LAB: BLIND SQL INJECTION WITH CONDITIONAL RESPONSES

https://portswigger.net/web-security/sql-injection/blind/lab-conditional-responses

GÖREV:

Çözülmesi istenen raporda sql sorguları çalıştırılarak sistemde zafiyet olup olmadığı tespit edilmeye çalışılmaktadır. Buradaki sql injection çeşidi "blind sql injection" olduğu açıklamada verilmiştir.

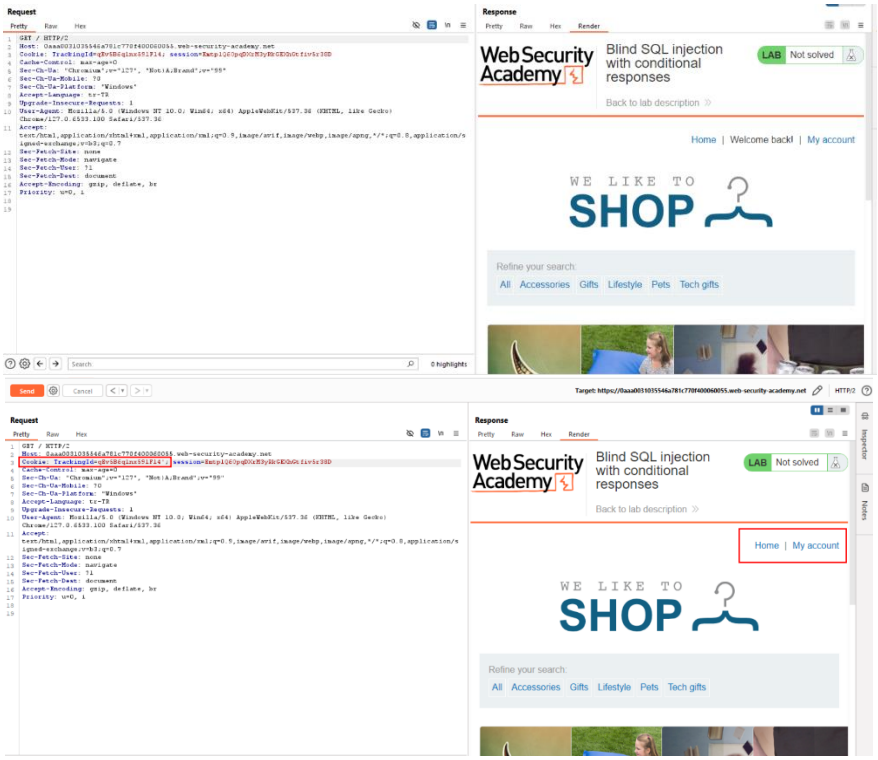
AÇIKLAMA:

Lab mantığında çalıştırılan sql sorgularının "true" olması durumunda sayfada "Welcome Back" ibaresinin göründüğü ancak yanlış bir sorgu çalıştırıldığında bu ibarenin görünmediği belirlenmiştir.

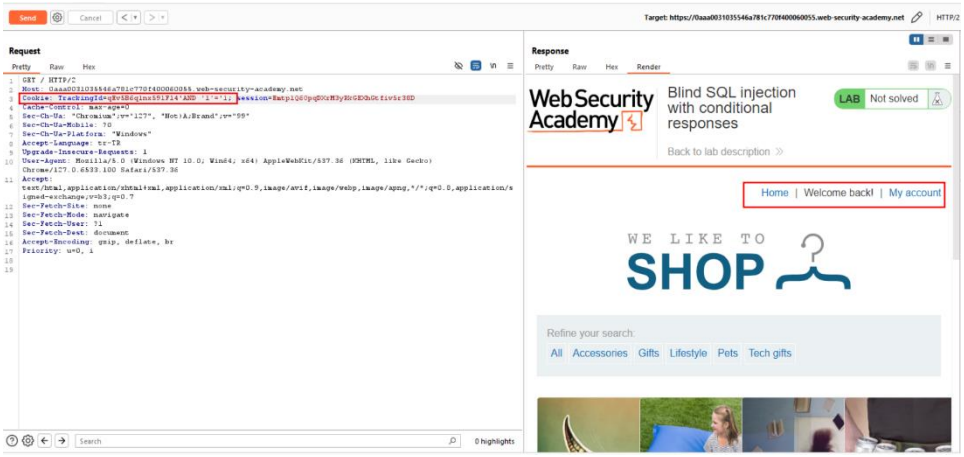
Bu noktadan yola çıkılarak sistemin veri tabanında sql sorguları çalıştırılarak kullanıcı adı ve parolaların tutuldulduğu "users" tablosunun olup olmadığı ve bu tablo eğer varsa administrator kullanıcısına ait parola bilgileri bulunmak isteniyor.

