|  |
| --- |
| ***BURP SUITE*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Web Uygulama Güvenliği testlerinde yaygın olarak kullanılan Proxy aracı olan BURPSUITE kullanımı hakkında bilgi vereceğim. |

**26.07.2021**

-Burpsuite;İstemci-Sunucu arasına girerek,isteklerin üzerinden değişiklikler yapıp zafiyetlerden faydalanabileceğimiz bir programdır.

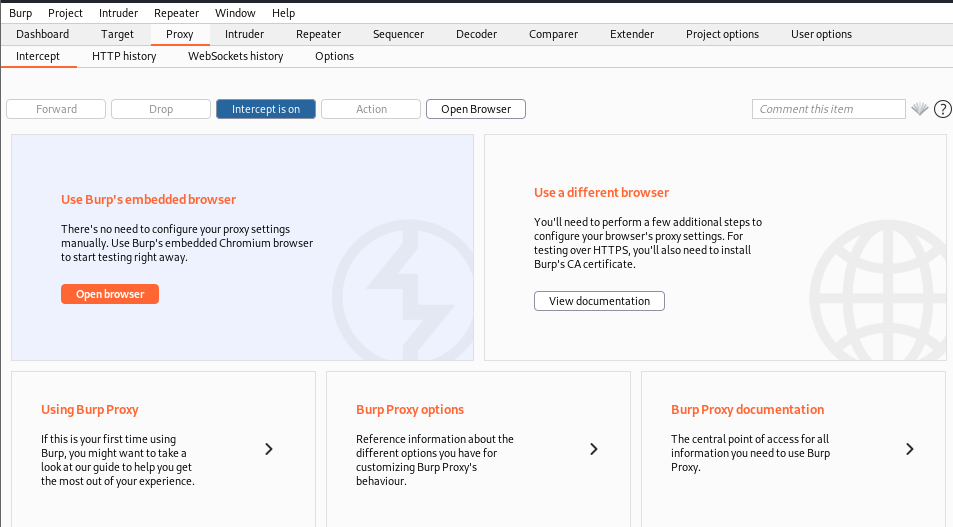
-Ücretsiz versiyonu bulunduğu gibi ücretli olup daha fazla içeriğe sahip olan versiyonu da vardır.” <https://portswigger.net/burp/communitydownload>” Bağlantısı üzerinden indirilip kurulum işlemi başlatılabilir.

-Kali Linux sürümlerinde Community(Ücretsiz) versiyonu kurulu olarak gelmektedir.

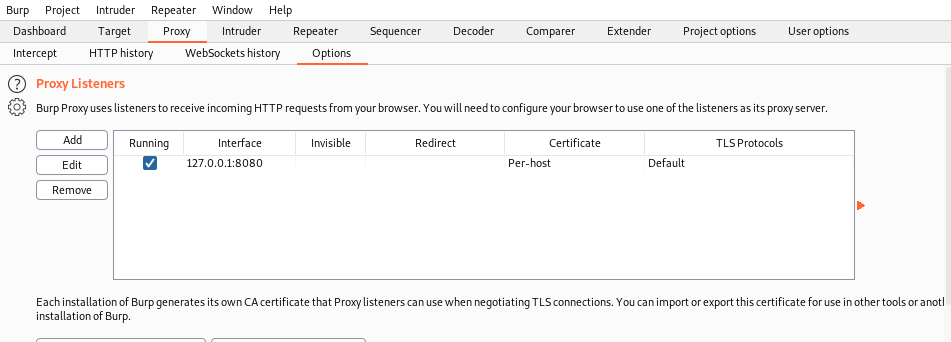
Basitdüze birkaç bilgi verdikten sonra yavaştan programa geçiş yapmak istiyorum.

**PROXY**

-Programı çalıştırdığımızda böyle bir ekran ile karşılaşıyoruz.Burpsuite üzerinde işlem yapabilmek için öncelikle bir port üzerinde dinleme yapmamız gerekmektedir.Bu sebeple ilk önce dinlenecek portun ayarlaması yapılması lazımdır.

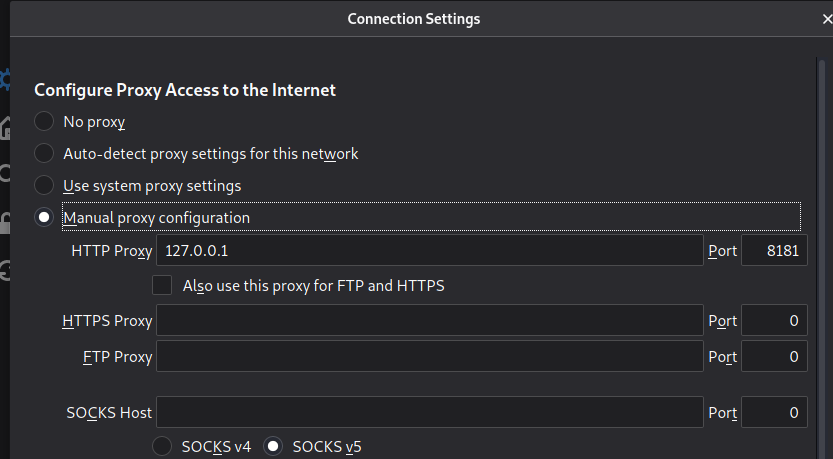


-Birlikte port ayarlamasına başlayalım. “Proxy>Options” sekmesine girdiğimde sabit olarak 127.0.0.1 IP adresini ve 8080 portunu dinlediğini görüntüleyebiliyorum.



