OWASP TOP 10 ÖDEV

Konu : OWASP Top 10 ‘dan 3 Adet zafiyet seçilip write-up yazılıcak.
Yazar : İbrahim Servet Çetinkaya

1. Zafiyet ; "**Authentication Vulnerabilities" (Kimlik Doğrulama Zayıflıkları)”**
Bu isimle şuan’da yer almamakta, OWASP TOP 2021 yeni ismi A7: **Identification and Authentication Failures**" başlığı altında ele alınmıştır.

Platform ; Port Swigger / Web Academy
LAB LİNKİ ; https://portswigger.net/web-security/learning-paths/authentication-vulnerabilities/password-based-vulnerabilities/authentication/password-based/lab-username-enumeration-via-subtly-different-responses

ÇÖZÜM

Lab: Username enumeration via subtly different responses

PRACTITIONER
LAB Solved

This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Bize söylediği şeyler ; Bu laboratuvar kullanıcı adı numaralandırma parola kırma saldırılarına karşı savunmasızdır, basit şifreleler kullanıldığından bahsediyor. Ve bizlere 2 adet wordlist veriyor bunlar brute force yaparken kullanacağımız listeler. Usernames adında olanı kullanıca adına , password isimde olanı’da parola alanına denicez. Ama burada kullanıcı adı numaralandırmadan bahsediyorsa muhtemelen , databasede kayıtlı olmayan bir isim girdiğimizde bu ismi red edicek bir alert çıktısı yazıyor olabiiir. Örnek ; kullanıcı adı yanlış/geçersiz/hatalı vb. İfadeler. Kullanıcı adalarına bu tarz ifade veriyorsa bu muhtemelen bir kullanıcı adı numaralandırma zafiyeti içerisine girer, çünkü kullanıcı adlarını öğrendiğimizde tek geriye kalan parola alanı.

Makinemizi ayağa kaldırıp bir bakalım.

Web Security Academy

Username enumeration via subtly different responses

Back to lab description

LAB Not solved

Home | My account

WE LIKE TO BLOG

Bir blog sayfasına geldik, sağ tarafta yer alan My account yazısına tıklıyalım, herhangi bir hesabda olmadığımız için login olmamız istenicektir.

Login

Username

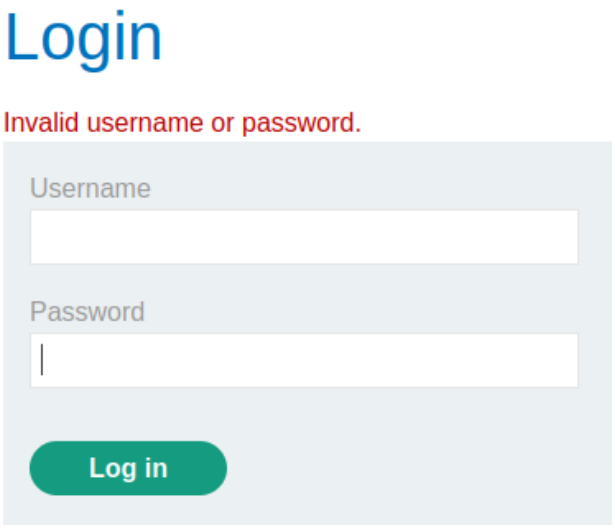
Servet_Pentest_Yavuzlar

Password

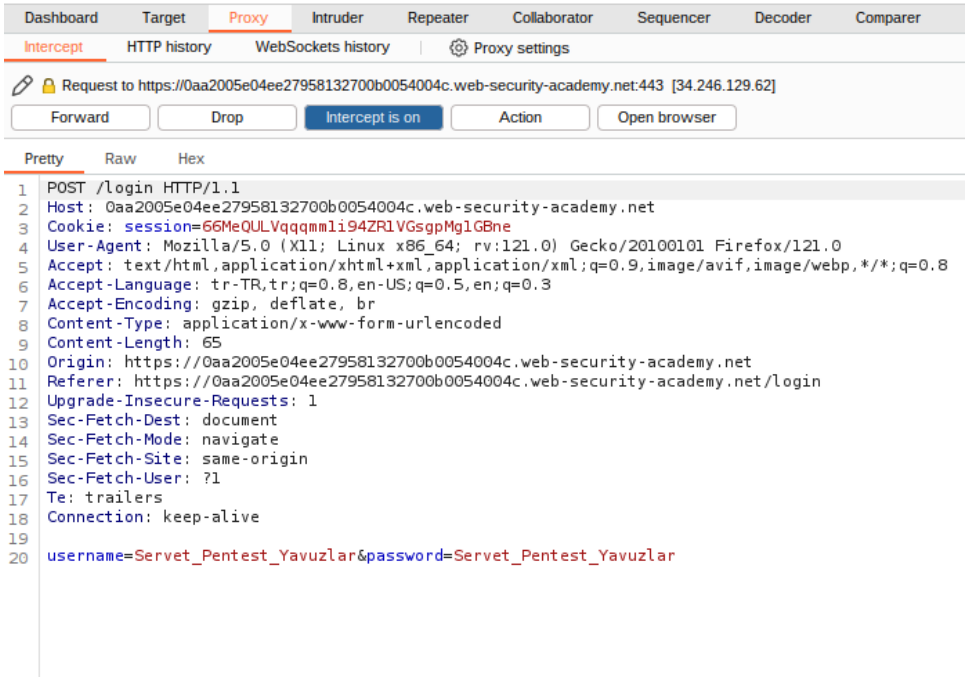
Servet_Pentest_Yavuzlar

Log in

Ve karşımıza login ekranı geldi 2 adet input alanımız var.
Not: sizde şifre *** gözükücektir ben write-up olduğu için html etiketlerinden **type=password** değerini kaldırdım.
Ve rastgele değerler yazdık **LOG İN** diyelim bakalım.



Ve istediğimiz uyarıyı aldık "**Invalid username or password**"
2 inputdan birisi geçersiz diyor. And ifadesi kullanırsa bu tarz durumlarda o daha kritik bir ifade olur bizim için. Şimdi bu uyarımızı not alalım ve brute force işlemi için Burp Suite'mizi açalım. Ve İntercept'i açıp giden isteğe bir bakalım.



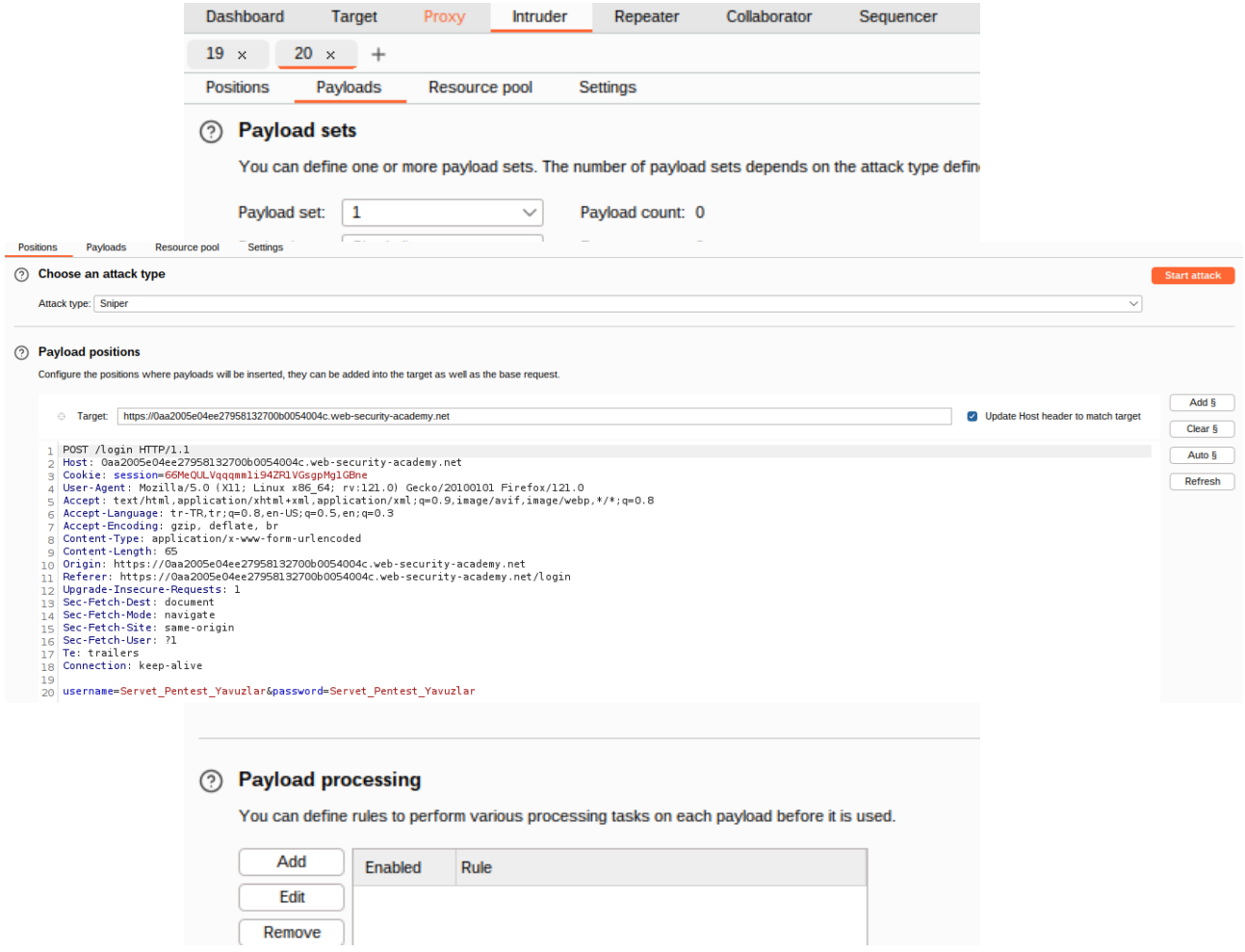
2 değerimiz'de username header ve password headerlarında yer alıyor. Bu alanı brute force için istersek bu pencereye sağtık yapıp "send to intruder" deyip gönderelim.

Bu ekran'da saldırı türümüzü Sniper seçip kullanıcı adını faremizin imleciyle tümü işaretleyip sağ da yer alan bar'da ADD butonuna tıklıyalım.

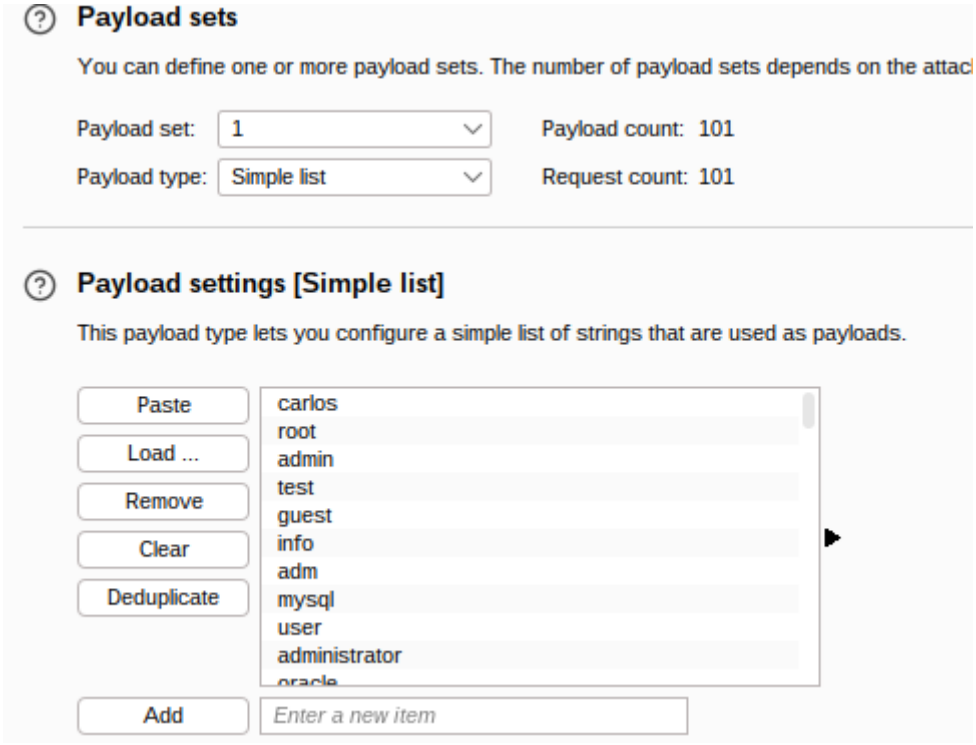
```
username=§Servet_Pentest_Yavuzlar§&password=Servet_Pentest_Yavuzlar
```