Sayfadaki "My Account" sekmesine tıklandığında doğru bir sorgu çalıştığı için "Welcome Back" ibaresi görülmektedir. Fakat istekte oynama yapıldığında (örneğin TrackingId değerinin sonuna ' koyulması gibi) sql yapısı bozulduğu için "Welcome Back" ifadesi geri dönderilmemiştir. Böylelikle sistemde blind sql injection zafiyetinin varlığı tespit edilmiştir.

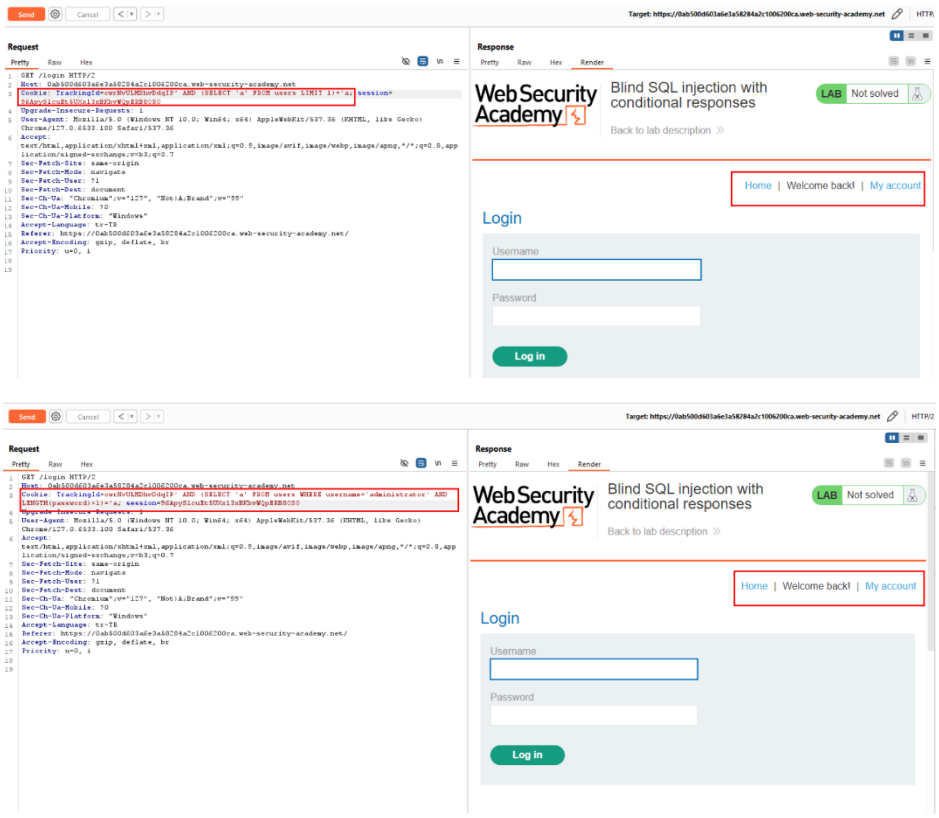
ÇÖZÜM:



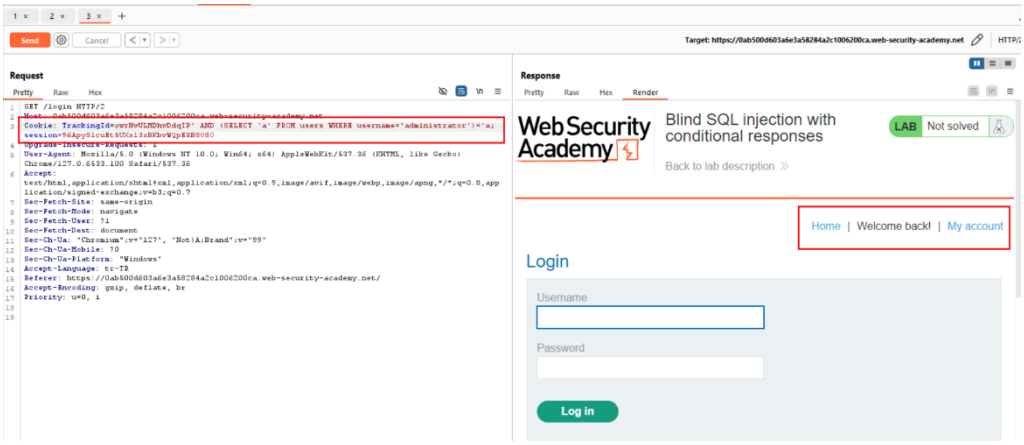
Daha sonra ' AND '1'='1 sorgusu eklenerek ilk sql sorgusu ile sistem tetiklenmiştir.