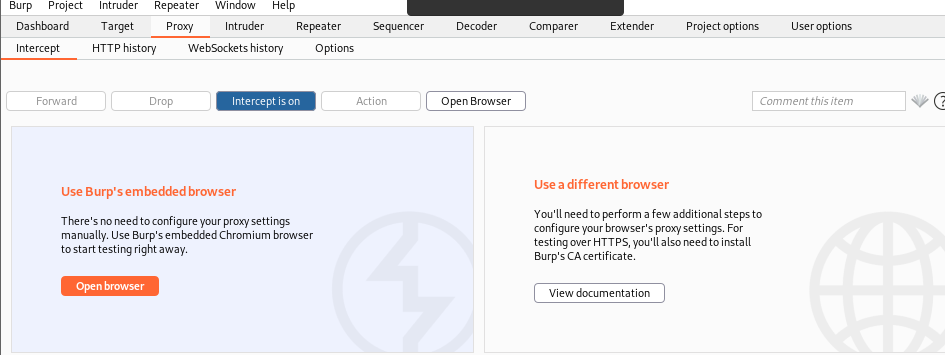
-Buraya port ekleme işlemi yapabileceğim gibi standart olarak bu port adresini de kullanabilirim.

-Öncelikle kullandığım tarayıcı üzerinden bir port ayarlama işlemi gerçekleştiriyorum.Ben Firefox üzerinden işlem yapacağım için sağ tarafta bulunan 3 Çizgiye basıyorum ardından Prefences>Network Settings ayarına geçiş yapıyorum.



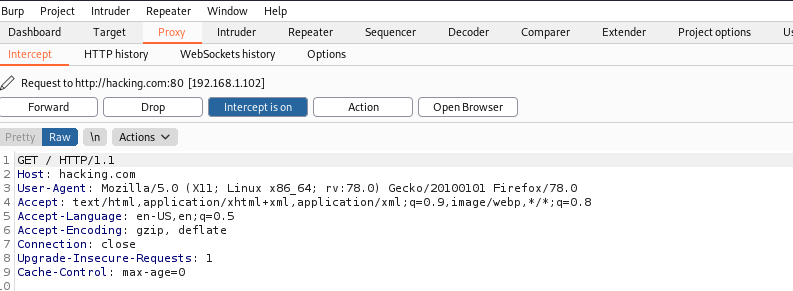
-Manual Proxy seçeneğini seçip buraya Burpsuite üzerinde belirlediğim IP ve Port değerlerini giriyorum.Ardından kaydedip çıkıyorum.

-Port ayarlamasından sonra Burpsuite aracına geçiş yapıyorum.Burada son olarak Proxy>Intercept ayarını On konumuna getiriyorum.

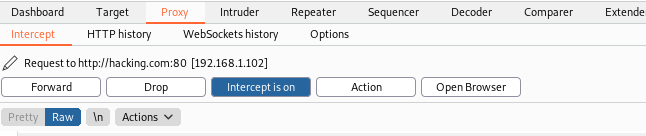


-Burpsuite ve tarayıcı üzerinde tüm gerekli işlemleri gerçekleştirdim.Artık tarayıcı üzerinde yapacağım işlemlerin bilgisi Burpsuite üzerine otomatik olarak çekilecektir.

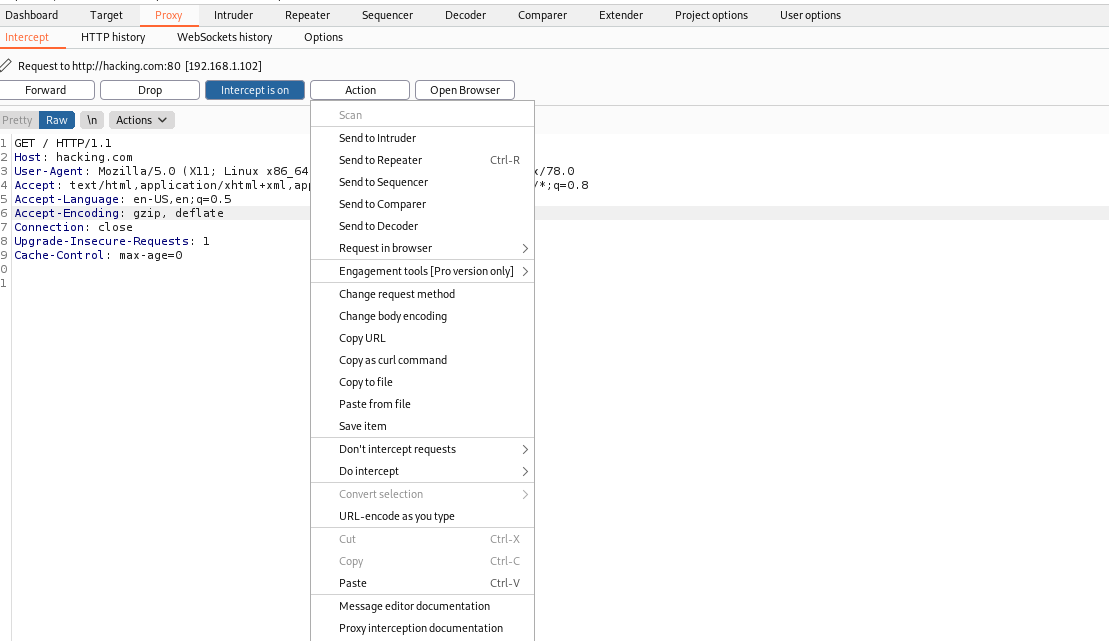
-Random olarak bir URL girip tarayıcı üzerinde çalıştırdım ve beni direk olarak BurpSuite üzerine gönderdi.Buradan yapılabilecek işlemleri birlikte bakacağız.



