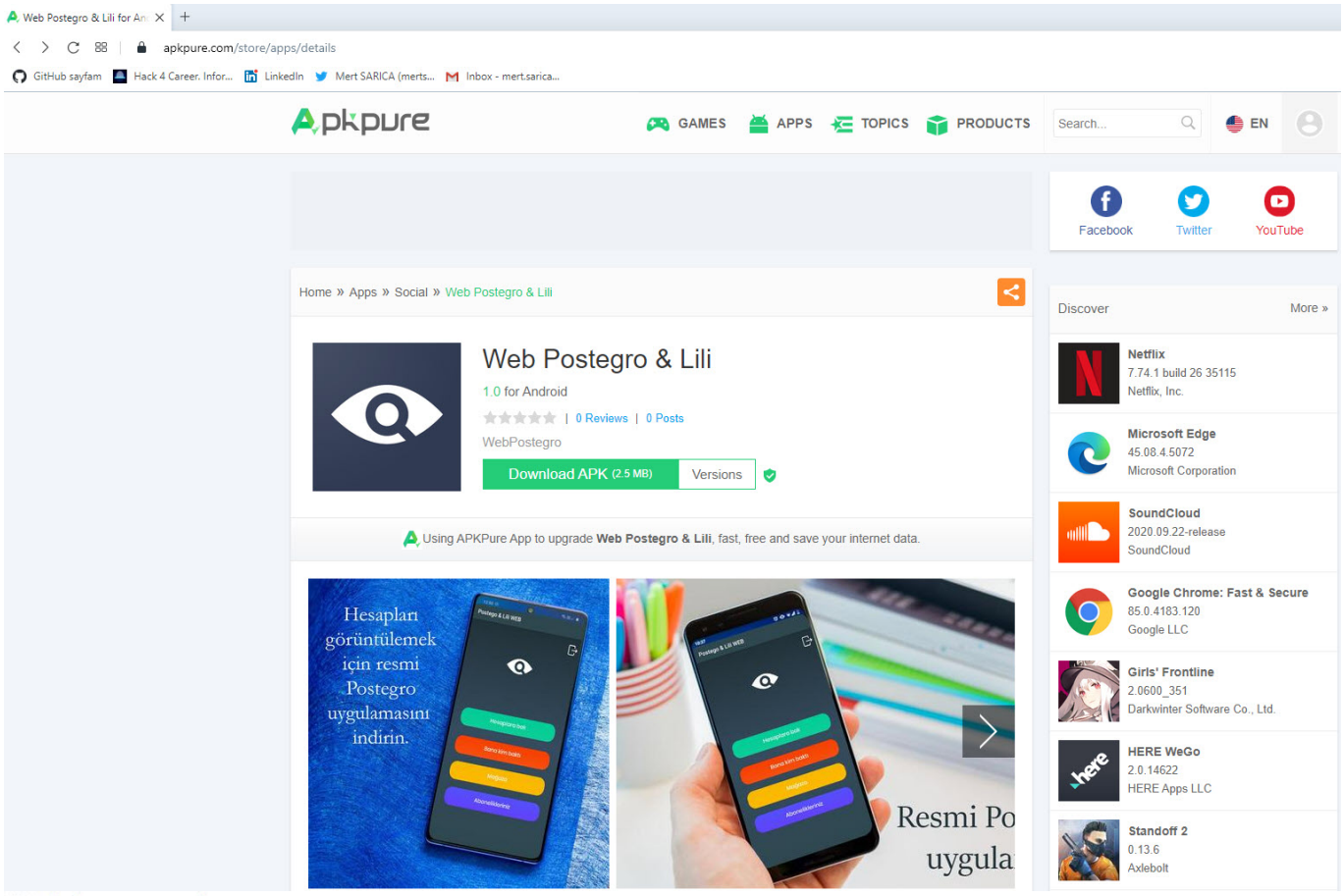

Web Postegro & Lili - Goo
play.google.com/store/apps/details
GitHub sayfam
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Uygulamalar
Kategoriler
Ana Sayfa
Üst sıralar
Yeni yayınlar
Uygulamalarım
Mağaza
Oyunlar
Aile
Editörün Seçimi
Hesap
Ödeme yöntemleri
Aboneliklerim
Kullan
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

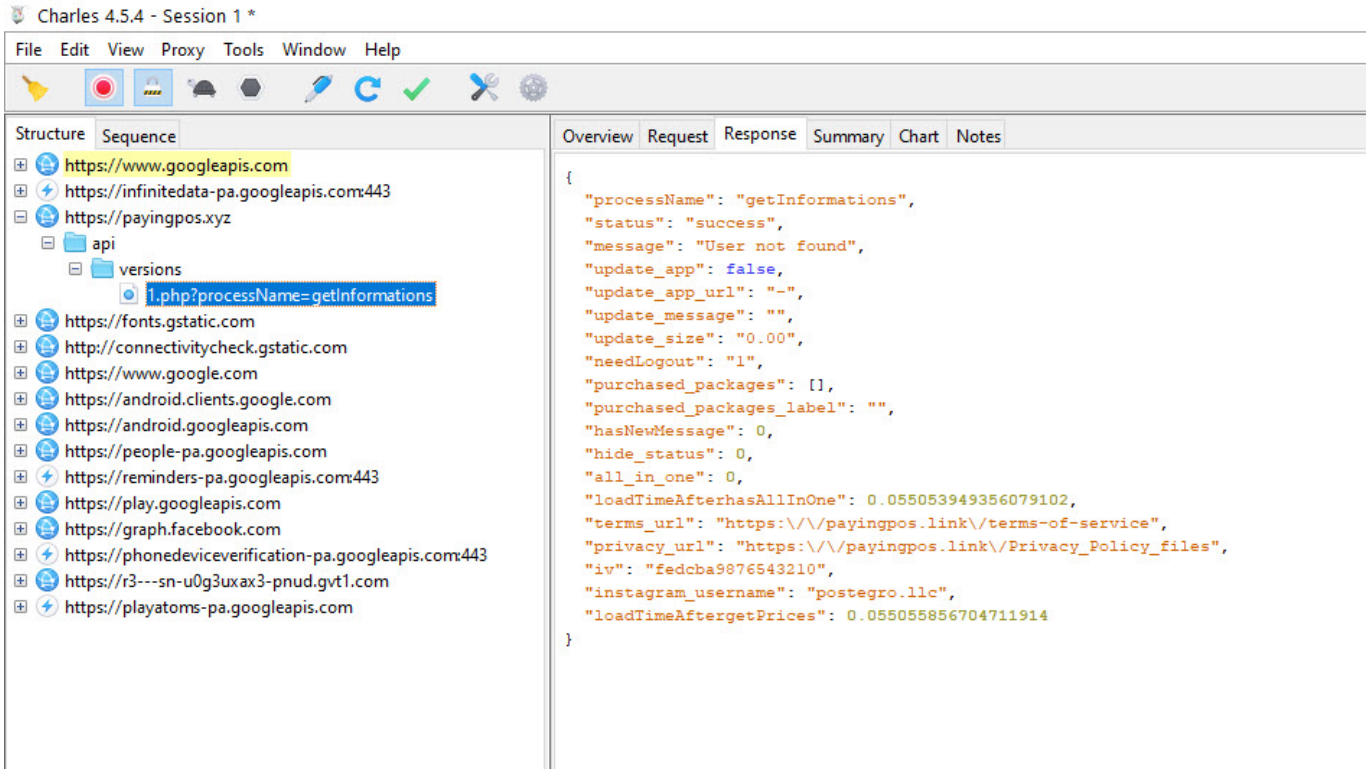

Web Postegro & Lili - Goog
play.google.com/store/apps/details
GitHub sayfam
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Uygulamalar
Kategoriler
Ana Sayfa
Üst sıralar
Yeni yayınlar
Uygulamalarım
Mağaza
Oyunlar
Aile
Editörün Seçimi
Hesap
Ödeme yöntemleri
Aboneliklerim
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

