T.C.
Kayseri Üniversitesi
Siber Guvenlik Uygulama ve Arastirma Merkezi Müdürlüğü

ARAŞTIRMA FAALİYETİ SONUÇ RAPORU

Arastirma Faaliyetinin Amacı	:	Web Uygulaması Sömürü Araçlarını Kullanma
Birim	:	Siber Güvenlik Uygulama ve Araştırma Merkezi
Arastırmadan Sorumlusu Öğretim Elemanı	:	Doç.Dr. Ali GEZER
Arastırma Faaliyetinde Kullanılan Araçlar	:	Burpsuite
Arastırma Faaliyeti Tarih Aralığı	:	1.4.2023-1.5.2023
Arastırmaya Katılan Kişi Sayısı	:	4 (Doç.Dr. Ali GEZER, Ali Altun, Ali Akdeniz, Mehmet Gülce)
İlgili Araştırmacı Adı ve İletişim Bilgisi	:	aliakdeniz1881@gmail.com

Genel Bilgilendirme ve Değerlendirme

Burp Suite Nedir ?

Burp Suite; web uygulama güvenliğini test etmek için kullanılan bir platformdur. PortSwigger şirketi tarafından geliştirilmiş ve Java programlama diliyle yazılmıştır. Grafik arayüzü olduğu gibi terminal aracılığı ile de platforma erişim sağlanabilir.

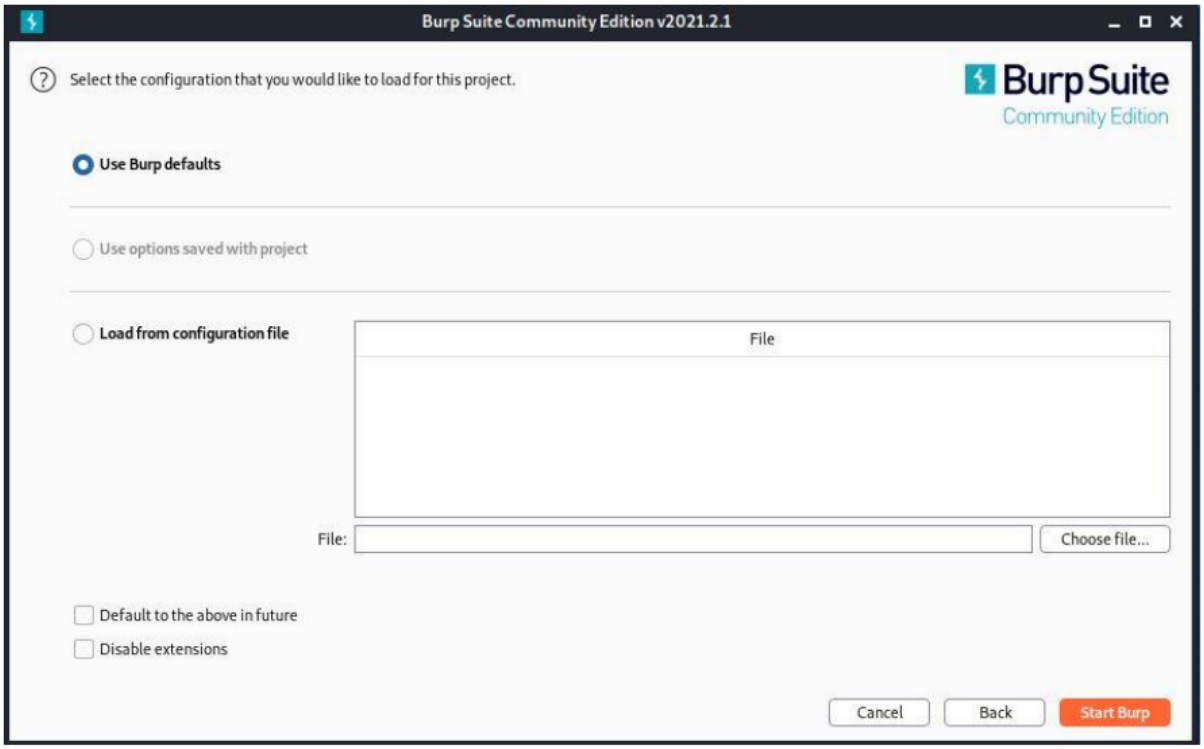
PortSwigger, Burp Suite kullanıcılarına 3 farklı sürüm sunar. Bunlar: Burp Suite Community, Burp Suite Professional ve Burp Suite Enterprise'dır. Comminity sürümü olup, Professional ve Enterprise sürümlerine göre daha sınırlı özelliğe sahiptir.

Burp Suite, Kali Linux dağıtımı üzerine kurulu olarak gelmektedir. Farklı sistem üzerine kurulum için: https://portswigger.net/burp/releases/professional-community-2021-62?requestededition=community bağlantısın üzerinden erişim sağlanıp, uygun sürüm ve işletim sistemi seçilerek indirilir.

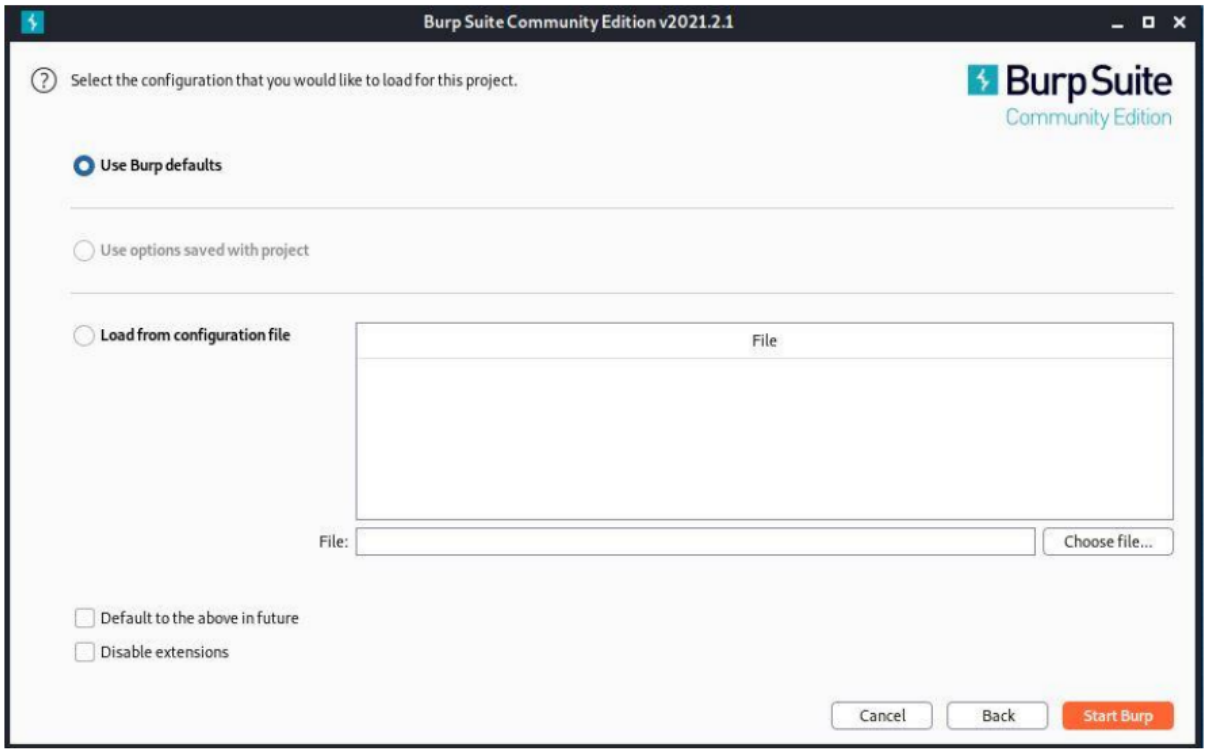
Burp Suite'in birçok faklı araç mevcuttur. Bunlar: Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender

Burp Suite Arayüzü

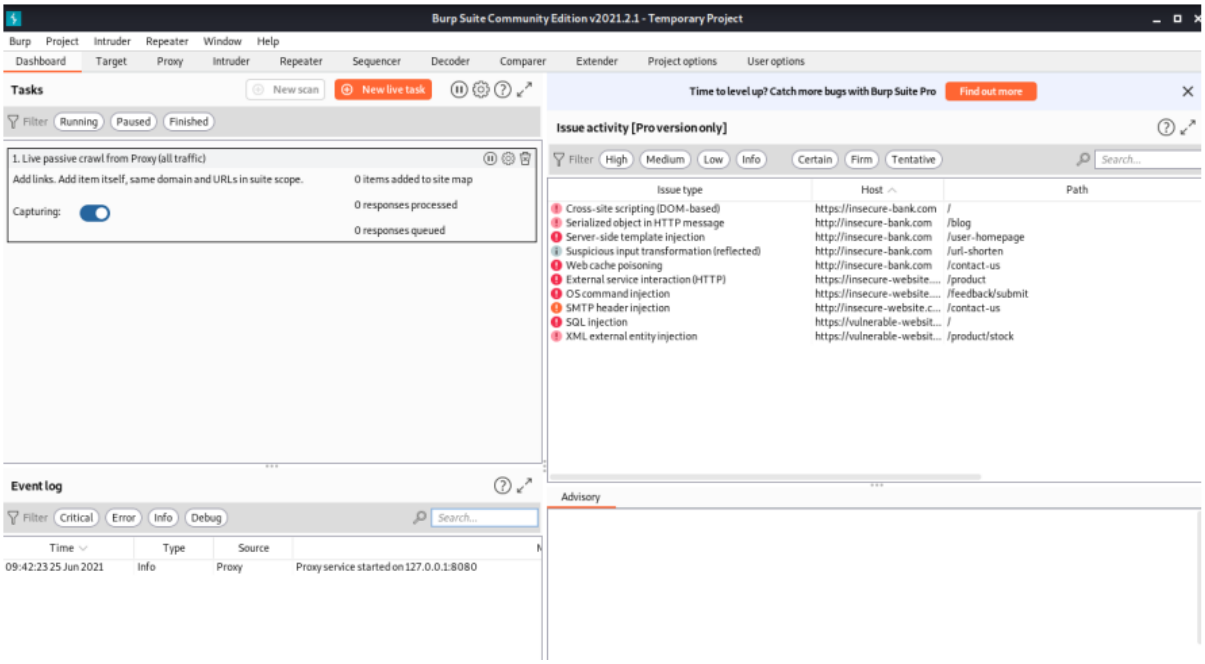
Uygulamalar bölümünden ya da terminal ekranından Burp Suite platformuna giriş yaptıktan sonra karşımıza “Proje Oluşturma” ekranı gelmektedir. “Temporary project” seçeneği ile geçici bir proje oluşturulur. “New project on disk” seçeneği ile yapılan proje disk üzerine kaydedilir. “Open existing project” seçeneği ile mevcut bir proje üzerinde uygulama yapılır. Community sürümünde sadece “Temporary project” seçeneği mevcuttur. “Next” seçeneğine tıklanır.



"Konfigürasyon" ekranında "Use Burp defaults" seçeneği seçilerek Burp Suite varsayılan yapılandırma dosyaları kullanılabilir ya da "Load from configuration file" seçeneği ile mevcut yapılandırma dosyası üzerinden yükleme işlemi yapılır. "Next" seçeneğine tıklanır.