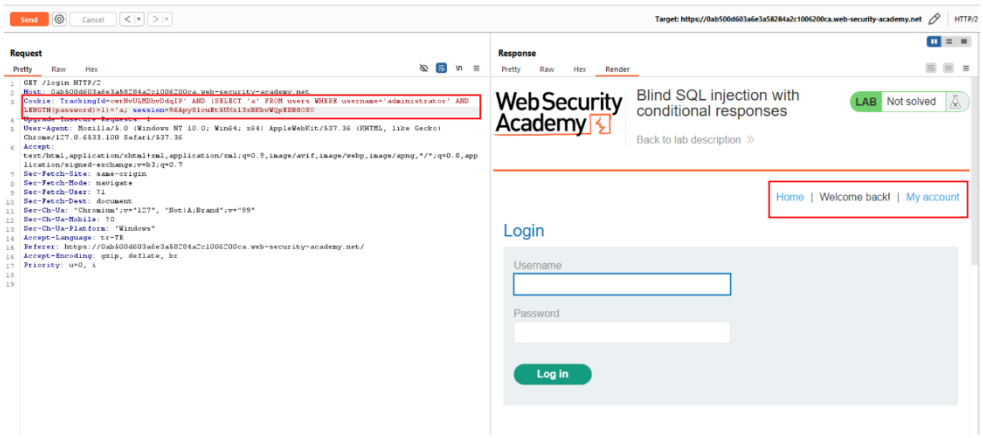
Zafiyetin varlığı kesin bir şekilde belirlendikten sonra users tablosunun varlığı araştırılmıştır. Bunun için ' AND (SELECT 'a' FROM users LIMIT 1)='a komutu ile users tablosunun varlığı tespit edilmiştir.



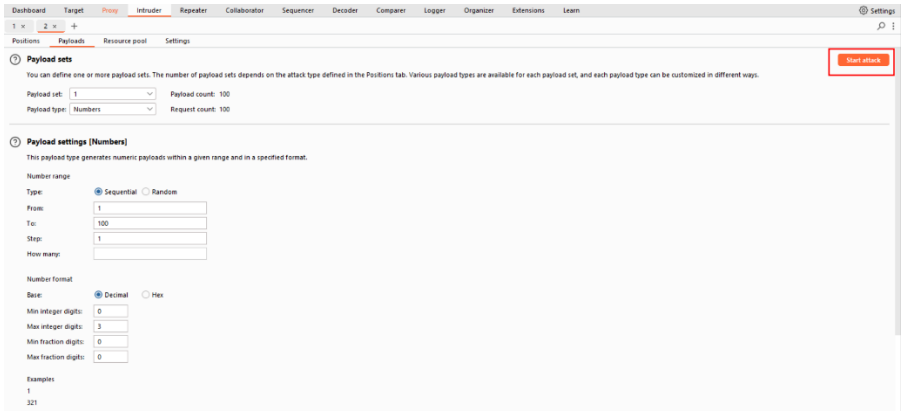
Daha sonra, tabloda bir 'administrator' kullanıcısı olup olmadığını kontrol edilmiştir. Bunun için 'a' ifadesini 'administrator' ile değiştirip, 'kullanıcı adı' başlıklı bir sütun olduğu bilindiğinden ' AND (SELECT 'a' FROM users WHERE username='administrator')='a sorgusu kullanılmıştır.