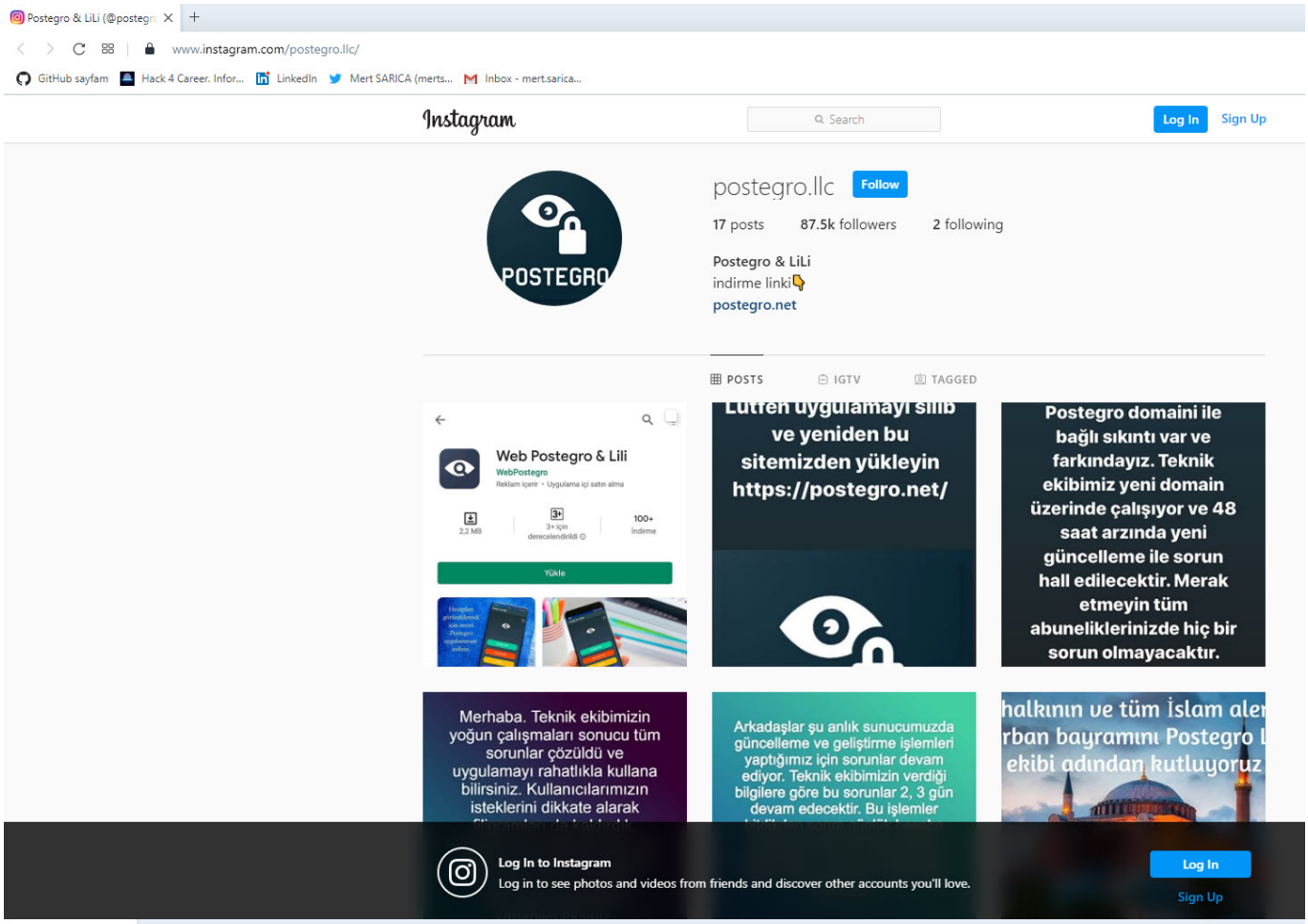


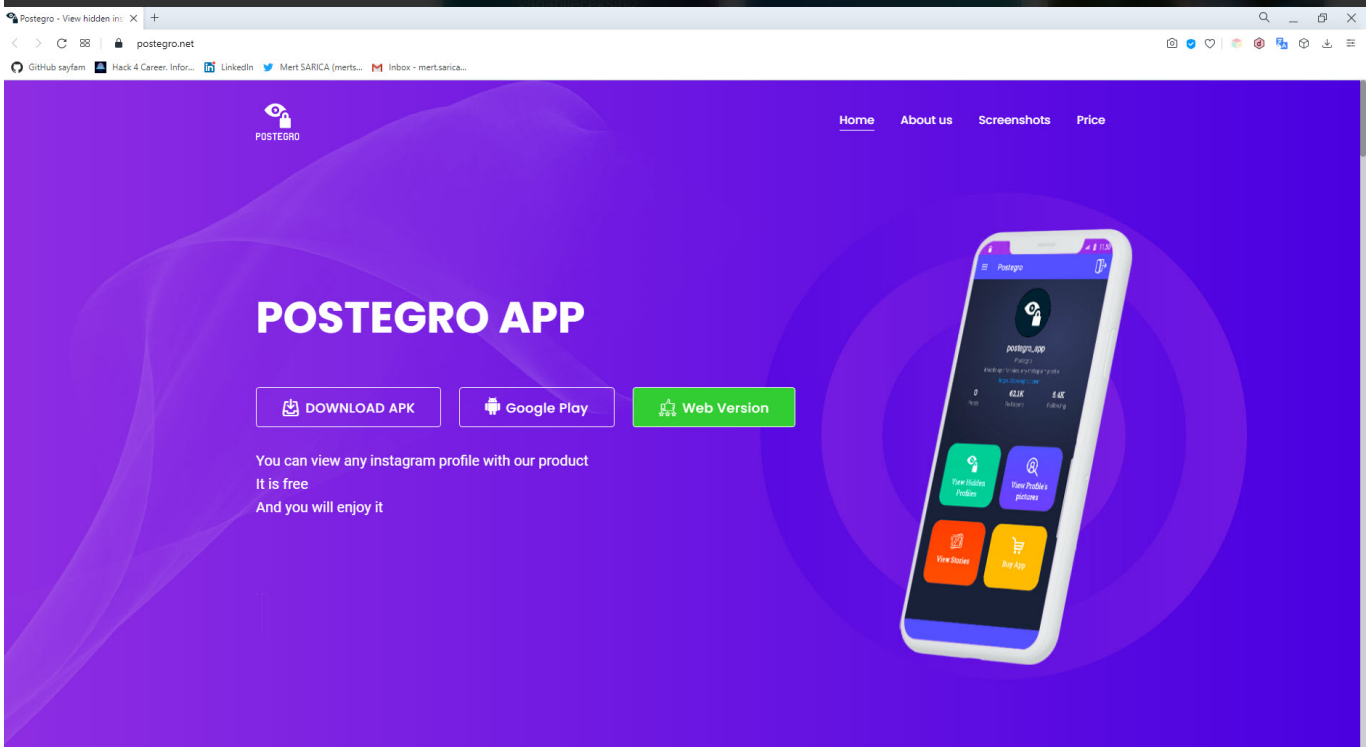
Google Play sayfasından ön bilgileri topladıktan sonra APKPure sitesinden Web Postegro & Lili uygulamasını analiz etmek için indirdim ve APK dosyasını VirusTotal'a yüklediğimde bu uygulamanın zararlı olduğuna dair herhangi bir ize rastlamadım.

Ardından bu uygulamayı GenyMotion öykünücüsüne yükleyip, favori araçlarından biri olan Charles Proxy yardımı ile çalışma esnasında gerçekleştirdiği HTTP trafiğini kayıt altına almaya başladım. Uygulamanın haberleştiği payingpos[.]xyz web sunucusundan gelen ilk yanıtta, uygulama geliştiricisine ait olan postegro.llc Instagram hesabını gördüm. Hesabında paylaştığı fotoğraflardan birinde Google Play'den daha önce bu uygulamanın kaldırıldığını paylaşması dikkatimden kaçmadı. Instgram hesabında yer alan ve alan adı 5 Eylül tarihinde kayıt edilen web adresini ziyaret ettiğimde, Web Postegro & Lili uygulamasını (39.apk) direkt web sitelerinden indirebildiğimi öğrendim.


