Broken Authentication

Dictionary Attack

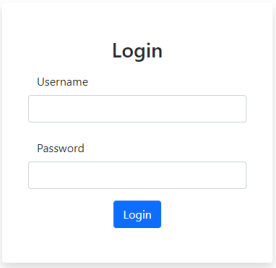
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, zayıf parolaya sahip bir oturum açma sayfası içerir.

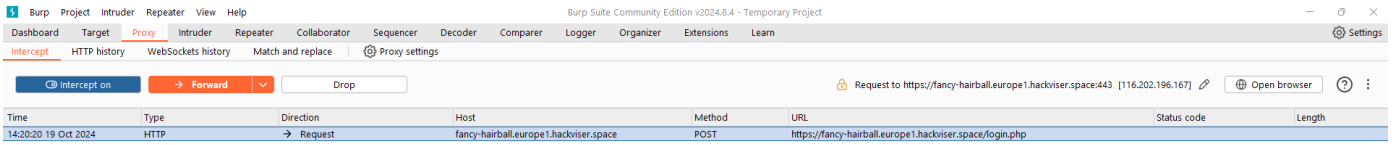
Laboratuvarı tamamlamak için, sözlük saldırısı ile "admin" kullanıcısının şifresini bulun.

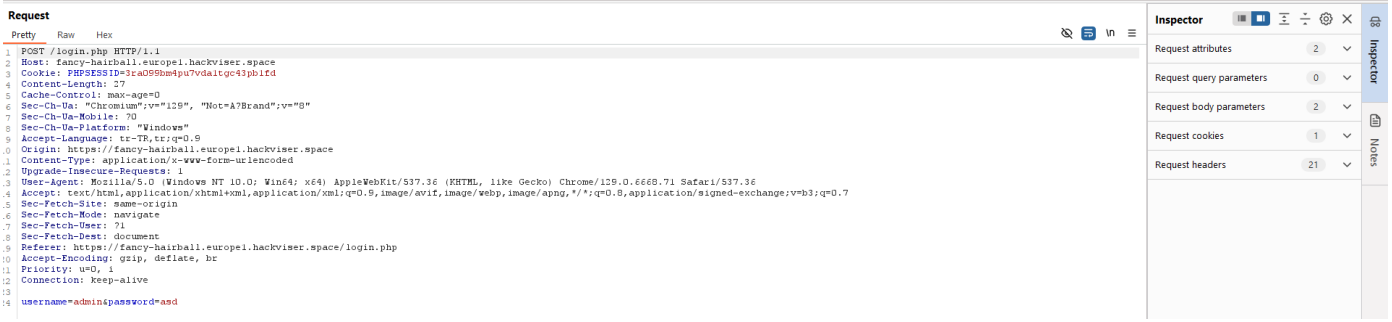
"admin" kullanıcısının parolası nedir?

Öncelikle web sitesini ziyaret edelim



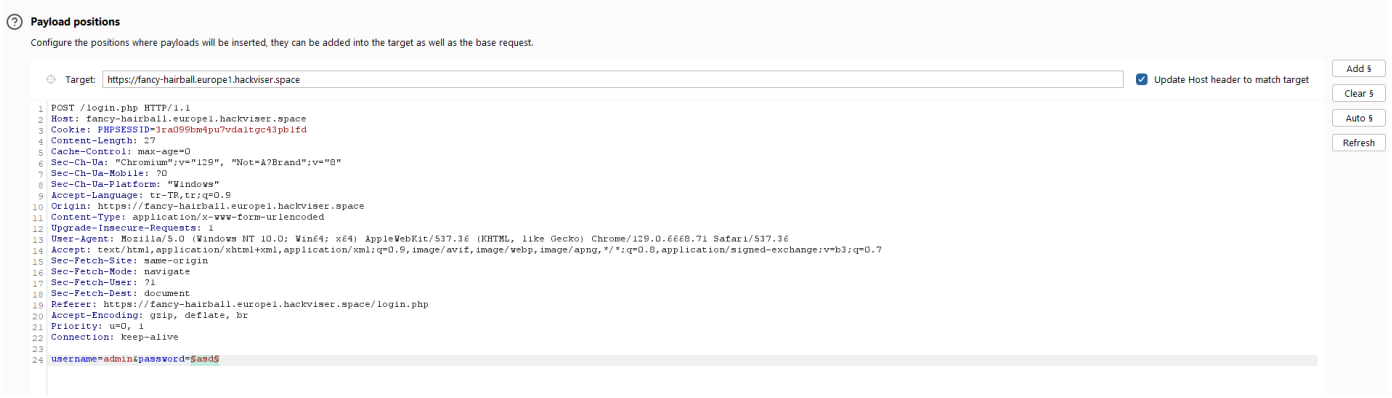
Şöyle bi login formu karşıladı bizi brute force atmak için öncelikle isteği burp ile izleyelim

