|  |
| --- |
| ***IDOR Zafiyeti*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| IDOR nedir ve bWAPP laboratuvarı üzerinde IDOR zafiyeti nasıl uygulanır bunun hakkında bilgi vereceğim. |

**02.08.2021**

***Insecure Direct Object References(IDOR)***

-Sunucu içinde ki dosya gibi objelerin direk referanslarının açık olması ve kontrol edilememesi,saldırganların bunları değiştirmesine veya izinsiz olarak erişim ile elde edilen zafiyettir.

-Burpsuite aracı üzerinden kullanılan bir zafiyettir.

-Herhangi bir uygulama üzerinden user ksımını değiştirebiliyorsam IDOR zafiyeti vardır.

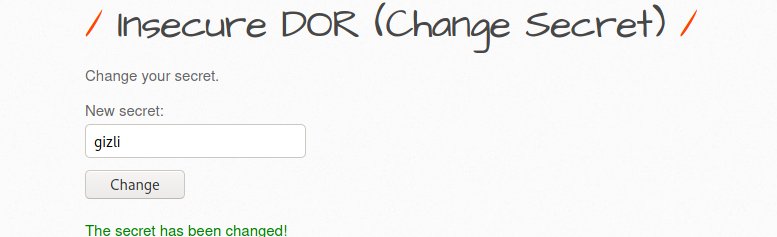
Örnek üzerinden bakmak gerekirse;

-Abankası.com/hesapno.php?hesap=412499 URL’si üzerinden bir müşterinin bilgilerine erişiyorum.

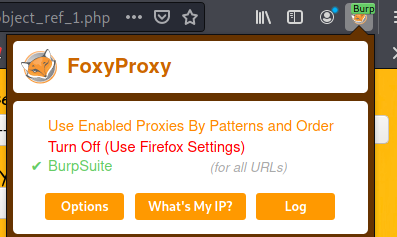
-Abankası.com/hesapno.php?hesap=989174 Müşteri numarasını değiştiğimde görüntüleyebiliyorsam burada IDOR zafiyeti vardır.

-Çok fazla kullanılan bir zafiyet olmadığı için bWAPP üzerinden 2 adet uygulama gerçekleştireceğiz.

**Uygulama1 :** Veritabanı üzerinden IDOR zafiyeti.

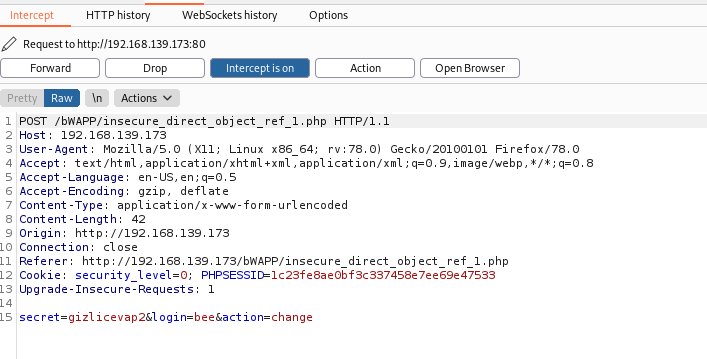


-bWAPP üzerinden zafiyetli siteyi görüntülüyorum.Veritabanı üzerine kayıtlı olan güvenlik sorusu üzerinden IDOR zafiyetini kullanmaya çalışacağız.

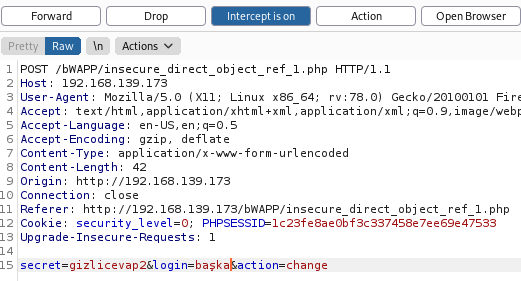


-Foxyproxy eklentisi sayesinde proxy ayarlarımı değişiripi,Burpsuite ve Zafiyetli site arasında bağlantı kuruyorum.

-Bağlantı işlemi sonrasında web bilgilerini Burpsuite aracına çekiyorum.