-Burpsuite üzerinde işlem yapılırken Tarayıcı üzerinde ki işlem kesintiye uğrar.

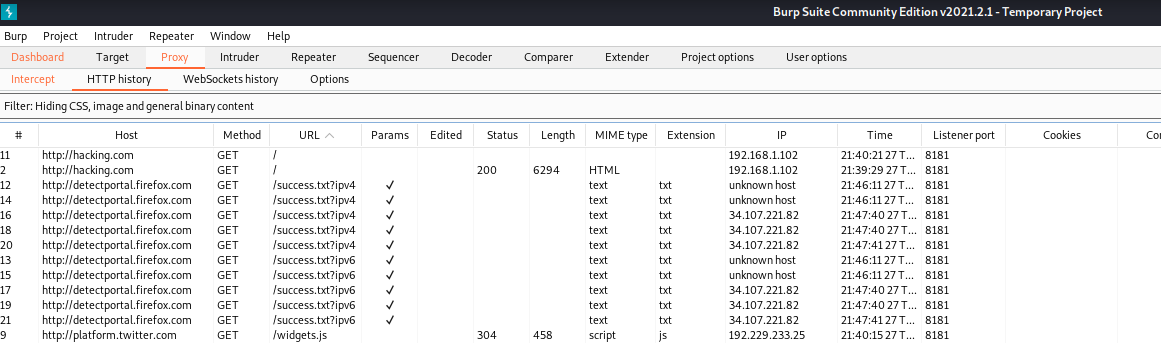


-Proxy>Intercept üzerinde bulunan “Forward” butonu ile bu işlemi tamamlayabiliriz ya da “Drop” butonu ile işlemin gerçekleşmesini engelleyebiliriz.



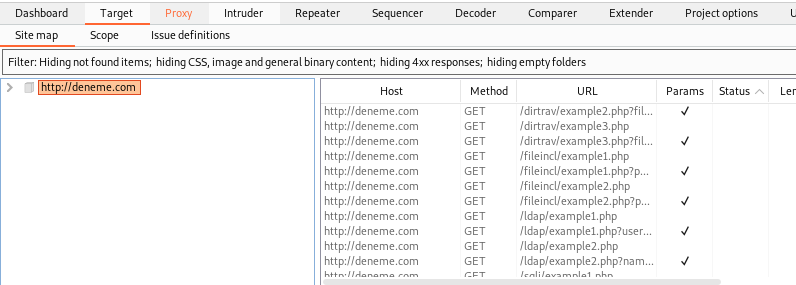
-Ayrıca “Action” butonu üzerinden diğer sekmelere bilgileri aktarma işlemini gerçekleştirebiliriz.

-Şimdi ise Proxy>HTTP History sekmesine geçiş yapıyoruz.



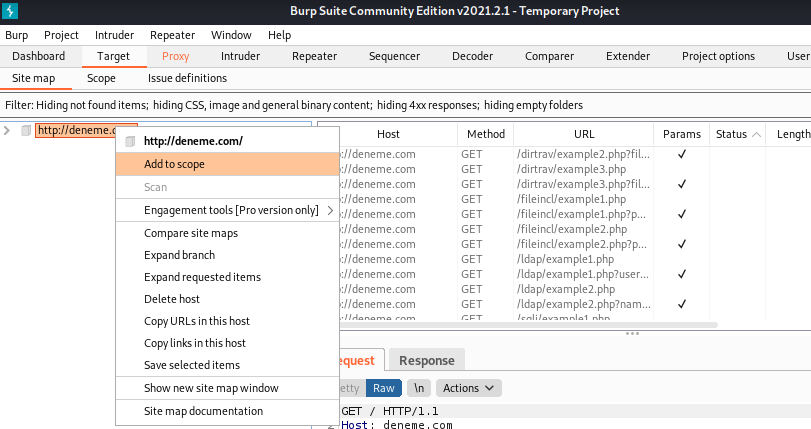
-Bu sekmede ise HTTP isteği gönderdiğimiz siteleri görüntüleyebiliriz.

-Target bölümüne geçiş yaptığımızda ise Site Map ile başlamak istiyorum.



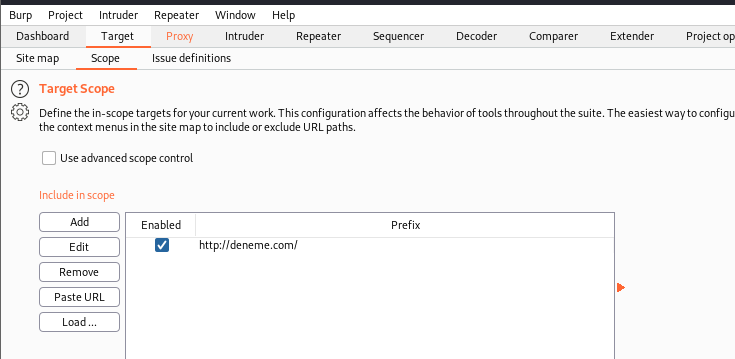
-Hedef sitenin site haritasını görmemi sağlıyor.

-Scope kısmına geçiş yaptığımızda öncelikle oraya bir URL atamamız gerektiği için Sitemap üzerinden scope üzerinde işlem yapacağımız URL’e sağ tıklayıp Add to Scope diyorum.



