CSRF

Cross Site Request Forgery açılımıdır. Bilindiği üzere birçok web uygulaması cookie (Çerezler) kullanır. Bunun başlıca nedeni kullanıcı hakkında özel ayarlar, oturum yönetimi, reklam önerileri gibi sebeplerdir. Günümüzde en çok kullanılan alanlardan biri de alışveriş ve banka uygulamalarıdır.

Peki nedir bu CSRF?

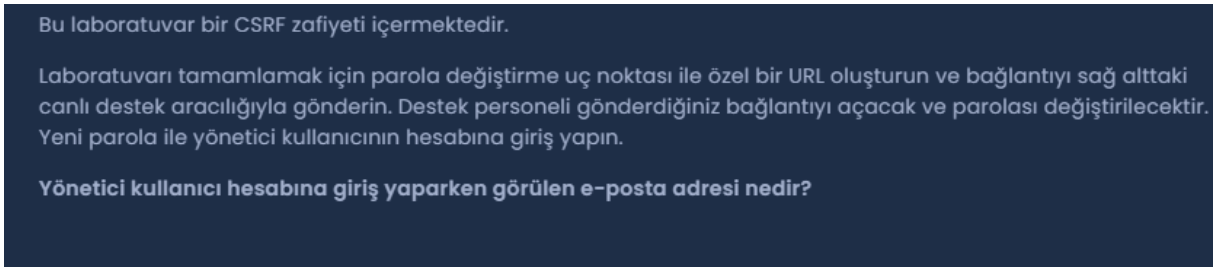
Çerezler bilindiği üzere kullanıcıya ait bilgileri taşıyabilirler. Tam da CSRF zafiyeti saldırganın, kullanıcının isteği dışında istek göndermesine sebep olan bir açıktır. Genellikle önceden hazırlamış zararlı bir web sitesine gönderilir fakat bazı durumlarda bu böyle olmayabilir. Örnek olarak açıklayacak olursak, bir uygulamanın destek mesaj box' una bu zararlı URL'i gönderebiliriz. Ve eğer ki kontrol düzgün sağlanamazsa sistemin kendisine de zarar verebiliriz.

Örnek senaryo olarak para gönderme uygulaması olsun ve bu uygulamanın bir de cevapları alıp işleyen bir destek kısmı olsun. (Bankalarda, yemek sitelerinde kullanılan yapay zekâ destekli müşteri hizmeti kısmı içinde olabilir) CSRF zafiyeti olduğunu varsaydığımız bu sitede eğer ki doğru URL i bulabilirsem kendime para akışı sağlayabilirim.

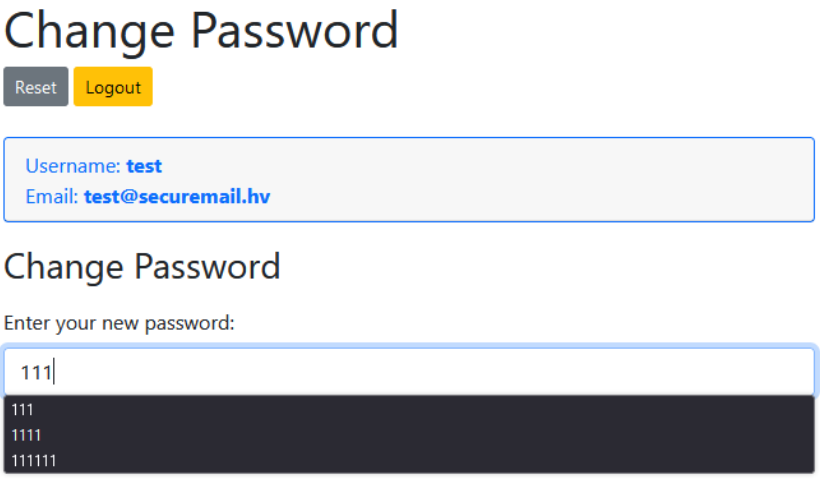
Mesela ben bu zafiyetli sitede para gönderimi yapacağım sırada burp ile araya girip URL i çıkartabilirim. Sonra- Bu zafiyet geçerliyse – mesaj Box' a gelip bu url i gönderirsem (Alıcı hesap bilgilerinin doğru bir şekilde işlenebildiğinden emin olun) kendime para akışı sağlamış olabilirim.

Bu zafiyetin en iyi çözüm yolu ise Token kullanmaktır. Gelen istek kullanıcıya verilen token ile karşılaştırılıp eşleniyorsa istek kabul edilir.

