

Profilime Kim Baktı?

written by Mert SARICA | 1 October 2020

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

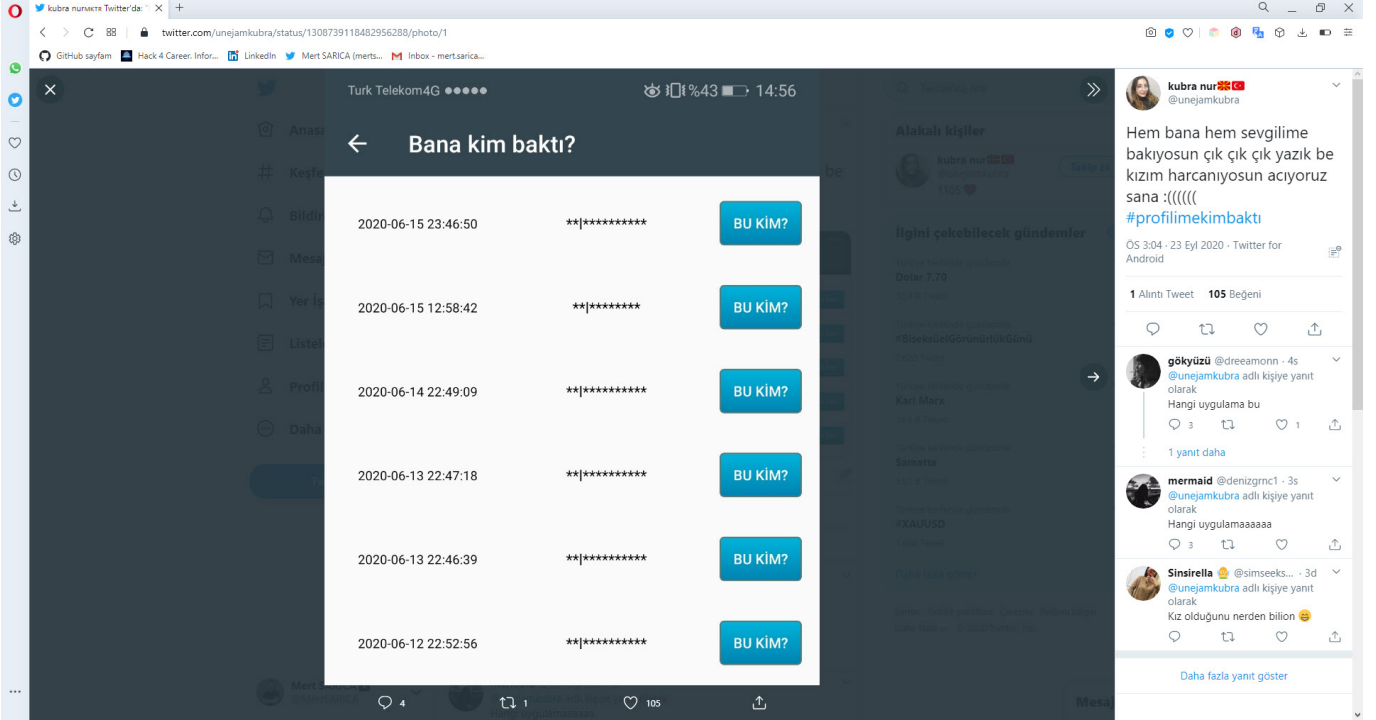
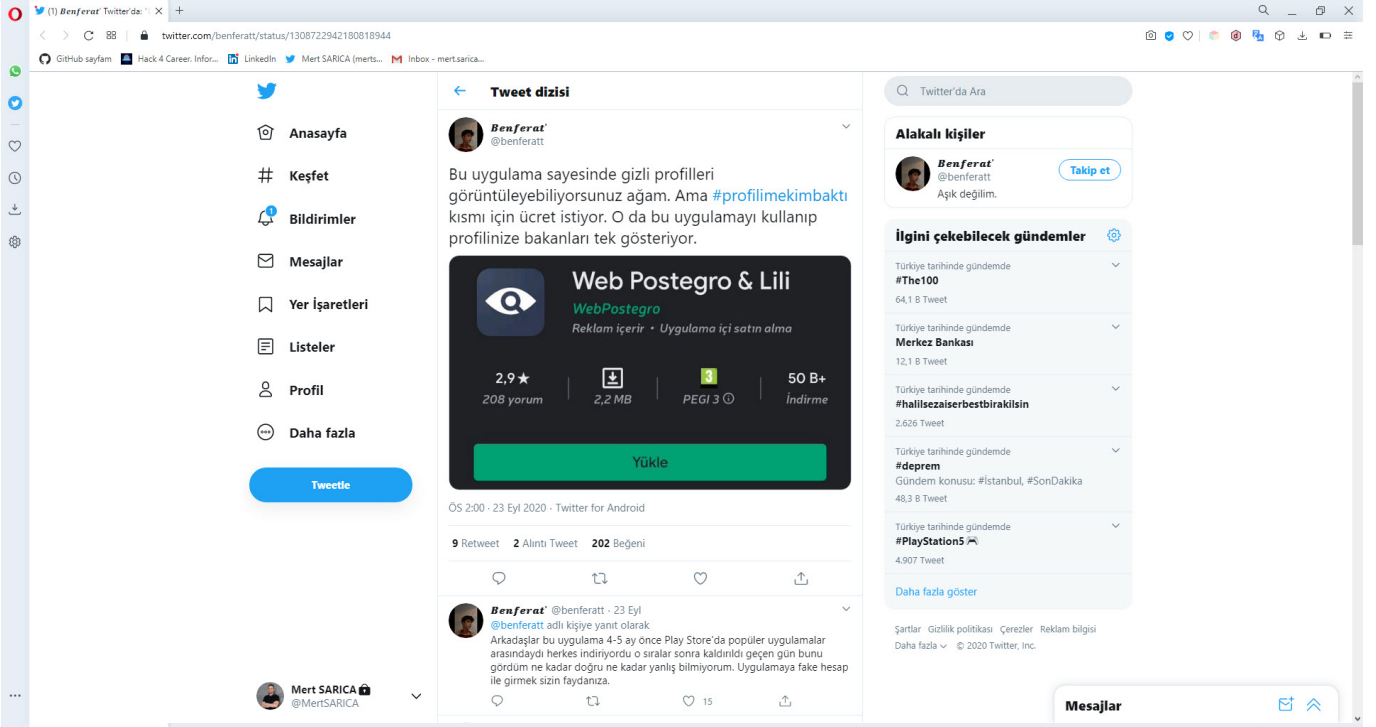
23 Eylül 2020 tarihinde Twitter'da siber güvenlik ile ilgili haberlere göz gezdirirken gündem olan başlıklarda #profilimekimbaktı etiketi dikkatimi çekti. Beni oldukça şüphelendiren bu etiketin gündem olmasının arkasında yatan sebebi bulmak için bu etiketi paylaşan hesaplara göz gezdirmeye karar verdim.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

