



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

T.C.
Kayseri Üniversitesi
Siber Güvenlik Uygulama ve Araştırma Merkezi Müdürlüğü

ARAŞTIRMA FAALİYETİ SONUÇ RAPORU

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

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. Community 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> bağlantısının üzerinden erişim sağlanıp, uygun sürüm ve işletim sistemi seçilerek indirilir.

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

Burp Suite Arayüzü

Hazırlayan
BKK

Onaylayan
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

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.

File

File: Choose file...

Default to the above in future

Disable extensions

Cancel Back Start Burp

Hazırlayan
BKK

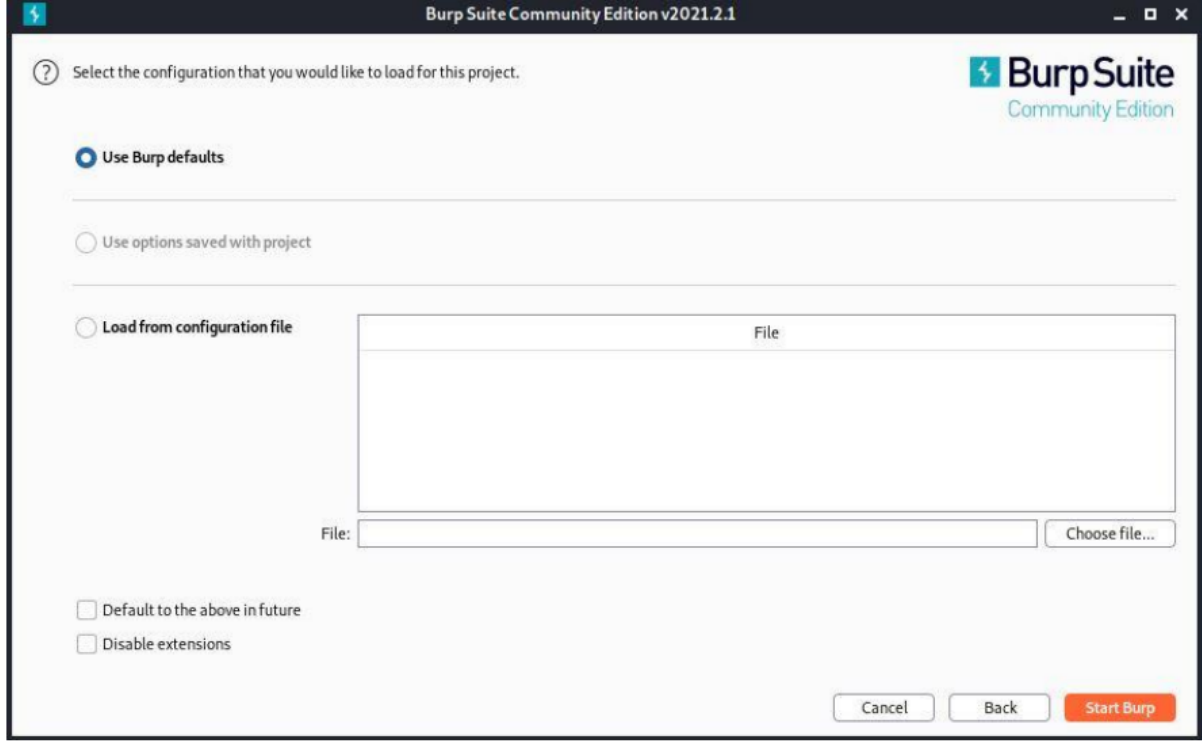
Onaylayan
KASGEM



**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

“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.

Hazırlayan
BKK

Onaylayan
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

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.

