CSRF:

Cookie headerda gider, Önemli bilgiler header da gider. Cookie broserın hikayesi temelde

Same origin policy : javascriptin başka bir web sitesine gönderdiği requestin responsu nu okuyup okuyamaması ile alakalı bir konu.

Bir cookie oluşturmak adına bir session başlattığında o sessiona yazdığığın tüm veriler defaulttta /tmp /disc altına yazılır. Cookie bir anahatar, kimlik.,

Same site bu csrf işini yok etti bunu da araştır.

Rest api de cookie olmaz, origin olur ve csrf zafiyeti de olmaz, o yüzden rest apide csrf zafiyeti yok.

Referer nedir ?

Chrome cookie yi set etmese bile samesite ı defaultta enable hale getirdi. Eskiden disable dı.

ödeme ekranında iframe açıp, bankanın ödeme sayfasını doğrudan import etmeyen, kendi formunu entegre edip userı gönderip geri getirenlerin hepsi sıçtı. Hiçbiri ödeme geçiremiyor. İframe entegrasyonu bu yüzden önemli. Bu yüzden csrf zamanla bitecek.

<https://howdns.works/ep1/>