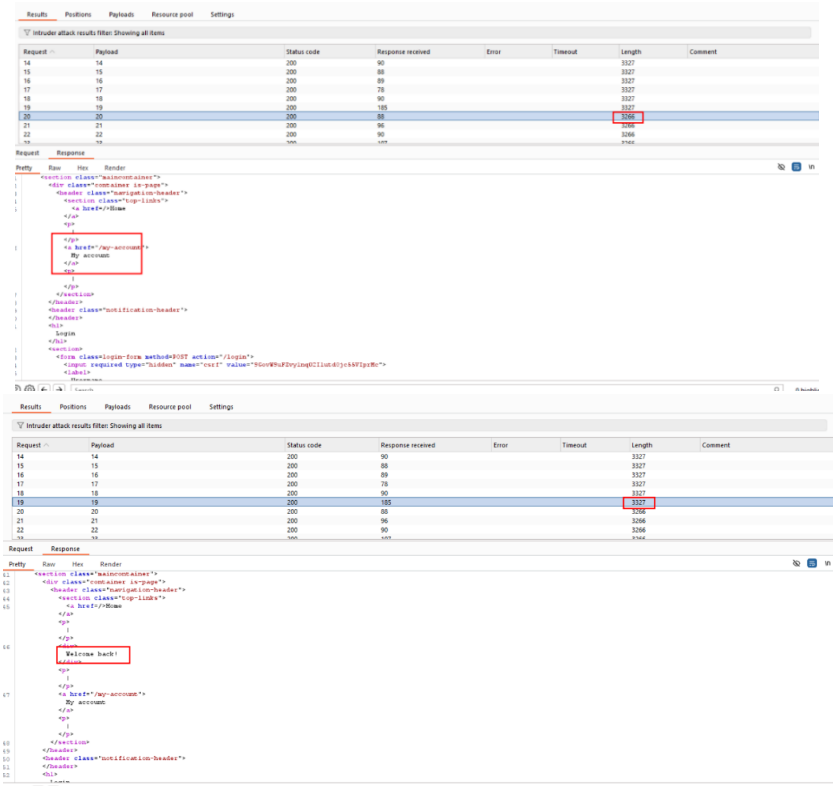
Sonrasında yapılacak işlem parolanın uzunluğunu bulmaktır. Bu işlem uygulamaya uzunluk hakkında sorular sorarak gerçekleştirilir. ' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a sorgusu ile parola uzunluğunu belirlemeye yönelik çalışma başlamıştır.



Parola uzunluğunu manuel olarak bulmak uzun ve meşakkatli olduğu için “brute-force” yani kaba kuvvet saldırısı uygulanmıştır.

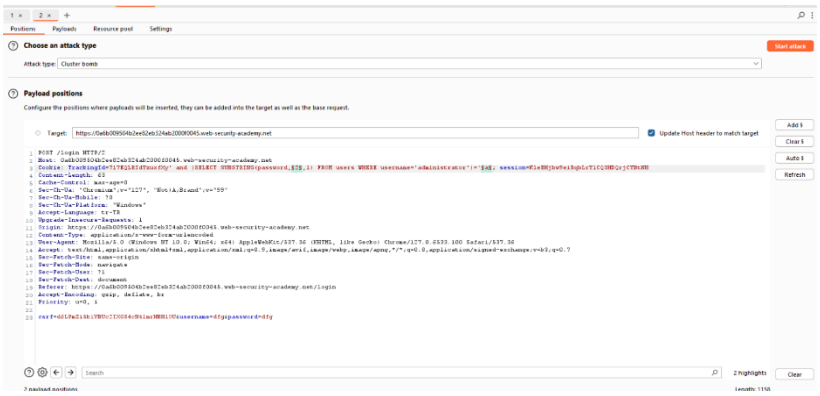


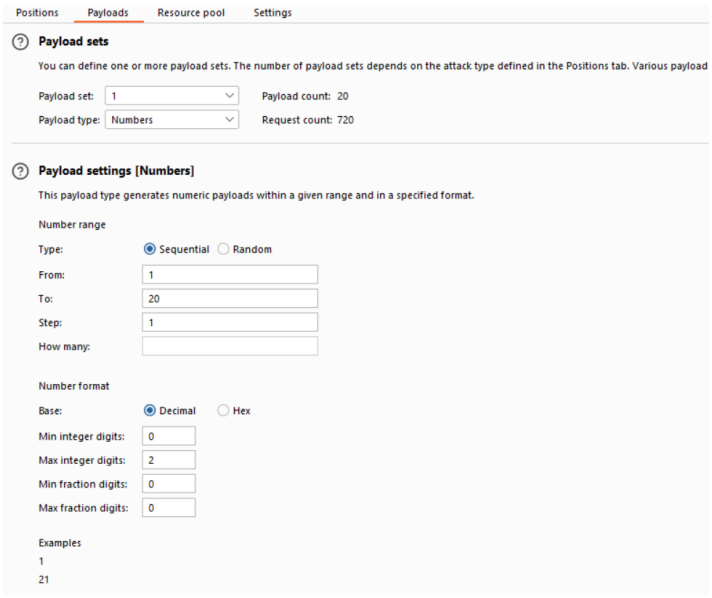
Saldırı sonucunda parola uzunluğunun 20 haneli olduğu tespit edilmiştir.