Hazırlayan
BKK

Onaylayan
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

5. Request ve response 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.

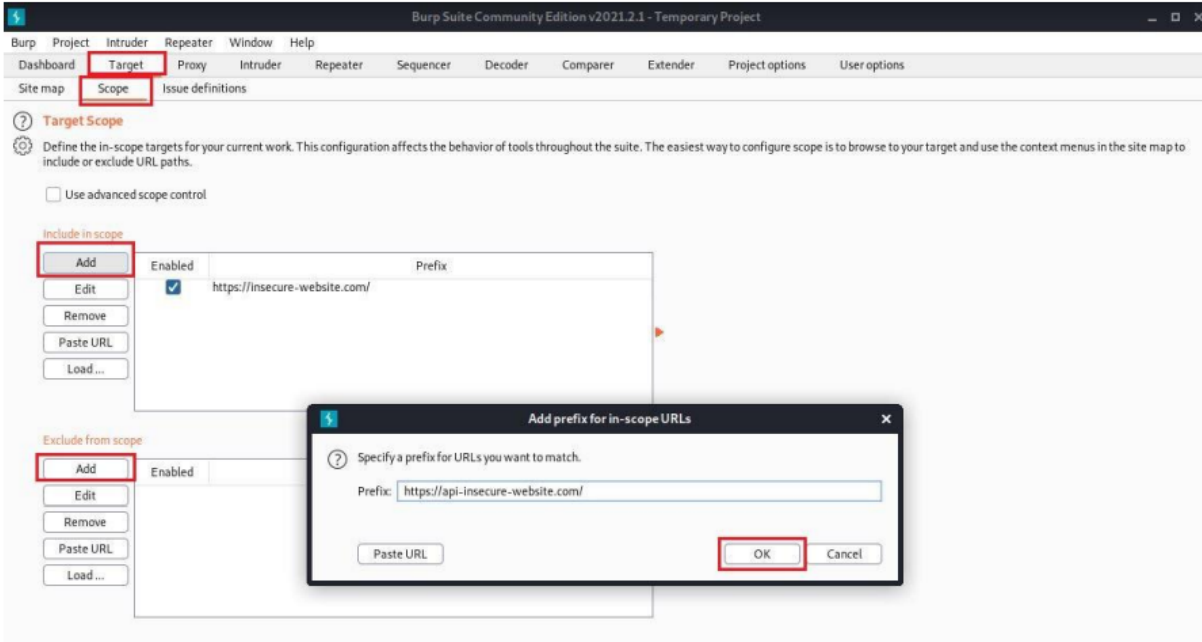
Hazırlayan
BKK

Onaylayan
KASGEM



SİBER GÜVENLİK ARAŞTIRMA SONUCU PAYLAŞIM FORMU

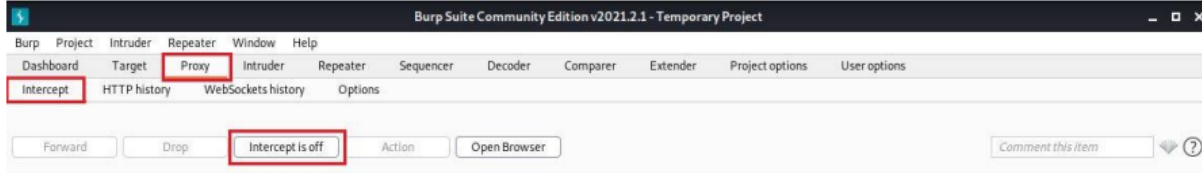
Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1



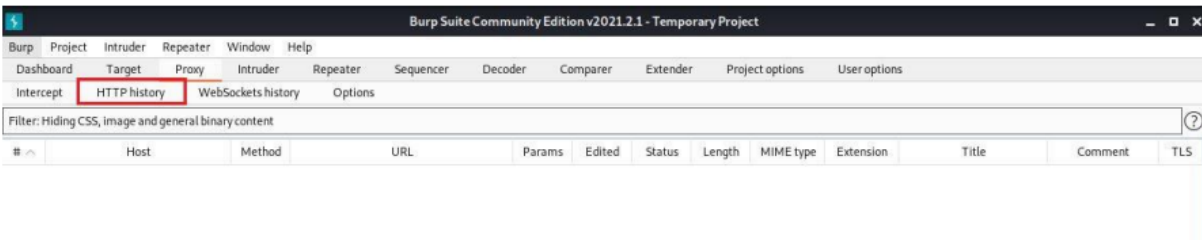
Burp Suite- Proxy

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

“Intercept” alanında gelen ve giden istek yapısı kontrol edilir. “Intercept is on” durumunda olduğu zaman istemciden çıkan isteği görüntülemek için kullanılır. “Intercept 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