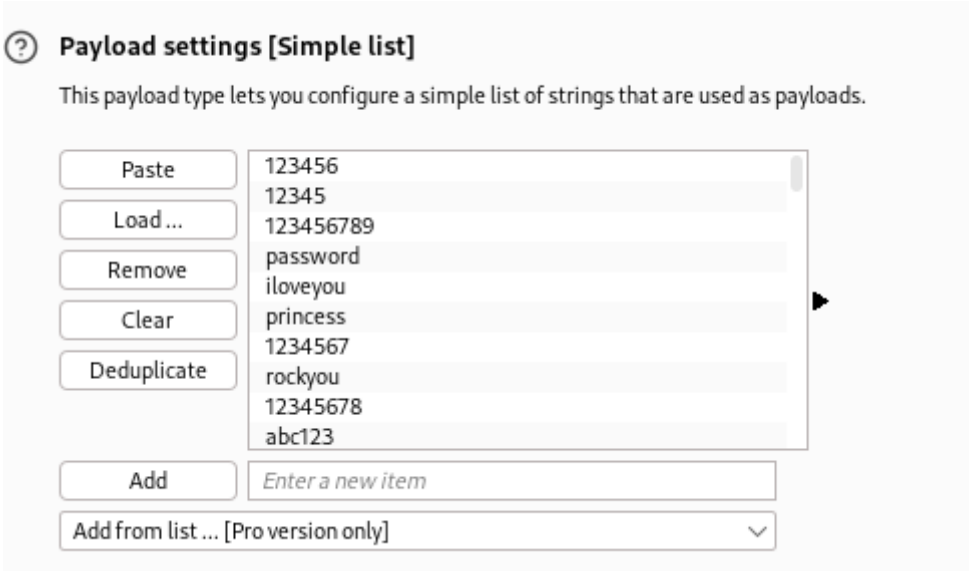




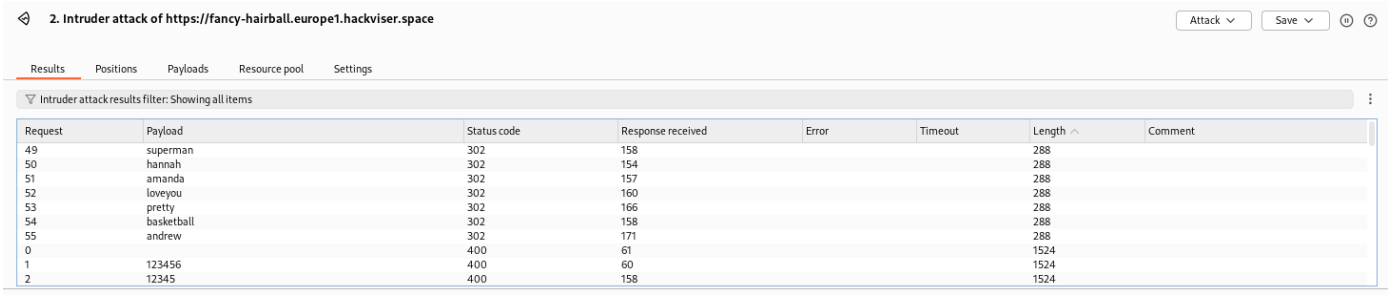
Böyle bi requstimizin olduğunu görüyoruz.