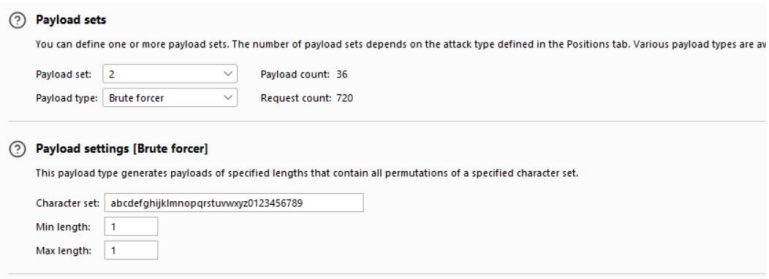


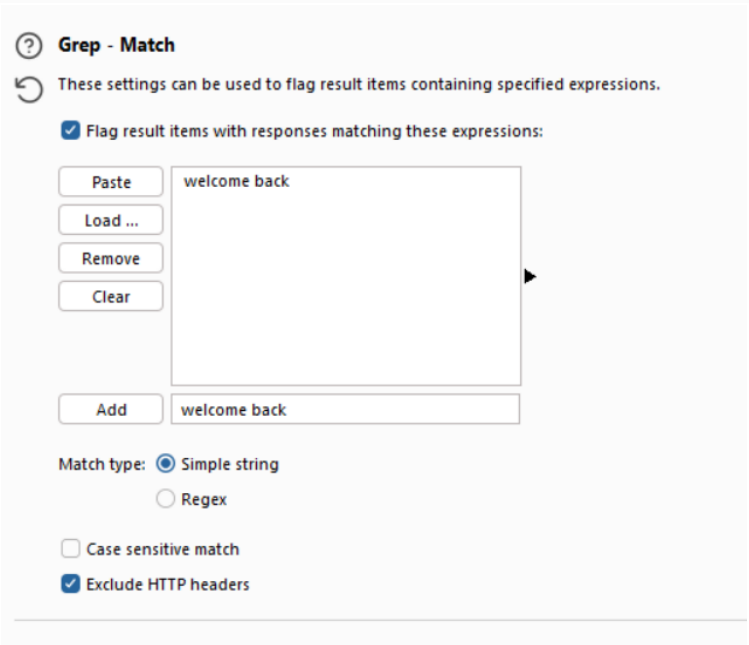
Parolayı tahmin etmek veya tek tek denemek zor olacağı için ona da brute force uygulanmıştır.

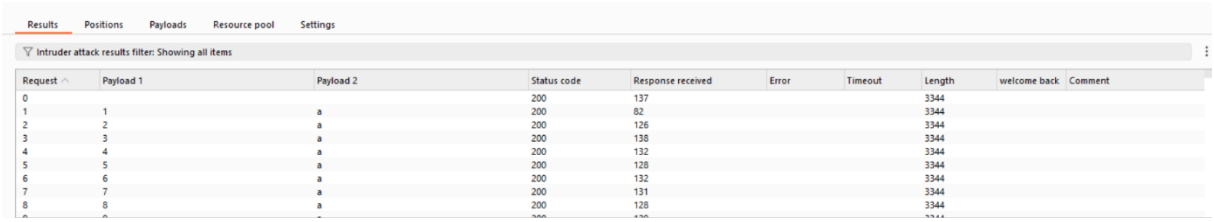
' AND (SELECT SUBSTRING(password,2,1) FROM users WHERE username='administrator')='a sorgusu ile parola bulma işlemine devam edilmiştir.











Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	welcome back	Comment
0			200	137			3344		
1	1	a	200	82			3344		
2	2	a	200	126			3344		
3	3	a	200	138			3344		
4	4	a	200	132			3344		
5	5	a	200	128			3344		
6	6	a	200	132			3344		
7	7	a	200	131			3344		
8	8	a	200	128			3344		

Saldırı sonucunda administrator kullanıcısına ait şifre bilgisi bulunmuş olur.

Şeyma SAYLAN