Hazırlayan
BKK

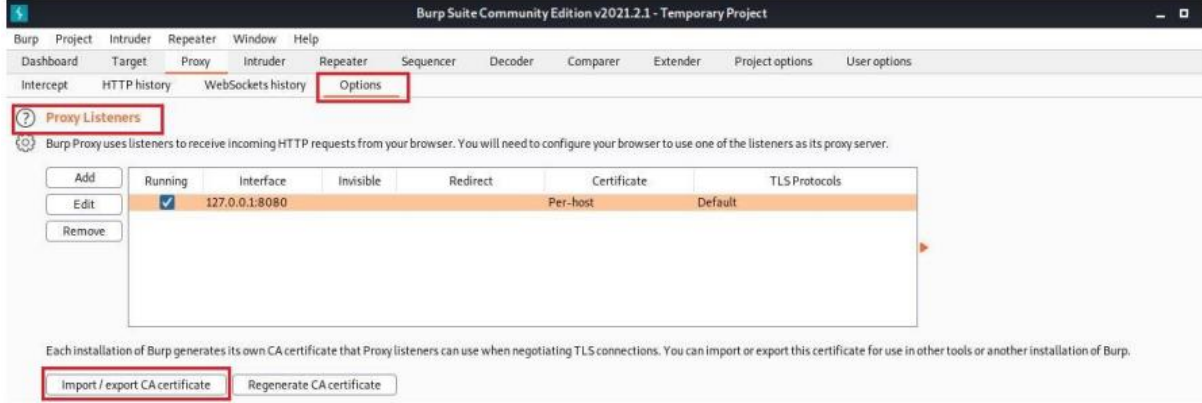
Onaylayan
KASGEM



**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

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.



**Hazırlayan
BKK**

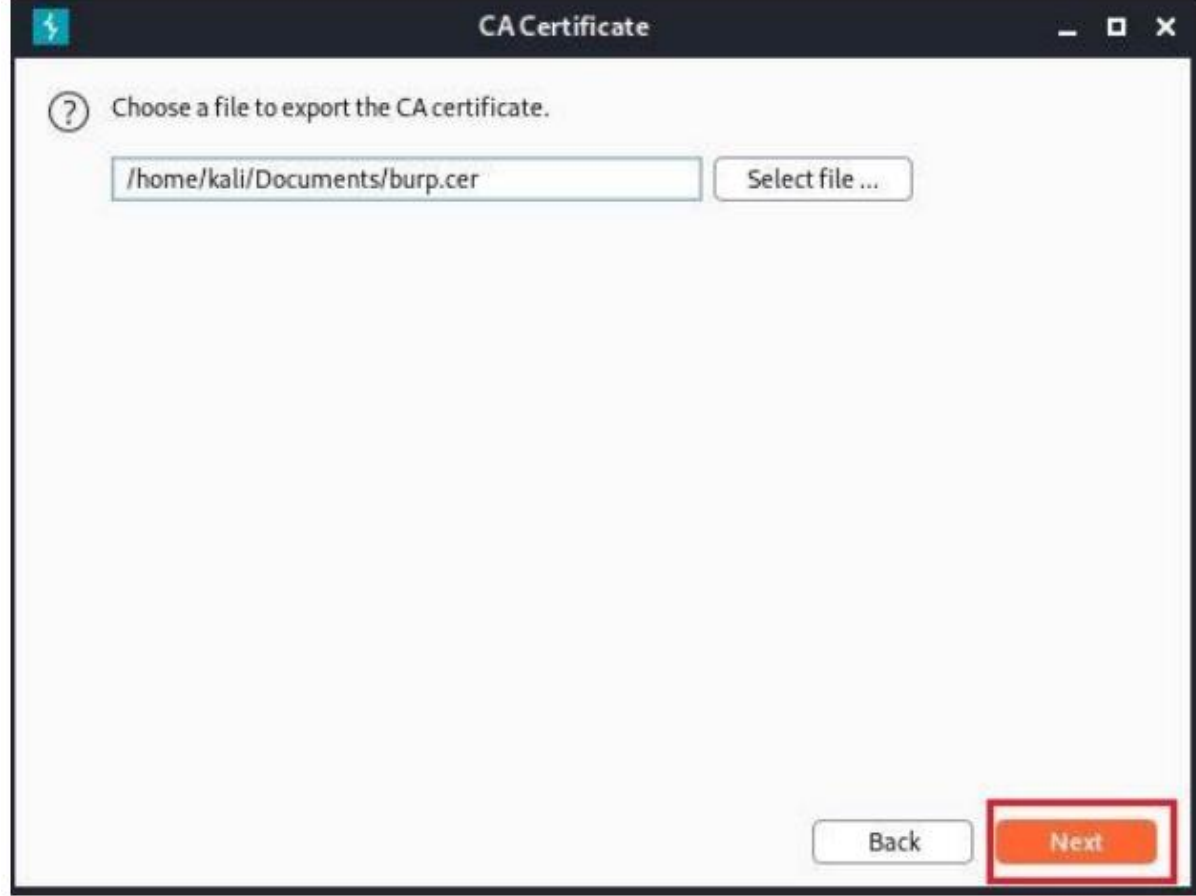
**Onaylayan
KASGEM**



**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

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.