Burp Suite ana ekranı aşağıdaki gibidir. Önceki bölümde verilmiş olan modüller görüntülenmektedir.



En sık kullanılan “Proxy”, “Intruder” ve “Repeater” sekmeleridir. Makalede bu alanlar detaylı bir şekilde ele alınmıştır.

Burp Suite- Target

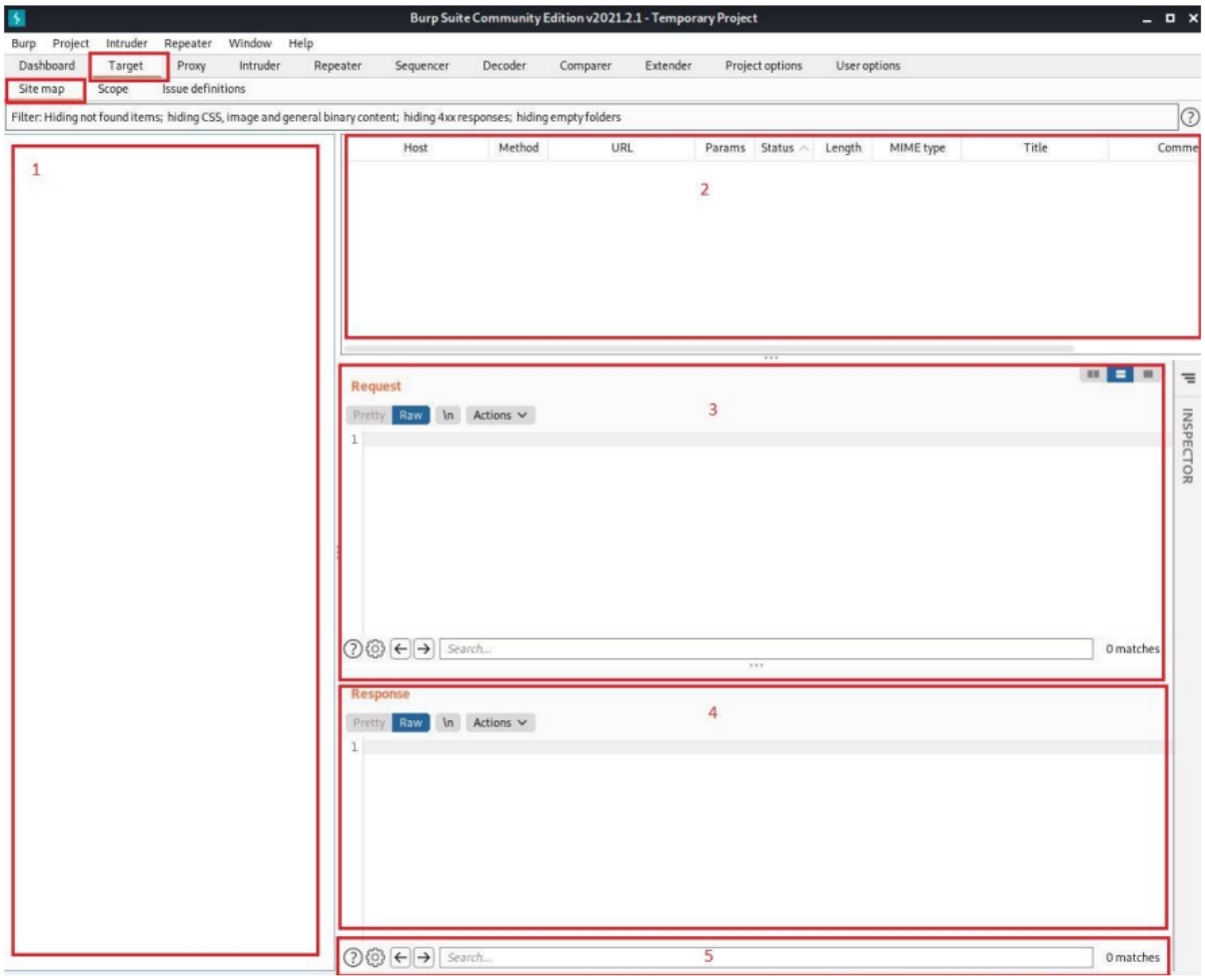
“Site map”, hedef ile ilgili sunucudan dönen cevapları bu sekmede görüntülenir.

1. Hedef site üzerindeki bağlantıları, dosya adlarını görüntüleme alanı.

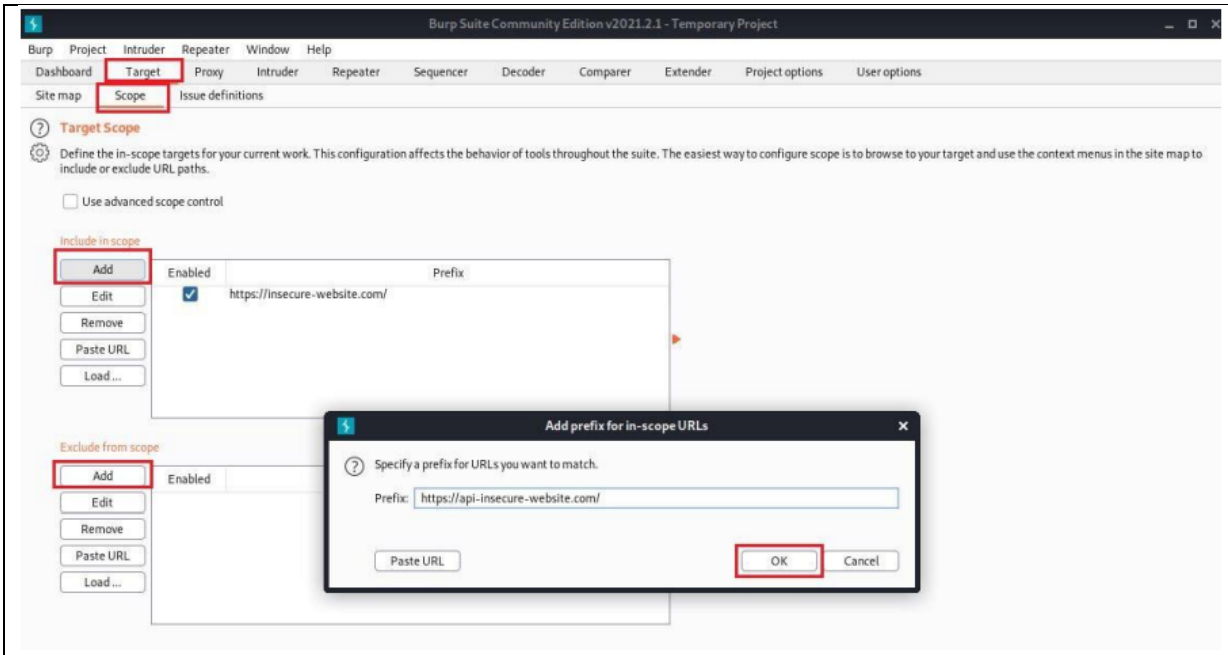
2. Gönderilen istek ile ilgili var olan bütün parametreler bu alanda görüntülenir. 3. Request, istemciler çıkan istekler bu alanda görüntülenir.

4. Responce, sunucudan dönen cevaplar bu alanda görüntülenir.

5. Request ve responce arasında arama yapılan alan. 6. Filtreleme işlemlerinin yapıldığı alan. Diğer alanlar için filtreler de mevcuttur.



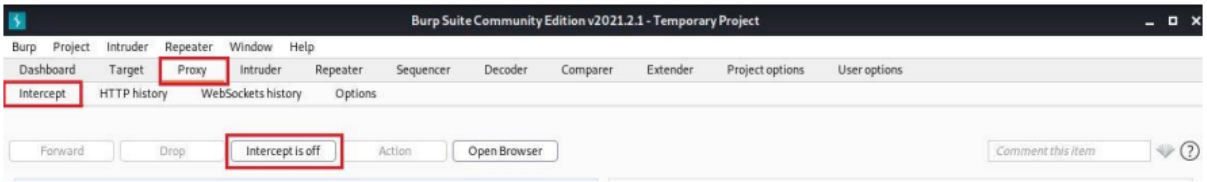
“Scope “, Hedef kapsam yapılandırması bu sekmede yapılır. Asıl incelenmek istenen hedef bağlantısı bu alana girilir.



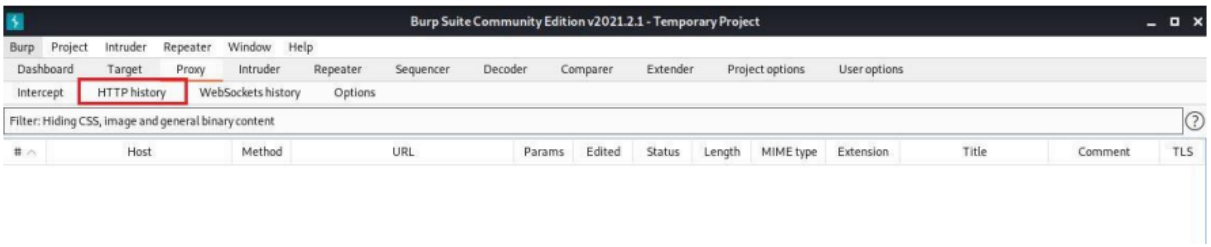
Burp Suite- Proxy

Proxy sekmesi Burp Suite'i Proxy olarak kullanmamıza olanak tanır.

"Intercept" alanında gelen ve giden istek yapısı kontrol edilir. "İntercept is on" durumunda olduğu zaman istemciden çıkan isteği görüntülemek için kullanılır. "İntercept is off" durumunda olduğu zaman Burp Suite aracı Proxy olarak kullanılamaz.

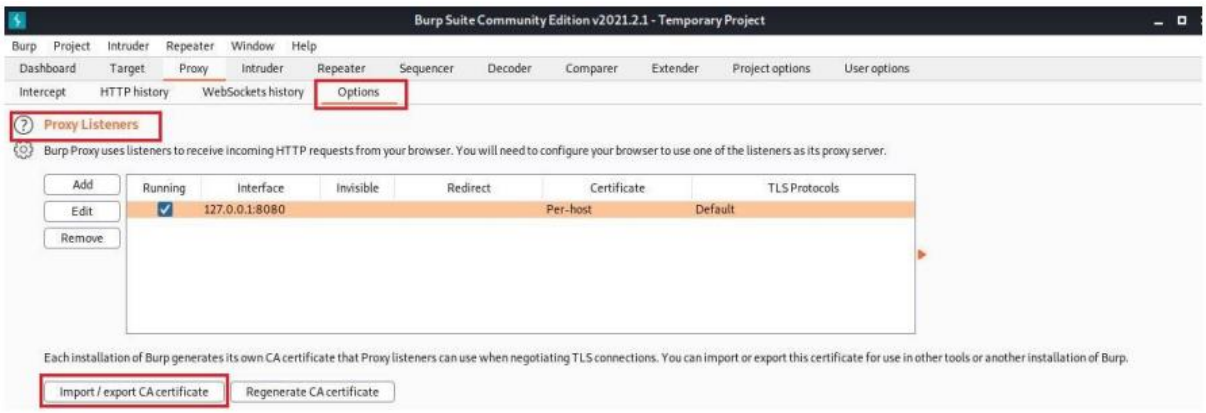


"Http history" alanında hedef üzerinde yapılan tüm işlemlere ait bağlantı bilgileri görüntülenir.

