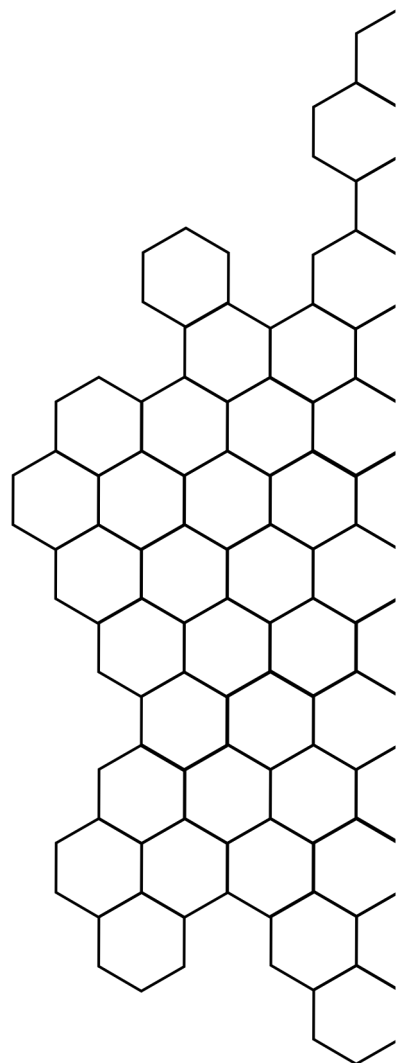
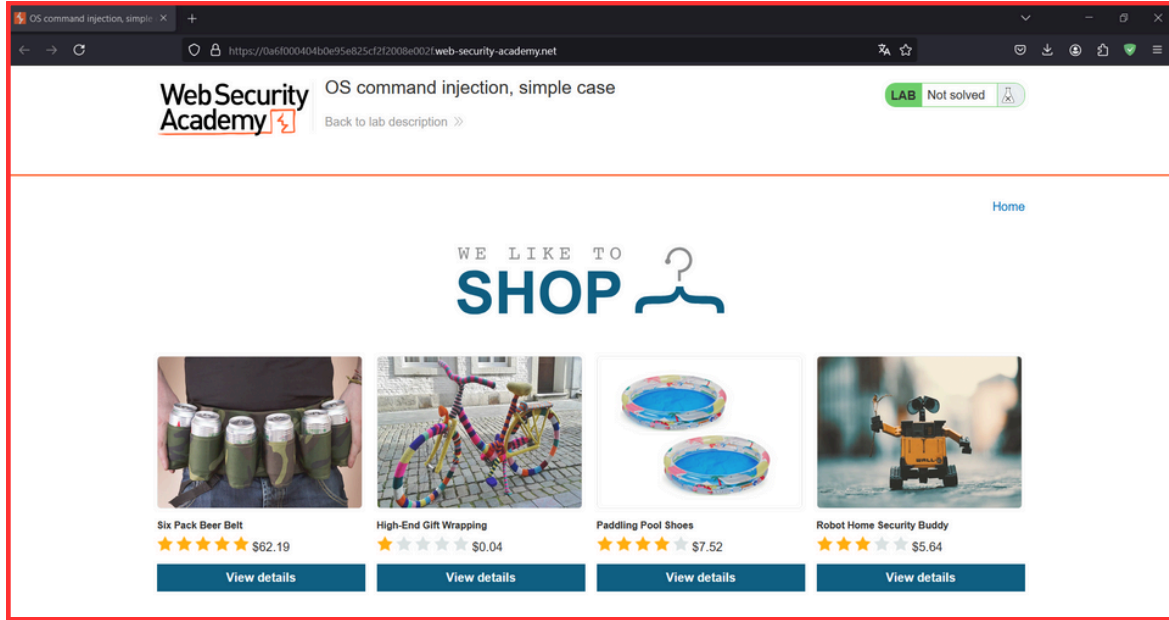


INJECTION

LAB 3

TARİH: 29.08.2024

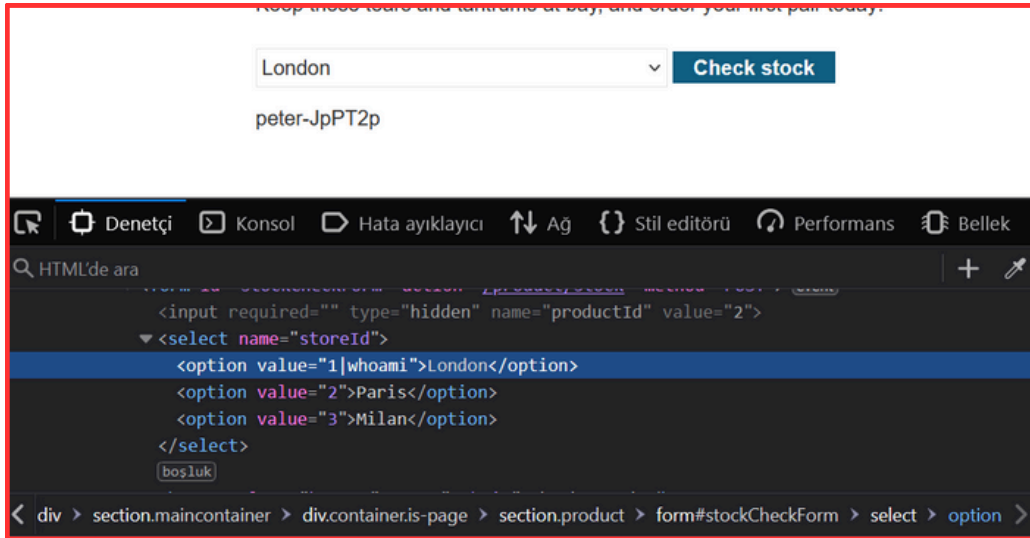




Bu sitede de bizden bir command injection zafiyeti bularak whoami komutunu çalıştırmamız isteniyor. Bu zafiyet için siteyi biraz araştıralım.

Ürünlerden birinin sayfasına girip en aşağı indiğimizde stok kontrol edebileceğimiz bir buton gördüm. Burada komut çalıştırıp çalıştıramayacağımı denemek için HTML kodları içinden seçeneklerin değerini değiştirdim.

```
<input required="" type="hidden" name="productId" value="1" />
<select name="storeId">
  <option value="1|whoami">London</option>
  <option value="2">Paris</option>
  <option value="3">Milan</option>
</select>
```



Değerini değiştirdiğim seçenek seçiliyken butona tıkladığımda bana whoami komutunun çıktısını getirdi. Böylece lab tamamlandı.