Bu
şekilde olması gerekiyor. Ve üst bar kısmından payload sekmesine gidelim.

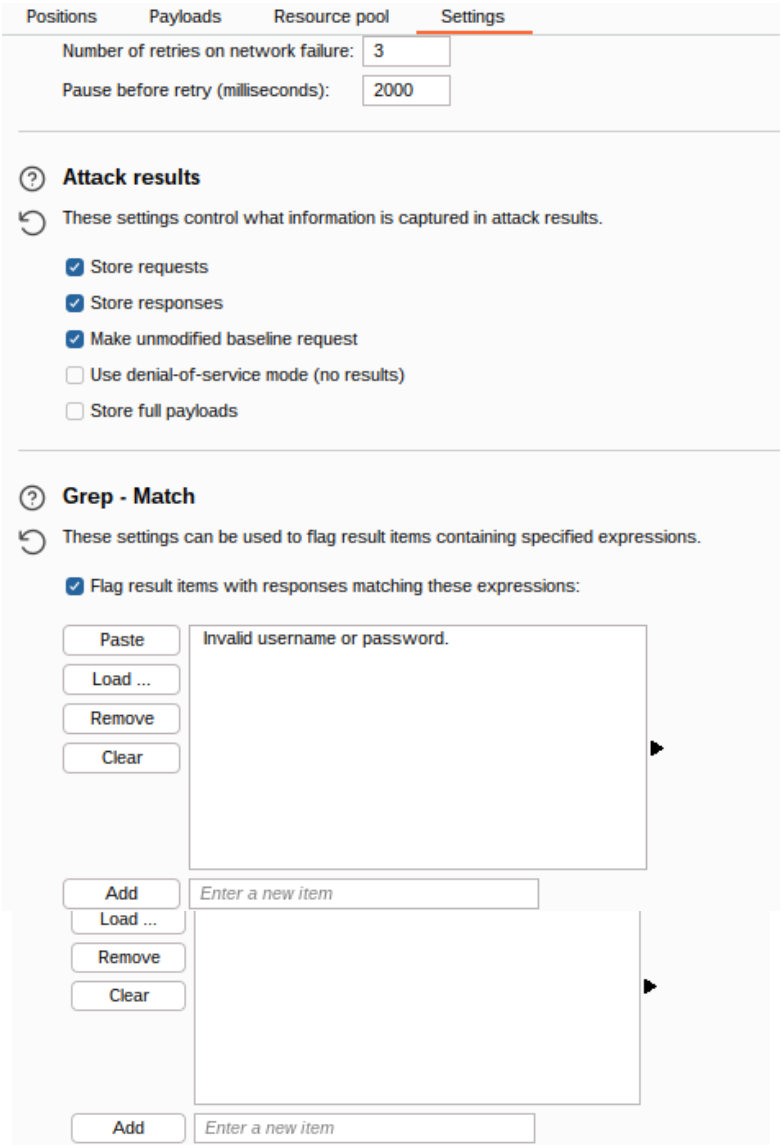
.



bu pencereden Payload settings'e geleleim ve bizlere verilen username isimlerini copy+paste şeklinde direkt olarak atabiliriz.



Şimdi ise hatalı kullanıcı adı girdiğimizde olan uyarıyı şu alana girelim.



Ve bu alanımızı da doldruduktan sonra saldırıyı başlatalım. Bu işlemi yapmamızın sebebi bu uyarıyı almadığımızın kulllanıcı adlarını karşımıza getiriricek.

Request	Payload	Status code	Response received	Error	Timeout	Length	Invalid usern...	Comment
65	announcements	200	134			3359		
0		200	136			3342	1	
1	carlos	200	219			3343	1	
2	root	200	135			3342	1	
3	admin	200	218			3343	1	
4	test	200	217			3339	1	
5	guest	200	174			3339	1	
6	info	200	213			3358	1	
7	adm	200	212			3340	1	
8	mysql	200	214			3339	1	
9	user	200	215			3341	1	

Ve denenen kullanıcı adları bunlar üst bar'da ;request, payload ,Status code yazan bar kısmında biz uyarımızı da başlık olarak eklemiş olduk, Alt sırasında 1 yazanlar sistemde kayıtlı olmayan kullanıcılar. Başlığa tıklayarak 1 dışında değerleri görebiliriz. Burada none değer dönmüş yani kullanıcı adı doğru. Ama bu kullanıcı adını şimdi yinede yazsak, şifreyi bilmediğimiz için yine aynı uyarıyı alıcaz çünkü or ifadesi kullanılmış. Sadece bunu Burp ile arkada dönen isteklerden bulabiliyoruz , şimdi ise şu adımları izlicez.

Kullanıcı adımızı bulduk : announcements

Sıra şifrede.

```
username=announcements&password=§Servet_Pentest_Yavuzlar§
```

Şimdi ise "**İntruder**"alanında sadece bu kullanıcıya yönelik brute force saldırısı yapıcaz. Liste olarak bu sefer password wordlistini kullanıcıaz. Ve saldırıyı başlatalım.