Şimdi brute force atmak için ben burpde intruder'i kullanacağım



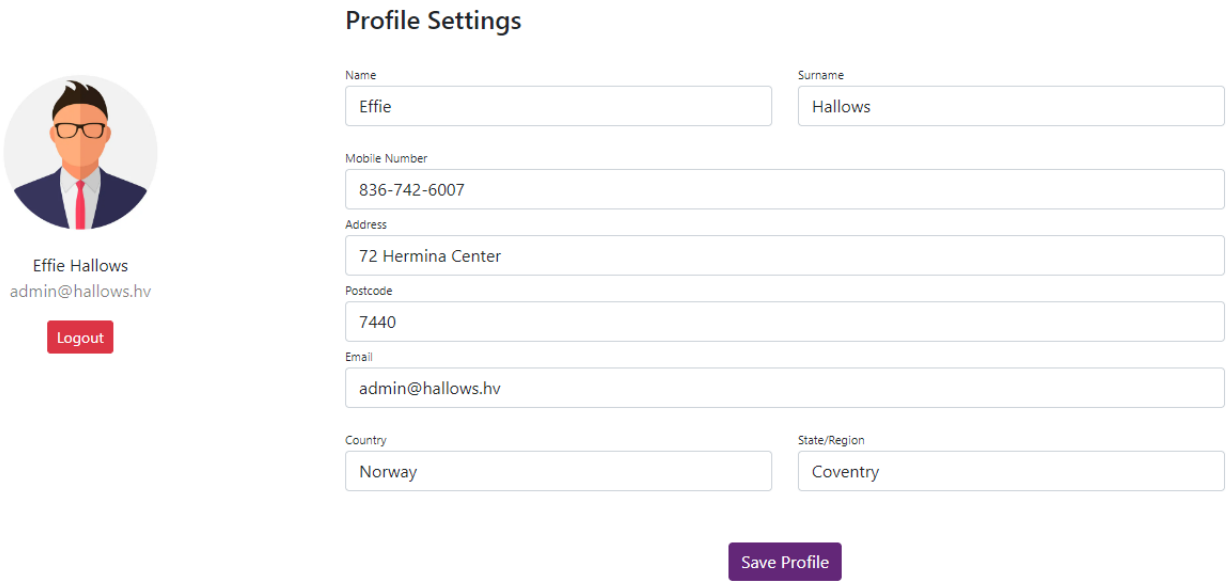


Wordlist olarak rockyou kullandım. Saldırıya başlayalım



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
49	superman	302	158			288	
50	hannah	302	154			288	
51	amanda	302	157			288	
52	loveyou	302	160			288	
53	pretty	302	166			288	
54	basketball	302	158			288	
55	andrew	302	171			288	
0		400	61			1524	
1	123456	400	60			1524	
2	12345	400	158			1524	

Ve evet 1 den fazla parola olduğunu görüyoruz



Herhangibirisini kullanarakta sisteme giriş yapabildim.

Execution After Redirect (EAR)

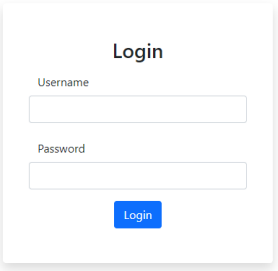
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar Execution After Redirect (EAR) zafiyeti içermektedir.

Laboratuvarı tamamlamak için, web sayfası yönlendirilmeden önce yüklenmesini durdurun ve içeriğini okuyun.