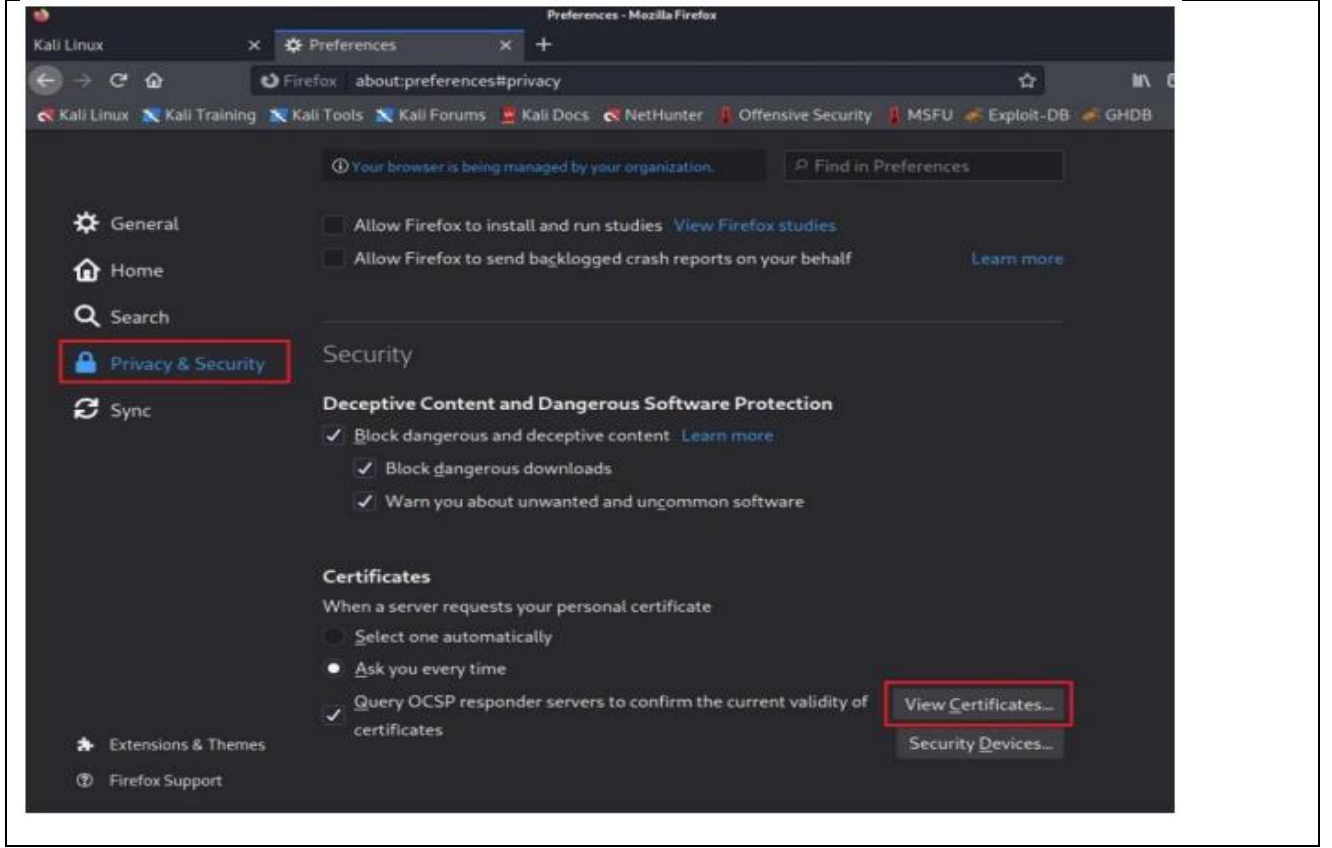
Hazırlayan
BKK

Onaylayan
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



Hazırlayan
BKK

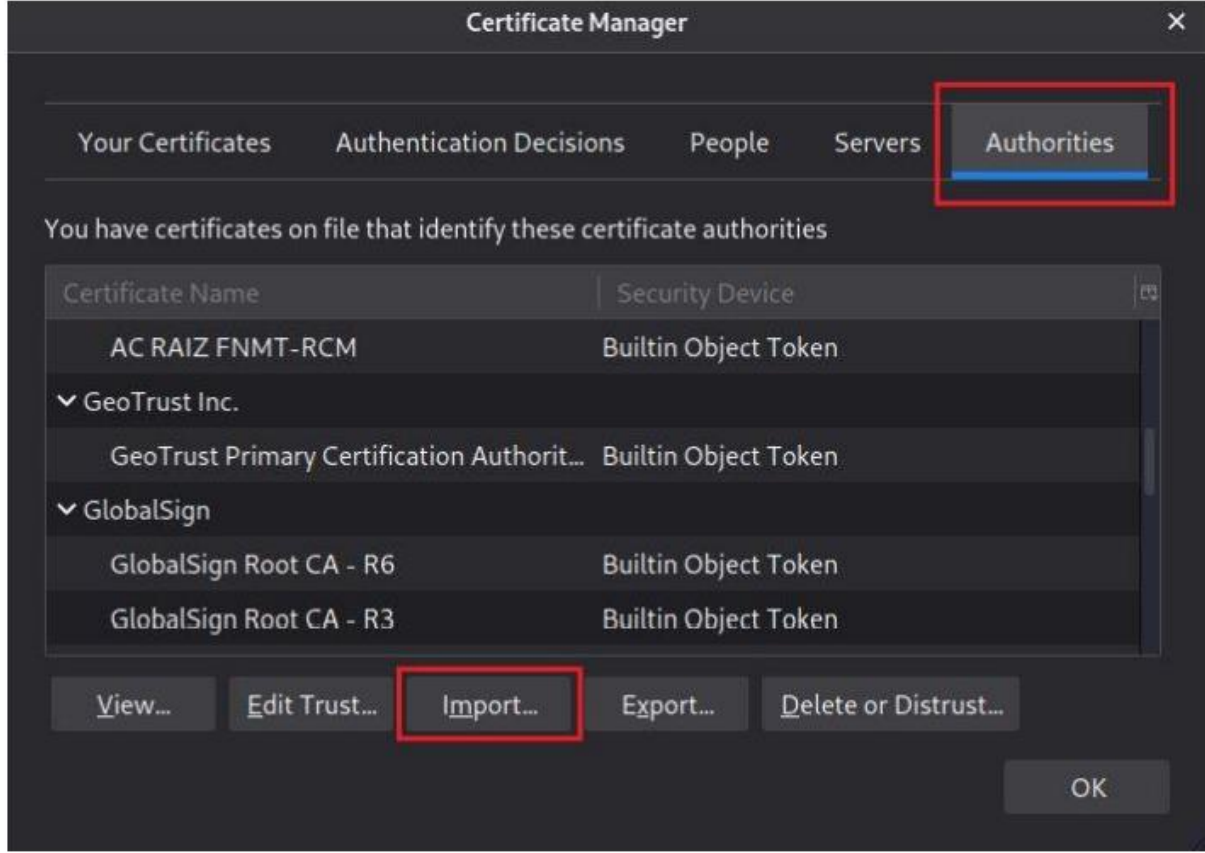
Onaylayan
KASGEM