Q Twitter'da Ara

İlgini çekebilecek gündemler

- Türkiye tarihinde gündemde 
#çöktü
Gündem konusu: Ali Babadan, Dolar 7.68
9.839 Tweet
- Türkiye tarihinde gündemde 
#BiseksüelGörünürlükGünü
Gündem konusu: #BiVisibilityDay
- Türkiye tarihinde gündemde 
#XAUUSD
1.524 Tweet
- Türkiye tarihinde gündemde 
#KemalizmiYikacaz
17,2 B Tweet
- Türkiye tarihinde gündemde 
#profilimekimbaktı 
2.264 Tweet

[Daha fazla göster](#)



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 - Google Play

play.google.com/store/apps/details

GitHub sayfam Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mert.sarica...

Google Play Ara

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 **WebPostegro Sosyal** ★★★★★ 248

PEGI 3

Reklam içeriyor
Bu uygulama tüm cihazlarınızla uyumlu.

İstek Listesine ekle **Yükle**

Hesapları görüntülemek için resmi Postegro uygulamasını indirin.

Res u

Açıklama, Google Çeviri kullanılarak Türkçe (Türkiye) diline çevrilsin mi? **Çevir**

Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamayı indirin.

- 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 uygulamayı 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 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 ihlalden biz sorumlu değiliz;
- * Bu uygulama, hiçbir sosyal medya platformu ile ilişkili değildir.

DARALT

YORUMLARI AR

Yorum Politikası

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

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

Türkiyedeymiş ve şifreyi girdiğimiz anda hesabınıza yabancı ülkeden giriş yapıyor. 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 kullanıcılarımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.

TÜM İNCELEMELERİ OKU

EK BİLGİ		
Güncellendi	Boyut	Yükleme sayısı
8 Eylül 2020	2,5M	50.000+
Mevcut Sürüm	Gereken Android sürümü	İçerik Derecelendirmesi
1.0	5.0 ve sonrası	PEGİ 3 Daha Fazla Bilgi
Etkileşimli Öğeler	İzinler	Rapor
Sınırsız İnternet	Ayrıntıları göster	Uygunsuz olarak işaretle
Sunan:	Geliştirici	
WebPostegro	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.

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

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

Merhaba. Gonderilerde beğenileri gösterme sorunu bir kaç gün içinde hall edilecektir. Şu an için uygulamaya girişte hiçbir sıkıntı yoktur. Eğer herhangi sorun yaşıyorsanız lütfen destek ekibimize iletişime geçin.

Enes Kuzu ★★★★★ 14 Eylül 2020

Adminler selamun aleykum öncelikle sizden ricamız lütfen bize bakanlar ücretsiz yapılırsanız 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 yaptı. Kesinlikle indirmeyin. Anında şifreyi değiştirmek zorunda kaldım.

WebPostegro 22 Eylül 2020

Merhaba. Uygulama tam güvenlidir buna emin ola bilirsiniz. Bizim için en önemli şey kullanıcılarımızın güvenliğidir ve bunun için elimizden geleni yapıyoruz. Daha fazla ayrıntı için lütfen Kullanıcı Şartlarımızı ve Güvenlik Politikamızı inceleyiniz.

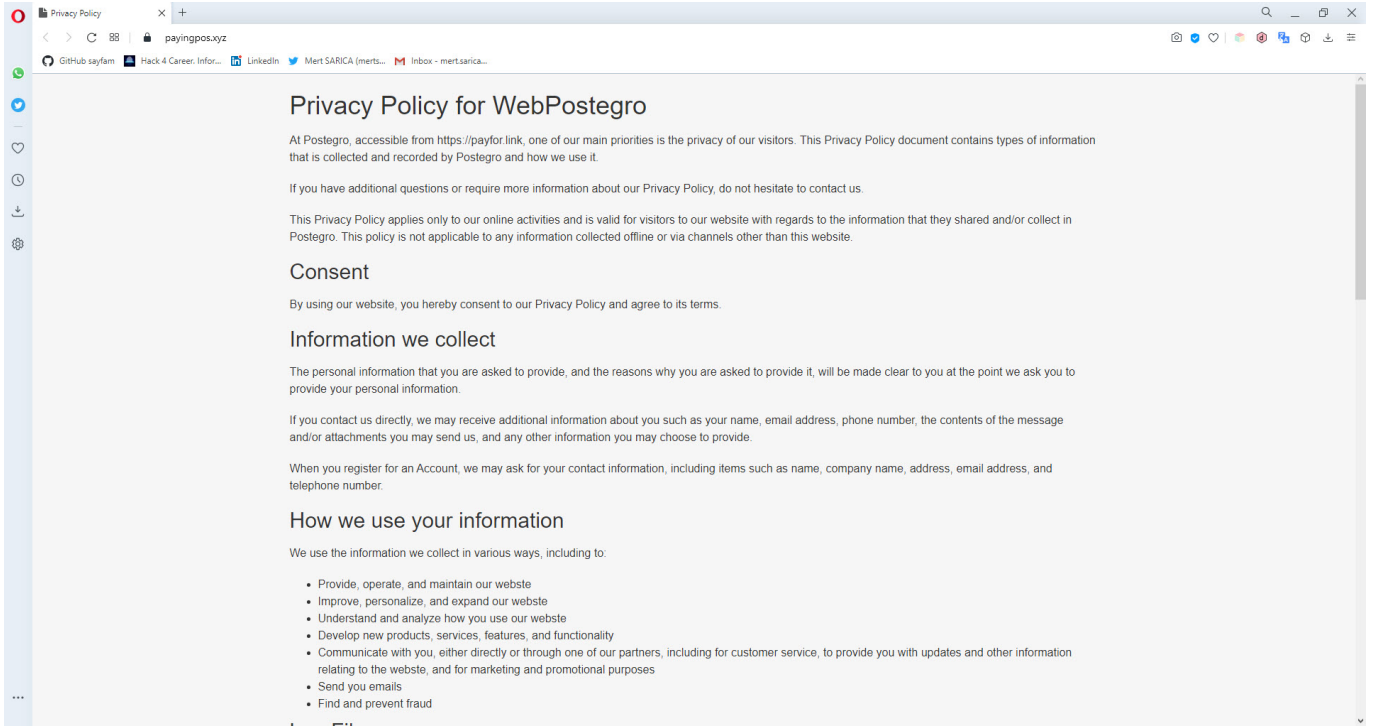
Elif Gürcan ★★★★★ 20 Eylül 2020

Yüklediğiniz ve şifreyi girdiğiniz anda hesabınıza yabancı ülkeden giriş yapıyor. 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 kullanıcılarımızın 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. Instagram 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.