Hesabına izinsiz erişilen kullanıcının telefon numarası nedir?

Öncelikle web sitesine bi girelim



Bizi bu şekilde bir login ekranı karşılıyor. Labda bahsedilen Execution After Redirect (EAR) zafiyetini uygulamak için yönlendirmeleri kontrol etmemiz gerekiyor bundan dolayı siteye ilk girdiğimde bunu burp

ile intercept edip araya gireceğim ve bu isteği durdurarak sitenin bana göndedreceği response yani yanıtları inceleyeceğim

Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: improved-michaelangelo.europe1.hackviser.space
Cookie: PHPSESSID=j4eobnr7tttvp17aqOrmd425e3
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR,tr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

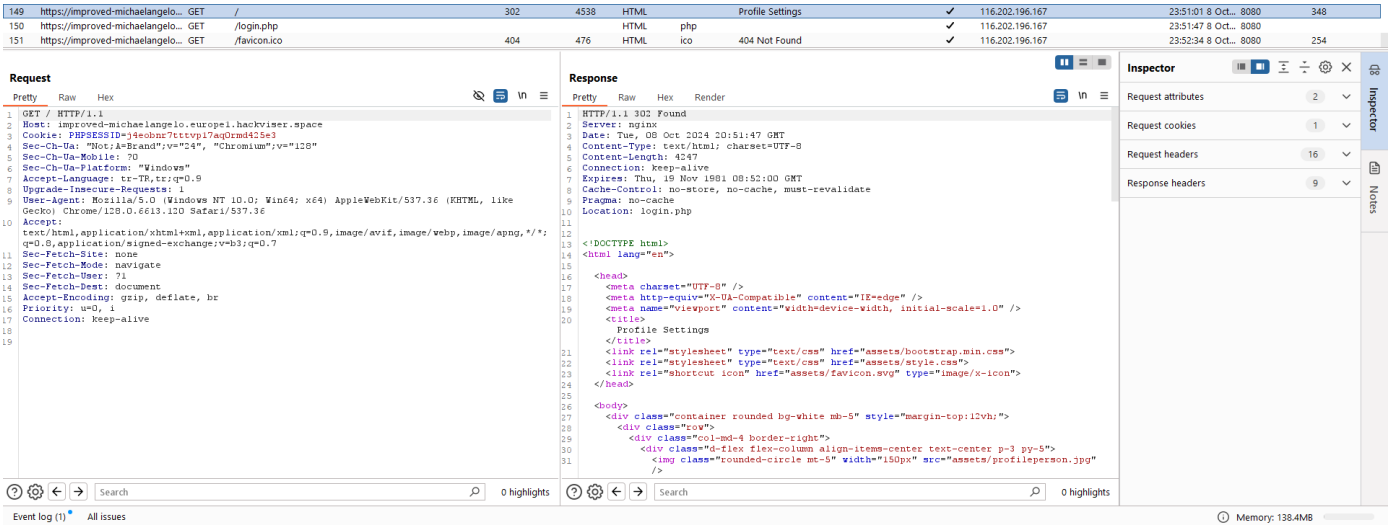
Siteye ilk girişimizde bizi direk normal bi yer karşılıyor ama devamında forward ettiğim zaman