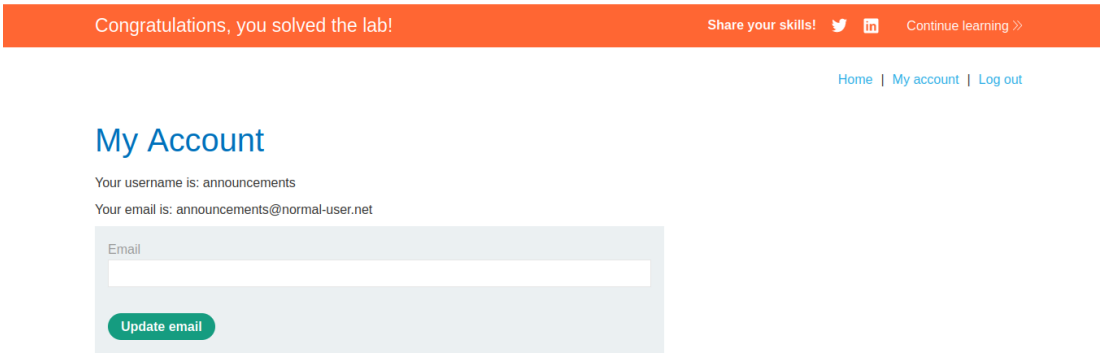
Bu sefer saldırı ekranında bakıcağımız alan " **Status Code** " ekranı eğer doğru parolayı bulursa bizi kendi hesabımıza yönlendiricektir. Bu da demektir ki HTPP isteklerinde yönlendirme ifadedi 302 li bir ifade bekliyoruz. Normalde yönlendirme Status Code'ları **300-400** arasıdır.

Request	Payload	Status code	Response received	Error	Timeout	Length	Inv
54	daniel	302	169			195	
0		200	85			3357	
1	123456	200	171			3358	
2	password	200	177			3356	
3	12345678	200	177			3357	
4	qwerty	200	84			3340	
5	123456789	200	93			3343	
6	12345	200	87			3341	
7	1234	200	103			3357	
8	111111	200	172			3340	

.

Ve parolamızın **Daniel** olduğunu bulduk 302 dönen tek htpp kodumuz daniel. Giriş yapmayı deniyelim.

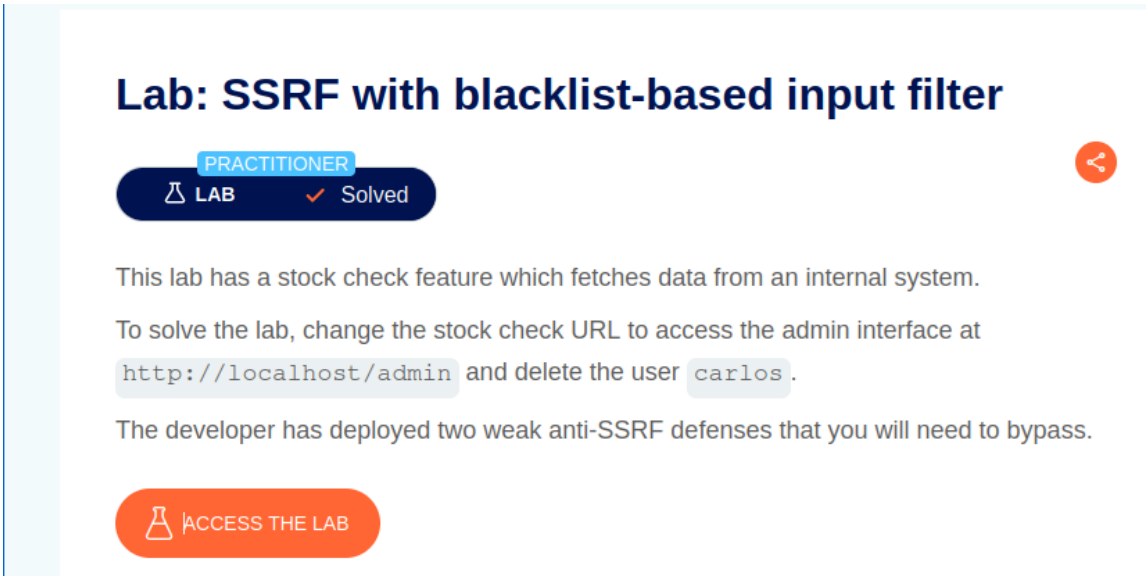
.



Ve başarıyla **announcements** kullanıcı'nın hesabına erişim sağladık.

2. Zafiyet ; "**Server-side request forgery (SSRF)**"
Platform ; Port Swigger / Web Academy
LAB LİNKİ ; https://portswigger.net/web-security/ssrf/lab-ssrf-with-blacklist-filter

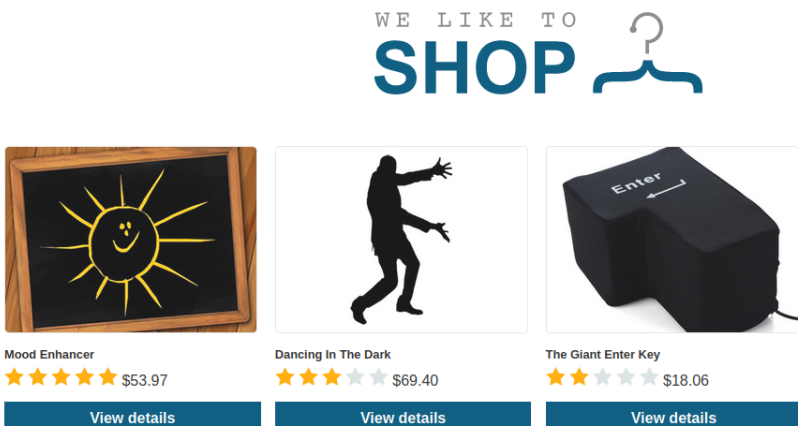
Merhaba hocam, bu SSRF makinesinde amaç 101 seviye çözmek değilde, güvenlik amaçlı saldırıları önlemek adına kullanılan black list içerisinde yer alan sık kullanılan payloadlarımız var. Bunları bypass ederek istek sahteciliğimizi yapıp admin panele ulaşmaya çalışıcağız.



