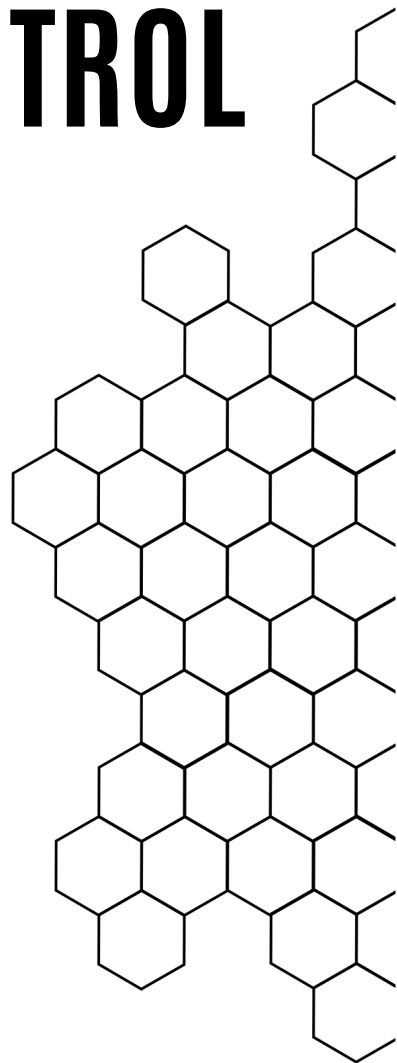
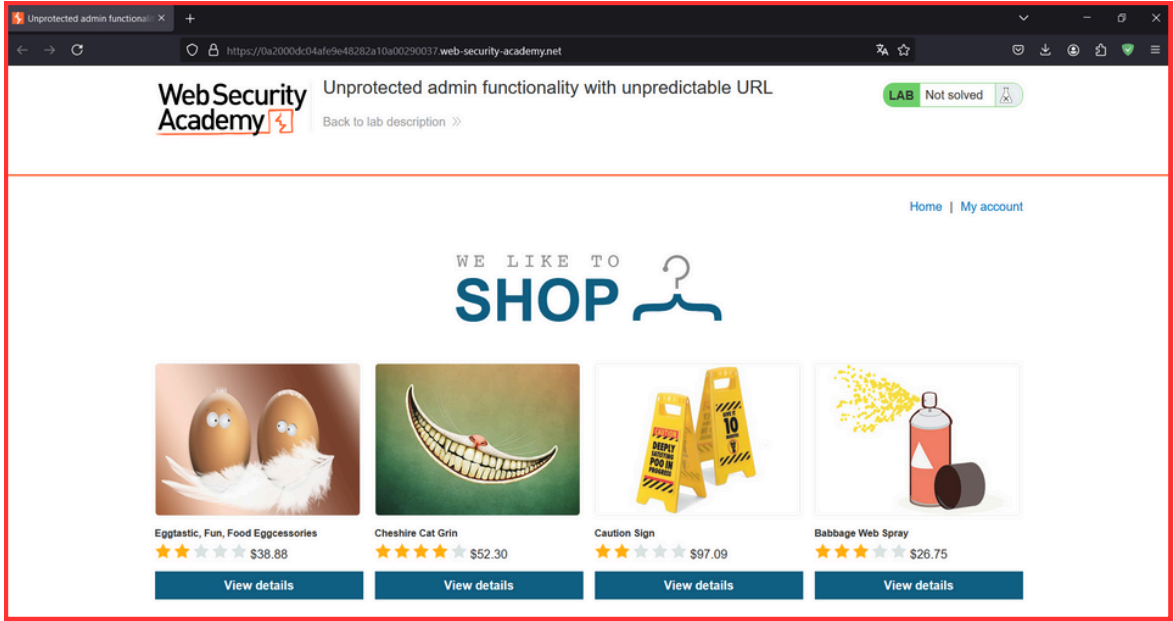