Request

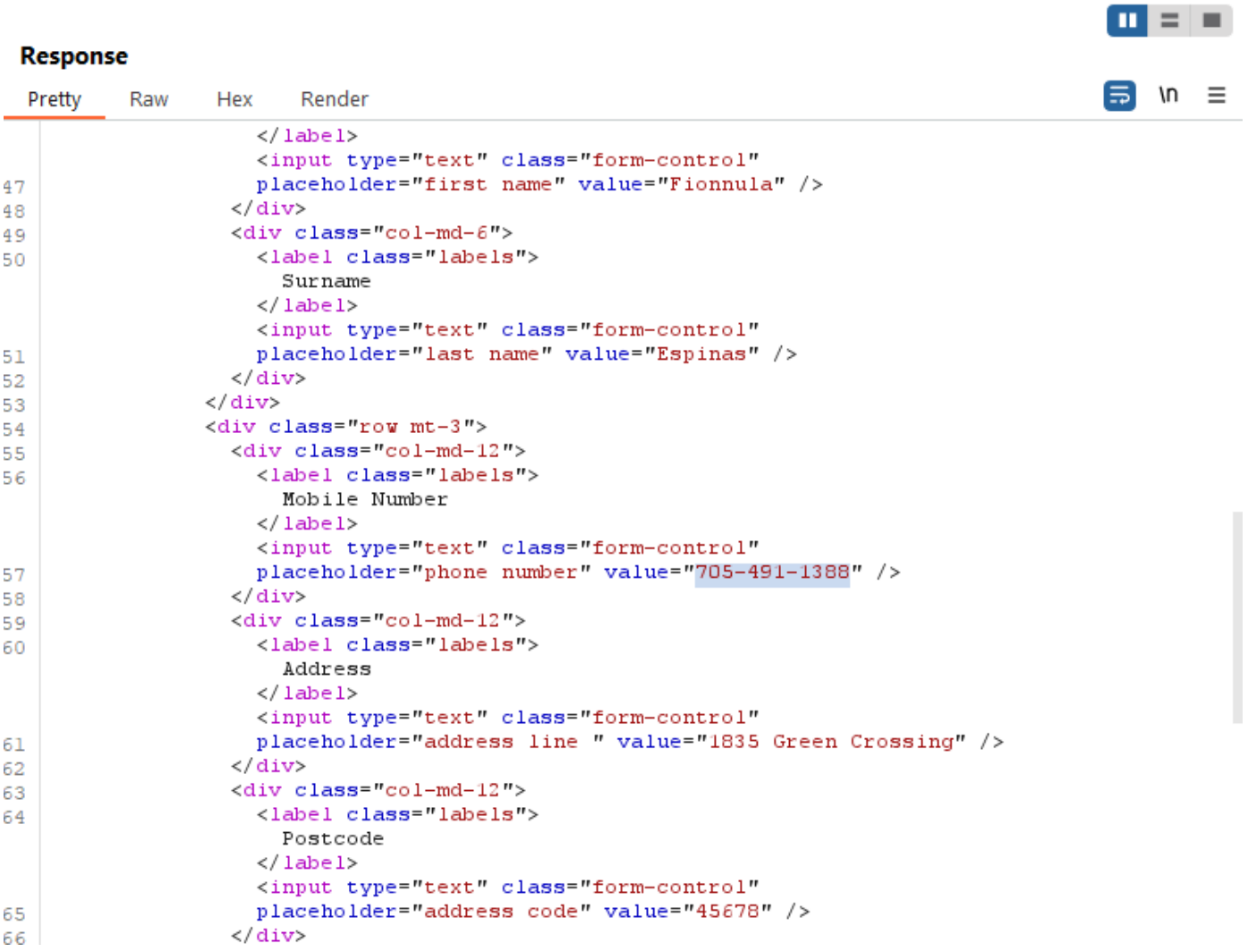
Pretty Raw Hex

```
GET /login.php HTTP/1.1
Host: improved-michaelangelo.europe1.hackviser.space
Cookie: PHPSESSID=j4eobnr7tttvp17aqOrmd425e3
Accept-Language: tr-TR,tr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Bir get isteği ile bize bi yönlendirme yapıyor. Şimdi bu isteği burada drop edip bize gönderilen response cevabını inceleyelim



Burada gördüğümüz gibi bize bir Profile Settings cevabı döndürülüyor ve bu cevabın içerisinde istenildiği üzere kullanıcının telefon numarası gözüküyor



Böylelikle labı başarıyla çözmüş oluyoruz.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş