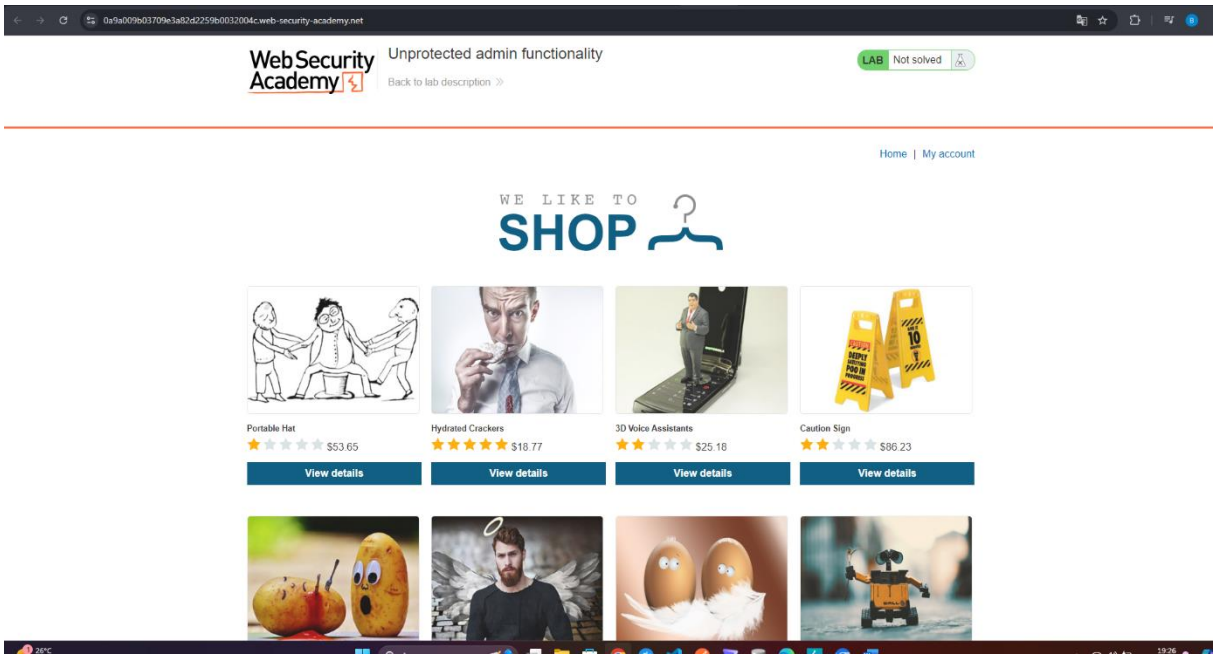
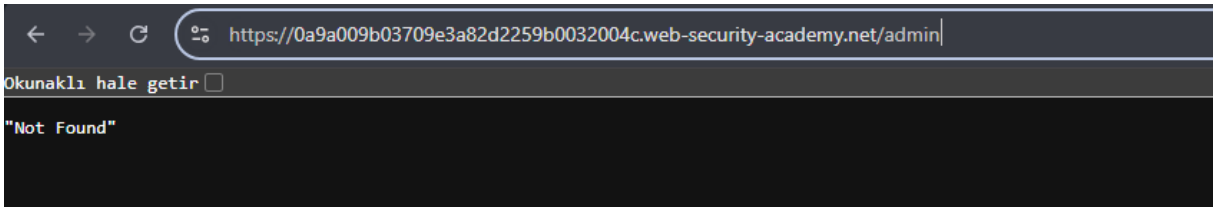
Broken Access Control

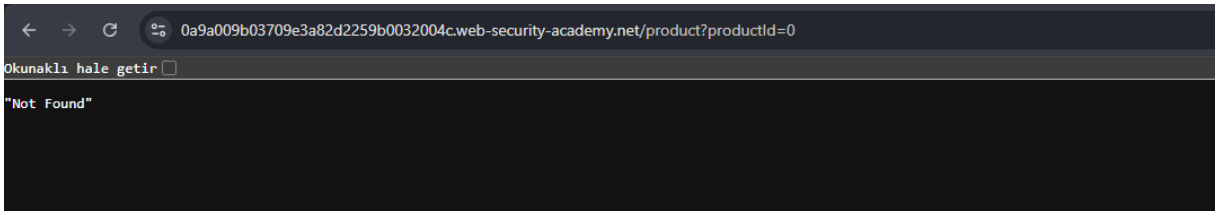
Broken Access Control, kullanıcıların erişim yetkilerinin kontrol edilmediği ya da yanlış yönetildiği durumlarda ortaya çıkar. Aşağıda Portswigger ile yapılmış birkaç örnek vardır.



İlk Labtaki siteye giriyorum. (İlk denememde SQL injection denedim, Broken Access olduğunu unuttum)

Herhangi bir ürüne tıkladığımda ürünlerin ID lerini değiştirdim ve bazı yöntemler denedim.





Broken Access Control zafiyetini araştırırken admin url'i robots.txt gibi dosyada da tutulabileceğini gördüm.

Korumasız işlevsellik

En temelde dikey yetki yükseltme, bir uygulamanın hassas işlevsellik üzerinde herhangi bir koruma uygulamadığı durumlarda ortaya çıkar. Örneğin, yönetim işlevlerine bir yöneticinin karşılama sayfasından bağlantı verilebilir, ancak bir kullanıcının karşılama sayfasından bağlantı verilmez. Ancak, bir kullanıcı doğrudan ilgili yönetici URL'sine göz atarak yönetim işlevlerine kolayca erişebilir.