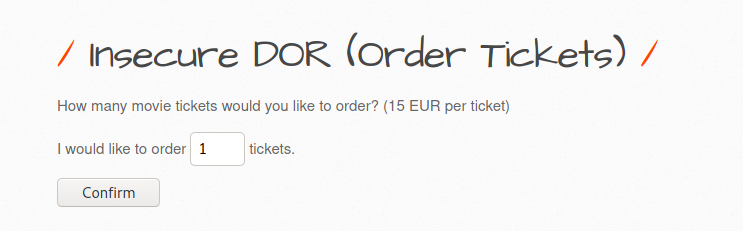


-Login kısmında kullanıcı adı olarak “-bee” yer almaktadır.Bu kullanıcı adını değiştirip arka planda aslında veritabanı üzerinde ki başka kullanıcının gizli sorusunu değiştirmeyi amaçlıyorum.

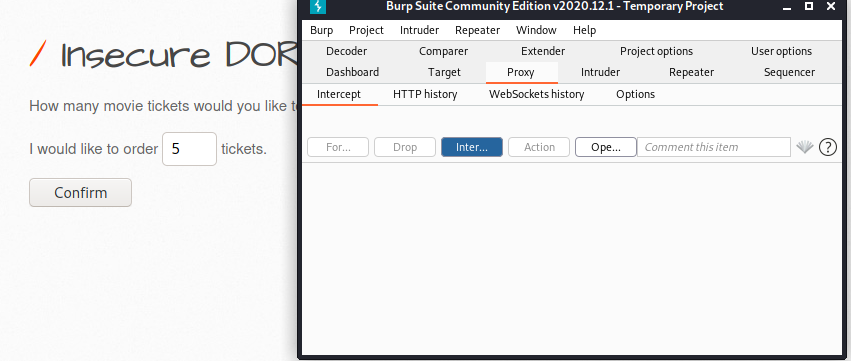


-Kullanıcı adı kısmını değiştiriyorum ve ardından gizli sorusunu da değiştirdiğimde veri tabanı üzerinde güvenlik sorusu da değişmiş olacaktır.

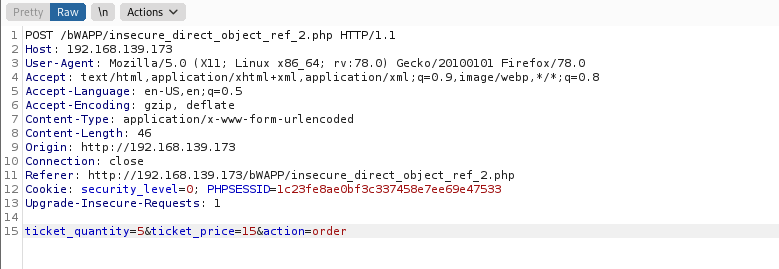
**Uygulama2 :** Bilet satış noktası.



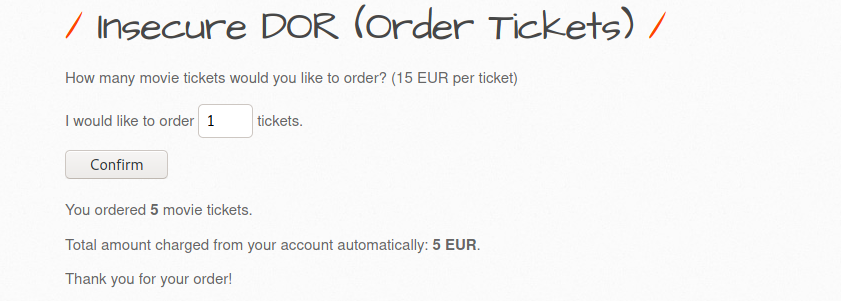
-Zafiyetli siteyi görüntülüyorum.Burada bilet fiyatını istediğim gibi değiştirip sistem üzerinde istediğim fiyata bilet almış olacağım.



-Önce gerekli “Proxy” ayarlarından sonra gerekli bilgileri Burpsuite üzerine çekiyorum.



-“Ticket Price” kısmı üzerinden fiyatını değiştiriyorum.



-Değiştirdiğim fiyat üzerinden istediğim kadar bilet alabilmiş oldum.

-Bu zafiyet için yapacağımız uygulamalar bu kadardır.

***Korunma Yöntemleri***

-Her referans ömrü yalnıca 1 kullanıcılık veya 1 oturumlu olmalıdır.

-Güvenilmeyen kaynaklardan gelen referanslar kullanılmadan önce erişim yetkileri kontrol edilmelidir.