Bize söylenilenler; bu web adresinde ürünler bulunmakta ve bu ürünlerin bir stok kontrol özelliği bulunmakta.

Ve bizden istenen şey ise stok kullanılan url'i sil `http://localhost/admin' e git ve carlos kullanıcısını sil.`

`Web Adresimize Gidelim.`



`Herhangi birini görüntüle butonuna tıklayalım.`

`Ürün ayrıntıların altında`

`kontrolu yapabileceğimiz içerisinde de ülkelerin bulunduğu ufak bir panel var.`

Stok kontrolunu yapalım ama burp ile araya girelim , galiba bahsettiği stok kontrol url' i burada olmalı.

```
stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

.

Ve isteğimizi bulduk stockApi= adında bir header var istekde bu url' i localhost daha sonra admine yönlendirmemiz gerekiyor.
Bu header alanına müdahalerde bulunmak için repater alanımıza gönderelim .
Pencereye mousle sağ tık yapıp repater to send yazana tıklıyabilir veya daha basiti CTRL + R yaparak gönderebiliriz.

Öncelikle hiçbir bypass yöntemi denemeden normal basit bir payload girelim.

```
stockApi=http://localhost/
```

Response bakalım ne dönmüş.

.

Response

Pretty Raw Hex Render

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"
```

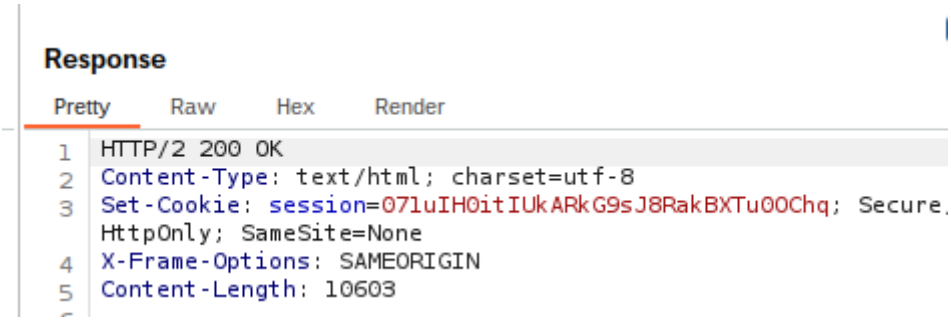
Evet kötü istek olarak algılandı. Şimdi çeşitli bypass yöntemlerimizi deniyelim.
Bizim ilerliyeceğimiz adımlar şunlar.
/localhost/admin/ öncelikle adminden önce localhosta ulaşmamız gerekiyor ilk onu bypas etmemiz gerek. Bunun için diğer çeşiştli local host olarak algılayacağı encoder şifreleme işlemleri 127.0.0.1 veya 127.0.1 gibi işlemler gerçekleştiricez.

Burada anlaşılan localhost dizinini yazmamızı engellemiş. Ben sizi fazla sıkmamak adına 127.0.1' i denicem en başta , çünkü 127.0.0.1 de blacklist içerisinde .

```
stockApi=http://127.0.1/
```

Deneyelim dönen response bakalım.

.

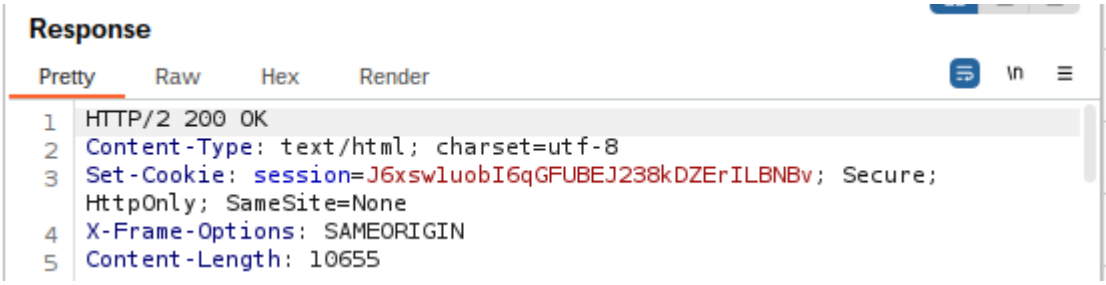


Ve evet değerimizi localhost olarak algıladı ve engeli aştık. 200 statüs kod döndü. Bu işlem başarılı demek. 200-299.

Ama bunu atlatmanın bir yolu daha var ip adresleri ondalıklı ve decimal değerlerden oluştuğu için 127.0.0.1 değerini decimale çevirdiğimizde de yasaklı olan 127.0.0.1 yazmanın farklı bir yolunu bulmuş oluruz, yani sonuca ulaşmış oluruz. Deniyelim.

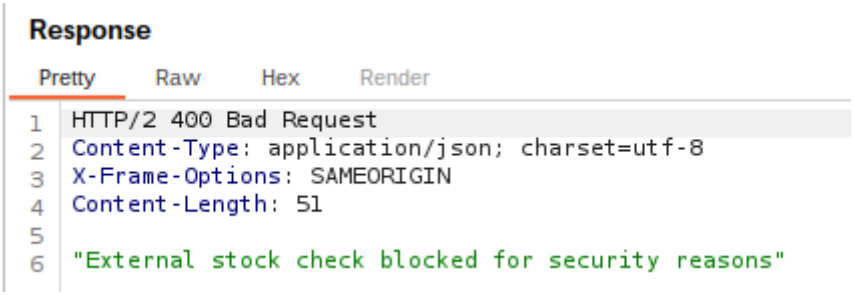

```
stockApi=http://2130706433/
```

.