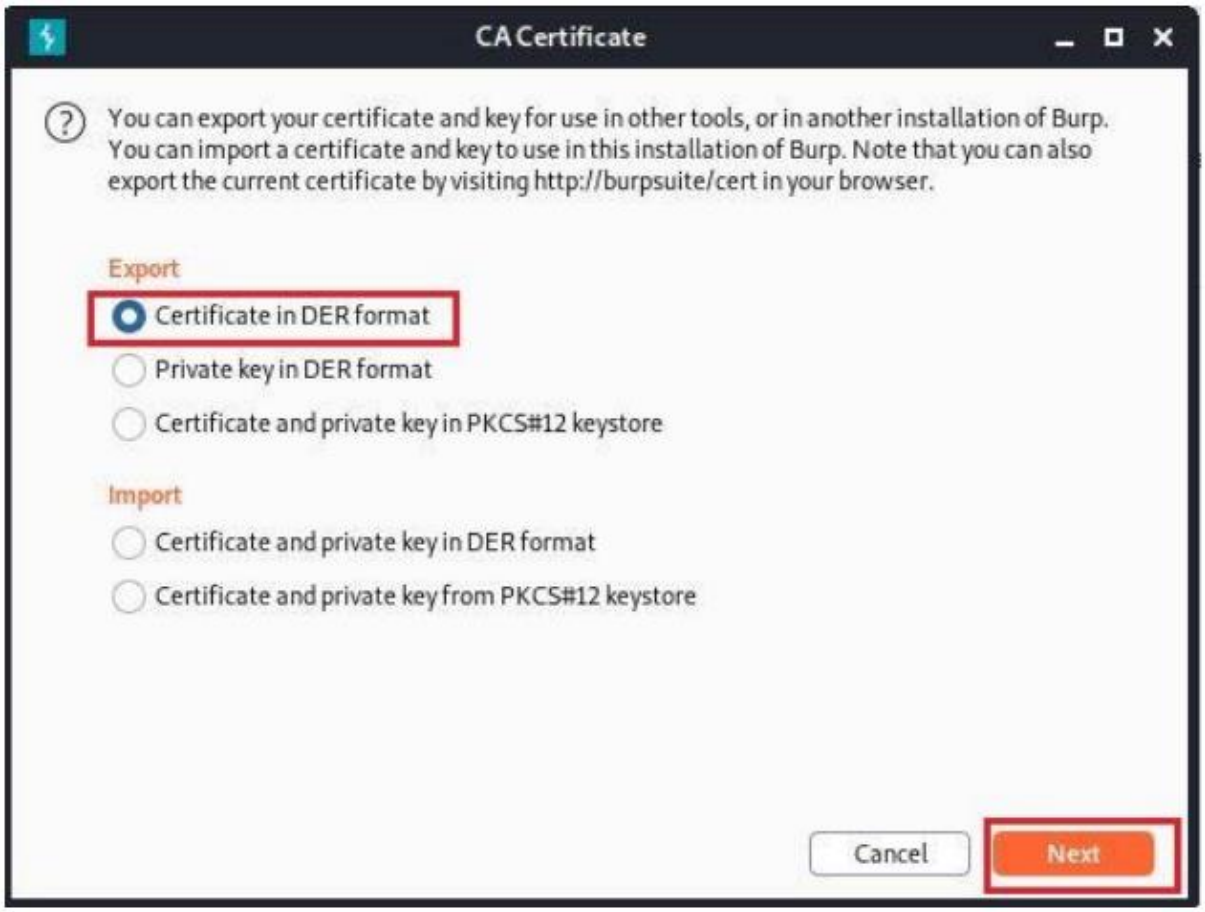


"Options", istemci ile sunucu arasındaki bütün ayarlamaların yapıldığı alan. "Proxy Listeners" alanında dinlenecek olan localhost adresi ve 8080 portu varsayılan olarak

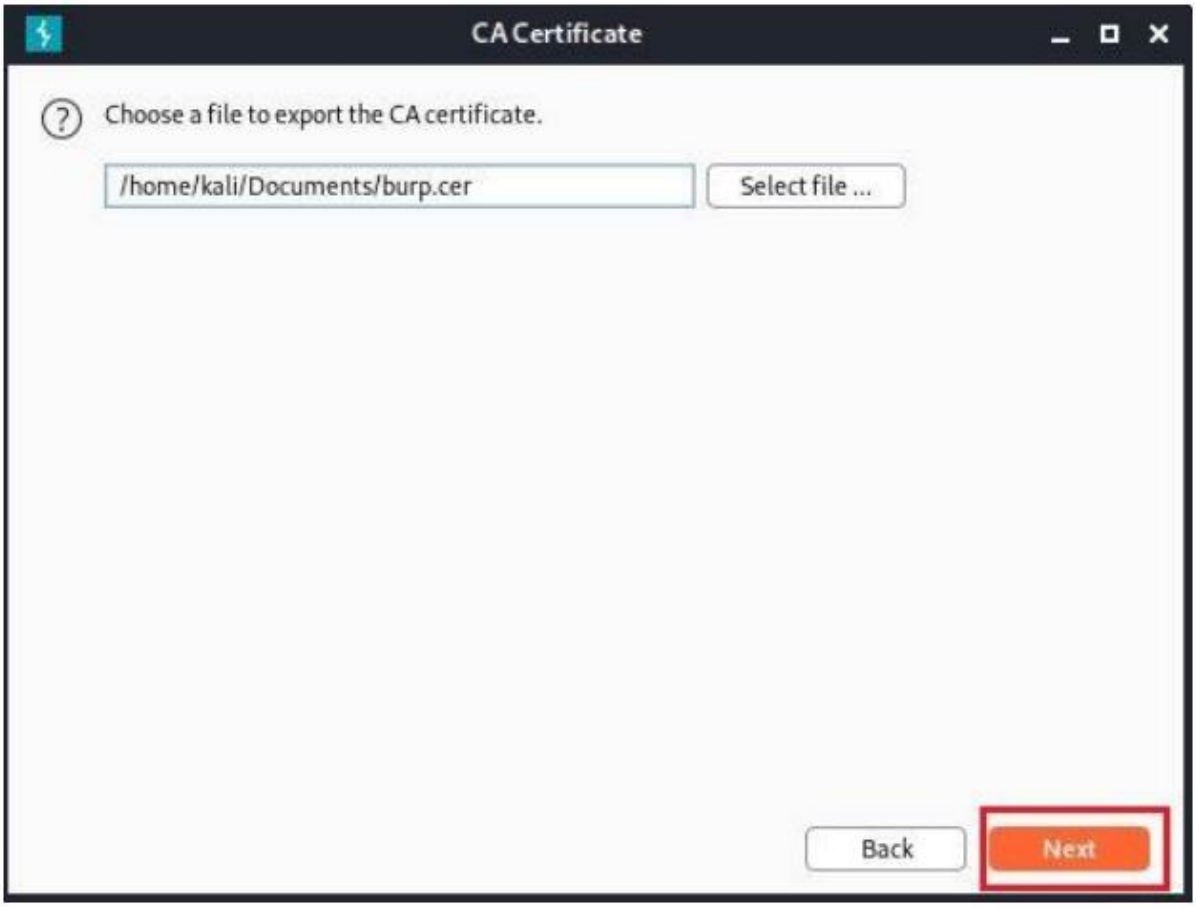
gelmektedir. Burp Suit ile Https sitelerini görüntülemek istenildiğinde sertifika hatası oluşur. Bu durumu ortadan kaldırmak için "Import/export CA certificate" seçeneğine tıklanarak yapılandırma işlemi yapılması gerekmektedir.



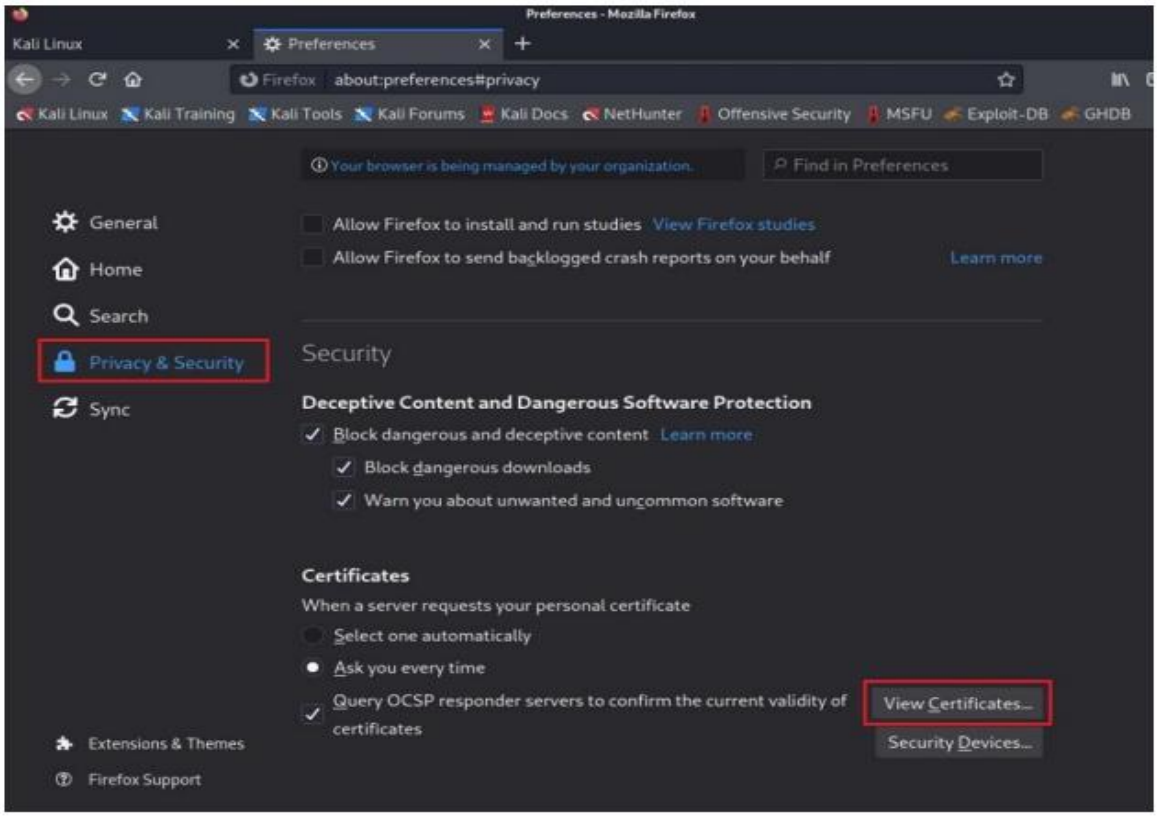
Açılan pencerede "Certificate in DER format" seçeneği seçilerek "Next" seçeneğine tıklanır.