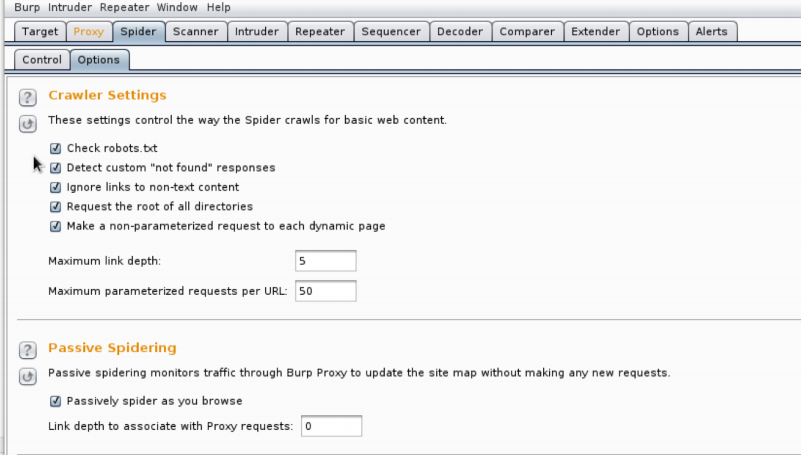
-Ekleme işleminden sonra Scope üzerine geçiş yaptığımda,Buraya target üzerinden eklemiş olduğum siteler görüntüleyebiliyorum.

.



**SPIDER**

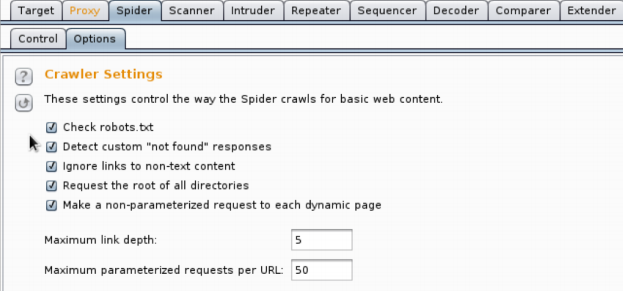
-Spider fonksiyonu Scope’a eklediğimiz siteleri dolaşarak sitedeki URL’leri listelemektedir.



-Spider sekmesine geçiş yaptığımızda bizi böyle bir ekran karşılamaktadır.

-Ayrıca “Option” sekmesi üzerinde özelleştirebilecek ayarlar görüntülenir.

-Option sekmesinde ki ayarlar ile başlıyoruz.Öncelikle Crawler sekmesinde;



-“Check robots.txt “ : Check robots.txt dosyasının kontrol edilip edilmeme durumunu belirler.

-“Detect custom “not found” responses” : 404 sayfası keşfinin aktifleşme durumunu belirler.

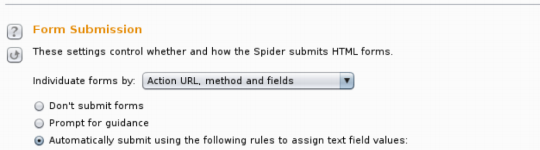
-“Request the root of all directories” Site içerisinde tüm dizinlerin indexlenmesi için seçilir.

-Passive Spidering sekmesi;



-“Passively spider as you browse” : Burp süite üzerinden geçen tüm istekleri ve yanıtları takip etmemizi belirler.

-Form submission sekmesi;

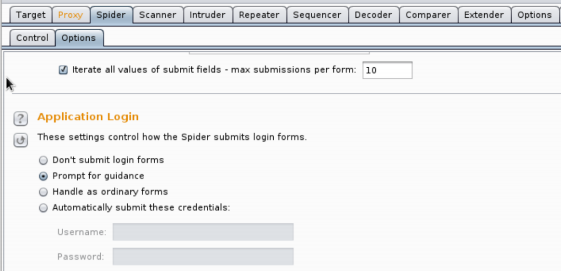


-“Indiviuate forms” : Burp süite yeni bir forla karşılaştığıda diğer sekmesine eklenmesi için kullanılır.

-“Prompt for guidance” : Burp süite her formla karşılaştığında formun nasıl submit edileceğini kullanıcıya sorar.

-“Autamatically submit” : Burp Suite her formla karşılaştığında formun otomatik submit eder.

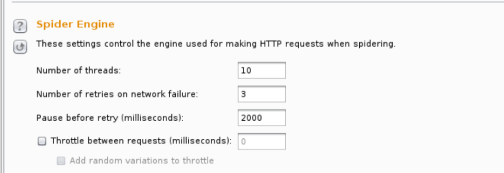
-Aplication Login sekmesi;



-“Handle as ordinary forms” : Burp Suite login formlarında nasıl konfigürasyon yapıldıysa ona göre aksiyon almasını sağlar.

-“Automatically submit these credentials” : Kullanıcı adı ve şifre bilgilerini otomatik olarak doldurup submit eder.

-Spider Engine sekmesi;



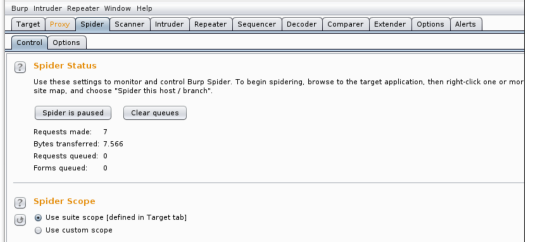
-Spider için ayarlamaların yapıldığı kısımdır.Threat sonrası deneme sayısı gibi ayarlar yapılabilir.