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

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



Hazırlayan
BKK

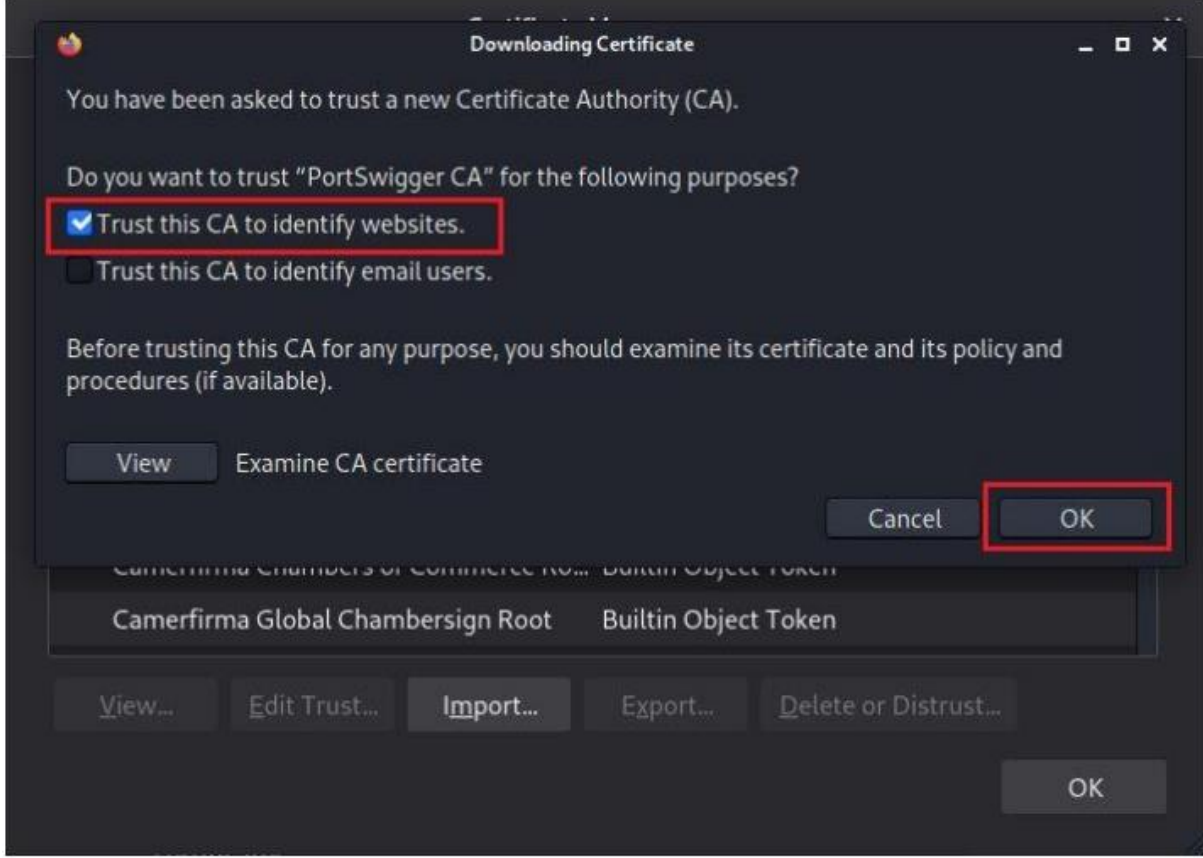
Onaylayan
KASGEM



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