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
}

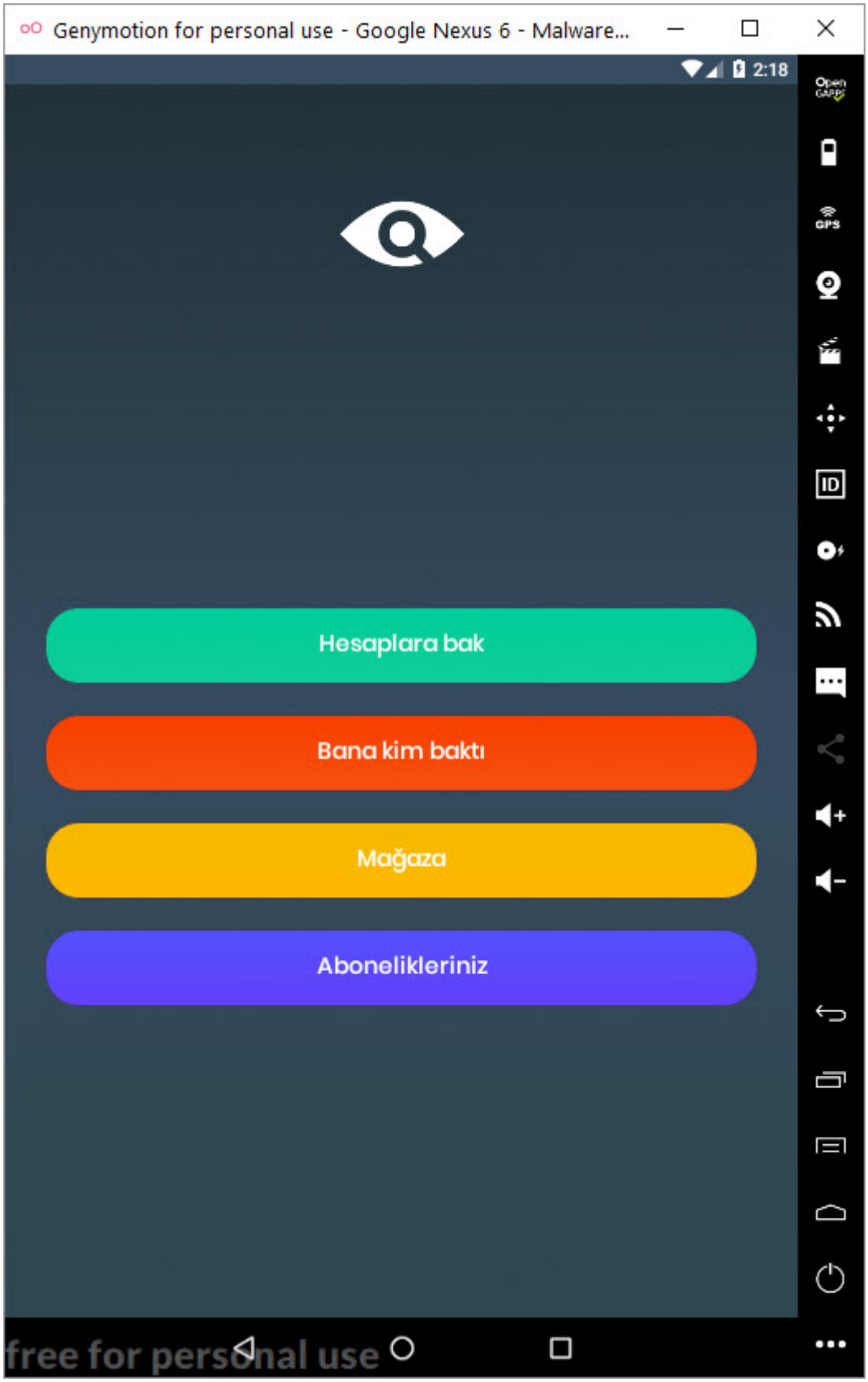


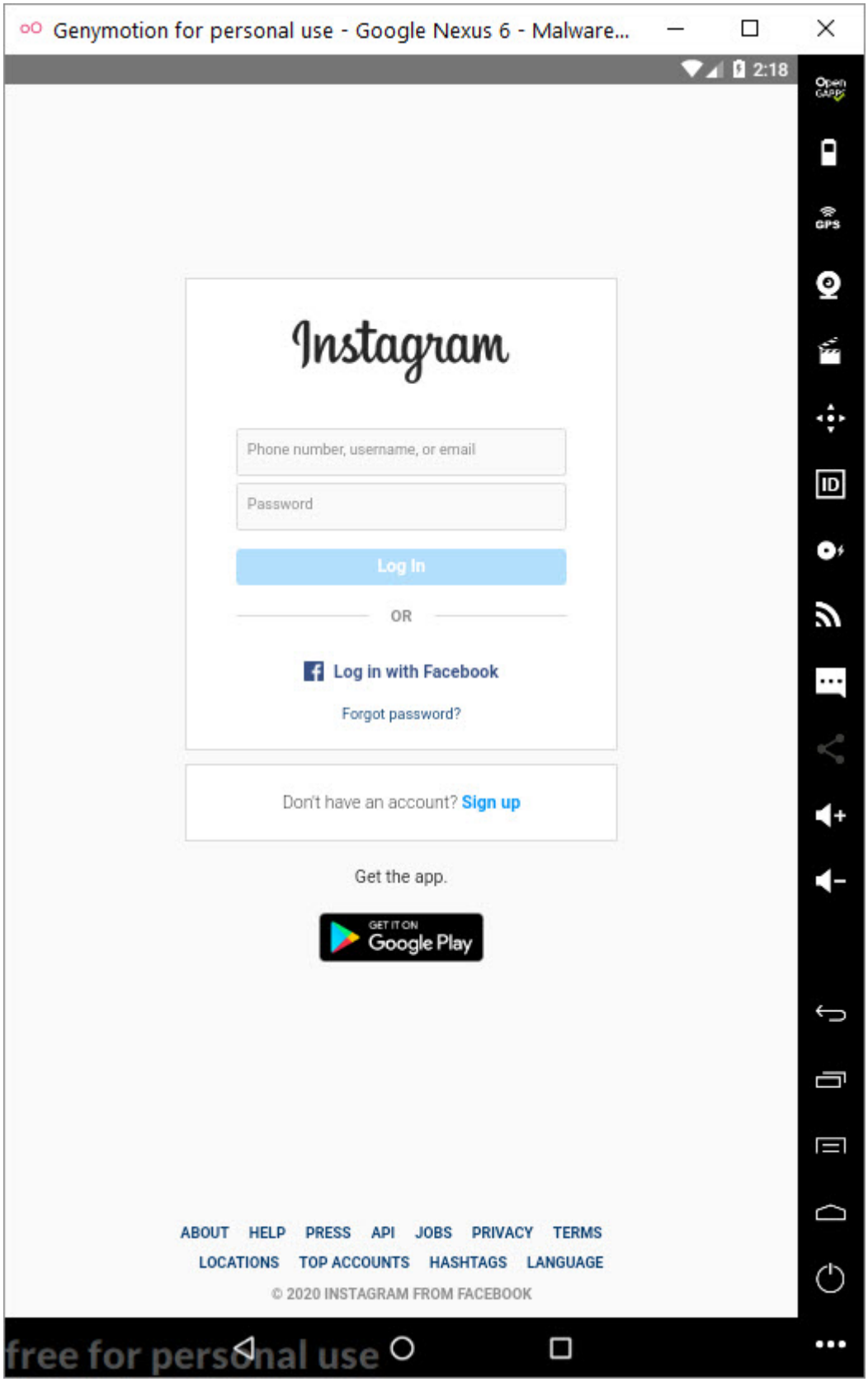


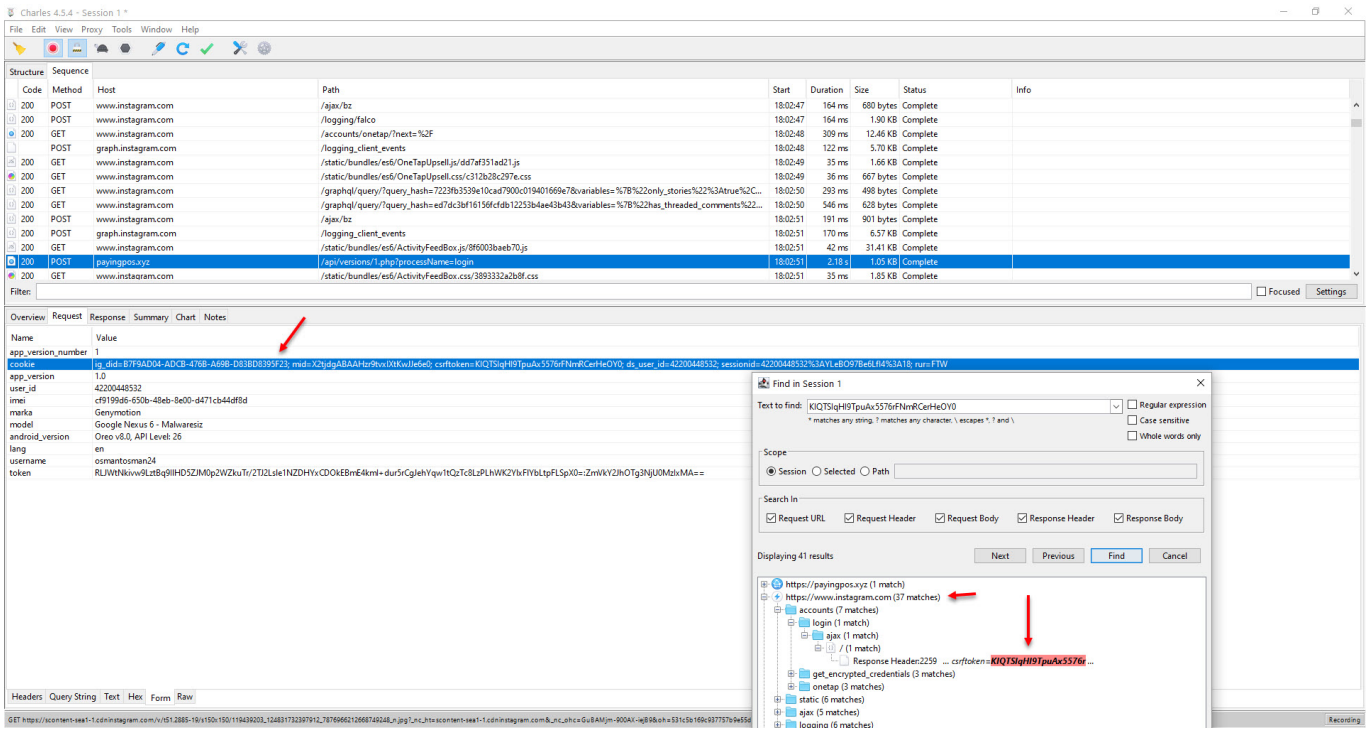
Charles Proxy ile kayıt altına alınan trafiği incelediğimde, Web Postegro Lili (Web Postegro Lili_v1.0_apkpure.com.apk) uygulamasının kullanım esnasında payingpos[.]xyz, webpostegro[.]net ve postegro[.]net sunucuları ile haberleştiğini gördüm.

39.apk isimli APK dosyasını da VirusTotal'a yüklediğimde benzer şekilde zararlı olduğuna dair bir uyarı ile karşılaşmadım. Web Postegro & Lili (39.apk) uygulamasının kullanım esnasında postegro202039348[.]com, imagecropper2020[.]com, postegro[.]net ve de kapalı olan postegro[.]com sunucuları ile haberleştiğini gördüm. postegro[.]com adresi çalışmadığı için Web Postegro & Lili (39.apk) uygulamasının profillere bakma, profile bakanları gösterme gibi genel fonksiyonları çalışmıyordu dolayısıyla analizime Web Postegro & Lili (Web Postegro Lili_v1.0_apkpure.com.apk) uygulaması üzerinden devam ettim.