-Request Headers sekmesi;



-Yapılacak olan isteklerde Headers bilgilerinin belirlendiği kısımdır.

-Spider>Options üzerinde ki ayarlamalarımız bitti.Şimdi ise Spider>Control sekmesi ile devam ediyoruz.



-Spider>Options sekmesi üzerinde yapmış olduğumuz ayarlar doğrultusunda işlemi başlatabileceğimiz sekmedir.

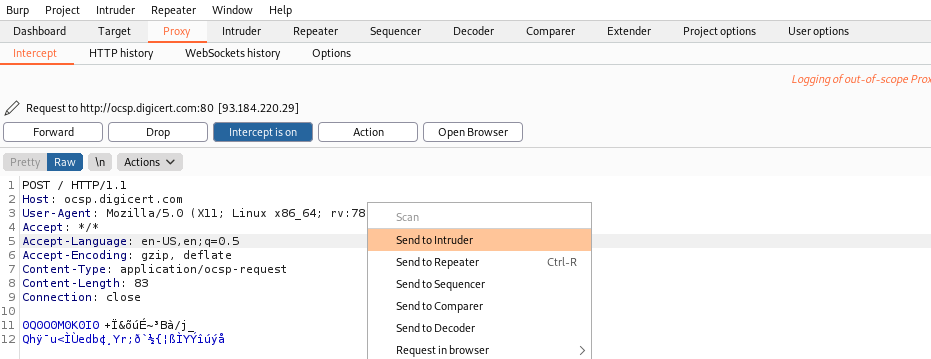
**INTRUDER**

-Burpsuite üzerinde zafiyetler için en çok kullanacağımız sekmedir.Zaafiyet taraması yapıp exploit edilmesi için kullanılır.

-Brute Force ile payload denemesi yapılabilir.

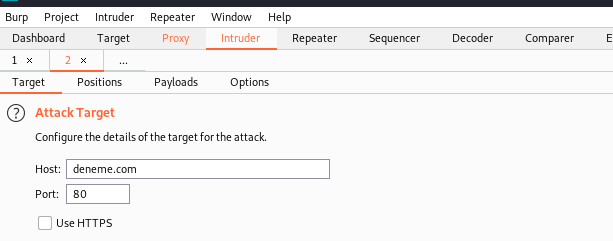
-SQLi,XSS vb. popüler zafiyetler bulunabilir.

-Intruder sekmesi üzerinden işlem yapabilmemiz için;bu sekmeye bir URL bilgisi gelmek zorundadır bu sebeple Proxy>Intercept bölümüne geçiş yapıyorum.



-İster burada sağ tıklayıp bu işlemi gerçekleştiriyorum istersem Action bölmesi üzerinden gönderme işlemini gerçekleştiriyorum.

Intruder>Target sekmesi;



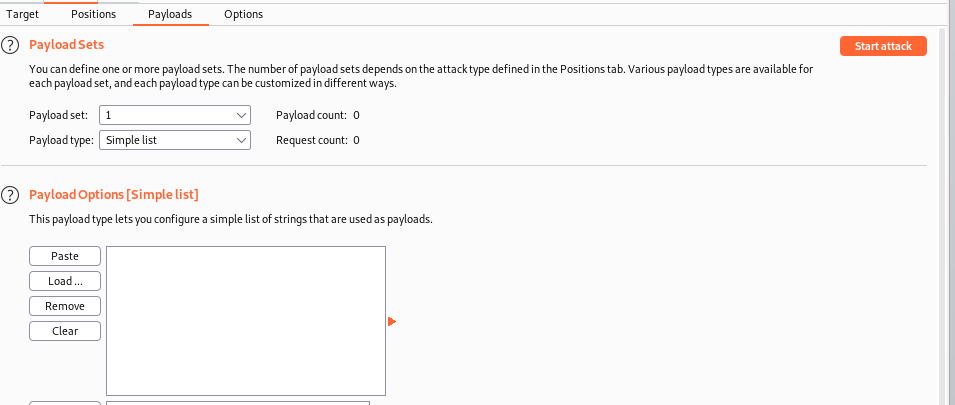
-Send to Intruder komutu ile gönderim yaptığımız URL’in site ve Port bilgisini verir.

Intruder>Positions sekmesi;



-Attack yapacağımız bölümü seçmemize olanak sağlar.Sağ tarafta ki sütunlar üzerindeki butonlar yardımıyla Ekleme,Silme,Otomatik belirleme gibi işlemleri gerçekleştirebiliriz.

Intruder>Payloads sekmesi;



-Bu sekme üzerinden eklediğimiz payloadlar ile Brute Force saldırı gerçekleştirebiliriz.Ayrıca Payload Type sekmesi üzerinden saldırı türü belirleyebiliriz.

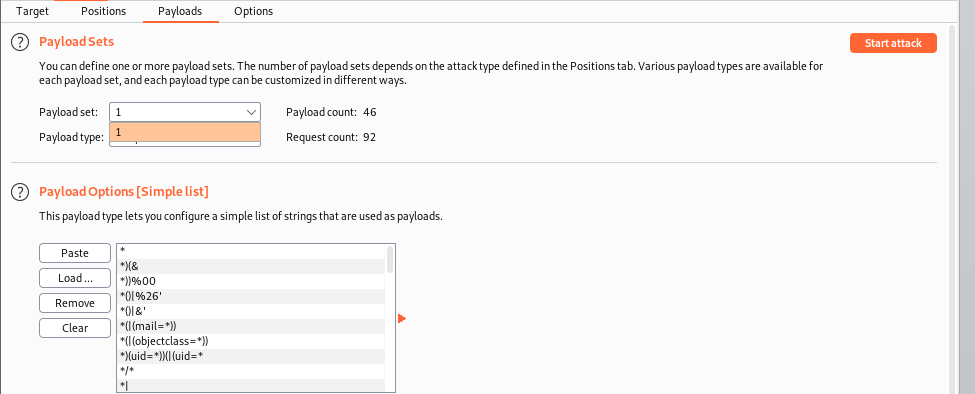
-Sniper : Tek bir parametreyi hedef alan saldırılarda kullanılır.