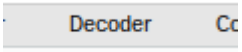
Gördüğünüz gibi 2. yolumuzda çalıştı ama daha kısa olduğundan dolayın 127.0.1 kullanma benim tercihimdir.
İp adresini decimale dönüştürdüğüm kaynak: https://www.ipaddressguide.com/ip

Şimdi localhosta ulaşabildik sırada kaldı admin dizini bunuda deniyelim .
Yani http://127.0.1/admin yazalım.



Galiba admin kelimesini yasaklamış.
İp adresini Decimale dönüştürdüğümüz gibi bunda da web sitenin anlaması için url' e encode yapabiliriz.

Encoder işlemi için Burp Suite' nin kendi içerisinde üst barda bulunan Decoder kısmından yardım alabiliriz.



.

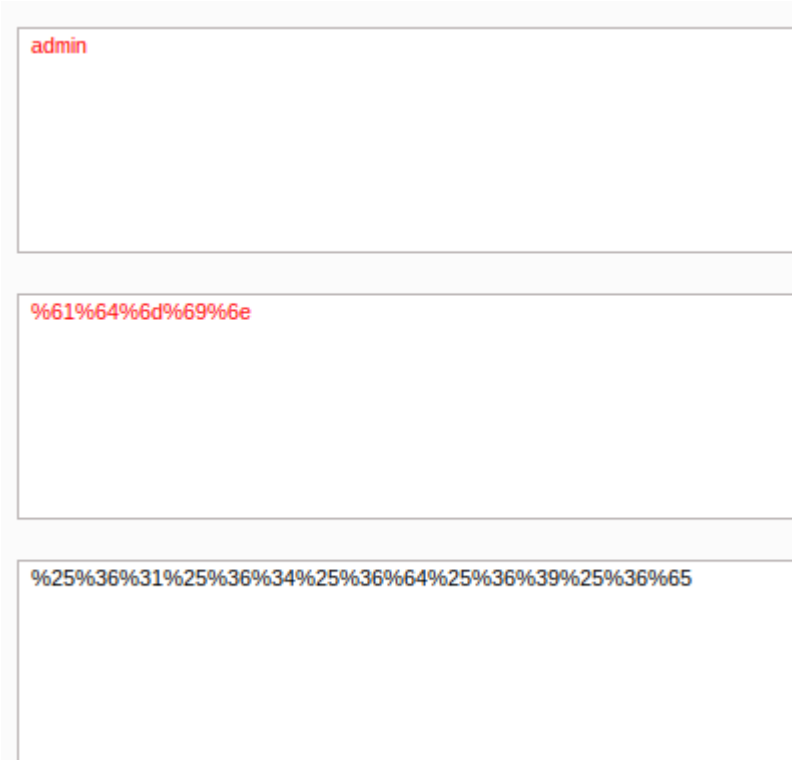
Sağ tarafta Encode ass.. kısmına gelip oradan URL seçerek encode halini alt kısmında veriyor bunu deniyelim.

.

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 51

"External stock check blocked for security reasons"
```

Yine kötü istek olarak algıladı. Url' i sistem galiba kendi içerisinde decode edip yasaklı kelimeyi bulmuş.
Bir defa daha encode işlemi yapalım. Yani Şu şekil;



Deniyelim.

```
stockApi=http://127.0.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Set-Cookie: session=G66tsyO5S14P246EuuTayJn2YDbBvqyr; Secure; HttpOnly
 SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 3074
```

Ve çalıştı. Response dikkat edelim , carlos kullancısı hakkında bir şeyler var mı. Bizden Carlosu silmemizi istediğine göre , bir silme butonu olmalı,silme butonunda da büyük ihtimalle bir $_GET isteği yaparak bir url' e bu kullanıcyı silmesi için link gömülmüş olmalı.

```
<div>
  <span>
    carlos -
  </span>
  <a href="/admin/delete?username=carlos">
    Delete
  </a>
</div>
```

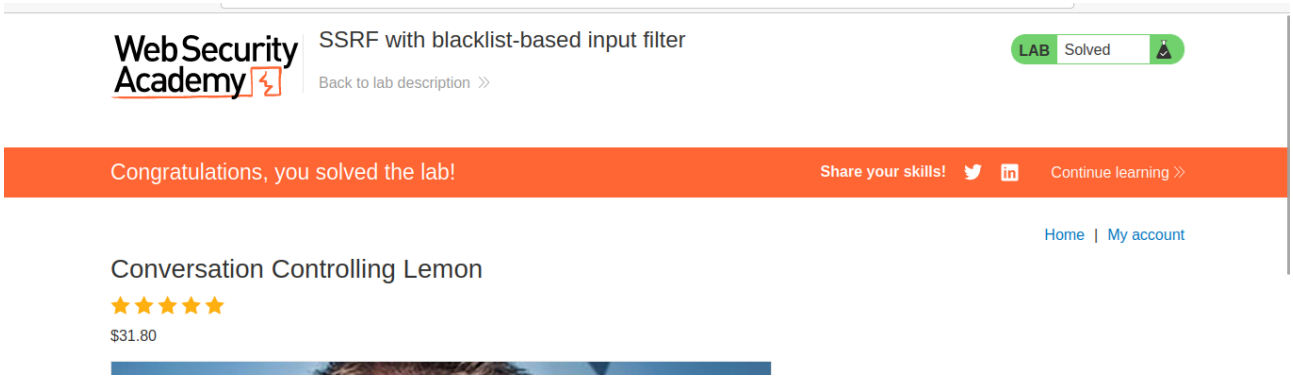
Evet tam olarak burada. Admin kısmını almiyacağız çünkü zaten admin dizinindeyiz.

Bir .

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=1DS8NiaKdN7ZvyhxGtmdQ1w8fZT2hZNq; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
```

yönlendirme isteği gerçekleşti galiba işe yaradı bu stockapi' ye yazdığımız payloadımızı proxy kısmından yerleştirip forward diyerek isteğimizi gönderelim.