Home » Apps » Social » Web Postegro & Lili

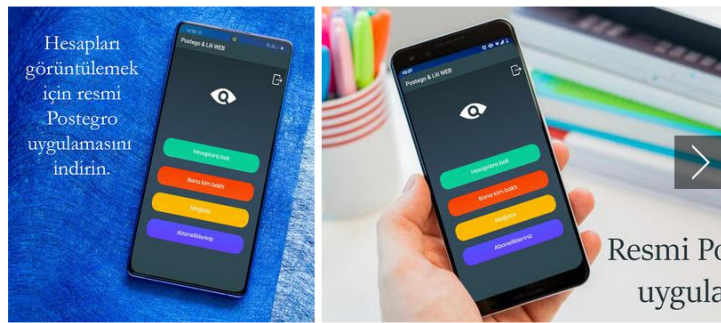


Web Postegro & Lili

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.



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}
```

Instagram profile page for postegro.llc. The profile shows 17 posts, 87.5k followers, and 2 following. The bio mentions "Postegro & LiLi indirme linki" and "postegro.net". The posts include a screenshot of the app, a link to "https://postegro.net/", and text announcements about domain changes and app updates.

Instagram
postegro.llc Follow
17 posts 87.5k followers 2 following
Postegro & LiLi indirme linki postegro.net
Lütfen uygulamayı silip ve yeniden bu sitemizden yükleyin https://postegro.net/
Postegro domaini ile bağlı sıkıntı var ve farkındayız. Teknik ekibimiz yeni domain üzerinde çalışıyor ve 48 saat arzında yeni güncelleme ile sorun hall edilecektir. Merak etmeyin tüm aboneliklerinizde hiç bir sorun olmayacaktır.
Merhaba. Teknik ekibimizin yoğun çalışmaları sonucu tüm sorunlar çözüldü ve uygulamayı rahatlıkla kullanabilirsiniz. Kullanıcılarımızın isteklerini dikkate alarak
Arkadaşlar şu anlık sunucumuzda güncelleme ve geliştirme işlemleri yaptığımız için sorunlar devam ediyor. Teknik ekibimizin verdiği bilgilere göre bu sorunlar 2, 3 gün devam edecektir. Bu işlemler
halkının ve tüm İslam alemlerinin bayramını Postegro ekibi adından kutluyoruz
Log In to Instagram
Log in to see photos and videos from friends and discover other accounts you'll love.
Log In Sign Up

Postegro App landing page. The page features a purple background with a smartphone displaying the app interface. The main heading is "POSTEGRO APP". Below it are buttons for "DOWNLOAD APK", "Google Play", and "Web Version". The text states: "You can view any instagram profile with our product. It is free. And you will enjoy it".