-Batterin Ram : Birden fazla parametreli saldırılarda kullanılır.Acnak tüm parametrelere aynı payloadı kullanır.

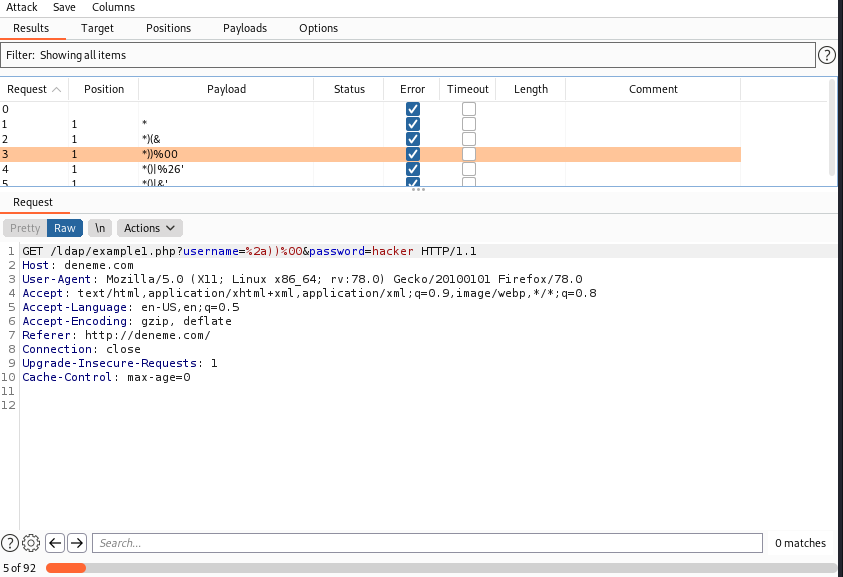
-Pitchfork : Tüm parametrelere farklı payload kullanarakdeneme yapar.Çoklu listeden parametre sırasına göre denemeler yapar.

-Cluster Bomb : Tüm parametrelere farklı payload kullanır.Listeden parametre sırasına göre çapraz denemeler yapılır.

-Örnek olarak bir kabakuvvet saldırı başlatmak istersek.Öncelikle payloadımızı kopyalıyoruz.Ardından “Paste” ile payloadı içerisine kopyalıyoruz.



-Positions sekmesi üzerinde belirlenen alanlar Payload-set bölümü üzerinden seçilebilir.Gerekli ayarlamalar yapıldıktan sonra “Start Attack” butonu ile işleme başlanır.



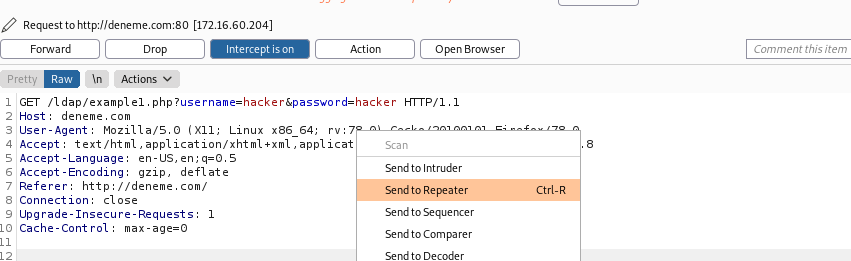
-Brute Force işlemini buradan takip edebiliriz.Ayrıca denenen payload üzerine bir kere bastığımızda onunla ilgili daha detaylı bilgiye erişim sağlayabiliriz.

-Payloadların başarılı olup olmama durumunu genellikle “Length” üzerinden takip edebiliriz.Bu durum Injection’lar arasında değişiklik göstermektedir.

**REPEATER**

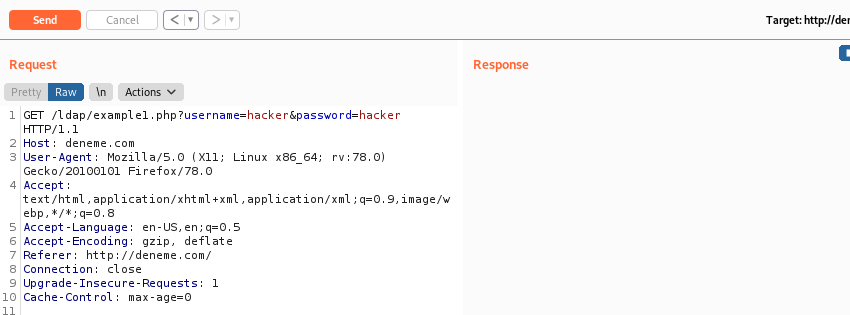
-Manuel olarak yapılan isteklerde değişiklik yapmamıza olanak sağlar.

- Repeater sekmesi üzerinden işlem yapabilmemiz için;bu sekmeye bir URL bilgisi gelmek zorundadır bu sebeple Proxy>Intercept bölümüne geçiş yapıyorum.