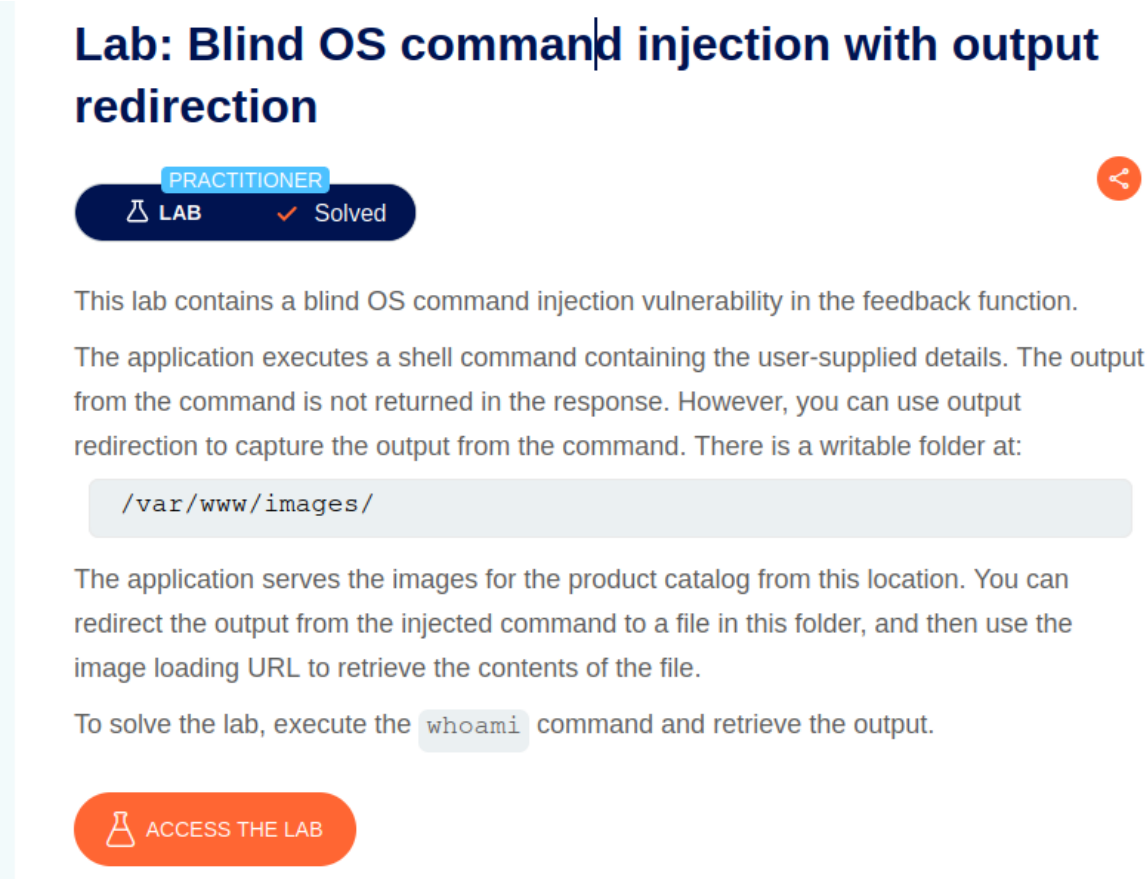
İsteğimizi gönderelim.



Ve kullanıcımızı sildik.

SSRF BİTTİ

2. Zafiyet ; "**OS Command İnjection**"
Platform ; Port Swigger / Web Academy
LAB LİNKİ ; https://portswigger.net/web-security/os-command-injection/lab-blind-output-redirection



Bu zafiyetimiz OWASP' ın 1. sırada yer alan İnjection başlığı altında OS Command adında geçiyor.

OS Command öncelikle nedir; OS(İşletim sistemi) Command zafiyeti web sitenin barındığı makine' ye bağlı komutların değişkenlik gösterecek şekilde, çalıştığı makineye , web siteden işletim sistemine uzaktan komutları çalıştırmaya denir.

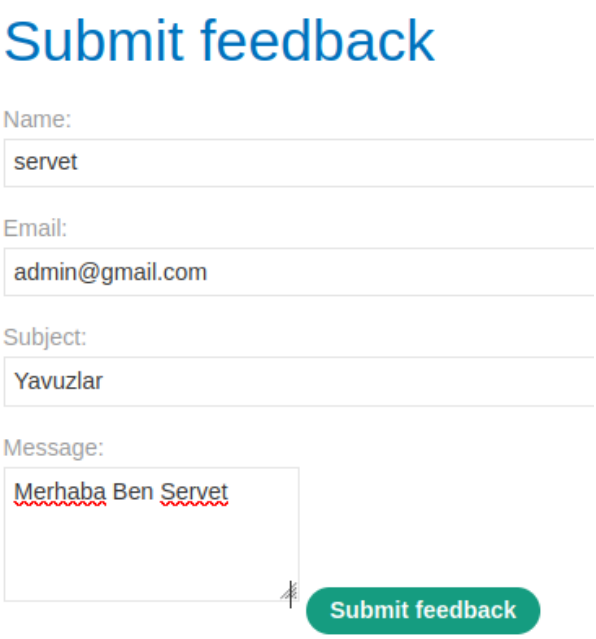
Bu açıklamada bize şunu söylüyor;

Bu laboratuvar, geri bildirim işlevinde kör bir işletim sistemi komut ekleme güvenlik açığı içeriyor.
Blind yani kör' den kastı bizim request(istek) 'imizi http responselarında / cevaplarında bizlere çıktıyı vermemesidir.

Ve diyor ki */var/www/images/ böyle bir dizin var, zafiyet Blind olduğu için mesela uname komuutu çalıştırdığımızda bize http yanıtlarında vermicektir. Ama bu dizine txt dosyası olarak atabilirsek okuruz. Zaten images diye dizin varsa , bize vereceği web adresinde fotoğraflar bulunuyor.*
Ve son olarak bizden "WHOAMİ" komutu çalıştırmamızı söylüyor.

