OTURUM SABİTLEME

Tanım: Kullanıcıya zorla oturum ID'sinin zorla kabul ettirilmesidir.

Bu saldırının mantığı kısaca şöyledir;

İllegal olarak oluşturmuş olduğum bir Oturum ID'sini hedef kullanıcıya onaylattırarak legal bir hale getirmektir.

Saldırı Adımları

I. İlgili web portalına giriş yaparak sunucu tarafından bir oturum id'si elde ediyoruz.
II. Elde ettiğimiz Oturum ID'sinin içerisinde bulunduğu linki kurbanımıza gönderiyoruz.(SM yöntemleri kullanarak linki tıklatmak zorundayız)
III. Kurban linke tıkladığı zaman ilgili web portalına bizim elde ettiğimiz Oturum ID'si ile giriş yapıyor.(örneğin facebook login sayfası)
IV. Kullanıcı adı ve parola bilgileri ile sisteme giriş yapan kullanıcının mevcut Oturum ID'si bizim elimizde olan ve bizim ürettirdiğimiz ID'dir.
V. Biz bu ID ile gerçek kullanıcıymış gibi herhangi bir işlem yapabiliriz. Yani sunucudan kendi aldığımız ID'mizi kullanıcıya satmış olduk ama tüm bilgiler bizim elimizde .

- Burada kullanıcının kullanıcı adı ve parola bilgilerini elde edemeyiz ancak oturum açılmış olduğu için kullanıcı bilgilerine ihtiyaç duymaksızın gerçek oturum sahibi gibi davranabiliriz.
- İlk başta elde ettiğimiz Oturum ID'sini sürekli canlı tutmamız gerekir.Bunun için ID'miz ile belirli aralıklar ile istekler yapmalıyız.
- Oturum bilgisi IP adresi ile ilişkilendirilmiş ise oturum sabitleme istismarını gerçekleştiremeyiz.
- NAT veya PROXY kullanılan ortamla işe yaramamaktadır.

Cookie Oluşturma Yöntemleri

1. URL ile cookie oluşturma
2. JavaScript ile cookie oluşturma
3. Meta etiketi ile cookie oluşturma
4. http cevap başlığı (Set-Cookie)ile cookie oluşturma

URL ile cookie oluşturma

İstismar edilirken en çok bu yöntem kullanılır.

ÖRNEK:
www.site.com/login.php?PHPSESSID=b1233d123

JavaScript ile cookie oluşturma

Bu yöntemi kullanmak için hedefte XSS zaafiyeti bulunmalıdır.

Örnek:
<script>document.cookie="PHPSESSID=123"</script>

➔ Hedef kişi saldırganın xss sömürüsü yaptığı linke tıkladığı zaman oturum id'si 123 olarak değişecektir.Saldırgan zaten bu ID'yi bildiği için kendiside 123 ID si ile hedef kişiymiş gibi davranışlar gösterebilecektir.

Meta etiketi ile cookie oluşturma

HTML etiketlerinden olan <meta> etiketini kullanarak oluşturulması yöntemidir.

Javascript benzeridir.Burada ki tek fark XSS yerine Html Kod Enjeksiyonu zaafiyeti bulunması gerekmektedir. Çünkü hedefe kod enjekte edeceğiz.

Örnek:

<meta http-equiv=Set-Cookie content="PHPSESSID=123">

Etiket kısmı yukarıdaki gibidir.Bu etiketi GET metoduyla URL üzerinden sayfanın kodları arasına enjekte edeceğiz.Dolayısıyla;

www.site.com/login.php?param=<meta http-equiv=Set-Cookie content="PHPSESSID=123">

şeklinde olur.

Http cevap başlığı (Set-Cookie)ile cookie oluşturma

Bu yöntemi kullanabilmek içi hedef üzerinde Http Başlık Enjeksiyonu Zaafiyeti bulunmalıdır.

Burada da diğer 3 yöntemde olduğu gibi istek değiştirilir.

Oturum Sabitlemeye Karışı Önlemler

- Her başarılı kimlik doğrulama işleminin ardından Oturum Anahtarı değiştirilmelidir.
- PHP programlama dili için session_regenerate_id metodu kullanılmalıdır.

Örnek:

```
İf(authenticate($username,$password))
{
Session_regenerate_id(TRUE);
}
```

Hasan Baskın

Adli Bilişim Mühendisliği

www.hasanbaskin.com