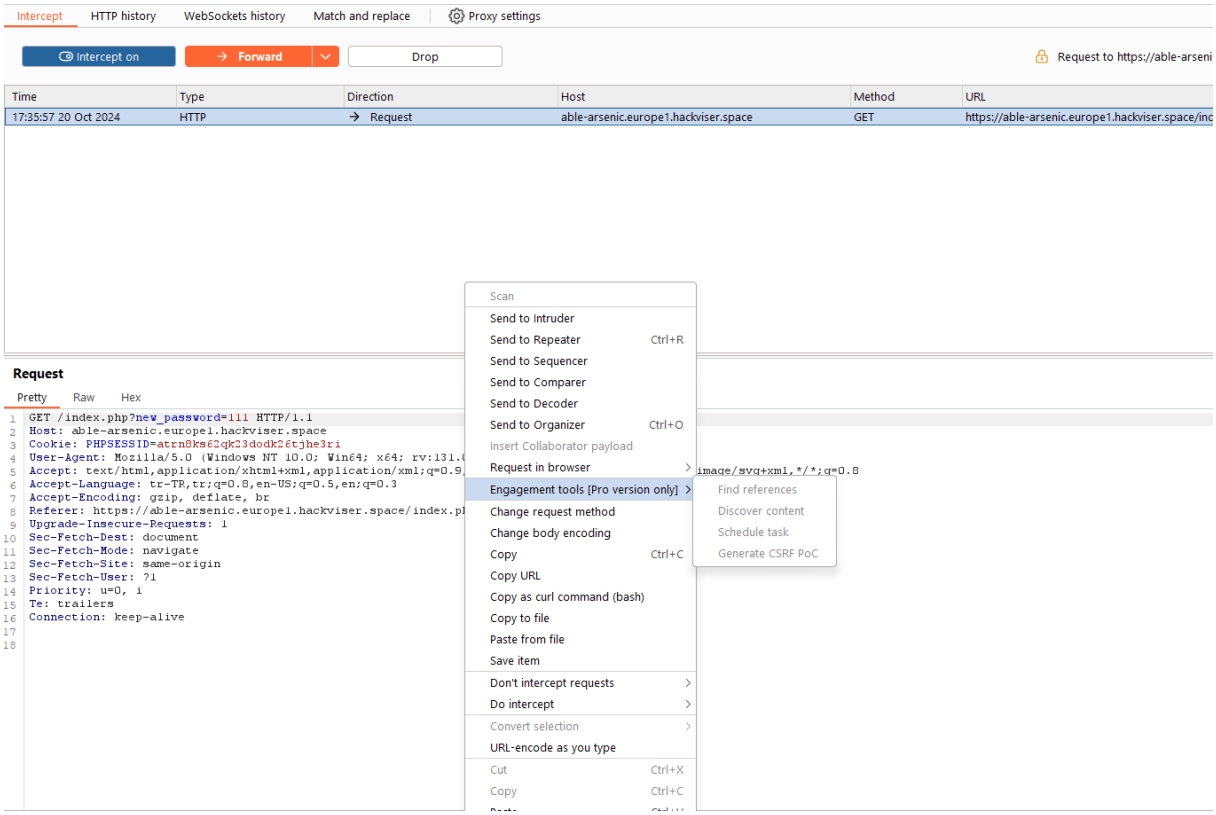
Örneklerin iyice pekişmesi için örnek Labımıza geçelim.



Görevimiz, oluşturacağımız zararlı URL bağlantısını destek paneline atmamızı istiyor. Personelin açacağı söyleniyor. Tekrar etmekte fayda var, otomatik cevaplandırmalarda hiçbir güvenlik önlemi olmayan durumlar için de geçerlidir.