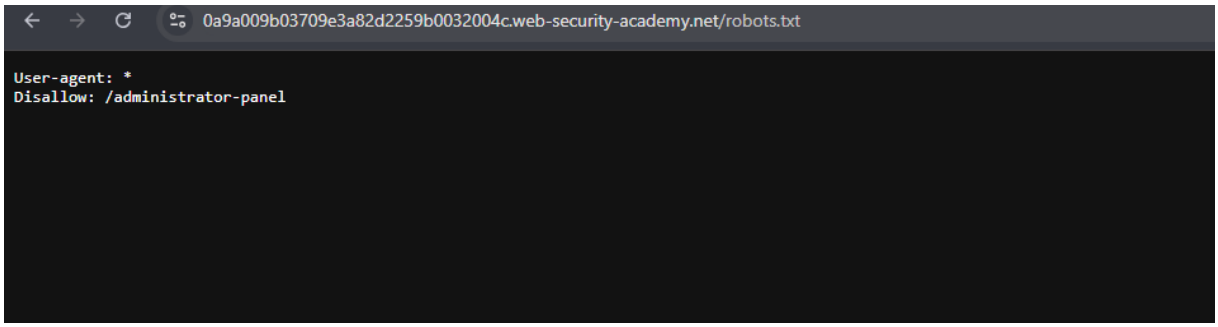
Örneğin, bir web sitesi hassas işlevleri aşağıdaki URL'de barındırabilir:

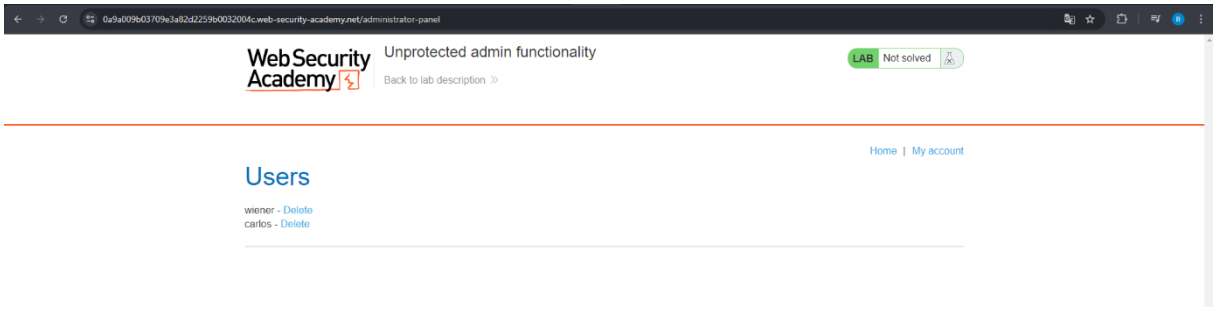
Bu, yalnızca kullanıcı arabirimlerindeki işlevselliğe bağlantısı olan yönetici kullanıcılar tarafından değil, herhangi bir kullanıcı tarafından erişilebilir olabilir. Bazı durumlarda, yönetim URL'si `robots.txt`dosya gibi başka konumlarda açıklanabilir :

URL herhangi bir yerde ifşa edilmemiş olsa bile, bir saldırgan hassas işlevselliğin konumunu kaba kuvvetle belirlemek için bir kelime listesi kullanabilir.

(https://www.ozztech.net/siber-guvenlik/broken-access-control-acigi-nedir/)

Siteye tekrar girip robots.txt dosyasını yazdığımda karşıma yönetim url' çıktı.

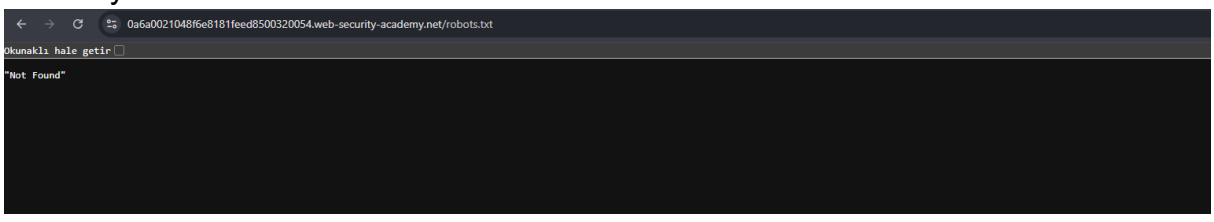




Sistemden Carlos'u sil görevini yaptıktan sonra lab'ı tamamlamış oluyoruym.

İkinci Lab'ta ise daha önce okuduğum yazının devamında olan hatayı görüyorum.

İkinci Lab'a girdiğimde robots.txt dosyasını çağırıyorum ama bu sefer not found ile hata alıyorum.



Login ekranına gidiyorum ve sayfanın kaynak koduna bakıyorum.

```
            <div class="container is-page">
                <header class="navigation-header">
                    <section class="top-links">
                        <a href=/>Home</a><p>|</p>
                        <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-y69nna');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
                        <a href="/my-account">My account</a><p>|</p>
```

Login ekranında doğrulandığı taktirde hangi konuma gönderileceğini scrpit kodları içinde görünür halde yazılmış. Görevim olan Carlos kullanıcısını silerek Lab'ı tamamlıyorum.