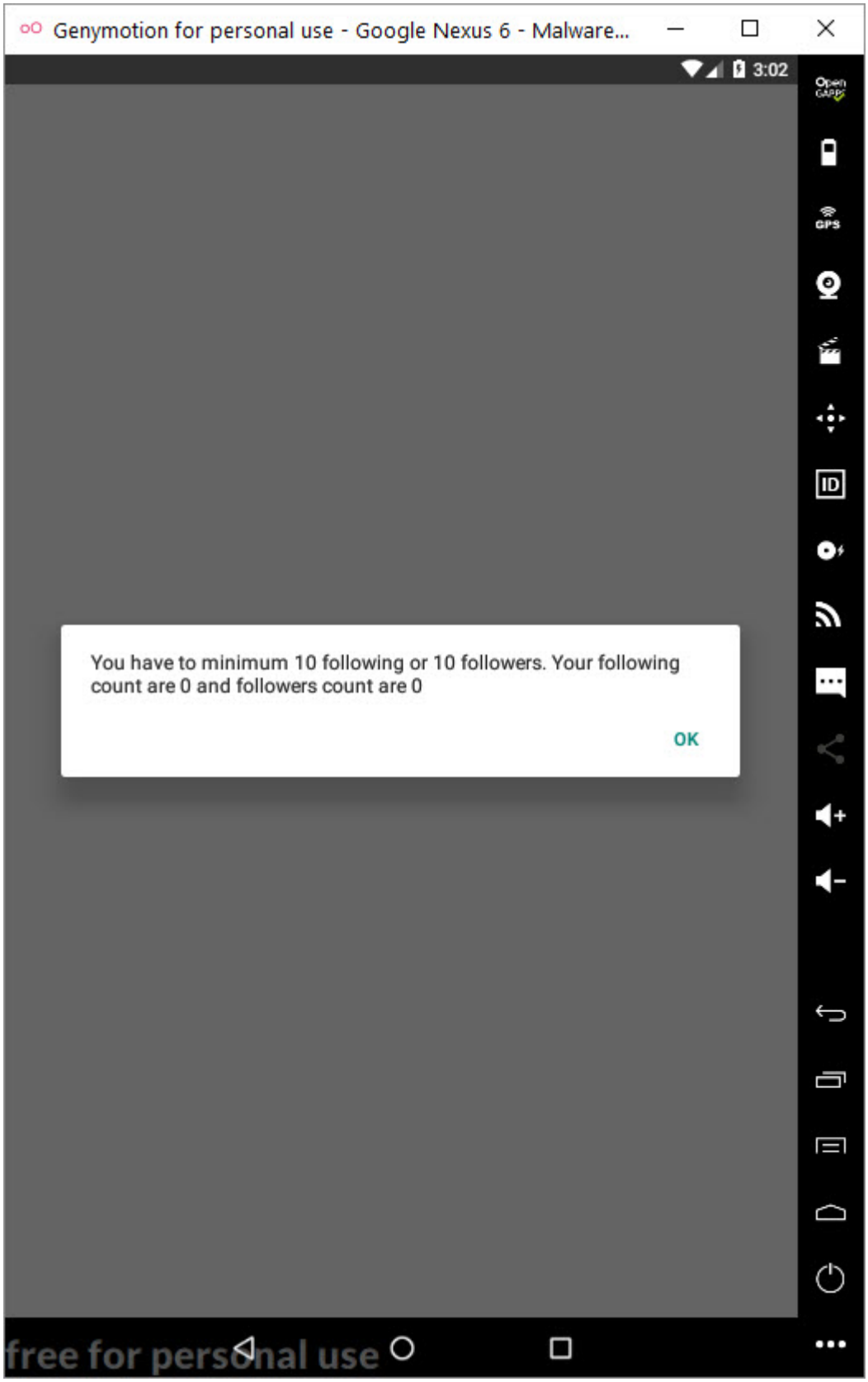
Web Postegro & Lili uygulaması çalıştığında karşıma profili gizli olanlara bakma (Hesaplara bak) ve profiline bakanları görmeye (Bana kim baktı) imkan tanıyan menüler geldi. Hesaplara bak menüsüne tıkladığımda uygulama kendi arayüzünden instagram.com sunucusu ile haberleşerek Instagram kullanıcı adı ve parolasının girildiği giriş sayfasını karşıma çıkardı. Bu araştırmaya özel olarak oluşturduğum osmantosman24 Instagram kullanıcı adım ve parolam ile giriş yapar yapmaz uygulamanın arka planda instagram.com sunucusu ile doğrulama sonrasında oluşan oturum bilgilerimi cookie parametresi ile payingpos[.]xyz adresine gönderdiğini ve bu ve daha fazla bilgimi /data/data/com.web.lilipostego/shared_prefs/com.web.lilipostego_preferences.xml dosyasına kayıt ettiğini tespit ettim!

