Cross Site Request Forgery (CSRF)

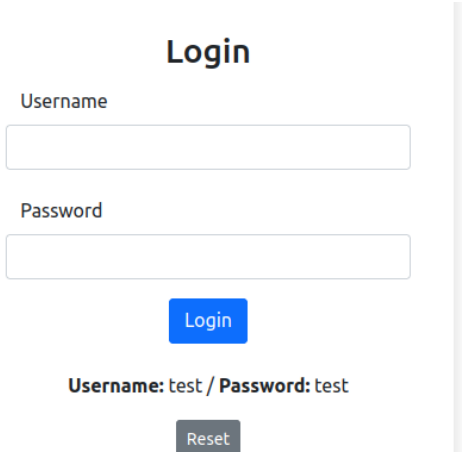
Nedir : Bir kullanıcının tarayıcısı üzerinden, kullanıcının isteği dışında bir işlem gerçekleştiren kötü niyetli bir saldırıdır.
Önlem: CSRF'yi önlemek için, her formda bir CSRF tokeni kullanılmalı ve kullanıcı oturumları için güvenlik kontrolleri uygulanmalıdır.

8.1 Change Password

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

ÇÖZÜM

Sitede karşımıza giriş ekranı ve bizlere verilmiş bir test:test kullanıcı görüyoruz.



Amacımız Admin kullanıcısının parolasını değiştirip hesabına girmek.

Giriş yapınca bizi böyle bir ekran karşılıyor parola değiştirme alanı bu test kullanıcısını değiştiriyor. Bizim amacımız Admin kullanıcısınıkini değiştirmek, bunun için adminle iletişime geçmemiz gerekiyor bu soruda.
Bunuda destek ekibinden yapıcaz. Sitenin sağ alt köşesinde bulunuyor.

Evet mesajlarımıza admin bakıyor, ona bir link gönderebiliriz ve o linke basınca otomatik olarak kendi parolasını değiştiretebiliriz. Öncelikle url göndermek için nasıl bir url göndereceğimizi bilmemiz gerekiyor bunun için Burp Suite ile dinliyelim, isteği.

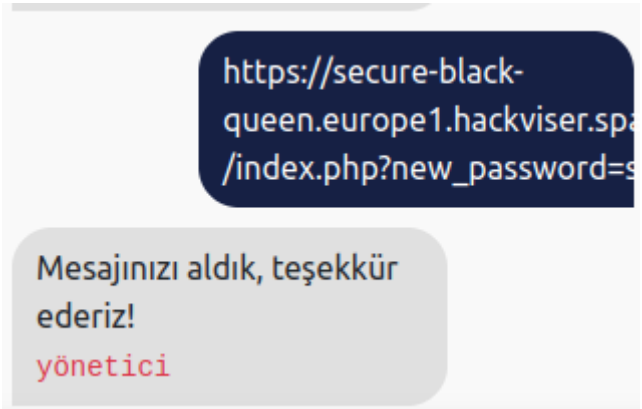
```
GET /index.php?new_password=servet
```

İsteğimiz bu şekilde birde full url'imize bakalım.

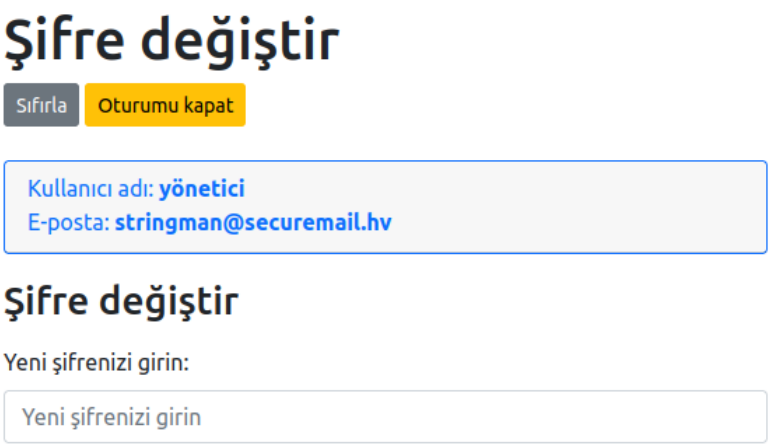
https://secure-black-queen.europe1.hackviser.space/index.php

Bu da bizim url'imiz göründüğü üzere index.php?den sorna fonksiyon var. Bu urlleri birleştirince ortaya bu çıkıyor.

https://secure-black-queen.europe1.hackviser.space/index.php?new_password=servet
bunu destek ekibe atalım.



Mesajımızı aldı , admin:servet olarak giriş yapmayı deniyelim.



Ve başarıyla giriş yaptım.

Cevap : stringman@securemail.hv