“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.

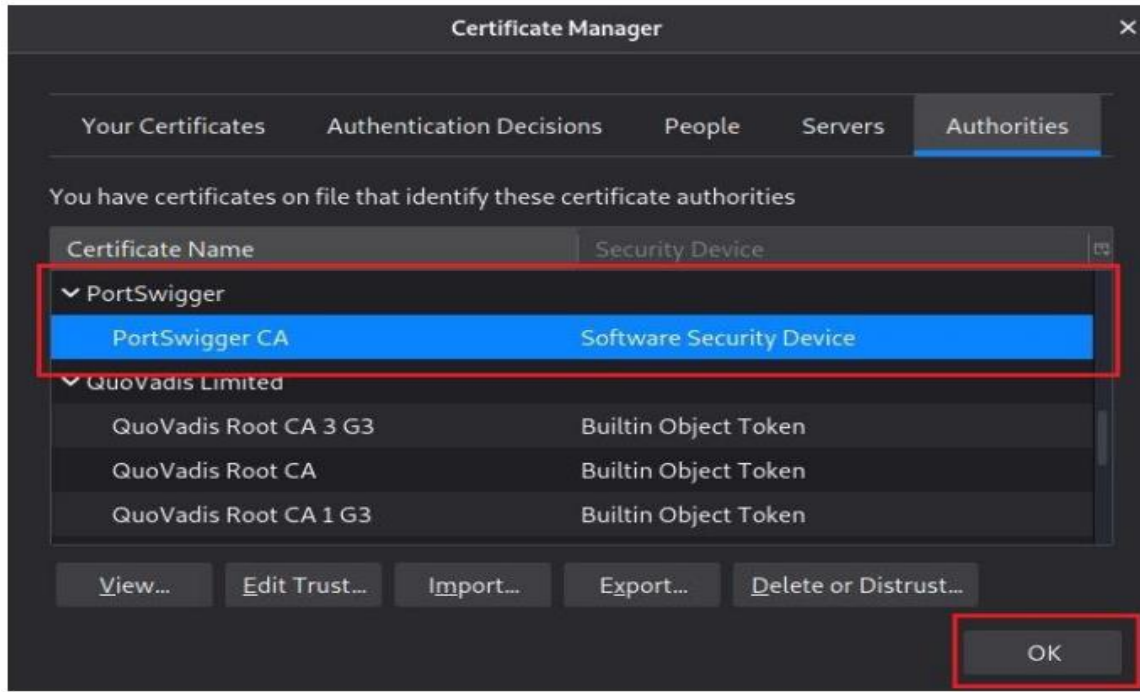
Hazırlayan
BKK

Onaylayan
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



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.