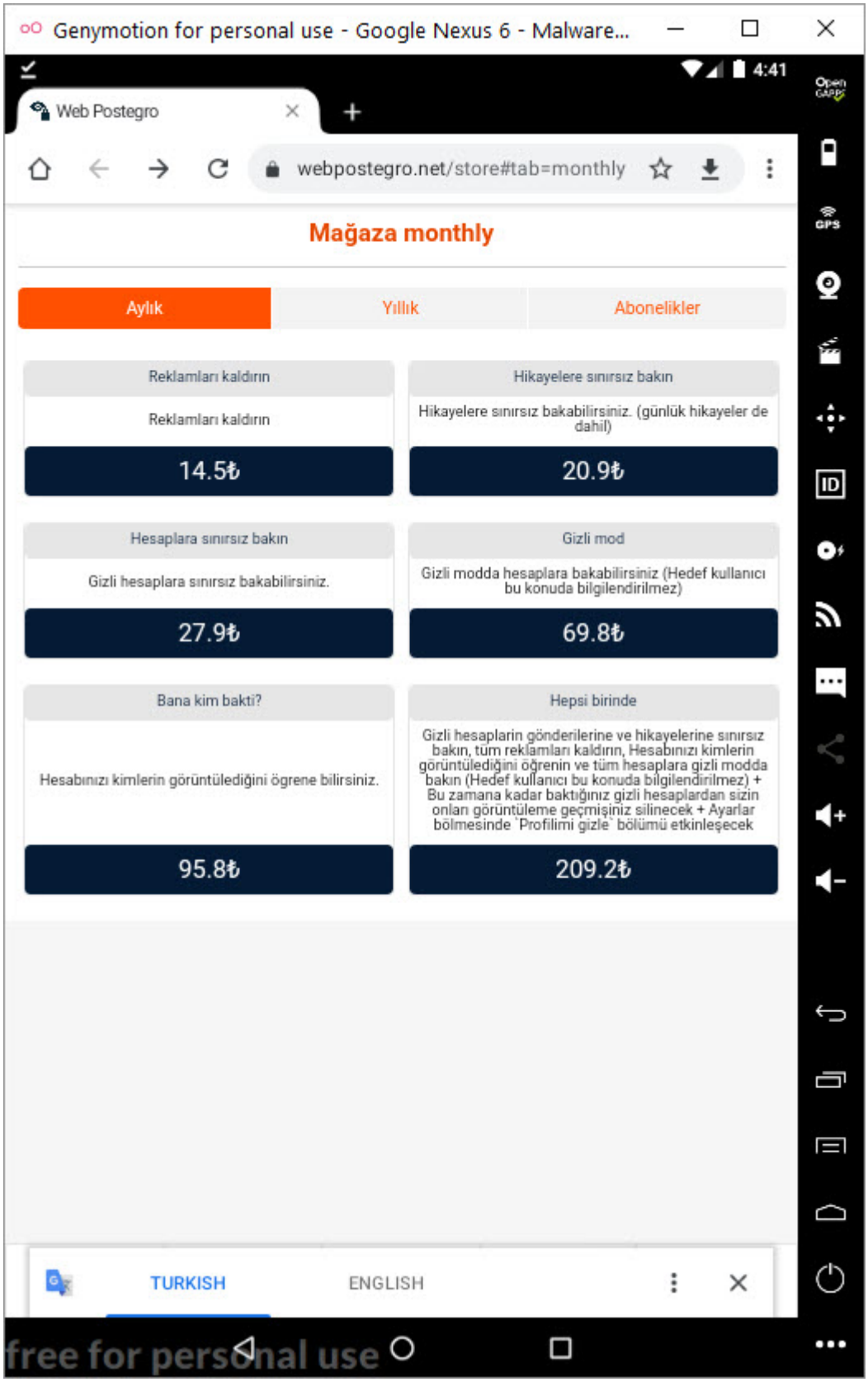

Genymotion for personal use - Google Nexus 6 - Malware...
2:18
Hesaplara bak
Bana kim baktı
Mağaza
Aboneliklerin
free for personal use

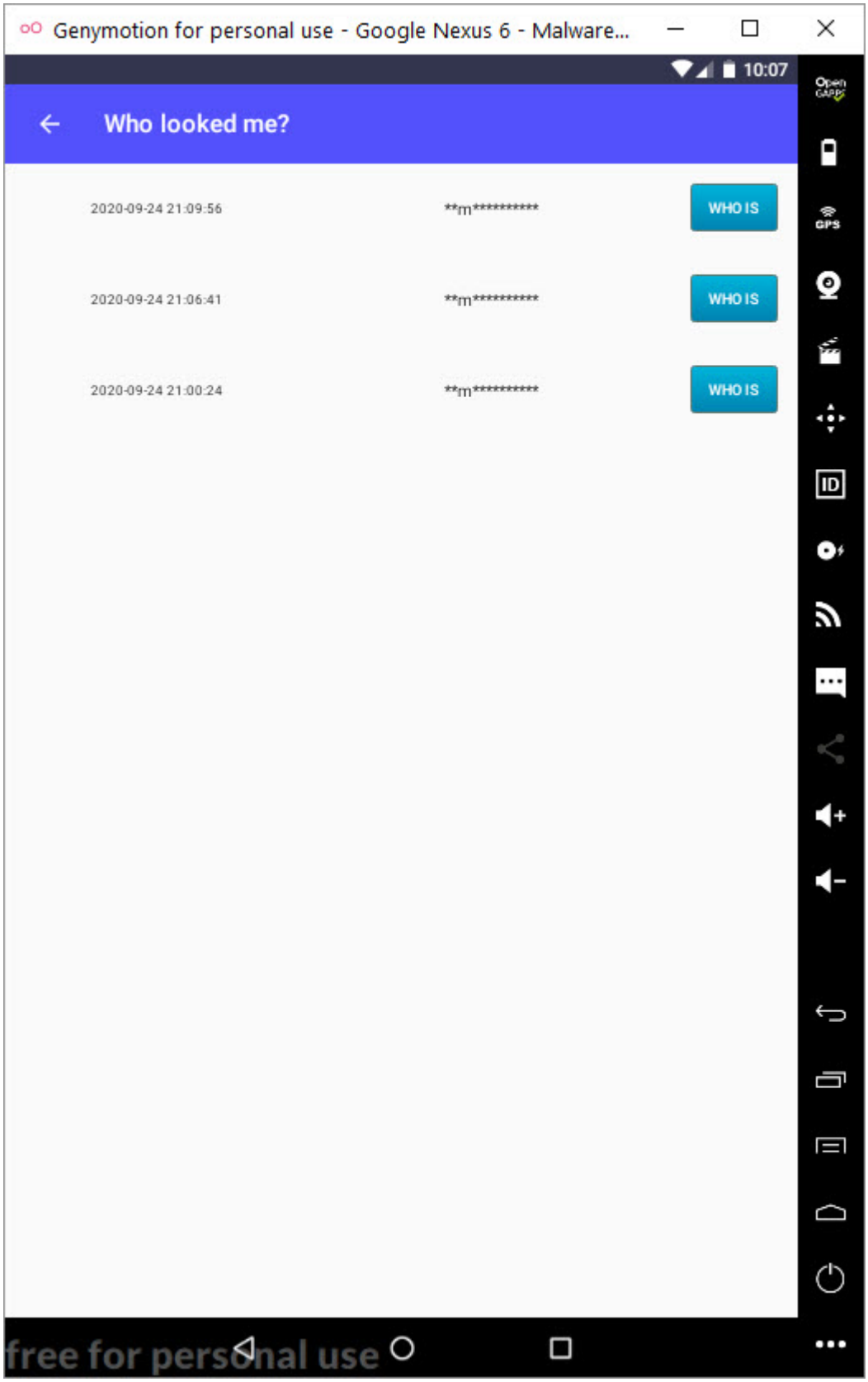

Genymotion for personal use - Google Nexus 6 - Malware...
2:18
Instagram
Phone number, username, or email
Password
Log In
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
GET IT ON Google Play
ABOUT HELP PRESS API JOBS PRIVACY TERMS
LOCATIONS TOP ACCOUNTS HASHTAGS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