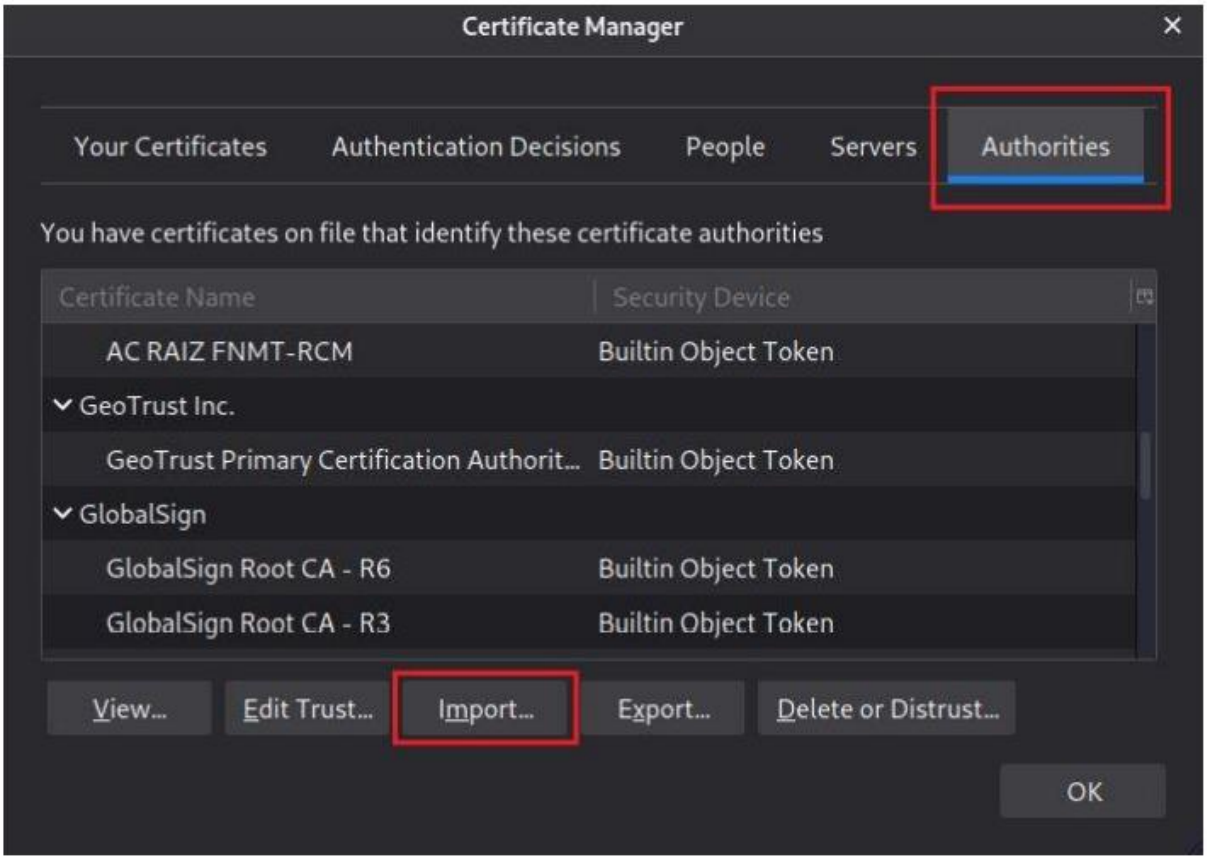
Kaydetmek istediğimiz dizini belirterek “burp.cer” şeklinde kaydediyoruz. “Next” seçeneğine ve ardından “Close” seçeneğine tıklayarak çıkılır.



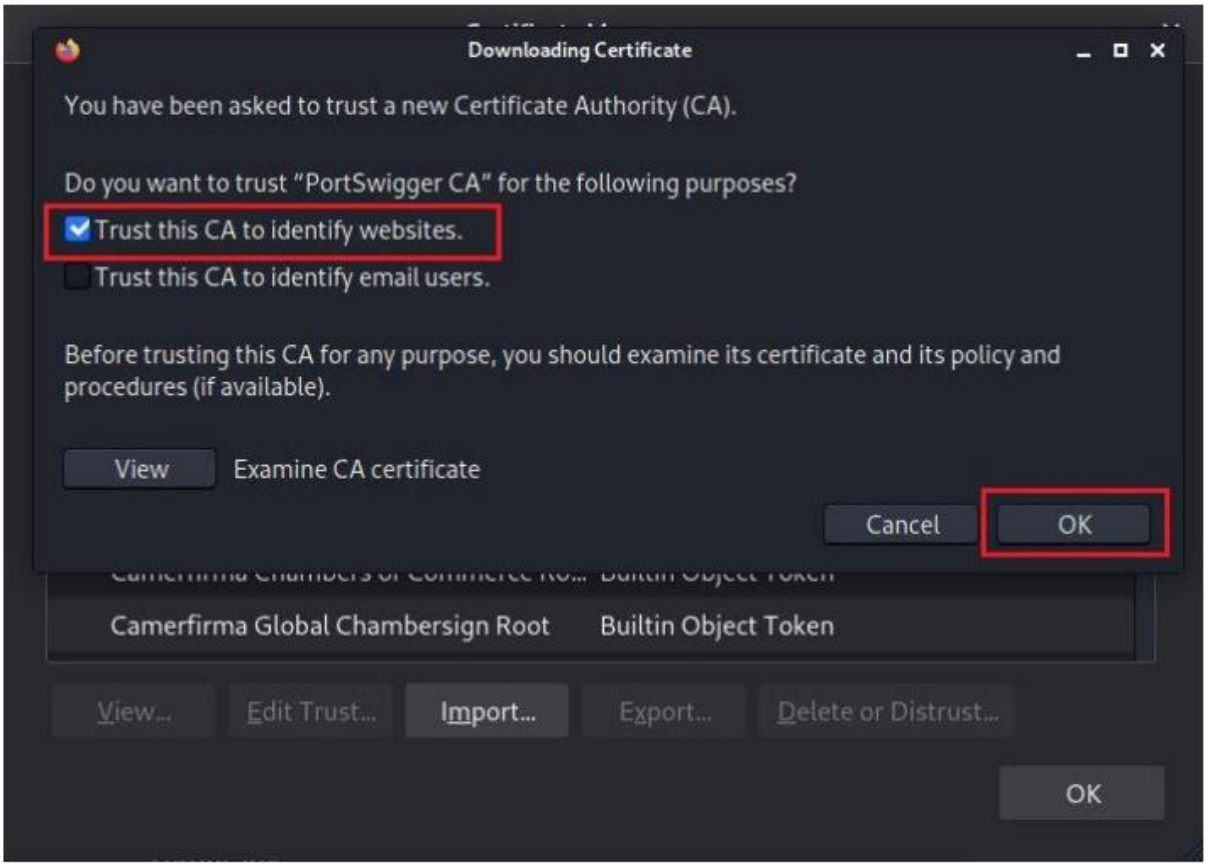
Burp Suite tarafında yapılan işlemleri tarayıcıya tanıtılması gereklidir. Bu makalede Firefox tarayıcısı kullanılmaktadır. Firefox ayarlara girilerek “Privacy & Security (Gizlilik ve Güvenlik)” sekmesine ardından “View Certificates (Sertifikaları Görüntüle)” seçeneğine tıklıyoruz.


Preferences - Mozilla Firefox
Kali Linux
Preferences
Firefox
about:preferences#privacy
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
Allow Firefox to install and run studies
View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf
Learn more
Security
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content
Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
When a server requests your personal certificate
Select one automatically
Ask you every time
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
Extensions & Themes
Firefox Support

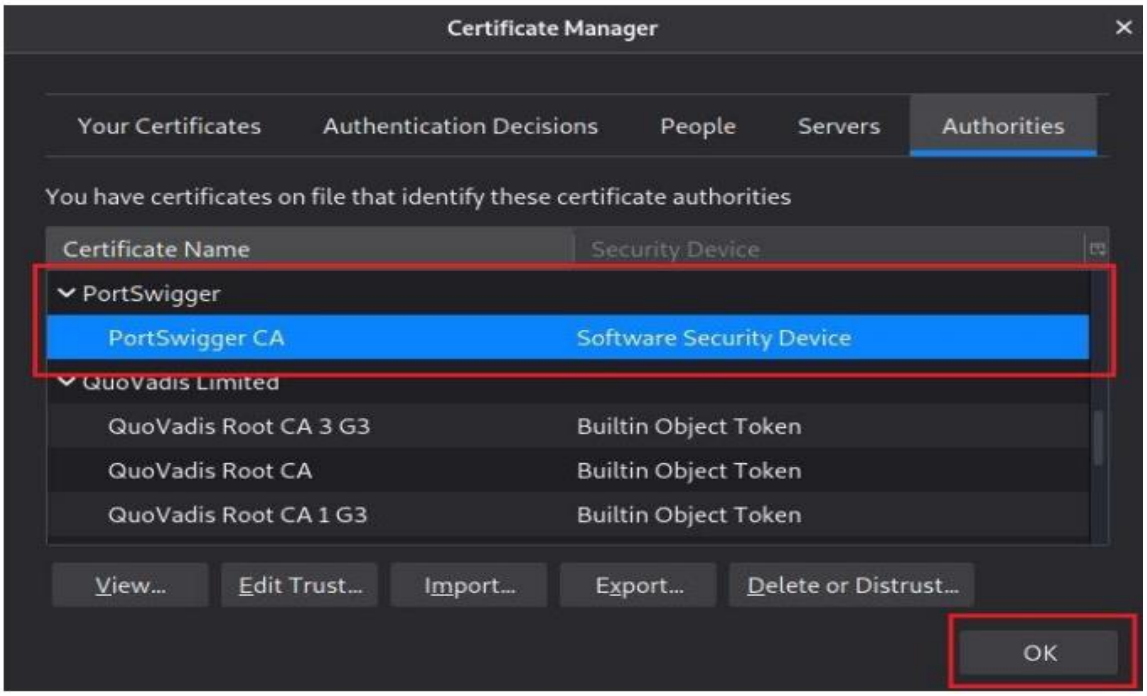
Açılan pencerede “Authorities (Yetkililer) → Import” seçeneğine girilir. Kayıt edilen dizinde sertifika seçilir.