Hazırlayan
BKK

Onaylayan
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

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

Hazırlayan
BKK

Onaylayan
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

The screenshot shows the Burp Suite interface on the left and the Mozilla Firefox browser on the right. In Burp Suite, the 'Forward' button is highlighted in the 'Intercept' tab. The 'Response from http://192.168.1.80:80/' is displayed, showing an HTML page with a title 'Welcome :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*'. The browser on the right shows the page content, including a search bar and a list of top sites.

Burpsuite üzerinden “Forward” seçeneğine tıklanarak istek gönderildi.

The screenshot shows the Burp Suite interface on the left and the Mozilla Firefox browser on the right. In Burp Suite, the 'Drop' button is highlighted in the 'Intercept' tab. The 'Response from http://192.168.1.80:80/' is displayed, showing an HTML page with a title 'Welcome :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*'. The browser on the right shows the page content, including a search bar and a list of top sites.

İstek “Drop” edildi

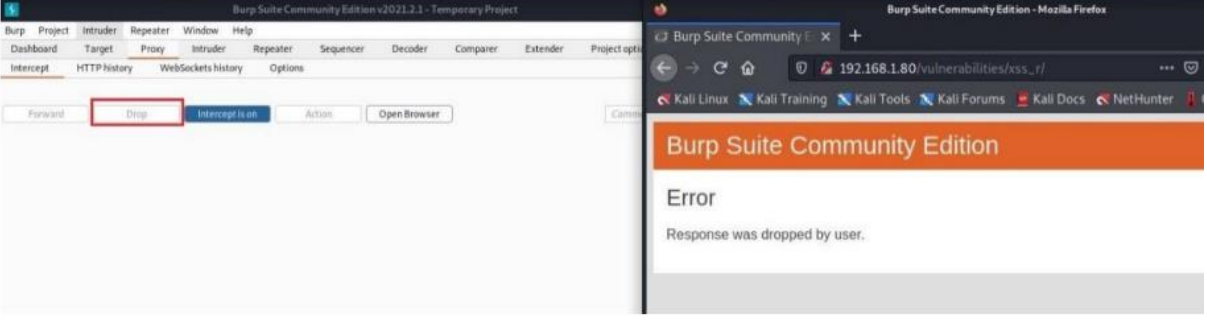
Hazırlayan
BKK

Onaylayan
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



“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.

Hazırlayan
BKK

Onaylayan
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

Burp Suite Community Edition v2021.2.1 - Temporary Project

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:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif ^jpg ^png ^css ^js ^ico\$...
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input checked="" type="checkbox"/>	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:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		Content type header	Matches	text
<input type="checkbox"/>	Or	Request	Was modified	
<input type="checkbox"/>	Or	Request	Was intercepted	
<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="checkbox"/>	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

Hazırlayan
BKK

Onaylayan
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

Response Modification

These settings are used to perform automatic modification of responses.

- Unhide hidden form fields
 - Prominently highlight unhidden fields
- Enable disabled form fields
- Remove input field length limits
- Remove JavaScript form validation
- Remove all JavaScript
- Remove <object> tags
- Convert HTTPS links to HTTP
- Remove secure flag from cookies

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

	Enabled	Item	Match	Replace	Type	Comment
Add	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (compatibl...	Regex	Emulate IE
Edit	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (iPhone; CP...	Regex	Emulate iOS
Remove	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (Linux; U; A...	Regex	Emulate Android
Up	<input type="checkbox"/>	Request header	^If-Modified-Since.*\$		Regex	Require non-cached response
Down	<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cached response
	<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer header
	<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-compressed responses
	<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ignore cookies

TLS Pass Through

These settings are used to specify destination web servers for which Burp will directly pass through TLS connections. No details about requests or responses made via the connection are available in the Proxy intercept view or history.