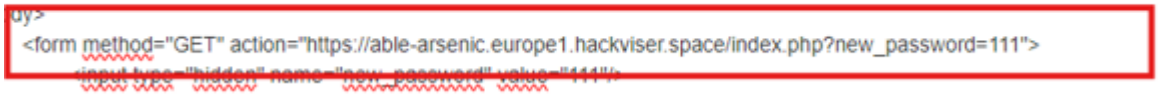


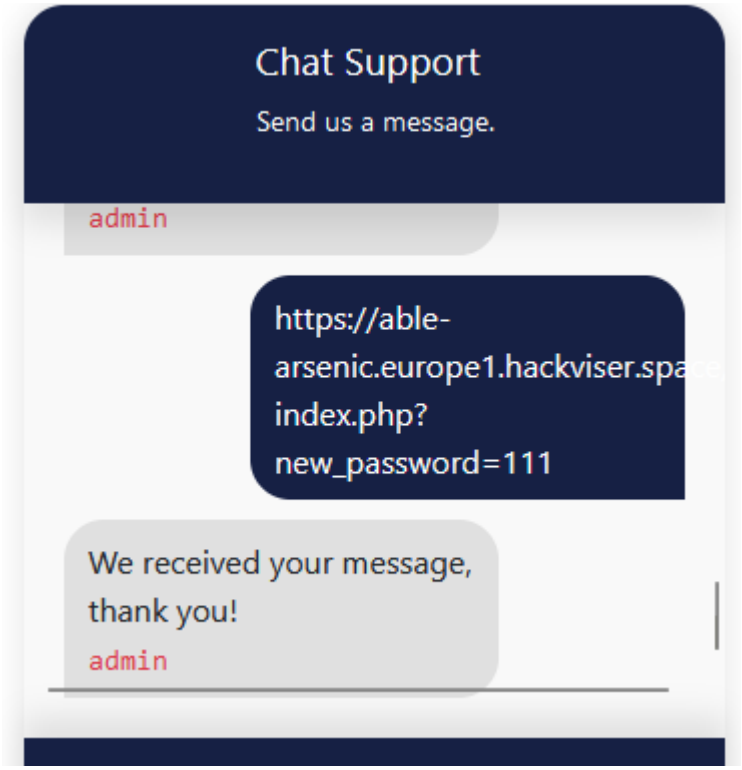
Öncelikle kendi hesabımdan bir parola değiştirme sayfasına giriyorum ve parolamı onaylamadan hemen önce burp ile araya girip isteğimi inceliyorum.

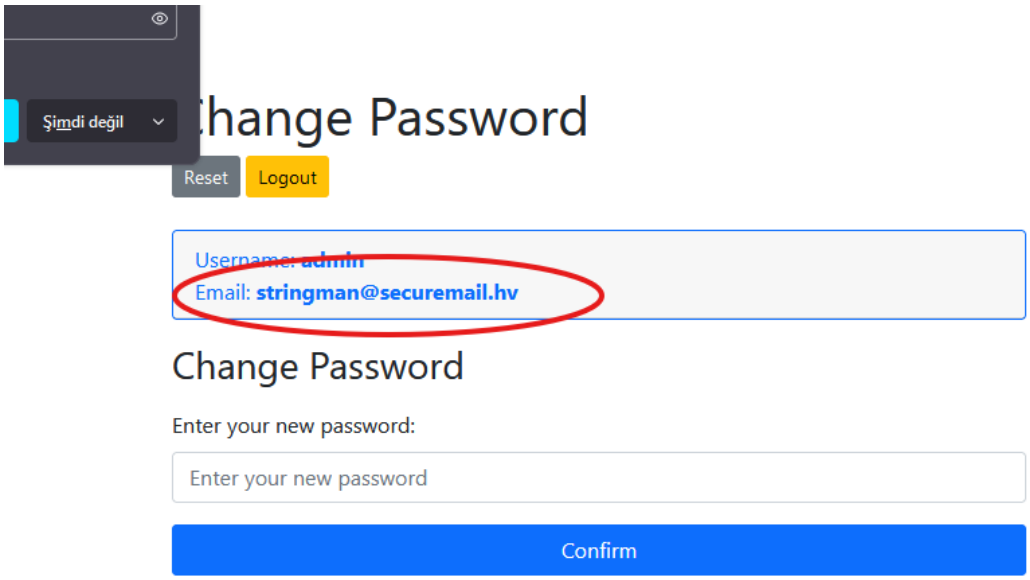


Burp aracının kendi pro özelliği olan Generate CSRF açık olmadığından online site üzerinden işlemime devam ediyorum. Bu özellik, response sayfasını html sayfasına eçvirip görüntülememizi sağlıyor.

Belirli bir sitede işlemime devam ediyorum ve form etiketimin Action attirbute' ünü kopyalıyorum. Bir sonraki işlemim bu url'i canlı destek hattına atmak olacak.