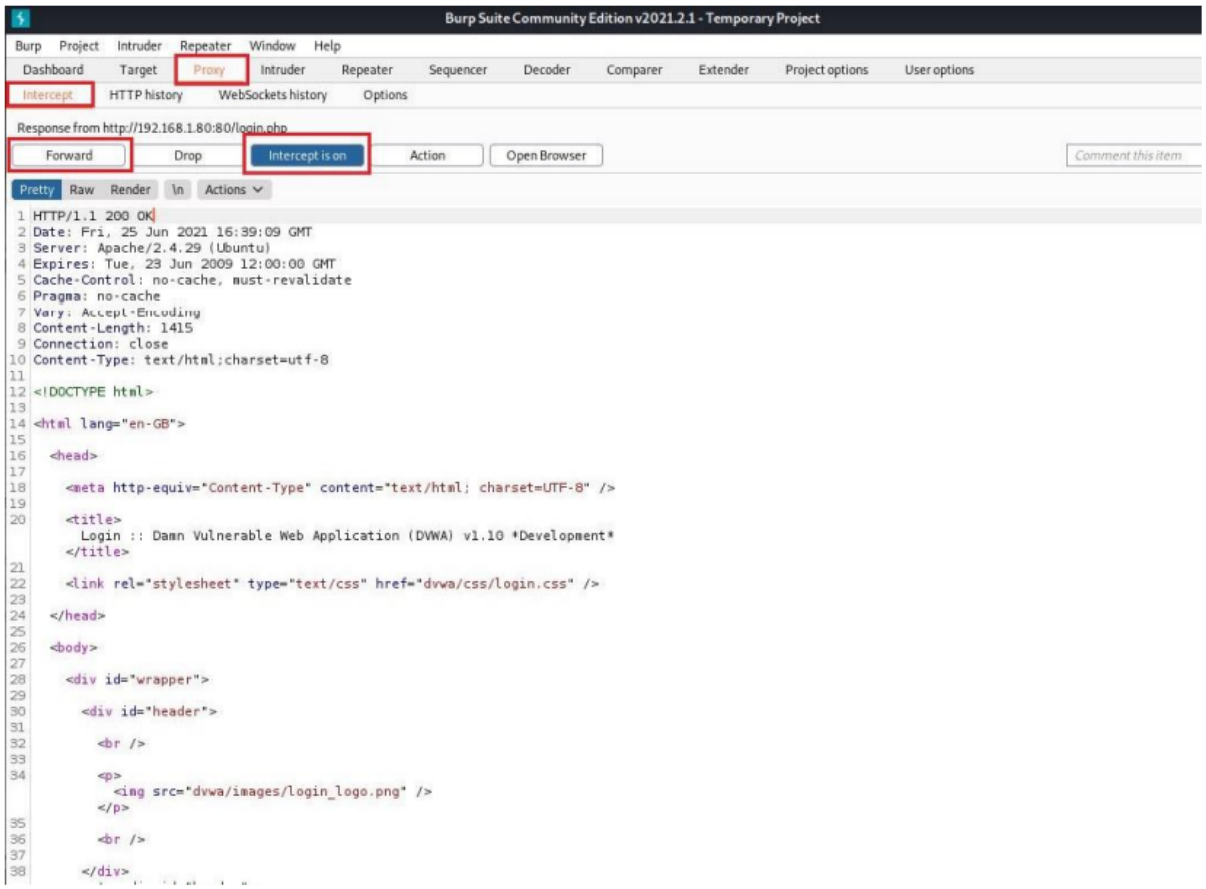
"Trust this CA to identify websites. (Web sitelerini tanımlamak için bu CA'ya güvenin.)" seçeneğine tıklanır.



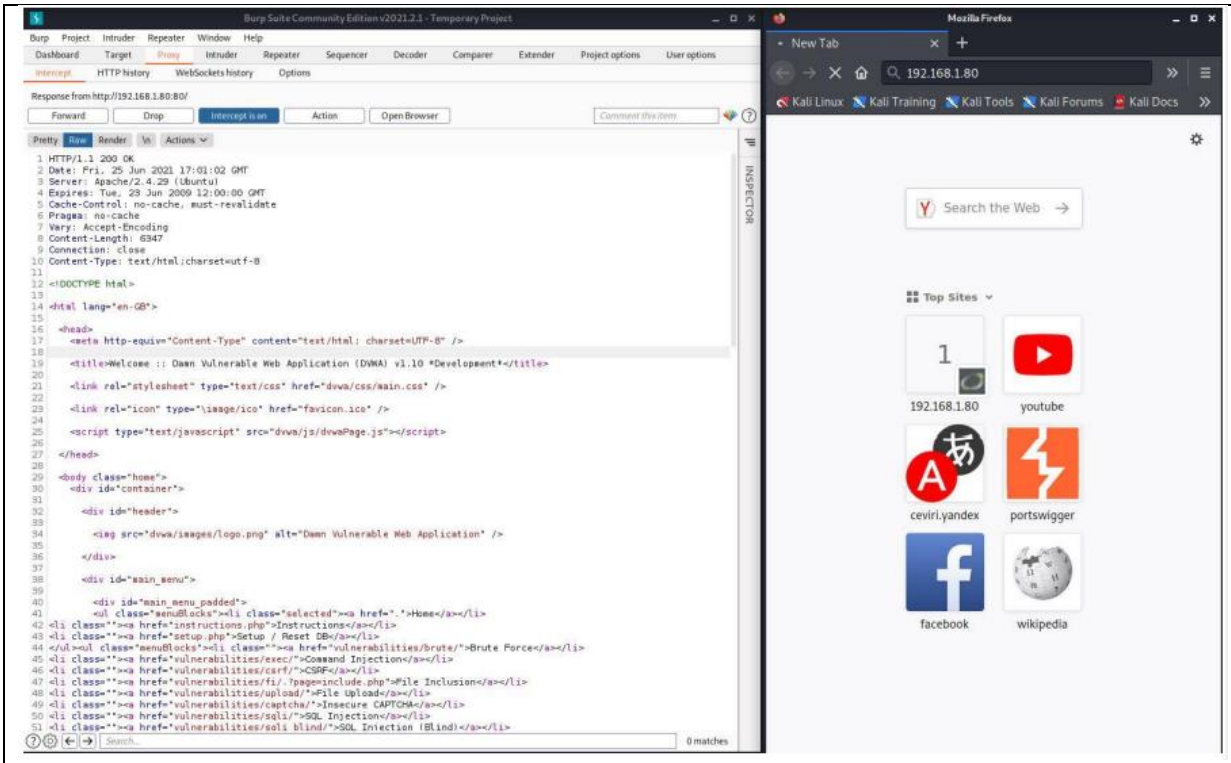
Sertifika tanımlama işlemi tamamlandıktan sonra Burp Suite şirketi sahibi ekranda çıkmaktadır. "PortSwigger Ca → OK" seçenekleri seçilerek sertifika tanımlama işlemi tamamlanmış olur.



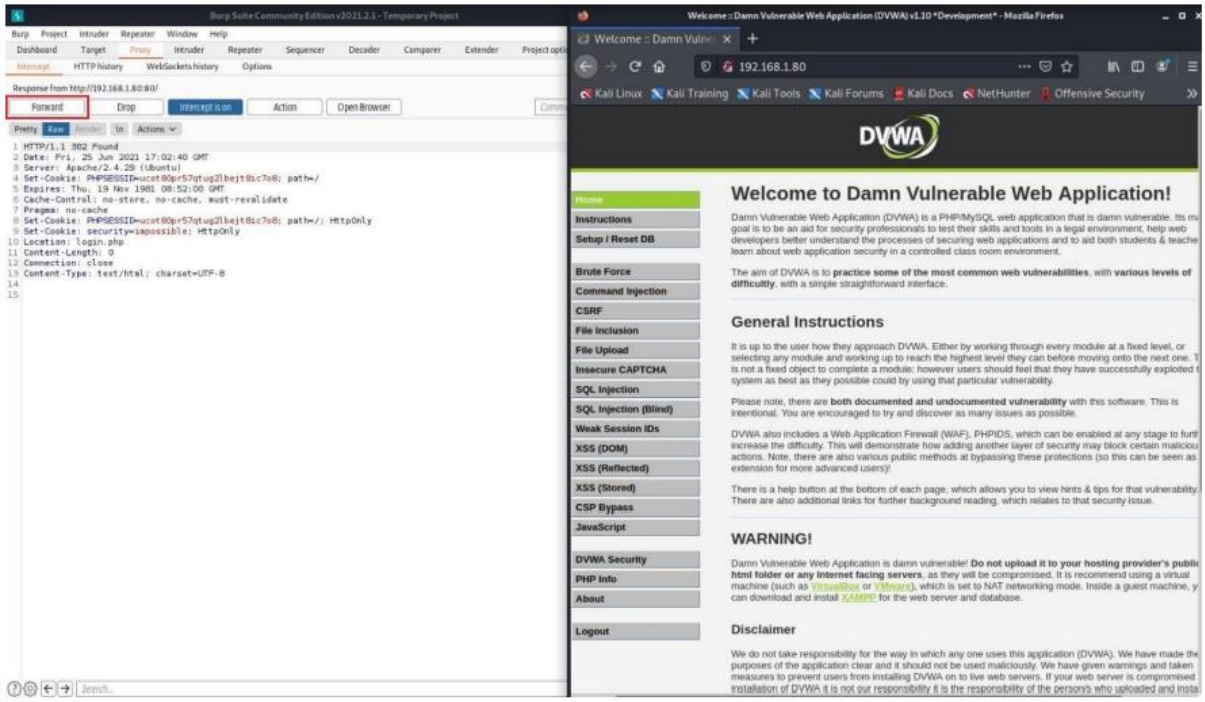
Tarayıcı Proxy ayarı yapıldıktan sonra bütün trafik Proxy üzerinden geçmektedir. Tarayıcıyı üzerinden istekte bulunulduğu zaman “Intercept” alanında istek görüntülenmektedir. Bu alanda isteğe müdahale edilebilir. “Forward” seçeneğine tıklayarak bir sonraki isteğe geçilir. “Drop” ile istek düşürülür.



İstek atıldıktan sonra “Forward” seçeneğine tıkladıktan sonra sunucuya istek iletilir. Burp Suite üzerinden Forward edilmez ise istek sunucuya gönderilmez aşağıdaki örnekte

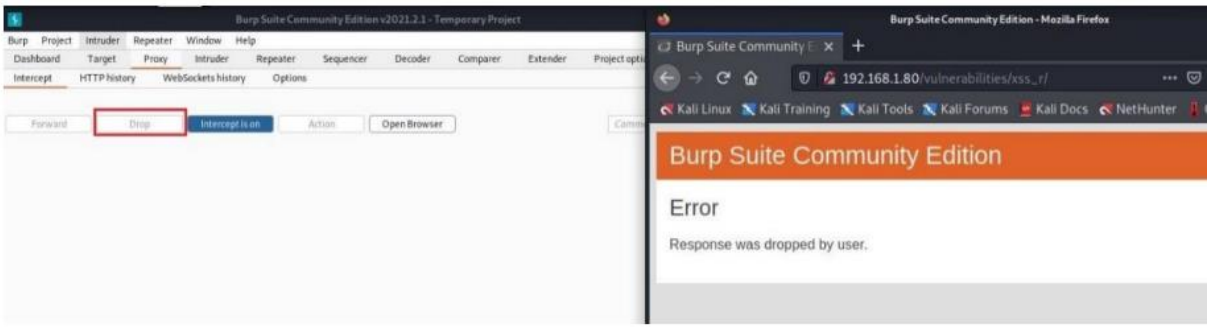


Burpsuite üzerinden “Forward” seçeneğine tıklanarak istek gönderildi.