-İster burada sağ tıklayıp bu işlemi gerçekleştiriyorum istersem Action bölmesi üzerinden gönderme işlemini gerçekleştiriyorum.

-Repeater sekmesine geçip yaptığımda burada bağlantı sağladığım URL üzerinde arka planda ki işlemleri incelememe olanak sağlar.Örnek olarak “DOOM XSS” zafiyetini verebilirim.Burada site üzerinde işlem gerçekleştikten hemen sonra URL işlem sayfasına geri dönmektedir.Bunu sadece kaynak kodu üzerinden görüntüleyebilirim.Repeater ise bu sekme üzerinde işlem yapabilmeme olanak sağlar.



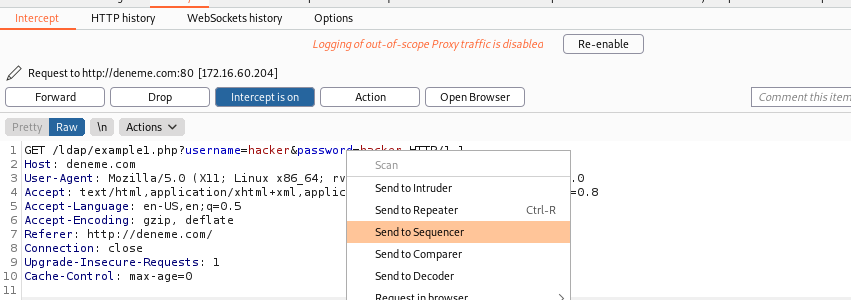
-Gelen istekleri “Send” butonu ile Response bölümüne aktarıp orada kaynak kodunu daha detaylı şekilde kontrol edebilme olanağı sağlar.

-Ayrıca site yönlendirmesini buradan yönetmemi ve zafiyetlerden yararlanabilmemi sağlar.

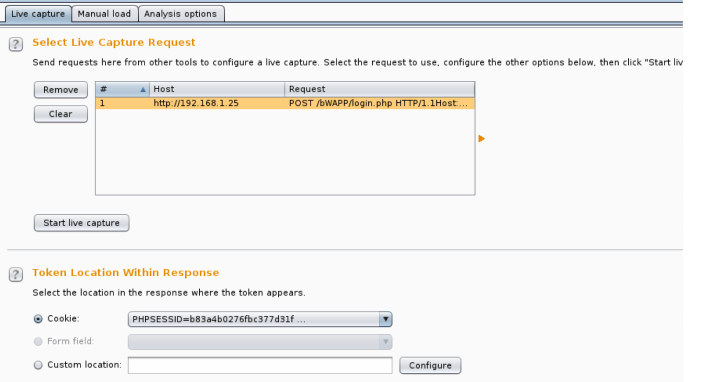
**SEQUENCER**

-Web uygulaması tarafından kullanıcıya oturum açıldıktan sonra üretilen ve kullanıcıların her yaptığı istekte web uygulamasına kendini tanıtmak amacıyla yolladığı bu keye Session key adı verilir.Sequencer’ın ypmaya çalıştığı bu keylerin tahmin edilebilirliğini kontrol etmektir.

-Sequencer sekmesi üzerinden işlem yapabilmemiz için;bu sekmeye bir URL bilgisi gelmek zorundadır bu sebeple Proxy>Intercept bölümüne geçiş yapıyorum.

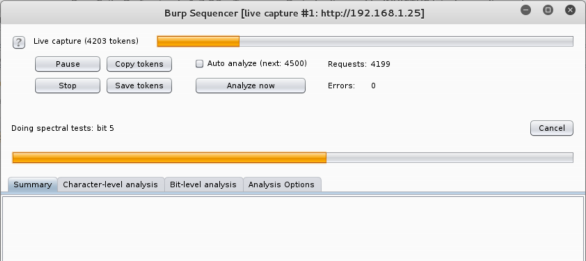


-İster burada sağ tıklayıp bu işlemi gerçekleştiriyorum istersem Action bölmesi üzerinden gönderme işlemini gerçekleştiriyorum.



-Sequencer’a yollanan isteği Token Location Within Response bölümünde PHPSESSID tutulduğunu görüntülüyoruz.

-PHPSESSID’ı seçip Start Live Capture a tıklayarak BurpSuite’in uyulamaya istekler yaparak PHPSESSID toplamasını sağlıyoruz.

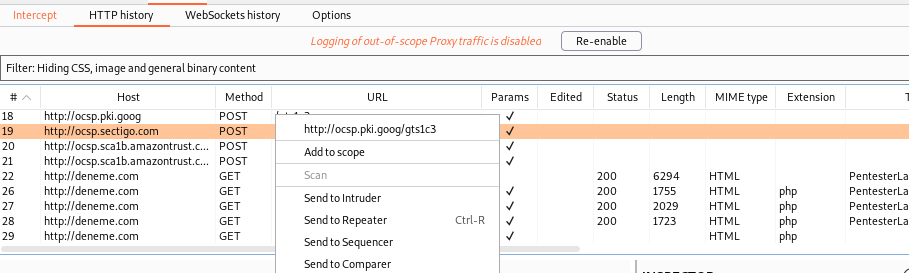


-Toplanan PHPSESSID’lerin sayısı ne kadar artarsa yapılacak olan analizin doğruluk oranının arttığı unutmamalıdır.