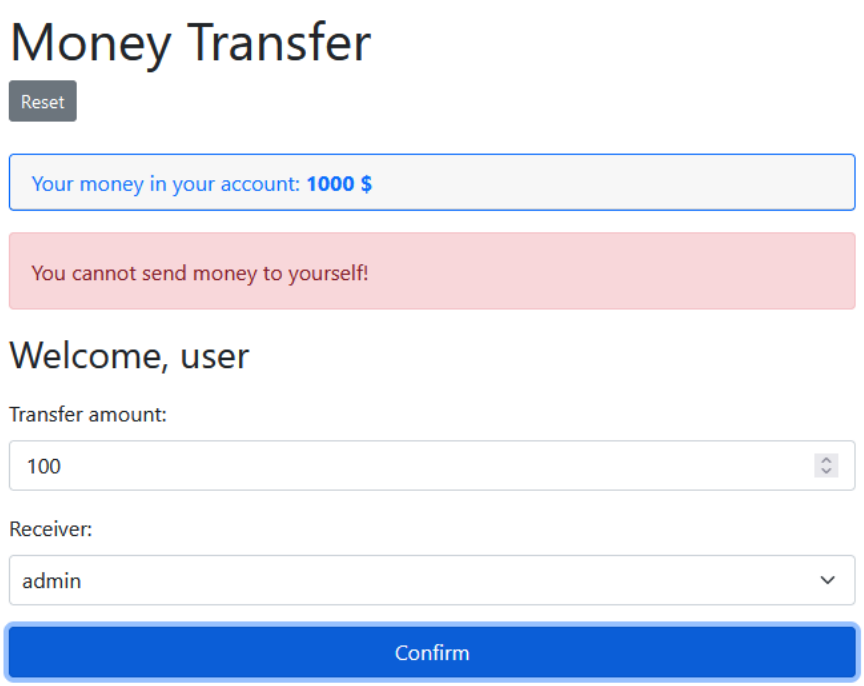
Admin hesabına kendi belirlediğimiz şifre ile girmiş bulunmaktayız.

Bu laboratuvar bir CSRF güvenlik açığı içermektedir.

Laboratuvarı tamamlamak için, hesabınıza para aktarmak için bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı çalıştıracak ve istemeden hesabınıza para aktaracaktır.

Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

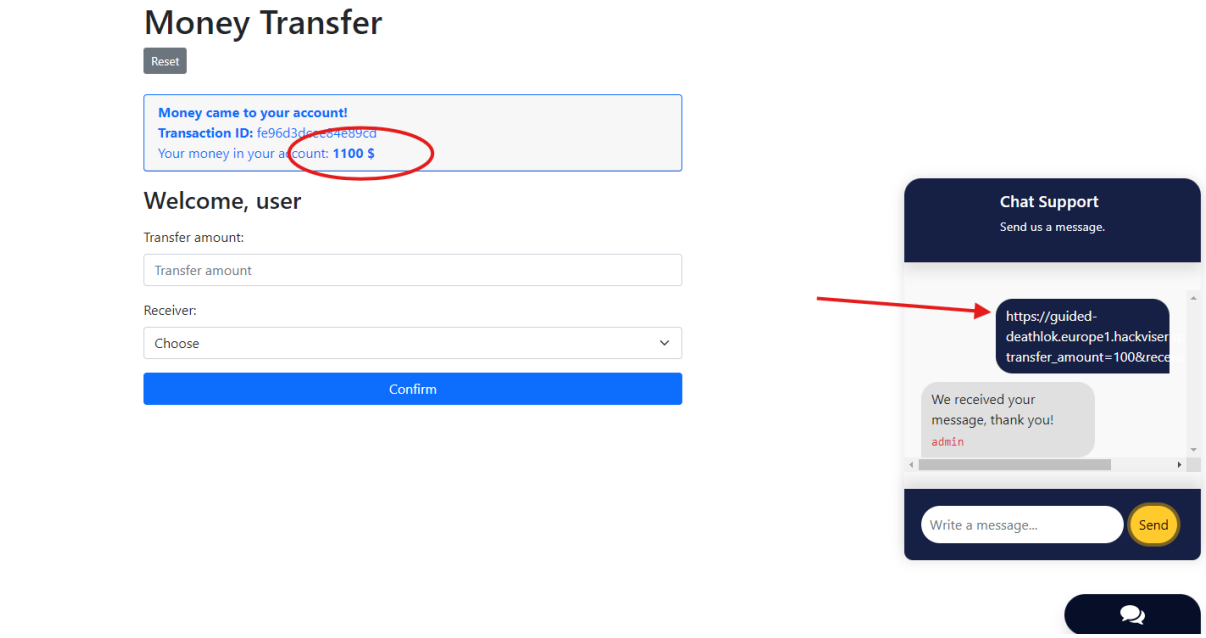
Bu senaryoya göre ise kendimize para aktarımı yapmamız gerekmektedir.



Aynı işlemleri tekrarlayarak örnek para gönderme isteği atıyorum ve bunu burp ile yakalayıp html sayfasına döndürüp url i kopyalıyorum. Url'de receiver kısmını kendi username'inizi yapmayı unutmayın.

CSRF PoC FORM

```
<html>
    <body>
        <form method="GET" action="https://guided-deathlok.europe1.hackviser.space/index.php?transfer_amount=100&receiver=user">
            <input type="hidden" name="transfer_amount" value="100"/>
            <input type="hidden" name="receiver" value="admin"/>
            <input type="submit" value="Submit">
        </form>
    </body>
<html>
```



Bu labımızı da başarılı bir şekilde tamamlamış olduk!