CHANGE PASSWORD WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında CSRF zafiyetinin Change Password labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar bir CSRF zafiyeti içermektedir.

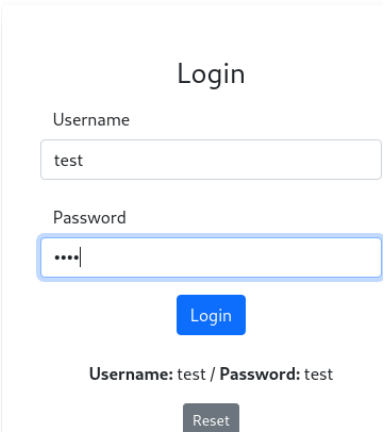
Laboratuvarı tamamlamak için parola değiştirme uç noktası ile özel bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı açacak ve parolası değiştirilecektir. Yeni parola ile yönetici kullanıcının hesabına giriş yapın.

Yönetici kullanıcı hesabına giriş yaparken görülen e-posta adresi nedir?

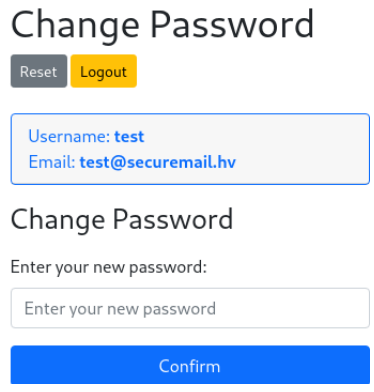
ÇÖZÜM:

CSRF: Sitenin açığından faydalanarak siteye sanki o kullanıcıymış gibi erişerek işlem yapmasını sağlar.

Şimdi labımızı çözmeye başlayalım. Siteye girelim.



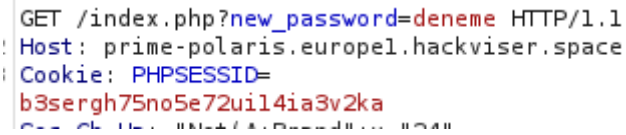
Bizi bir login sayfası karşılıyor. Test:test ile giriş yapıyoruz.



Şimdi bu isteklerin ikisini de Burp Suite programına atalım.

Giriş yaparken elimizde bir cookie olduğunu gördük. Ama bu cookie bizim işimize bu labta çok yaramayacak gibi duruyor.

Şimdi giriş yaptıktan sonra şifre değiştirme kısmına deneme yazıp buranın da Burp ile isteklerini yakalayıp inceleyelim.



Bu kısım şifre değiştirme kısmı.

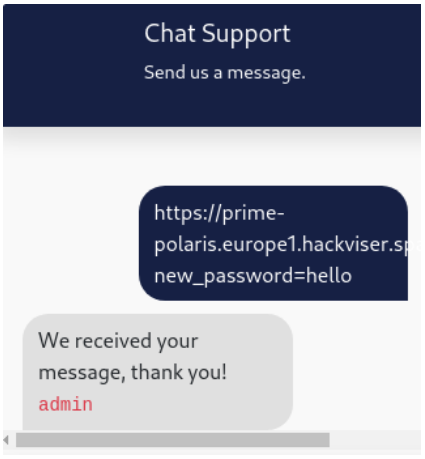
Şimdi bu şifre değiştirme kısmında dikkat çeken bir kısım var. URL sonuna /index.php?new_password= yazıp girdiğimiz değeri buraya ekliyor. Ama bunu GET isteği ile yani URL üzerinde yapıyor. Bu kısımda bir CSRF açığı mevcut.

Bize senaryoda da bahsettiği gibi biz canlı desteğe mesaj atarak bu CSRF açığından yararlanacağız.

Şimdi URL'i tam anlamı ile hazırlıyoruz.

https://prime-polaris.europe1.hackviser.space/index.php?new_password=hello

Şimdi bunu canlı destek kısmına yazalım ve gönderelim.



Şimdi şifrenin gerçekten değişip değişmediğini öğrenmek için admin:hello şeklinde giriş yapmayı deneyeceğim.

Ve başarılı bir şekilde giriş yaptık ☺

Cevap: **stringman@securemail.hv**