.

Evet sayfamız bu şekilde, dediğim gibi görsellerimiz bulunuyor. Ve zafiyetimizin bulunduğu geri bildirim kısmı sağ üst köşede, "Submit Feedback" .

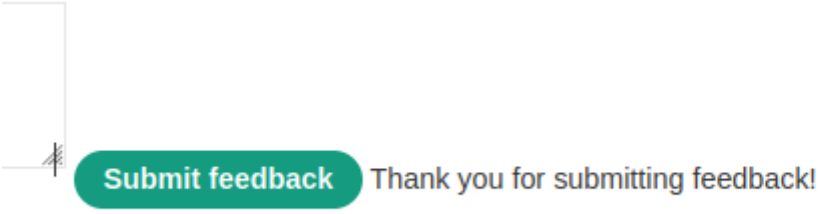


Bu şekilde isteği göndericem. Arkada Burp Suite Açık şekilde.

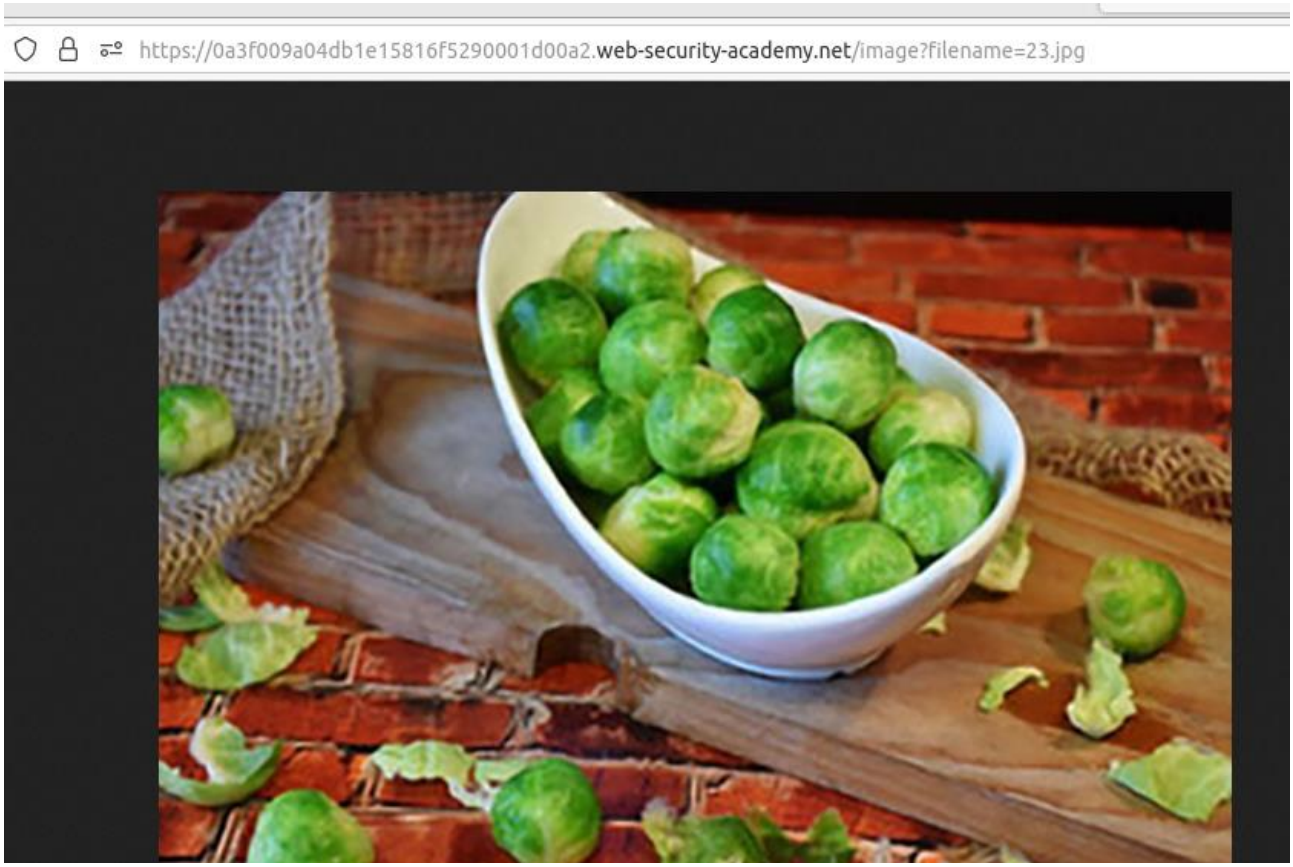
Ve isteği yakaladım, email headerine gelip, başta pipe | attık bunun sebebi bir den fazla tek satırda komut çalıştırmak için. Sonra komutumuzu yazdık ve > yönlendirdik ardından, bize bahsedilen dizine pathi verdik ve yavuzlar.txt adında bir dosyaya whoami komutunun çıktısını oraya yazmasını istedik.
Peki bu "var www imagesi " dizini doğrulamak amaçlı bir görseli yeni sekmede aç diyip de kontrol edebiliriz.

Ama ilk önce bu isteğimizi gönderelim bakalım geri bildirimi kabul edicek mi ?

Evet *geri*



bildirimi kabul etti, bu mantıkla dosyamızı da oluşturmuş olması gerekmekte.



.

Herhangi bir resmi yeni pencerede açtım, gördüğüzün gibi pathimizi doğru. Eğer bize path verilmeseyedi, önceden bu araştırmaya kayolumamız gerekiyordu.
Şimdi ise görsel ismini silip dosyamızın adını yazalım.

Ve karşımıza whoami komutunun çıktısını almamız gerekiyor. Labımızı bu şekilde bitirmiş olduk.

Web Security Academy

Blind OS command injection with output redirection

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning