SAML Raider (Burp Suite Eklentisi) Eğitim Materyali

# 1. SAML Raider Nedir?

# SAML Raider, Security Assertion Markup Language (SAML) tabanlı kimlik doğrulama sistemlerini test etmek için kullanılan bir Burp Suite eklentisidir. Bu araç, SAML istek ve yanıtlarını yakalamak, görüntülemek, düzenlemek ve tekrar göndermek için kullanılır. Özellikle SSO (Single Sign-On) testlerinde güvenlik açığı tespitine yardımcı olur.

# 2. Kullanım Alanları

- SAML tabanlı tek oturum açma (SSO) uygulamalarını test etmek  
- SAML Assertion mesajlarını düzenlemek  
- XML imza doğrulama mekanizmalarını test etmek  
- Yetkilendirme bypass zafiyetlerini tespit etmek

# 3. Kurulum

1. Burp Suite Community veya Professional sürümünü açın.  
2. 'Extender' sekmesine gidin.  
3. 'BApp Store' kısmından 'SAML Raider' eklentisini bulun ve yükleyin.  
Alternatif olarak GitHub üzerinden JAR dosyasını indirip manuel olarak ekleyebilirsiniz.

# 4. Temel Kullanım

- SAML tabanlı giriş akışını başlatın ve Burp Proxy ile trafiği yakalayın.  
- Eklenti, yakalanan SAML mesajlarını otomatik olarak tespit eder.  
- 'SAML Raider' sekmesinde assertion verilerini düzenleyebilir, imzaları kaldırabilir veya değiştirebilirsiniz.  
- Düzenlenmiş veriyi hedef uygulamaya geri göndererek zafiyeti test edin.

# 5. Sık Kullanılan Özellikler

- Assertion içeriğini Base64 decode/encode  
- XML imza kaldırma veya değiştirme  
- Kullanıcı rol veya yetkilerini değiştirme  
- Zaman damgalarını düzenleme  
- Oturum geçerlilik süresini değiştirme

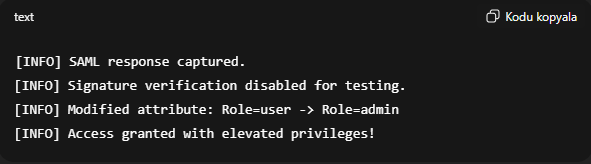
# 6. Örnek Eğitim Senaryosu

1. Test ortamında SAML tabanlı giriş yapan bir uygulama çalıştırılır.  
2. Burp Proxy ile giriş isteği yakalanır.  
3. SAML Raider ile assertion mesajındaki kullanıcı rolü 'user' yerine 'admin' olarak değiştirilir.  
4. Hedef uygulamanın yetkisiz erişime izin verip vermediği kontrol edilir.  
5. Öğrencilere, imza doğrulamanın neden önemli olduğu gösterilir.

**5. Örnek Kullanım ve Çıktı**

**Örnek Senaryo:**  
Bir SAML tabanlı giriş sisteminde oturum açma isteğini yakalayarak, SAML yanıtındaki "Role" değerini "admin" olarak değiştirip yetki yükseltme testi yapılabilir.

**Örnek Komut / İşlem:**



# 7. Korunma Yöntemleri

- SAML imza doğrulamasının zorunlu tutulması  
- Assertion içeriğinin sunucu tarafında yeniden doğrulanması  
- Zaman damgalarının kontrol edilmesi  
- Güvenilir kimlik sağlayıcıları kullanmak

# 8. Etik Uyarı

SAML Raider ile yapılan testler yalnızca izinli uygulamalarda gerçekleştirilmelidir.   
İzinsiz testler hukuka aykırıdır ve ciddi yaptırımları olabilir.