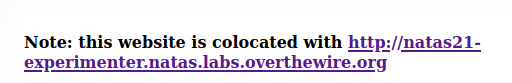
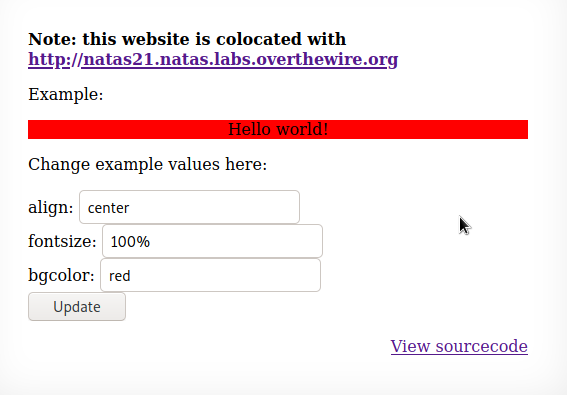
NATAS21

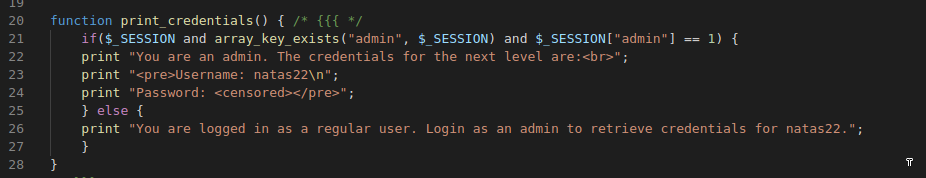
siteyi ilk açtığımızda karşımıza çıkan yazıda şu ifadeler yer alıyor :

Bu site … sitesi ile aynı yerde tutuluyor diyor. Linkteki siteyi natas21 bilgileri ile gittiğimiz zaman bizi basit bir tasarım formu karşılıyor



Hemen kaynak kodlarına bakıyoruz.

Burada lafı çok uzatmaya gerek yok açıkçası, basitçe form değerlerinde verileri alıyor session a yazıyor ve ekrana basıyor. Örneğin bgcolor değerini yellow yaparsanız arka plan rengi sarı oluyor vs. Burada bizim gene bakacağımız alan ilk sayfanın kaynak kodlarında bulunan print\_credentials fonksiyonu:

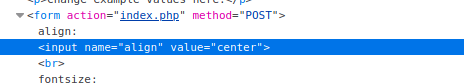


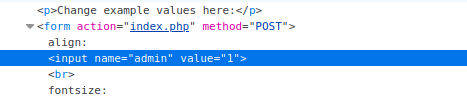
Gene session da bir admin değişkeni olmasını istiyor ve admin değerininde 1 olmasını istiyor.

İkinci sayfanın kaynak kodlarını incelediğimizde form elemanlarının session a yazıldığını görüyoruz:



Yapılan işlem yukarıda anlattığımız gibi. Burada session değerine erişmek diğer lablara nazaran daha kolay çünkü kod içerisinde session değiştiriliyor. 32. satıradaki if koşulu bize kolaylık sağlıyor eğer gelen değerler $validkeys dizisinde yok ise session a yazıyor. Burada yapmamız gereken tek şey html içerisinde herhangi bir input un ismini değiştirmek ve post etmek. Böylece istediğimiz değeri session a yazabiliriz. Öyleyse



Alanını :

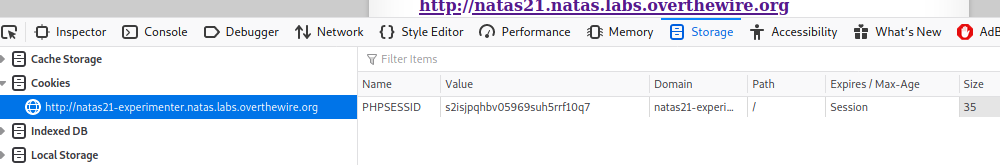
Şeklinde güncelleyelim.

Şimdi session da admin değerinin ve bu değerin 1 olduğuna eminiz ama bu bizim nerede işimize yarayacak.

Web siteleri genellikle sesionları bir dosya olarak saklar ve dosyadan okurlar. Hangi kullanıcının hangi dosyayı okuyacağını ise sessionid değerleri ile tanımlarlar örneğin session id değeriniz 1 ise dosya yolunun altında bulunan 1 isimli klasörde sesion değerleriniz serialize edilmiş şekilde tutulur.

Php de bulunan session\_save\_path değeri sessionların hangi klasör altında tutulduğunu gösterir.

Bu labda bu iki site aynı lokasyon altında olduğu için büyük ihtimal ile sessionları tuttukları dosya yolu da aynıdır. Biz ikinci sitede oluşturduğumuz session değerini ilk siteye taşırsak 22. lab bilgilerini elde edebiliriz. Bu işlemi gerçekleştirmek için birden fazla yol denenebilir. Ben kullandığım tarayıcının araçlarından yapacağım bu işlemi.



Tarayıcının geliştirici seçeneklerinden depolama (storage) alanına gelirseniz burada tutulan cookileri görebilirsiniz. Bizim sessionid değerimiz de bir cookie de tutulduğu için buradaki sessionid değerini koplayıp ilk sitedeki cookinin session id değerine yapıştırırsak bu labı da atlatmış oluruz