**COMPARER**

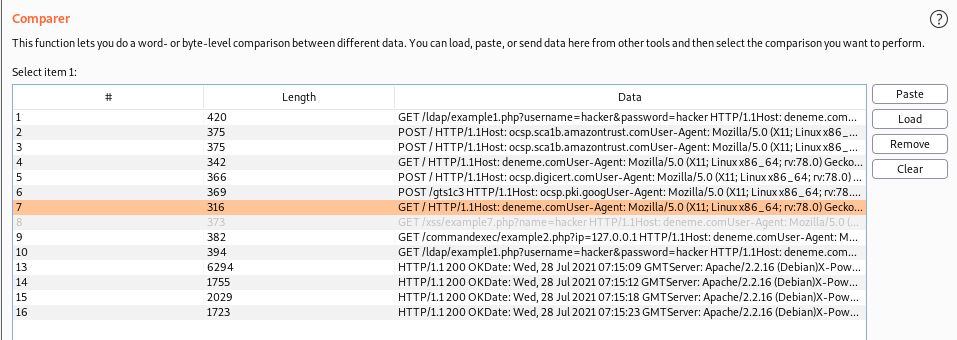
-İki istek ya da iki yanıt arasında ki farkı anlamamıza yardımcı olur.

-Comparer sekmesi üzerinden işlem yapabilmemiz için;bu sekmeye bir URL bilgisi gelmek zorundadır bu sebeple Proxy>HTTP history bölümüne geçiş yapıyorum.

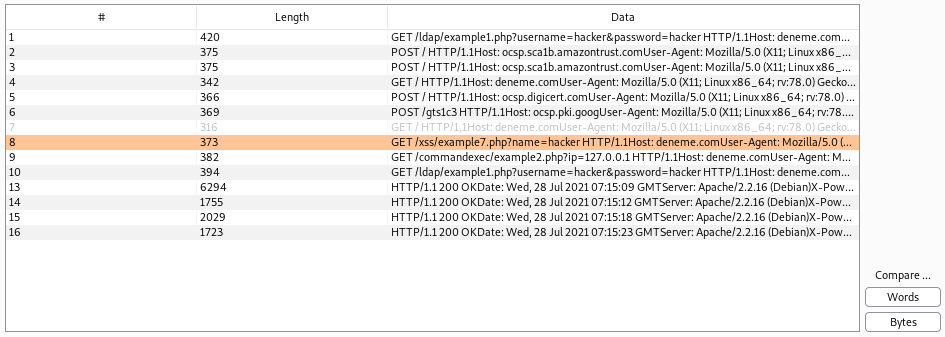


-Comparer sekmesine göndereceğim URL’e sağ tıklayıp “Send to Comparer” butonu ile Comparer üzerine gönderim yapıyorum.

-Comparer sekmesi üzerinden karşılaştırma yapacağım URL’i işaretliyorum ve Response bölümüne gönderim yapıyorum.

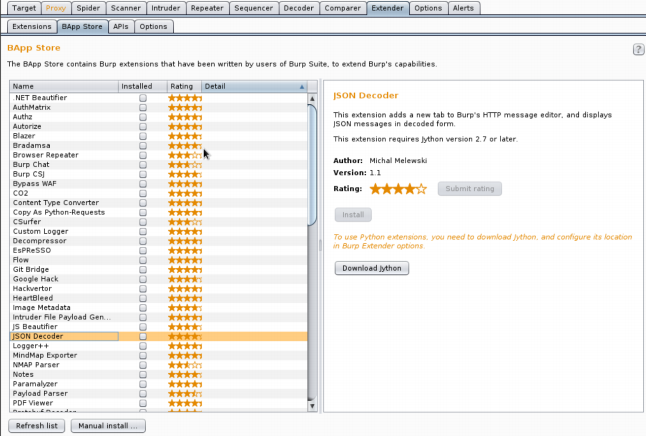
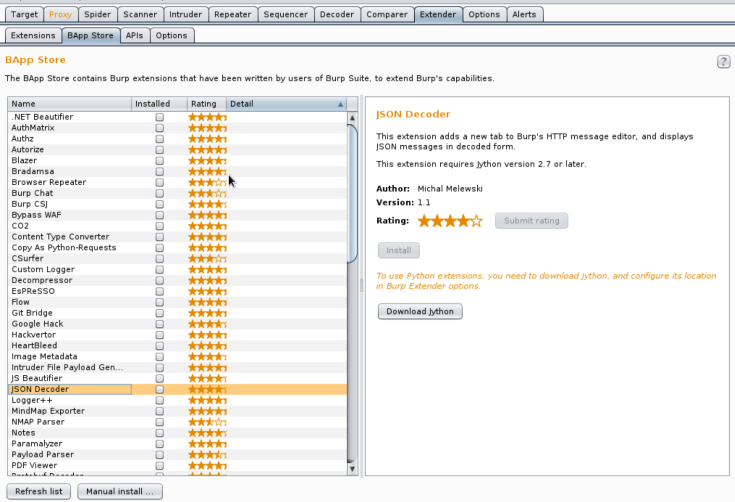


-Comparer>Response böümüne geçiş yapıyorum.



-Karşılaştırılmasını istediğimiz 2 isteği seçerek sağ alttan Words veya Bytes türünden karşılaştırılır.

-Ayrıca Extender sekmesi üzerinden,BurpSuite’e çeşitli eklentiler kurarak yapabileceklerini genişletebiliriz.



-Extender>BAppStore üzerinden istediğimiz eklentiyi seçip install butonu ile kurulumu gerçeleştirebiliriz.