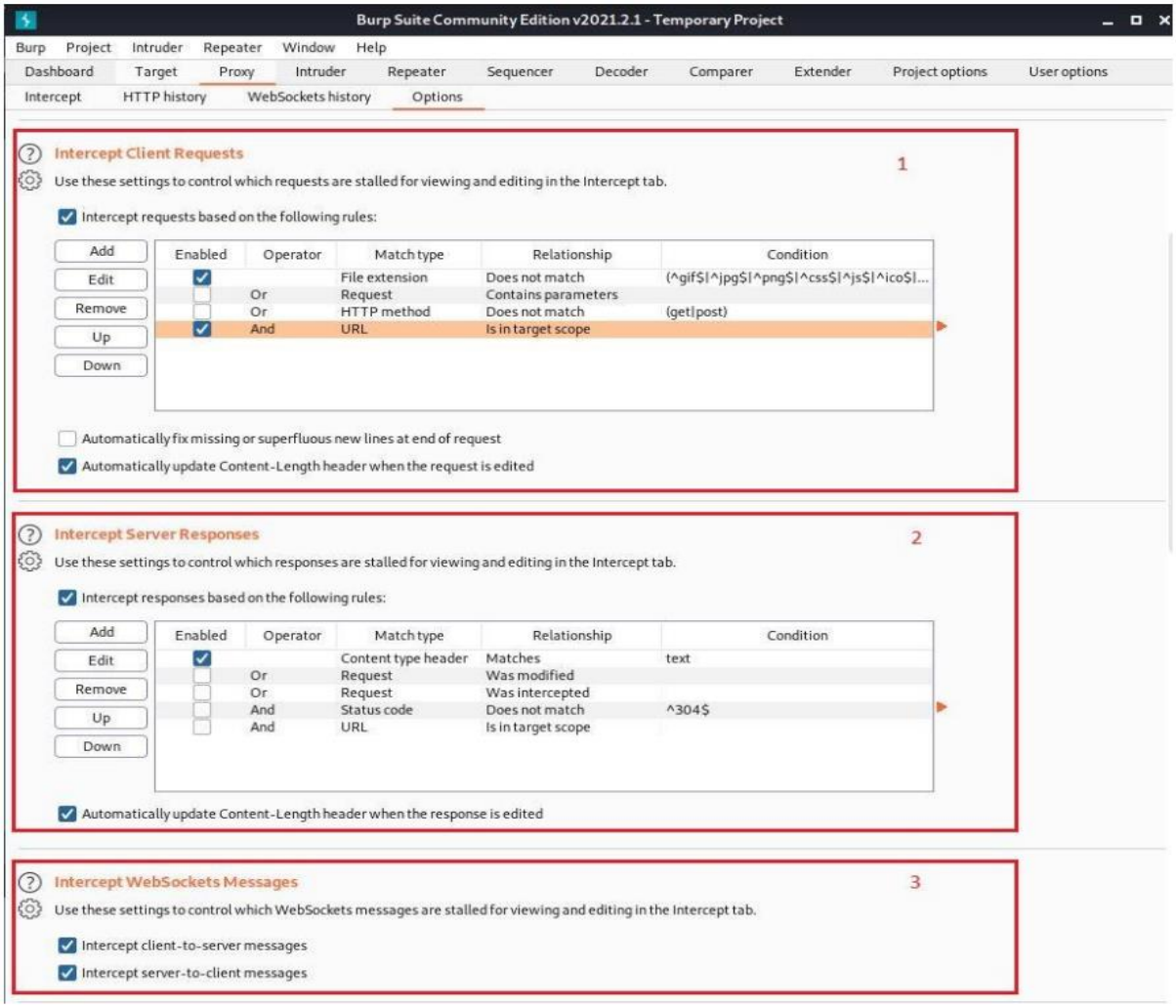


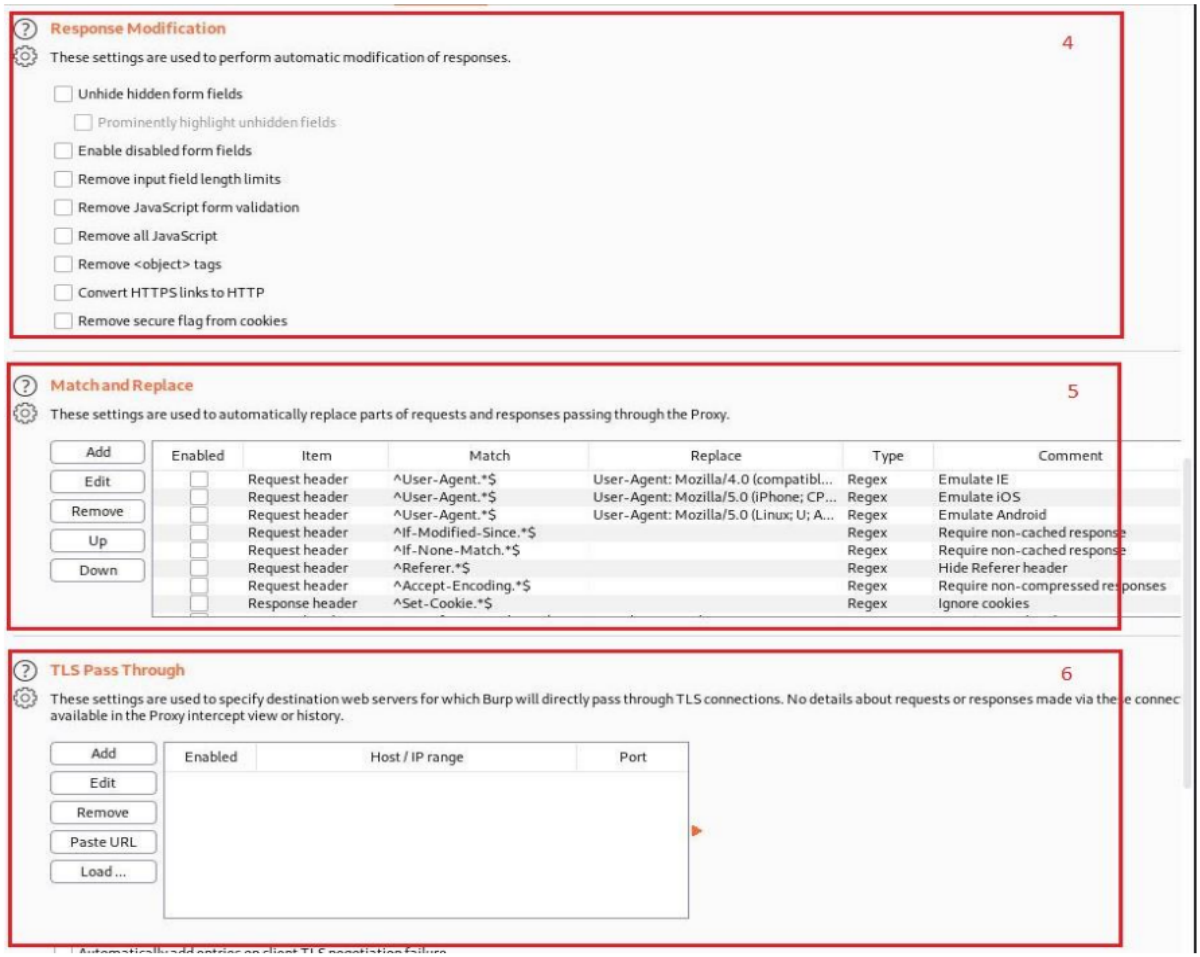
İstek “Drop” edildi

Hazırlayan	Onaylayan
BKK	KASGEM

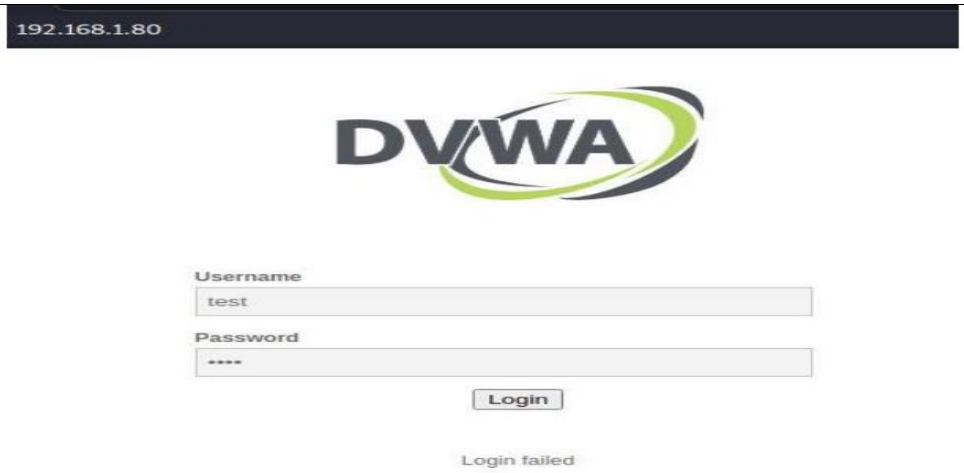


"Options" sekmesindeki diğer ayarlar. 1. İstemci üzerinden gelen isteklerin ayarlarının yapıldığı alan. 2. Sunucu üzerinden gelen isteklerin ayarlarının yapıldığı alan. 3. Web soket yapısı ile ilgili mesaj yapısının ayarlandığı alan. 4. Sunucudan gelen istekleri otomatik değiştirmek için ayarlamalar yapılan alan. 5. Proxy üzerinden geçen istek ve yanıtların bölümlerini otomatik olarak değiştirmek için kullanılan alan. 6. TLS bağlantılarını doğrudan yönlendirileceği hedef web sunucularını belirtmek için kullanılır.