Uygulamayı kullanabilmem için en az 10 kişinin beni veya benim 10 kişiyi takip etmem gerektiği için hızlıca takibe takip yapan Instagram hesaplarını takip etmeye başlayarak onların da beni takip etmesini sağladım. Takipçi sayımı arttırıp, takip ettiğim tüm hesapları takip etmeyi bıraktıktan sonra uygulamanın menüleri arasında gezmeye başladım ve profili genele kapalı, gizli olan hesapların içeriğini görüntüleyebildim. Görünüşe göre bu uygulama gelirini, uygulama üzerindeki limitlerin (reklam kaldırma, hikayeleri sınırsız görüntüleme, hesaplara sınırsız bakma, profil görüntüleyenlerin isimlerinin sansürsüz görünmesi gibi) belirli bir ücret karşılığında kaldırılması ile sağlıyordu.

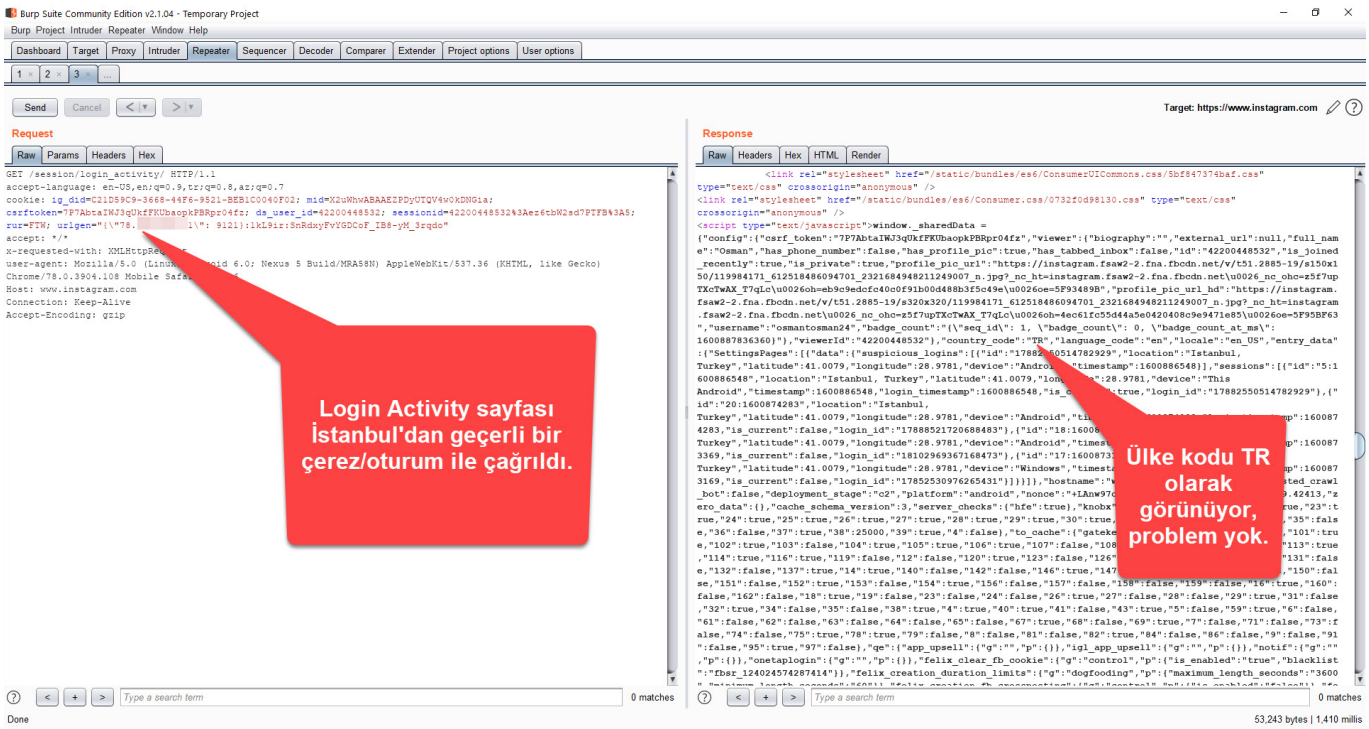

Genymotion for personal use - Google Nexus 6 - Malware...
3:02
You have to minimum 10 following or 10 followers. Your following count are 0 and followers count are 0
OK
free for personal use

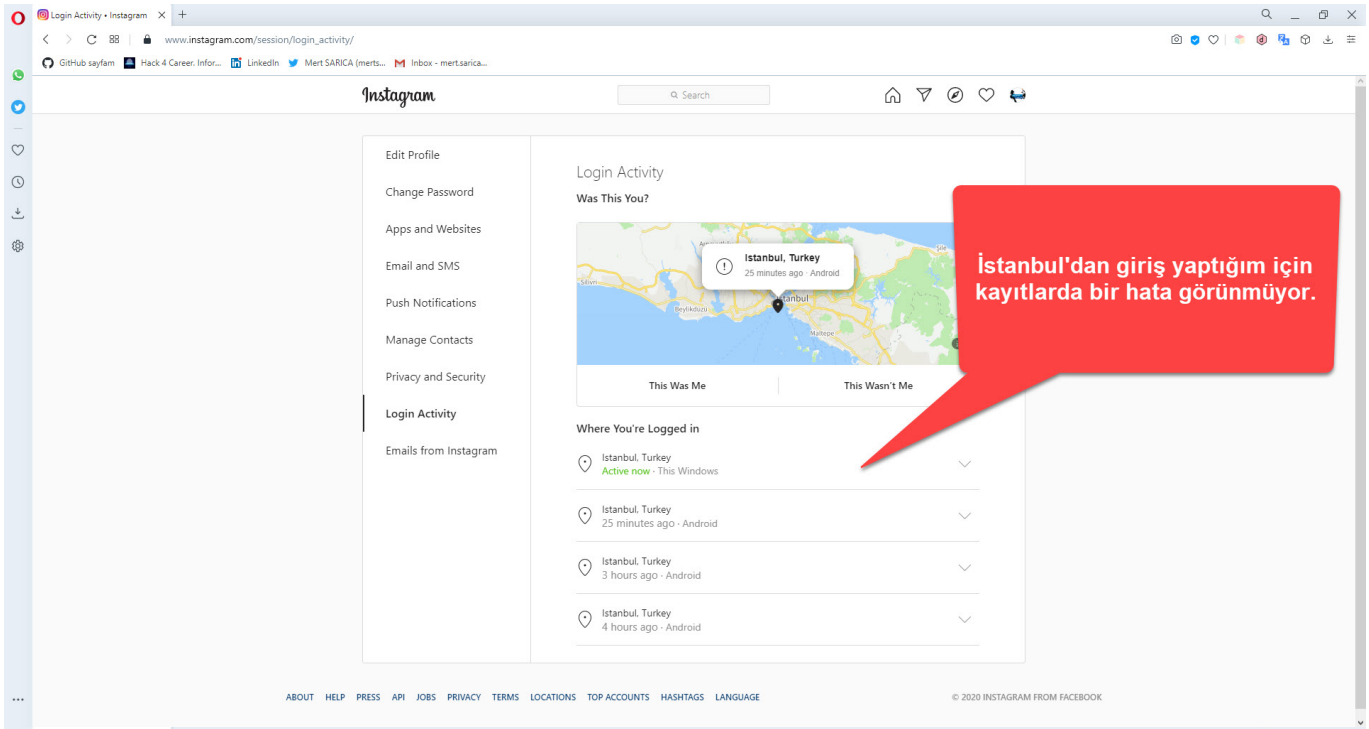

Genymotion for personal use - Google Nexus 6 - Malware...
4:41
Web Postegro
webpostegro.net/store#tab=monthly
Mağaza monthly
Aylık
Yıllık
Abonelikler
Reklamları kaldırın
Reklamları kaldırın
14.5₺
Hikayelere sınırsız bakın
Hikayelere sınırsız bakabilirsiniz. (günlük hikayeler de dahil)
20.9₺
Hesaplara 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