	Enabled	Host / IP range	Port
Add	<input type="checkbox"/>		
Edit	<input type="checkbox"/>		
Remove	<input type="checkbox"/>		
Paste URL	<input type="checkbox"/>		
Load...	<input type="checkbox"/>		

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.

Hazırlayan
BKK

Onaylayan
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

192.168.1.80



Username
test

Password

Login

Login failed

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

Request to http://192.168.1.80:80

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw In Actions

```
1 POST /login.php HTTP/1.1
2 Host: 192.168.1.80
3 Content-Length: 83
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.80
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
10 Referer: http://192.168.1.80/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=ck9to7fb7ck10744qesee70k97; security=impossible
14 Connection: close
15
16 username=test&password=test&Login=Login&user_token=8c1f02048100b1dd1de22948d4c...
```

Scan

- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

Hazırlayan
BKK

Onaylayan
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

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

Burp Suite Community Edition v2021.2.1 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Extender Project option

1 x 2 x 3 x ...

Target Positions Payloads Options

Attack Target

Configure the details of the target for the attack.

Host: 192.168.1.80

Port: 80

Use HTTPS

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.

Burp Project Intruder Repeater Window Help

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

3 x ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

1 POST Battering ram

2 Host: Pitchfork

3 Content-Type: application/x-www-form-urlencoded

4 Cache: Clusterbomb

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.1.80

7 Content-Type: application/x-www-form-urlencoded

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36

9 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=0.9

10 Referer: http://192.168.1.80/login.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: en-US,en;q=0.9

13 Cookie: PHPSESSID=\$ck9to7fb7ck10744qesee70k97\$; security=\$impossible\$

14 Connection: close

15

16 username=\$test\$&password=\$test\$&login=\$login\$&user_token=\$8c1f02048100b1dd1de22948d4c79e5c\$

Maskelenmiş Alan

Start attack

Add \$

Clear \$

Auto \$

Refresh

Hazırlayan
BKK

Onaylayan
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

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 saldırırken 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.

Hazırlayan
BKK

Onaylayan
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

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

1 Add Enabled Rule
Edit To lower case 3
Remove
Up
Down

2 Enter the details of the payload processing rule.
Modify case
To lower case
OK Cancel

“Start attack” seçeneği seçilerek atak başlatılır.

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Extender Project options User options
3 x ...
Target Positions **Payloads** Options
1 Payload Sets Start attack
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, and each payload type can be customized in different ways.
Payload set: 1 Payload count: 4
Payload type: Simple list Request count: 8

Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request ^ Position Payload Status Error Timeout Length P grep Comment
0 1 root 302
1 1 admin 302
2 1 bug 302
3 1 abc 302
4 2 root 302
5 2 admin 302
6 2 bug 302
7 2 abc 302
8 2 abc 302
Request Response
Pretty Raw In Actions
Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
d-exchange;v=b3;q=0.9
10 Referer: http://192.168.1.80/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=ck9to7fb7ck10744qesee70k97; security=impossible
14 Connection: close
15
16 username=test&password=bug&Login=Login&user token=8c1f02048100b1dd1de22948d4c79e5c

Burp Suite – Repeater

Hazırlayan
BKK

Onaylayan
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

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.

```
1 POST /login.php HTTP/1.1
2 Host: 192.168.1.80
3 Content-Length: 84
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.80
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
9 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=0.9
10 Referer: http://192.168.1.80/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=ck9to7fb7ck10744qesee70k97; security=impossible
14 Connection: close
15
16 username=admin&password=abcd&Login=Login&user_token=106566115b23d69e7
```

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

```
Request
1 GET /login.php HTTP/1.1
2 Host: 192.168.1.80
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 Origin: http://192.168.1.80
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
7 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=0.9
8 Referer: http://192.168.1.80/login.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Cookie: PHPSESSID=ck9to7fb7ck10744qesee70k97; security=impossible
12 Connection: close
13
14

Response
1 HTTP/1.1 200 OK
2 Date: Fri, 25 Jun 2021 19:41:47 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1465
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-G8">
15
16 <head>
17
18 <meta http-equiv="Content-Type" content="text/html; charset=UTF
19
20 <title>
21 Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Devel
22 </title>
23
24 <link rel="stylesheet" type="text/css" href="dvwa/css/login.cs
25
26 </head>
27
28 <body>
```

Hazırlayan
BKK

Onaylayan
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
BKK**

**Onaylayan
KASGEM**