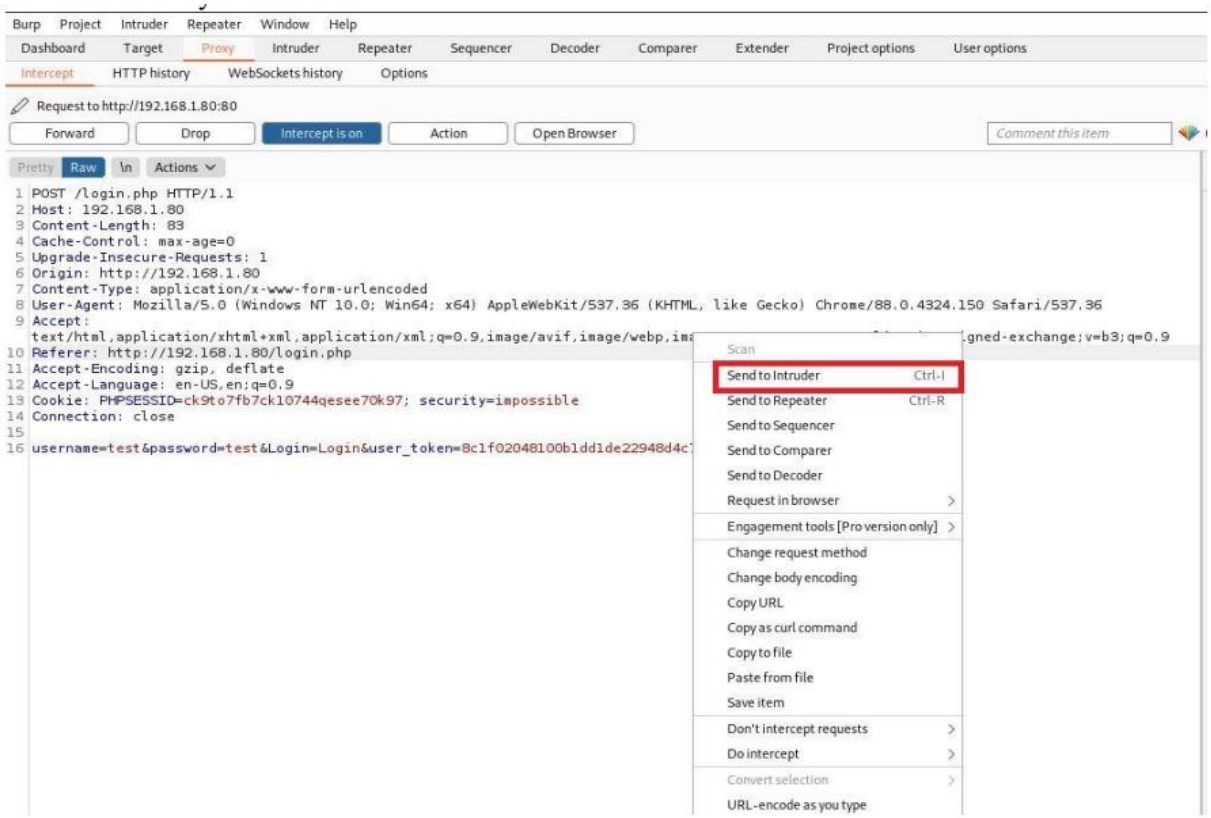

Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Intercept Client Requests
1
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Remove
Up
Down
Enabled Operator Match type Relationship Condition
File extension Does not match (^gif$|^jpg$|^png$|^css$|^js$|^ico$|...
Or Request Contains parameters
Or HTTP method Does not match (get|post)
And URL Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited
Intercept Server Responses
2
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.
Intercept responses based on the following rules:
Add
Edit
Remove
Up
Down
Enabled Operator Match type Relationship Condition
Content type header Matches text
Or Request Was modified
Or Request Was intercepted
And Status code Does not match ^304$
And URL Is in target scope
Automatically update Content-Length header when the response is edited
Intercept WebSockets Messages
3
Use these settings to control which WebSockets messages are stalled for viewing and editing in the Intercept tab.
Intercept client-to-server messages
Intercept server-to-client messages



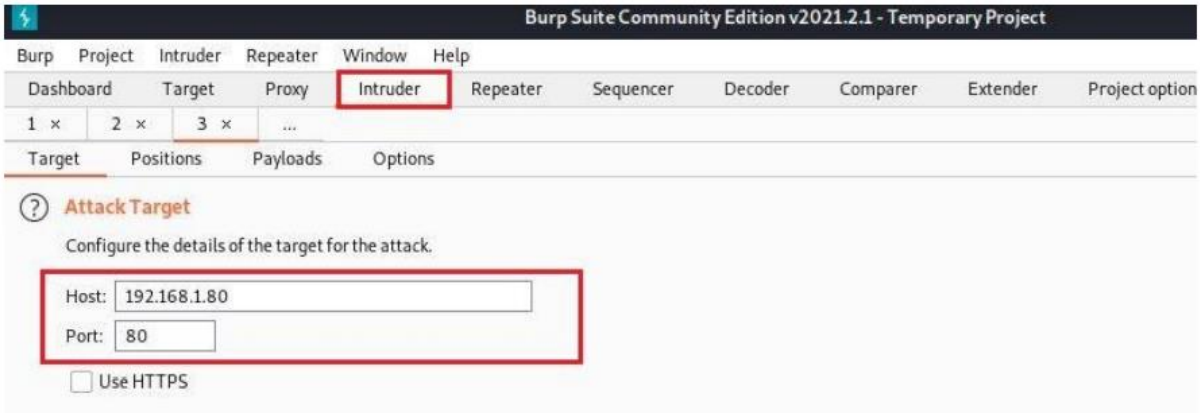
Burp Suite- Intruder Burp Intruder, web uygulamalarına karşı otomatikleştirilmiş payload denemeleri ve brute force işlemlerini sağlayan araçtır. Intruder aracı sayesinde bir isteğin parametreleri değiştirilerek çok sayıda deneme gerçekleştirilebilir. Genellikle form alanlarında veya ilgili parametre alanlarında kullanılır. 192.168.1.80 ip adresli bir adet web sunucusu mevcut. Üzerinde deneme yapabilmek için DVWA (Damn Vulnerable Web Application) kurulumu yapılmıştır. Öncelikle DVWA kullanıcı adı giriş denemesi yaparak “Intercept” alanında görüntülenir.



"Intercept" alanında görüntülenen isteğe sağ tıklayarak "Send to Intruder" seçilir. Bu sayede istek Intruder alanına yönlendirilir.

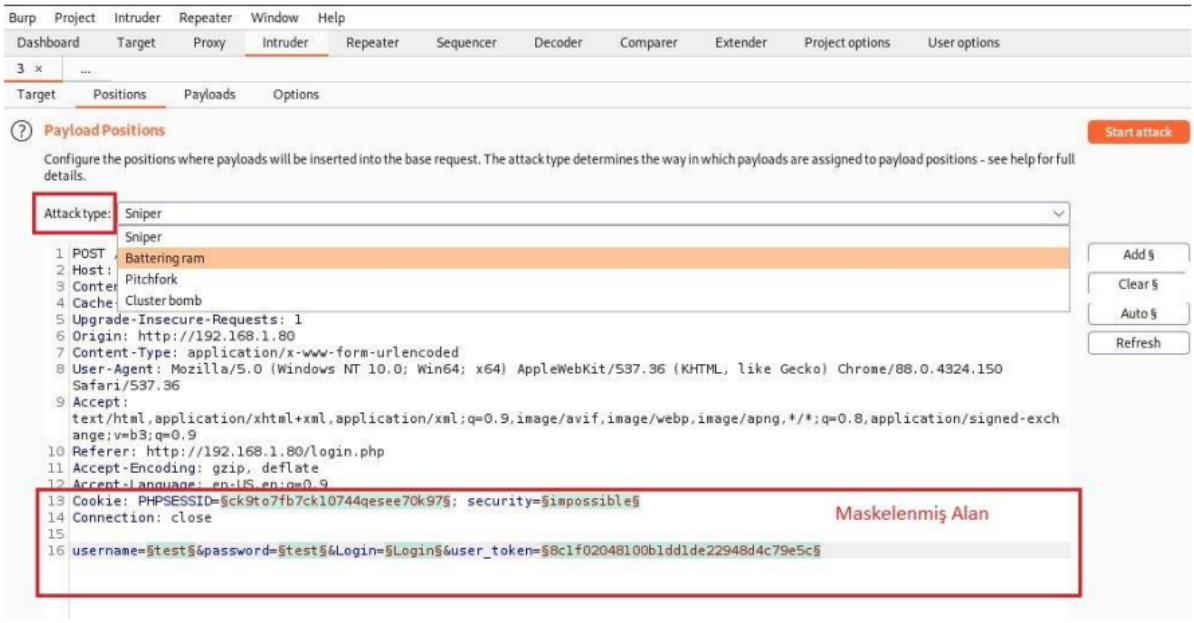


Intruder alanında gelen isteğin host ve port numarası “Intruder→ Target” alanında yer alır.

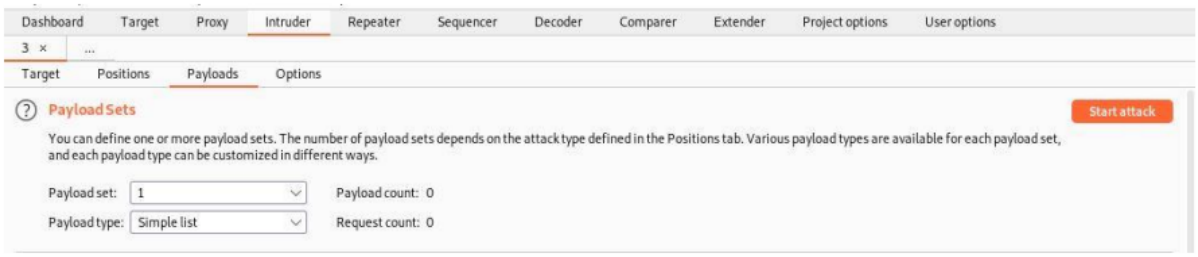


“Payload Possitions” alanında gelen isteğin içeriğini görüntülenerek atak tipleri seçilir. Örnek için “Sniper” atak tipi seçilecektir. Sniper atak tipi öncelikle birinci parametreyi değiştirerek deneme yapar. Ardından ikinci parametre denenir.

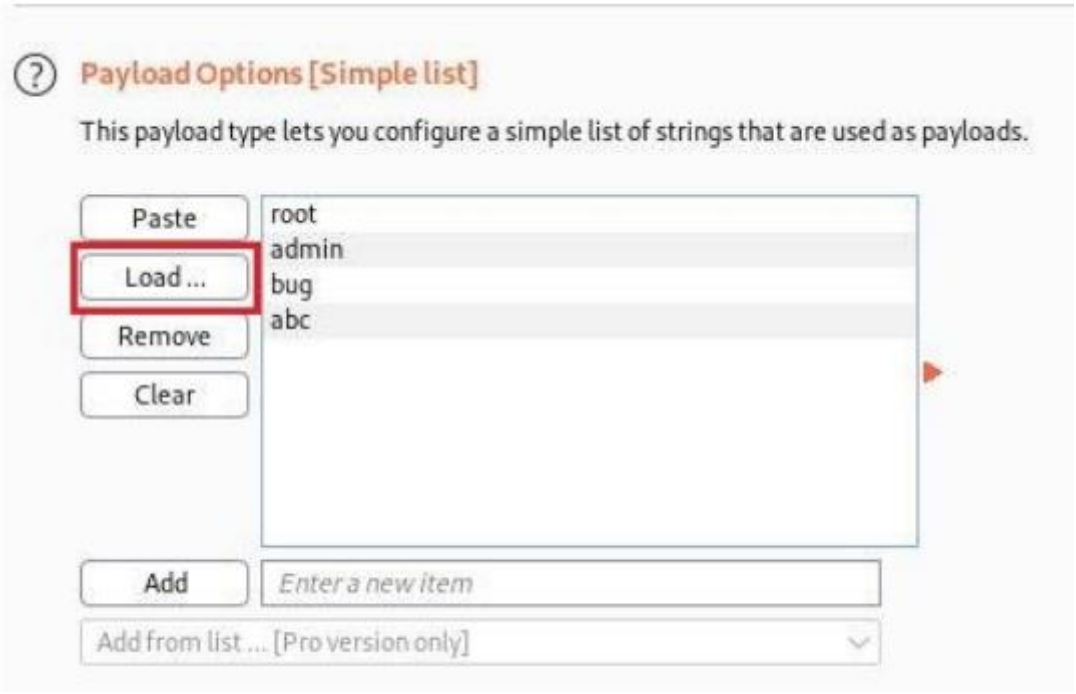
Gelen isteğin parametrelerinin ilgili alanları maskelenmiş durumdadır. Bu değerler Intruder tarafından dinamik olarak kabul edilir ve atak yapılabilen parametreler olduğunu belirtir.