BROKEN ACCESS CONTROL

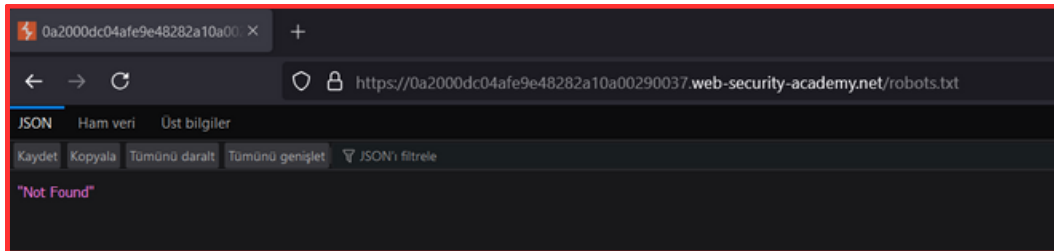
LAB 2

TARİH: 28.08.2024





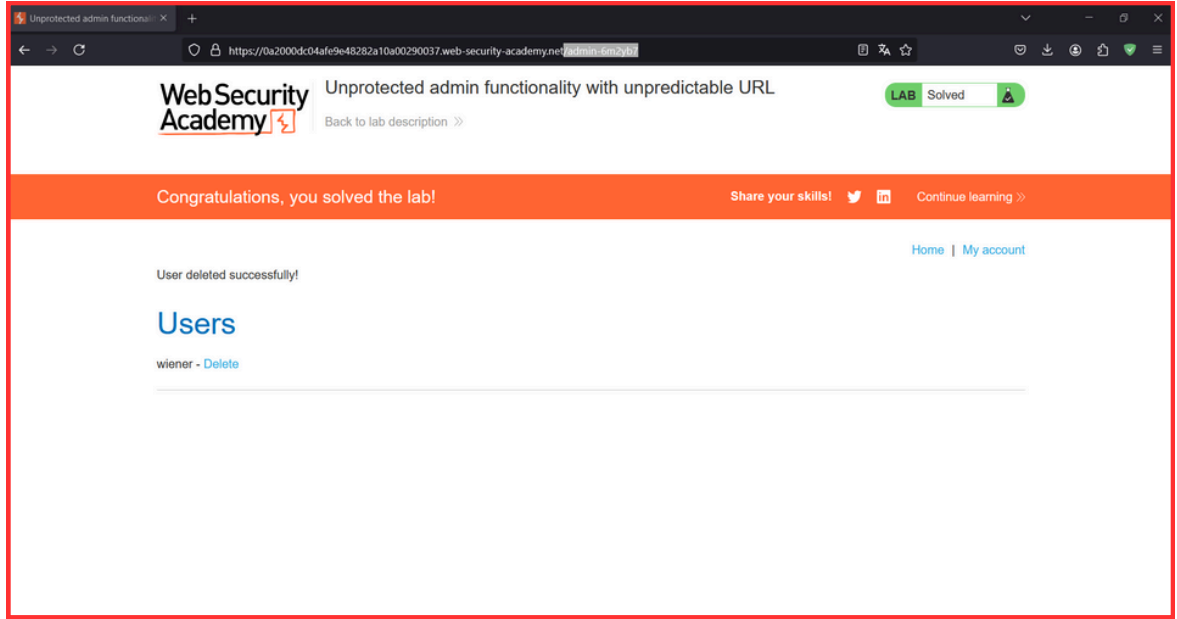
Sayfaya giriş yaptım ve öncelikle gizli dizinleri tespit etmek için robots.txt dosyasını kontrol ettim.



Robots.txt dosyası bulunmadığı için gizli bir dizine de ulaşamadım. Bu yüzden tekrar ana sayfaya dönerek siteyi incelemeye karar verdim.

```
Unprotected admin functional... X https://0a2000dc04afe9e48282a10a00290037.web-security-academy.net/
view-source:https://0a2000dc04afe9e48282a10a00290037.web-security-academy.net/
22 </p>
23 </div>
24 </div>
25 </div>
26 <div class="widgetcontainer-lab-status is-notsolved">
27 <span>LAB</span>
28 <p>Not solved</p>
29 <span class="lab-status-icon"></span>
30 </div>
31 </div>
32 </div>
33 </div>
34 </div>
35 <div theme="ecommerce">
36 <section class="maincontainer">
37 <div class="container">
38 <header class="navigation-header">
39 <section class="top-links">
40 <a href="/home/"><p></p></a></p>
41 </script>
42 var isAdmin = false;
43 if (isAdmin) {
44 var topLinksTag = document.getElementsByClassName("top-links")[0];
45 var adminPanelTag = document.createElement("a");
46 adminPanelTag.setAttribute("href", "/admin-6m2yb7");
47 adminPanelTag.innerText = "Admin panel";
48 topLinksTag.appendChild(adminPanelTag);
49 var pTag = document.createElement("p");
50 pTag.innerText = " ";
51 topLinksTag.appendChild(pTag);
52 }
53 </script>
54 <a href="/my-account/">My account</a><p></p>
55 </div>
56 </div>
57 <div class="notification-header">
58 </div>
59 <div class="ecommerce-pageheader">
60 
61 </div>
62 <div class="container-list-tiles">
63 <div>
64 
65 <h3>Eggastic, Fun, Food Eggcessories</h3>
66 
67 $38.88
68 <a class="button" href="/product?id=1">View details</a>
```

Ana sayfaya dönüp HTML kodlarını incelediğim JavaScript kodları içerisinde bir admin dizini farkettim.



Kod içerisinde belirtilen dizine gittiğimde yine kullanıcıları silebildiğimiz sayfaya karşılaştım. Burada da yine carlos kullanıcıasını silerek labı tamamladım.