POSTEGRO
Home About us Screenshots Price
POSTEGRO APP
DOWNLOAD APK Google Play Web Version
You can view any instagram profile with our product
It is free
And you will enjoy it
Postegro App interface showing a profile page with buttons for "View Profile", "View Posts", "View Stories", and "Buy App".

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!



Hesaplara bak

Bana kim baktı

Mağaza

Abonelikleriniz



Instagram

Log In

OR

 Log in with Facebook

[Forgot password?](#)

Don't have an account? [Sign up](#)

Get the app.



The screenshot shows the Charles Proxy interface. The top panel displays a list of requests with columns for Code, Method, Host, Path, Start, Duration, Size, Status, and Info. A red arrow points to the 'app_version' field in the 'Request' tab, which is set to '1.0'. The 'Find in Session 1' dialog is open, showing a search for the token 'KIQTSIqH9TPuAx5576rFNvrCerHeOY0'. The search results show 41 matches, with a red arrow pointing to the 'Response Header: 2259 ... csrfToken=KIQTSIqH9TPuAx5576r...' entry.

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.

You have to minimum 10 following or 10 followers. Your following count are 0 and followers count are 0

OK

- Open GAPP
- Lock
- GPS
- Camera
- Microphone
- Location
- ID
- Bluetooth
- Wi-Fi
- Notifications
- Share
- Volume Up
- Volume Down
- Refresh
- Clipboard
- App Drawer
- Home
- Power

Web Postegro

webpostegro.net/store#tab=monthly

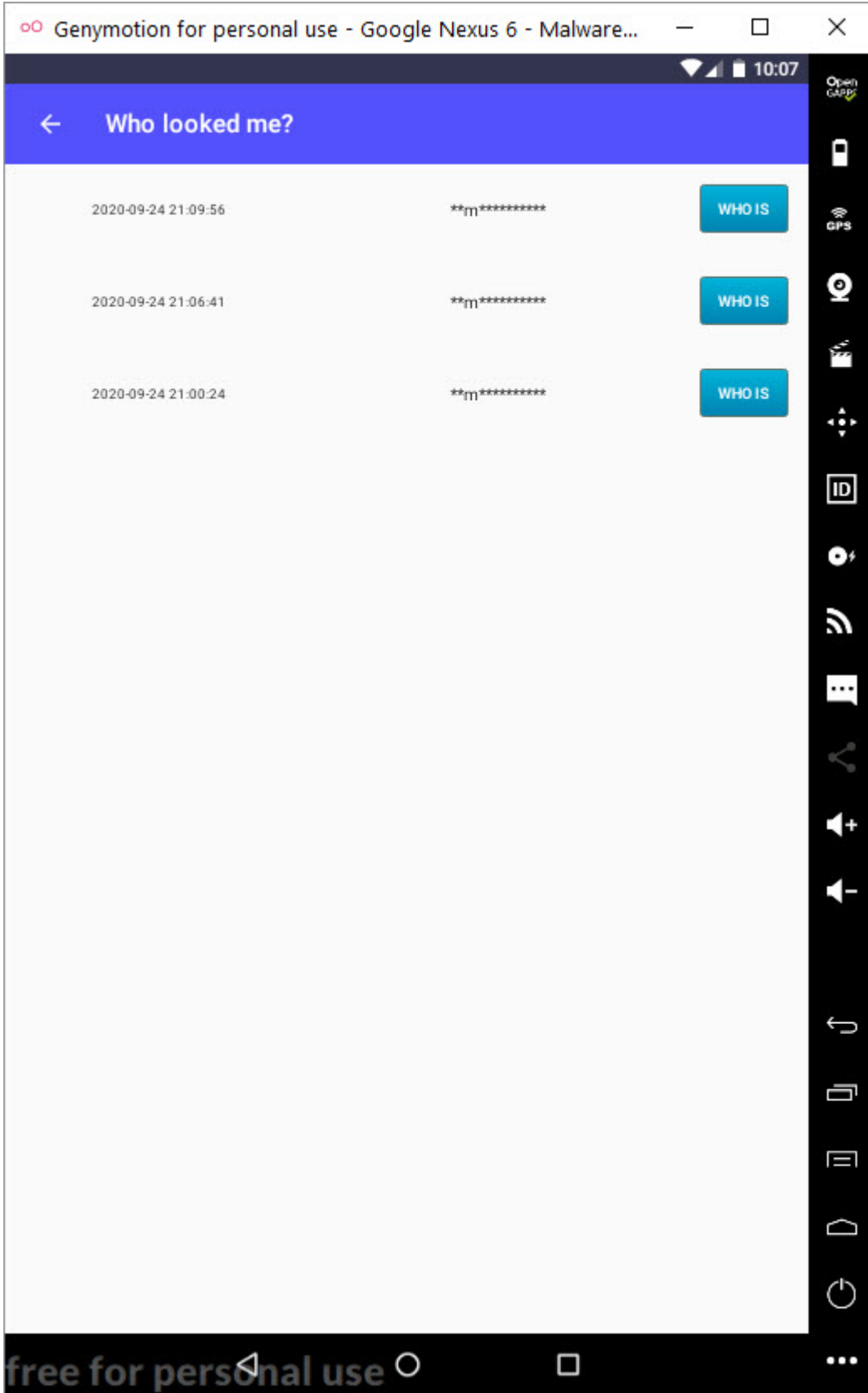
Mağaza monthly

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 baktı? Hesabınızı kimlerin görüntülediğini öğrenebilirsiniz. 95.8₺	Hepsi birinde Gizli hesapların gönderilerine ve hikayelerine sınırsız bakın, tüm reklamları kaldırın, Hesabınızı kimlerin görüntülediğini öğrenin ve tüm hesaplara gizli moda bakın (Hedef kullanıcı bu konuda bilgilendirilmez) + Bu zamana kadar baktığınız gizli hesaplardan sizin onları görüntüleme geçmişiniz silinecek + Ayarlar bölümünde 'Profili mi gizle' bölümü etkinleşecek 209.2₺

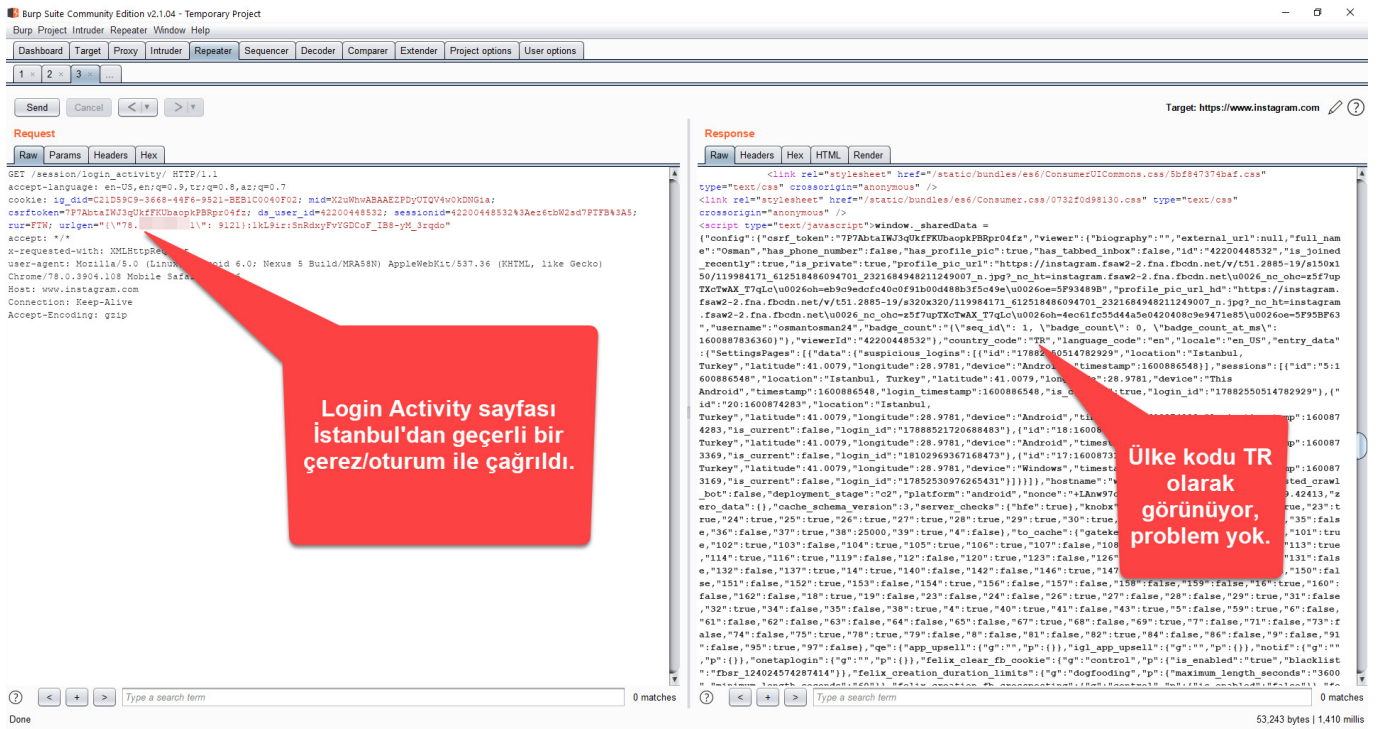
TURKISH ENGLISH

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!



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.

WhatIsMyIP.com

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

Internet Speed Test

What Is My Public IP?

DNS Lookup

IP Whois Lookup

Email Header Analyzer

Port Scanner

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

Because of TV and movies, most of us have a similar picture of a hacker: a young, thin, and somewhat nerdy-looking person sitting at a computer screen in a dark room, typing furiously.

Italy, Roma'ya VPN yapıldı.

What Is My IP?

WhatIsMyIP.com® is the industry leader in providing REAL IP address information. We have extensive tutorials 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 address looks like this 76.133.323.355. [Read more...]

Daha önceki çerez, oturum ile VPN üzerinden İtalya'dan Login Activity sayfasını çağırdım.

Oturum başarıyla kuruldu. (session-hijacked)

Ülke kodu değişti fakat lokasyon bilgileri hala değişmedi.

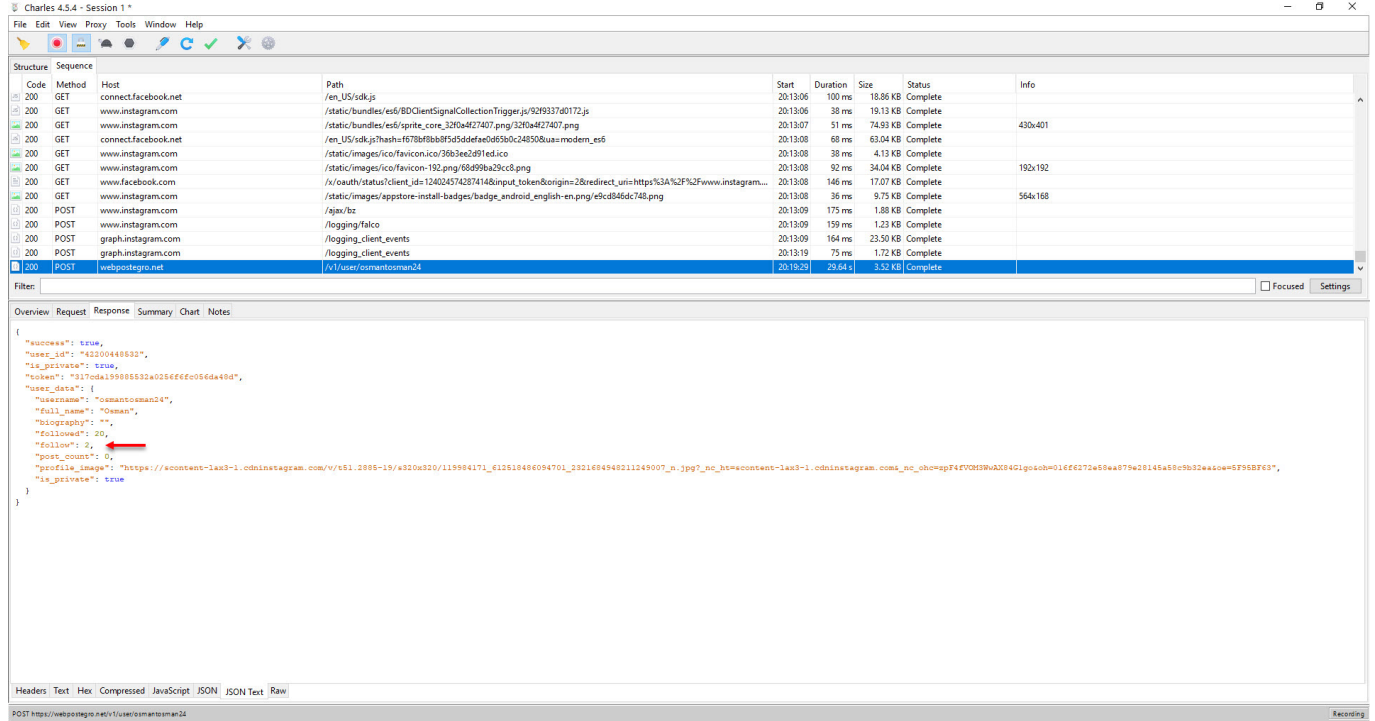
Roma yazması gerekirken hala İstanbul yazıyor.

VPN ile İtalya, Roma'dan giriş yapmama rağmen hala İstanbul görünüyor.

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!



The screenshot shows the Charles 4.5.4 interface. The top part displays a sequence of network requests and responses. The bottom part shows the response body for the selected request to webpostegro.net, which is a JSON object containing user information.

Code	Method	Host	Path	Start	Duration	Size	Status	Info
200	GET	connect.facebook.net	/en_US/sdk.js	20:13:06	100 ms	18.86 KB	Complete	
200	GET	www.instagram.com	/static/bundles/esd/6DClientSignalCollectionTrigger.js/2f9327d0172.js	20:13:06	38 ms	19.13 KB	Complete	
200	GET	www.instagram.com	/static/bundles/esd/sprite_core_32f0e427407.png/32f0e427407.png	20:13:07	51 ms	74.93 KB	Complete	430x401
200	GET	connect.facebook.net	/en_US/sdk.js?hash=f678bf8b8f5d5d4e0d65b0c248506a0a+modern_es6	20:13:08	68 ms	63.04 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon-ico/36b3e2d91edico	20:13:08	38 ms	4.13 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon-192.png/68d99ba29c8.png	20:13:08	92 ms	34.04 KB	Complete	192x192
200	GET	www.facebook.com	/x/oauth/status/client_id=124024374287414&input_token=&origin=https%3A%2F%2Fwww.instagram.com	20:13:08	146 ms	17.07 KB	Complete	
200	GET	www.instagram.com	/static/images/appstore-install-badges/badge_android_english-en.png/e9c846d-74b.png	20:13:08	36 ms	9.75 KB	Complete	564x168
200	POST	www.instagram.com	/api/v1/	20:13:09	173 ms	1.88 KB	Complete	
200	POST	www.instagram.com	/logging/fbco	20:13:09	159 ms	1.23 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:09	164 ms	23.50 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:19	75 ms	1.72 KB	Complete	
200	POST	webpostegro.net	/v1/user/osmantosman24	20:19:29	29.64 s	3.52 KB	Complete	