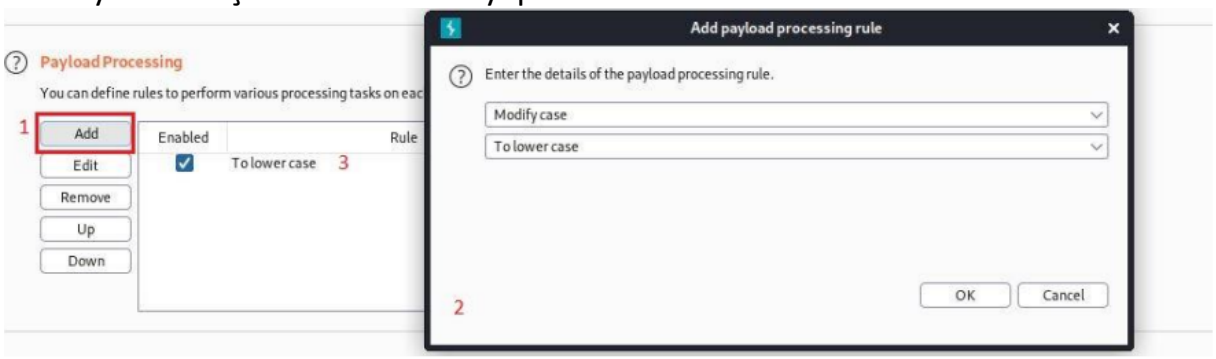
Saldırılacak parametreler belirlendikten sonra parametre pozisyonu belirtilmelidir. “Payloads Set” alanında öncelikle payload tipi seçilir.



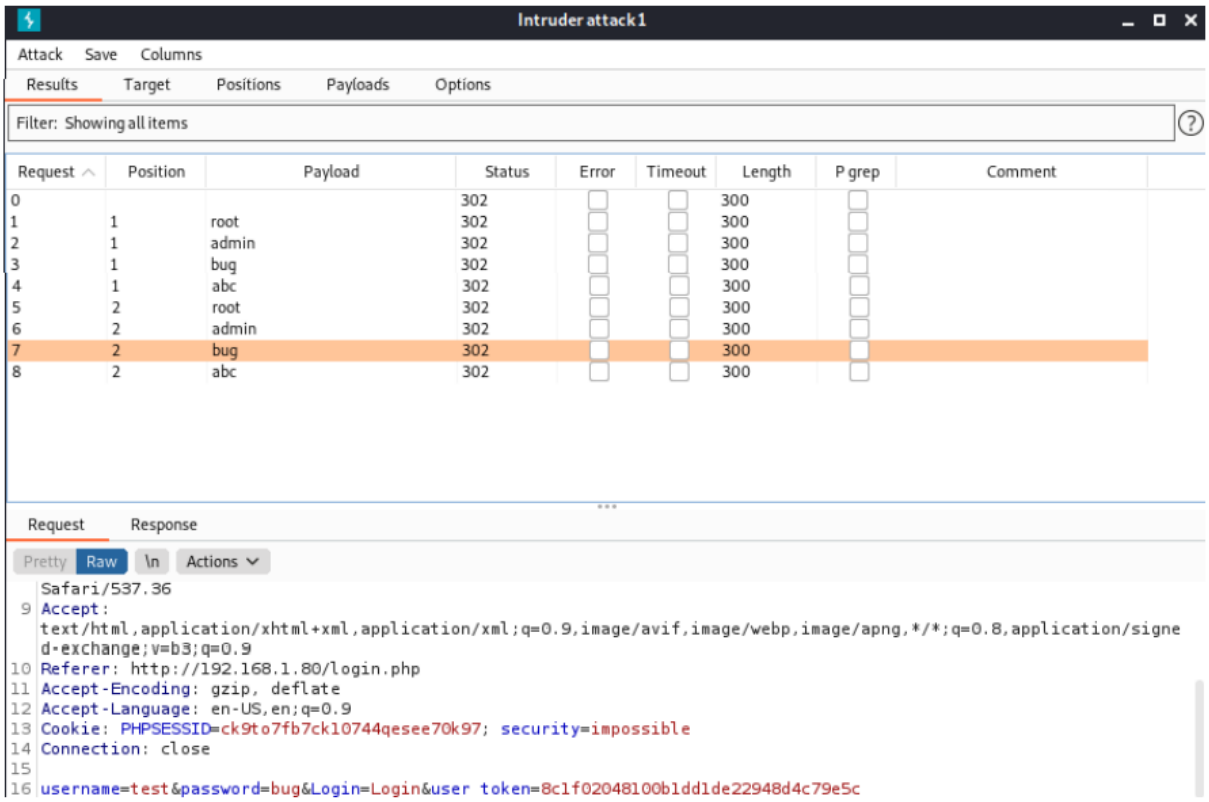
Basit bir işlem için “Simple List” tipi seçilebilir. Simple List ile saldırken kendi oluşturduğu listeyi payload olarak verir. “Load” seçeneğine tıklayarak oluşturduğumuz listeyi seçeriz. Dilerseniz “Add” seçeneğinden birer birer de girilebilir. Denenmek üzere totalde 4 bilgi girildi. Denenmesi gereken 2 parametre mevcut (Kullanıcı adı ve şifre şeklinde). Bu durumdan dolayı 8 adet istek yapılacaktır.



"Payload Processing" alanında belirli fonksiyonlar mevcut. Deneme işlemi seçilmiş olan fonksiyon dönüşümünden sonra yapacaktır.

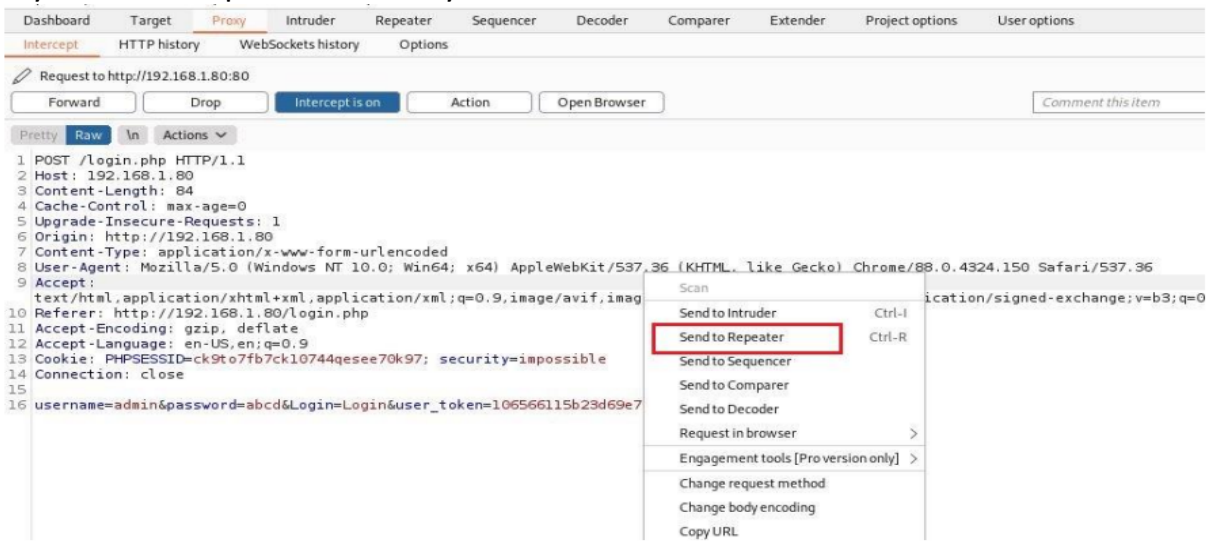


"Start attack" seçeneği seçilerek atak başlatılır.

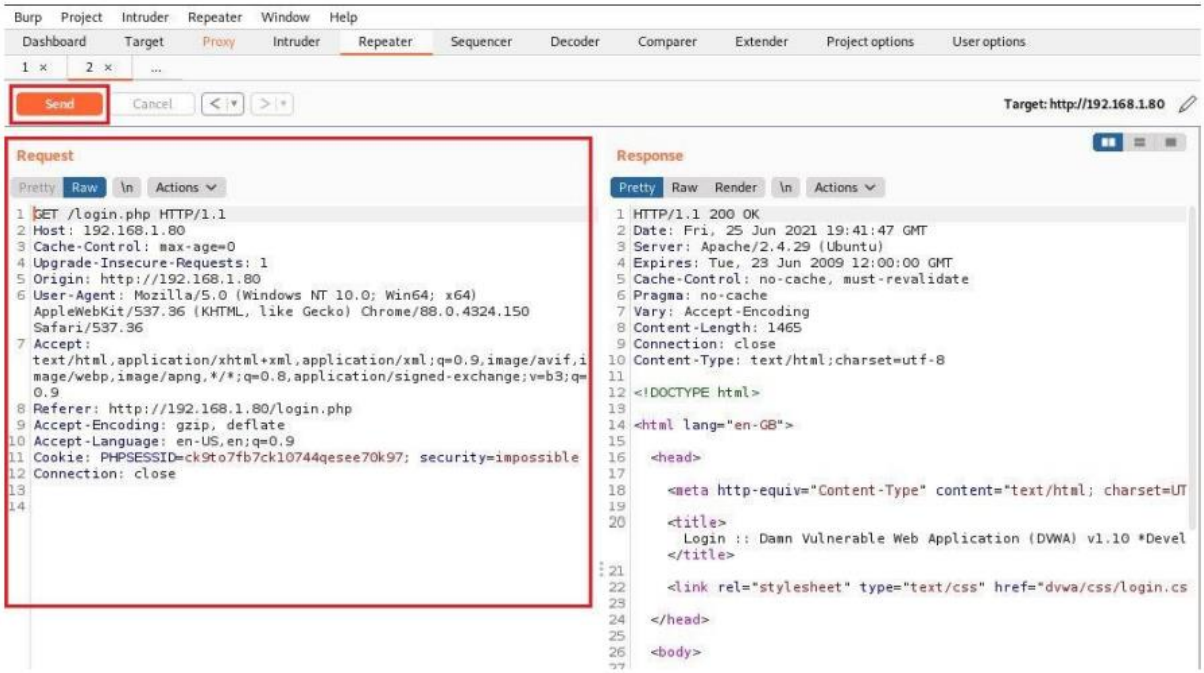


Burp Suite – Repeater

Proxy ile araya girdikten sonra gelen istek içerisindeki değerleri değiştirerek tekrarlayan biçimde istek yapıp uygulamanın yanıtlarını analiz etmek için kullanılan araçtır. “Intercept” alanında görüntülenen isteğe sağ tıklayarak “Send to Repeater” seçilir. Bu sayede istek Repeater alanına yönlendirilir.



Intercept alanından gönderilen istek kırmızı kutu içerisinde verilmiştir. “Sent” seçeneğine tıklandıktan sonra “Response” alanında isteğin yanıtı görüntülenir. Yakalanılan istekleri değiştirilerek tekrar gönderilir böylece istekler daha hızlı ve karışıklık olmadan analiz edilebilir.



Hazırlayan	Onaylayan
BKK	KASGEM

	SİBER GÜVENLİK **ARAŞTIRMA SONUCU PAYLAŞIM FORMU**	Doküman No	FR-471
		İlk Yayın Tarihi	19/07/2023
		Revizyon Tarihi	-
		Revizyon No	0
		Sayfa No	1/1

Sorumlu Öğretim Elemanı

Unvan: Doç.Dr.

Adı Soyadı:Ali GEZER

Görevi: Siber Güvenlik Uygulama ve Araştırma Merkezi Müdür

Hazırlayan	**Onaylayan**
BKK	KASGEM