

Uygulama Güvenlik Denetimi

Uygulama Güvenlik Açıklarına
Yönelik Yapılan Testler

Uygulama Test Kategorileri

1. IT Altyapısı Güvenlik Açıkları
2. Dizin Tespiti
3. Çapraz Site Kod Kullanımı
4. Parametre Zorlanması ve Gizli Alan Değişikliği
5. Cookie Değişikliği
6. Gizli Komut Gönderme
7. Backdoor & Debug Opsiyonları
8. Üçüncü Taraf Konfigürasyonları
9. Veritabanı Sabotajı ve SQL Enjeksiyonu
10. Tampon Bellek Taşıma
11. Veri Kodlama
12. Protokol Seviyesi Saldırıları
13. Diğer Testler



1. IT Altyapısı Güvenlik Açıkları

- Entegre sistem bütünündeki güvenlik açıklarının kontrol edilmesi ve kullanılması
 - Sunucu ve Ağ Güvenliği Açıkları
 - Yaygın dosya ve izin açıkları
- Örnekler:
 - /samples
 - Apache – PHP3 ortamında
<http://target/index.php3.%5c../..%5cconf/httpd.conf>
 - IIS 4.0 ortamında
<http://target/me.idq>

3



2. Dizin Tespiti

- Uygulamanın bulunduğu erişilebilir sunuculardaki dosya ve izin hiyerarşisinin tespit edilmesi.
- Sistem ile ilgili gereksiz bilgi sızıntılarının tespit edilmesi
- Diğer saldırı tipleri için bu bilgilerin girdi olarak kullanılması.

4



3. apraz Site Kod Kullanımı



- Sistem zerindeki gvenlik aıklarını kullanarak yapılır.
- Saldırganın sistemi zerinde bulunan kod dosyalarının alıřtırılması ile gerekleřtirilir.
- Sistemde istenmeyen deėiřikliklerin yapılması ve gedik aılması hedeflenmektedir.

5



4. Parametere Zorlanması ve Gizli Alan Deėiřikliėi



- HTML kodu veya tespit edilebilen ASP/ PHP kodların tespit edilmesi
- Kod ierisindeki gizli parametrelerin deėiřtirilerek sunucuya gnderilmesi

6



5. Cookie Deęişiklięi



- Uygulama içinde cookie içerisinde taşınan bilginin kullanımının incelenmesi
- Cookie içeriğinin deęiştirilerek uygulamaya cookie kanalıyla beklenmeyen parametreler gönderilmesi veya deęer deęişiklięi
- Böylece oturumun çalınması (session hijacking) gibi sonuçlarla istenmeyen veri ve bilgilere ulaşılmaya çalışılması

7



6. Gizli Komut Gönderme



- Uygulama içindeki girdi tipi metin olan alanları tespit etmek
- Bu alanların içerisine truva atları yerleştirilerek uygulamanın istenmeyen davranış göstermesine çalışılması

8



7. Backdoor & Debuging Opsiyonları



- Tespit edilebilen kod parçaları veya programın çalışma şekillerinin incelenmesi
- Açık bırakılan arka kapıların tespiti
- Kod içerisinde hata kontrolü (debug) amaçlı bırakılmış işaretlerin tespit edilmesi
- Uygulama üzerinde test verileri ile çalışma ve hata kontrollerinin yapılması

9



8. Üçüncü Taraf Yazılım Konfigürasyonları



- Sistemle entegre çalışan diğer yazılımların test edilmesi
 - Web sunucusu yazılımı
 - Veritabanı sunucusu yazılımı
 - Hazır CGI Programları,
 - ...

Örnek:

- Otorizasyon eksikliği olan bir hazır cgi programına yönelik saldırılar

[http://target/book.cgi?price=\\$1.30](http://target/book.cgi?price=$1.30)

10



9. Veritabanı Sabotajı & SQL Enjeksiyonu



- Uygulama güvenlik açıklarının en yaygın bulunduğu alandır.
- Çeşitli girdi alanları ve mesajlarına SQL komutları yerleştirerek istenmeyen veri tabanı işlemleri yapılması
- Saldırı tekniklerine ait alt grup örnekleri:
 - Otorizasyon Aşılması
 - Sentaks Kırımıyla Doğrudan Enjeksiyon
 - Sentaks Kırımıyla Dolaylı Enjeksiyon
 - Sentaks Hata Mesajı ile Sorgu Dökümü
 - Parantez Kırımıyla Dolaylı Enjeksiyon
 - LIKE komutu ile Dolaylı Kırım ve Enjeksiyon
 - WHERE komutu ile Kolon Kırılması
 - Hazır Sistem Prosedürleri Kullanılması

11



10. Tampon Bellek Taşıma Saldırıları



- Uygulama veya sistem parametrelerine büyük boyutlu girdiler göndermek
- Girdiye ayrılan tampon bellek adresinin taşması ile sistemin dengesiz hale geçmesi ve istenmeyen komutlara cevap verir hale gelmesini sağlamak
- Sistemin her seviyesindeki kodlar bu saldırı amacıyla kullanılabilir
 - Altyapı yazılımları
 - Entegre 3.taraf yazılımları
 - Geliştirilen yazılımlar

12



11. Veri Kodlama Saldırıları



- Her çeşit talep ve alan içeriğinin farklı veri kodlama standartları ile gönderilmesi
- Girdi kontrollerinin aşılmaya çalışılması
- Örnek standartlar:
 - Unicode,
 - UTF-8
 - UTF-16

13



12. Protokol Seviyesi Saldırıları



- Kullanılan uygulama ve iletişim protokolleri yapılarının değiştirilmesi
- Kullanılan protokol gereği alt seviyede gönderilen bit içeriklerinin değiştirilerek sistemde düzensizlik yaratılmasına çalışılması

14



13. Diğer Testler

- Tersine mühendislik (reverse engineering), kara-kutu ve beyaz-kutu test metodolojileri kullanılarak diğer uygulama güvenlik problemlerinin tespit edilmesi.
- Çeşitli koşullar karşısında sistem davranışının takip edilmesi ile saldırı amaçlı kullanılacak zafiyetleri tespiti.
- Yaygın olmayan ancak sisteme bağlı özellikler gösteren diğer güvenlik testlerinin gerçekleştirilmesi.