```
{
  "success": true,
  "user_id": "4200448830",
  "is_private": true,
  "username": "3170d415988553a02566e0c056da49d",
  "user_data": {
    "username": "osmantosman24",
    "full_name": "Osman",
    "biography": "",
    "followers": 0,
    "posts_count": 0,
    "profile_image": "https://content-lax3-1.cdninstagram.com/v/t51.2885-19/4320x320/119994171_1212618466094701_2021494948211249007_n.jpg?_nc_ht=content-lax3-1.cdninstagram.com&_nc_ohc=apF4FVOM9RnAX04G1g0sobw01e6E2t2w65a879a26145a56c9b32aa04w5F958BF63",
    "is_private": true
  }
}
```

Web Postegro & Lili uygulamasının ve geliştiricisinin Instagram hesabına, 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.

The screenshot shows the Charles proxy interface. The top panel displays a list of network requests with columns for Code, Method, Host, Path, Start, Duration, Size, Status, and Info. The bottom panel shows the response for a POST request to webpostegro.net, which is a JSON object with "success": false and "error": {}.

Code	Method	Host	Path	Start	Duration	Size	Status	Info
200	GET	www.instagram.com	/static/bundles/es6/BDClientSignalCollectionTrigger.js/92f933740172.js	20:13:06	38 ms	19.13 KB	Complete	
200	GET	www.instagram.com	/static/bundles/es6/sprite_core_32f0a427407.png/32f0a427407.png	20:13:07	51 ms	74.93 KB	Complete	43b401
200	GET	connect.facebook.net	/en_US/sdk.js?hash=1678bfb85d5d5d4e0d65b0c24850b0aa:modern_es6	20:13:08	68 ms	63.04 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon.ico/36b3e2d91ed.ico	20:13:08	38 ms	4.13 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon-192.png/6d999ba29c8.png	20:13:08	92 ms	34.04 KB	Complete	192x192
200	GET	www.facebook.com	/i/oauth/status/client_id=1230243742374148?input_token=borigin=2&redirect_uri=https%3A%2F%2Fwww.instagram.com	20:13:08	146 ms	17.07 KB	Complete	
200	GET	www.instagram.com	/static/images/appstore-install-badges/badge_android_english-en.png/v6cd846d-c748.png	20:13:08	36 ms	9.75 KB	Complete	564x168
200	POST	www.instagram.com	/ajax/bz	20:13:09	175 ms	1.88 KB	Complete	
200	POST	www.instagram.com	/logging/falco	20:13:09	159 ms	1.23 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:09	164 ms	23.50 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:19	75 ms	1.72 KB	Complete	
200	POST	webpostegro.net	/v1/user/osmantosman24	20:19:29	29.64 s	3.52 KB	Complete	
200	POST	webpostegro.net	/v1/user/osmantosman24	20:24:35	47.09 s	3.24 KB	Complete	

```
{
  "success": false,
  "error": {}
}
```

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.