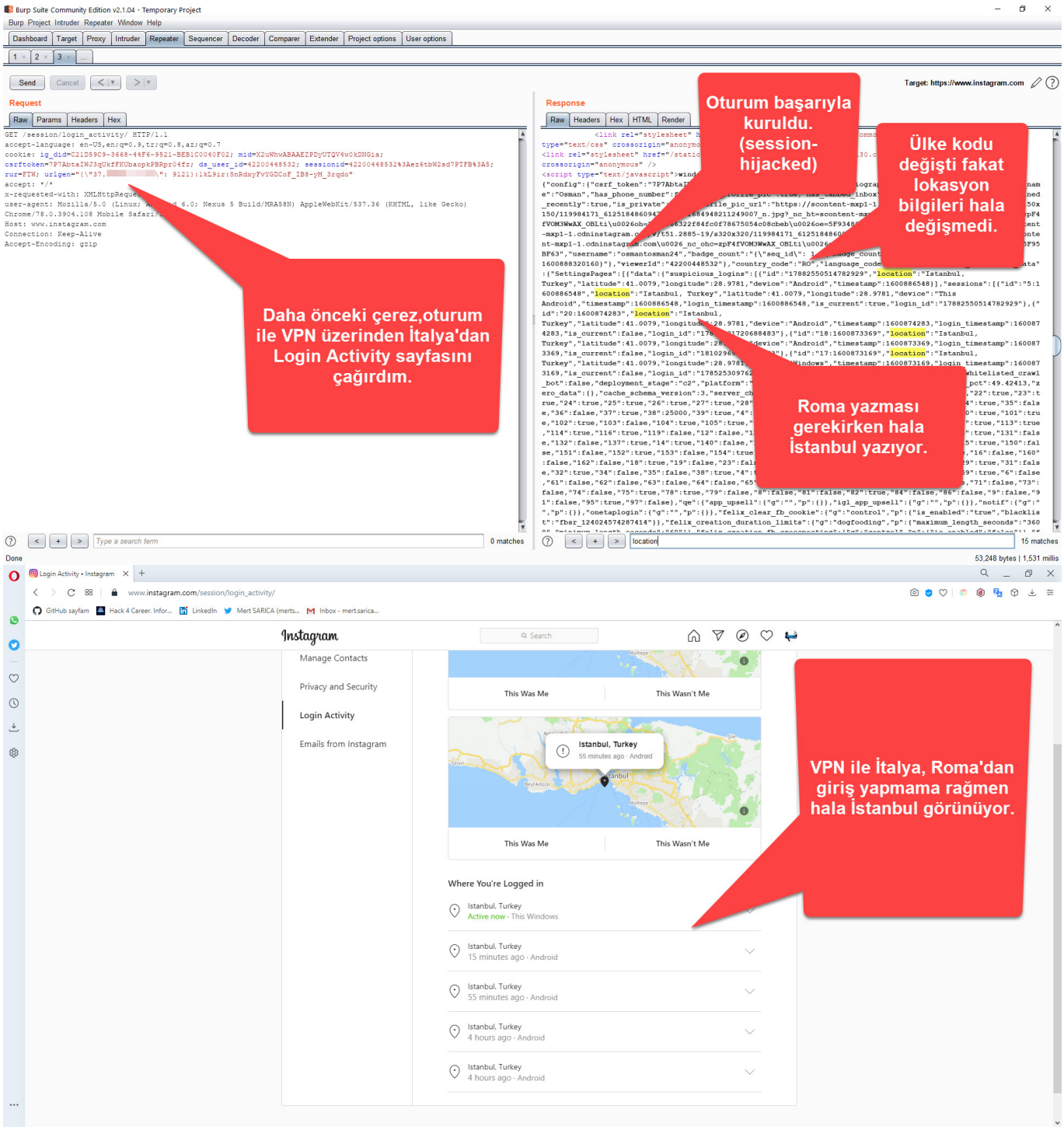
Normal şartlarda güvenli mimariye sahip bir uygulama sizin Instagram bilgilerinize erişmek istediğinde yetkilendirme işlemi için Oauth protokolünden faydalanır ve sizden onay ister fakat Web Postegro & Lili uygulamasında kullanıcıdan izin, onay isteyen bir kısım bulunmuyordu. Bu durumda bu uygulamanın gizli profilleri görüntülemeye, profilleri görüntüleyenleri listelemeye imkan tanıyabilmesi için uygulama üzerinden

Instagram’a giriş yapan kullanıcılara ait oturum bilgileri ile Instagram sunucularına bağlanıp tüm bu kullanıcılara ait hesapların bilgilerine sürekli erişmesi gerekiyordu. (session hijack) Bu yöntemi izlediğini anlamak için Web Postegro & Lili uygulamasının payingpos[.]xyz adresine cookie parametresi ile gönderdiği oturum bilgilerinin Instagram hesabıma erişme adına yeterli olduğunu anlamak için Burp Suite ile VPN üzerinden bir test gerçekleştirdim. Web Postegro & Lili uygulaması üzerinden Instagram’a tekrar giriş yaparak uygulamanın sunucuya gönderdiği yeni oturum bilgileri ile Burp Suite üzerinden Instagram hesabımın Login Activity sayfasına (https://www.instagram.com/session/login_activity/) istekte bulunduğumda başarıyla sunucudan yanıt alabildiğimi gördüm! Instagram tarafında hesabına bu şekilde erişenleri anlamamın bir yolu var mı diye Login Activity sayfasına tekrar baktığımda maalesef VPN ile yurt dışından yaptığım erişim görünmüyordu!




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

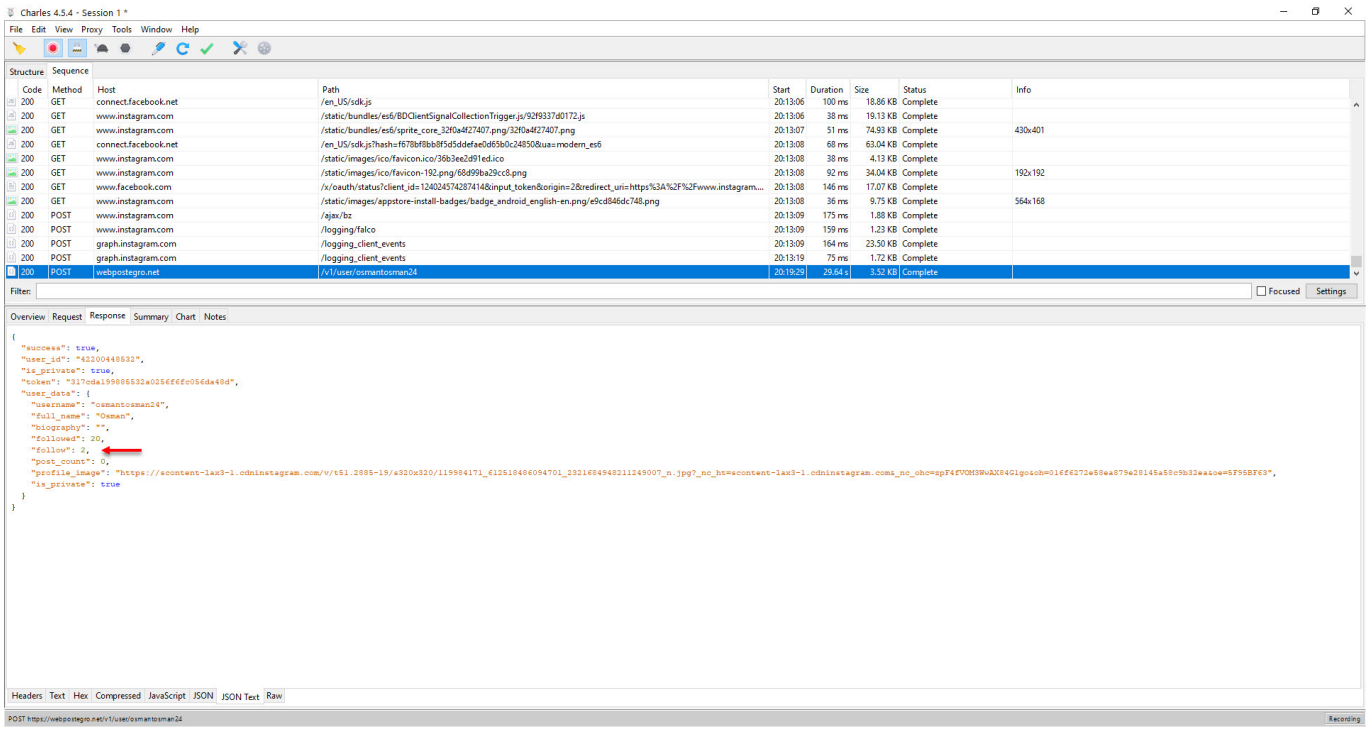

www.whatismyip.com
WhatIsMyIP.com
My IP
Speed Test
IP Lookup
Change IP
Hide IP
Search ...
Sign Up
Login
My Public IPv4 is: 37.1
My Public IPv6 is: Not Detected
Location: Rome, 62 IT
ISP: Secure Data Systems SRL
My IP Information
IP Address Lookup
Recent Articles
Protect Yourself With Two-Factor Authentication
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 allow users 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



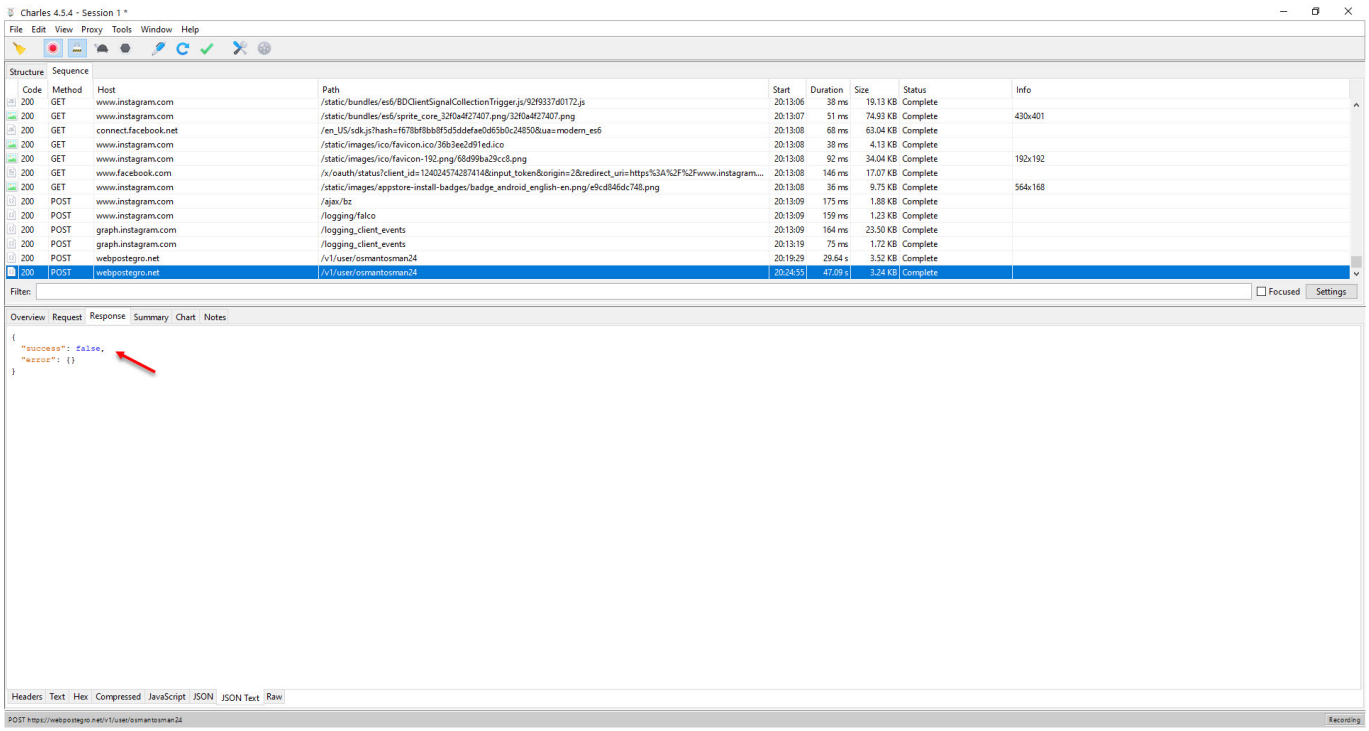
Facebook'un güvenlik ekibine bu durumu yukarıdaki ekran görüntüleri ile adım adım, çok defa anlatmış olmama rağmen maalesef en basit dolandırıcılık senaryosuna karşı yapmaları gerekenin ne olduğunu (5 dakika içinde Instagram hesabına önce bir ülken daha sonra ise başka bir ülkeden giriş yapılıyorsa kullanıcıyı uyarılır, Login Activity sayfasında hangi ülkeden bağlantı kurulduysa gösterilir vb.) bir türlü anlayamadılar.

Hesabımın kontrolünü geri kazanmak ve Web Postegro & Lili uygulamasından çıkış yaptıktan sonra geliştiricinin hesabıma erişiminin devam edip etmediğini öğrenmek için Instagram hesabıma Windows üzerinden erişip takip

ettiğim kişilerin sayısını 1 arttırdım. Ardından webpostegro[.]net sunucusundan kullanıcıma ait güncel bilgileri getirmesini istediğimde takip etmeye başladığım son kullanıcının bilgilerini de getirebildiğini, kısaca erişiminin devam ettiğini gördüm!



Web Postegro & Lili uygulamasının ve geliştiricisinin Instagram hesabıma, oturumuma olan erişimlerini nasıl engelleyebilirim diye düşünürken Instagram parolamı değiştirmenin işe yarayıp yaramayacağına bakmaya karar verdim ve parolayı değiştirir değiştirmez hesabıma erişemediklerini webpostegro[.]net üzerinden teyit etmiş ve araştırmamı burada sonlandırmış oldum.



Yaptığım araştırmayı kısaca özetleyecek olursam;

1. Profilinize bakanları görmek için kullandığınız Web Postegro Lili Android uygulaması, Instagram hesabınıza erişirken kullandığınız oturum bilgilerinizi alarak Instagram hesabınızın tamamına erişim sağlamaktadır!
2. Web Postegro Lili uygulamasından çıkış yapsanız da silseniz de geliştiricinin Instagram hesabınıza erişimi devam etmektedir. Bunu engellemek için Instagram parolanızı değiştirmeniz gerekmektedir.

Naçizane tavsiye olarak kullandığınız bir sosyal ağ, medya uygulamasının özellikleri arasında profilinizi görüntüleyenleri gösterme gibi hayal ettiğiniz bir özellik bulunmuyorsa, bunu yaptığını vaadeden bir kişi, uygulama, web sitesi vb. ile karşılaştığınızda kullanmadan, güvenmeden önce arka planda hangi bilgilerinizi feda edebileceğinizi hatırlamanızda fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.