



Yazılım Geliştirme Yaşam Döngüsü ve Güvenlik

*Burak Dayıođlu, CISSP
Genel Koordinatör*

Bilişim güvenliği ihlallerinin

YAZILIM GÜVENLİĞİ
0/80

problemlerinden kaynaklı hatalarının oranı

(Kaynak: Gartner)





Yazılım Güvenliği Problemi

- Konu oldukça yeni, taşlar yerine oturmadı
- Pek çok yazılım ekibi güvenli yazılımları nasıl geliştireceği konusunda bilgi sahibi değil
 - Geliştiricilerin %64'ü güvenli yazılımlar geliştirebildiklerinden emin değil (*Microsoft*)
- Çok fazla geliştiricimiz var, güvenlik öncelik değil
- Güvenlik uzmanlarının pek çoğu yazılım konusunda uzman değil
- Okulda güvenlik öğretmiyoruz



Boa Factory - fresh credit card dumps - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Available		Visa Signature (no limits)	USA	10	1490.00	149.00
Available		Visa Signature (no limits)	USA	100	9500.00	95.00
Available		Visa Purchasing	USA	10	1490.00	149.00
Available		Visa Business Debit	USA	40	1198.00	29.95
Available		Visa Business Debit	USA	100	2495.00	24.95
Available		Visa Business Credit	USA	40	1198.00	29.95
Available		Visa Business Credit	USA	100	2495.00	24.95
Available		Visa Business unsorted	USA	40	1198.00	29.95
Available		Visa Business unsorted	USA	100	2495.00	24.95
Available		MasterCard unsorted	USA	100	695.00	6.95
Available		MasterCard Gold	USA	40	1198.00	29.95
Available		MasterCard Gold	USA	100	2495.00	24.95
Available		MC Gold (balance \$20-30.000)	USA	10	995.00	99.95
Available		MC Gold (balance \$20-30.000)	USA	100	6995.00	69.95
Available		Diners Club	USA	10	1199.00	119.90
Available		Discover (Novus) unsorted	USA	40	638.00	15.95
<input type="checkbox"/> Available		Discover Platinum & Gold	USA	20	999.00	49.95
Available		AmEx unsorted	USA	50	997.50	19.95
Available		AmEx unsorted	USA	100	1495.00	14.95
Available		AmEx Corporate	USA	20	1599.00	79.95

USA processing centre.

63KB
European and worldwide countries - December 2002.

We have a lot of databases besides which it mentioned above. From time to time we shall change and update the databases, which are accessible to free sale.

First paid - serve first. No credits & loans.

You can choose the dumps of one type for every order. Each order can not be less, than is specified in the table at the left.

Visa Signature card dumps

Now you can buy Visa

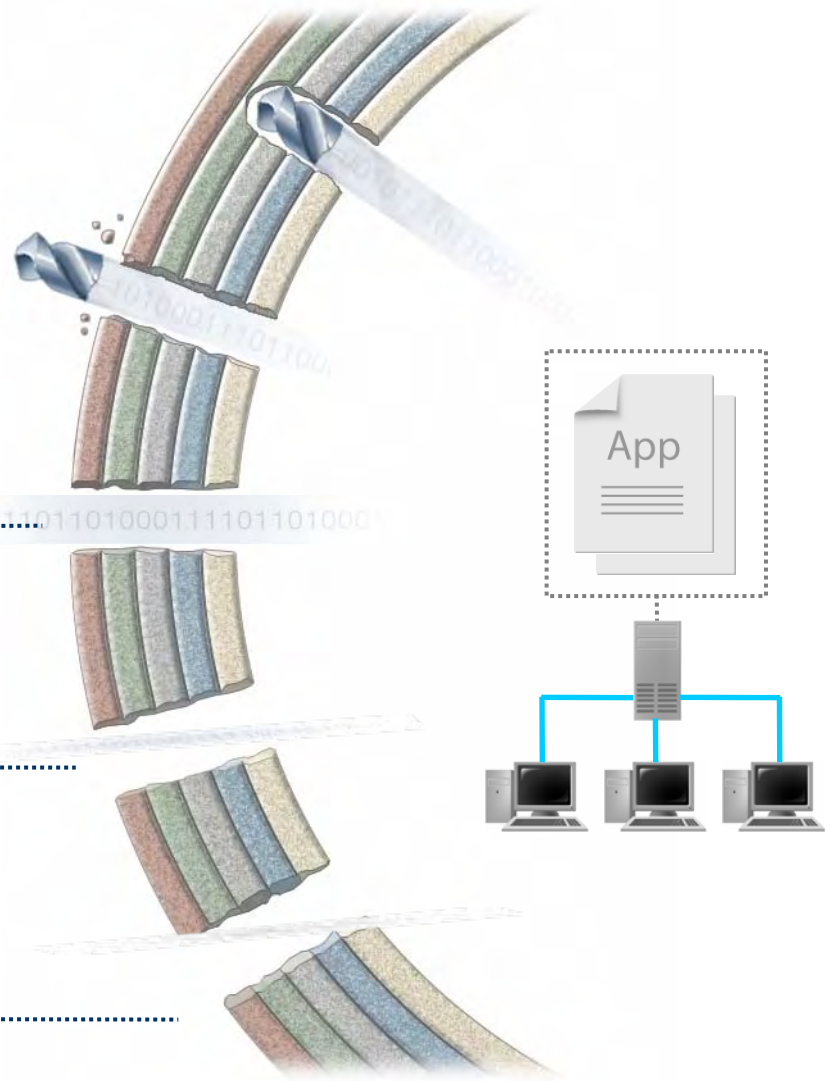
Bugünün Bilişim Dünyası

Uygulama Entegrasyonu

Web Uygulamaları

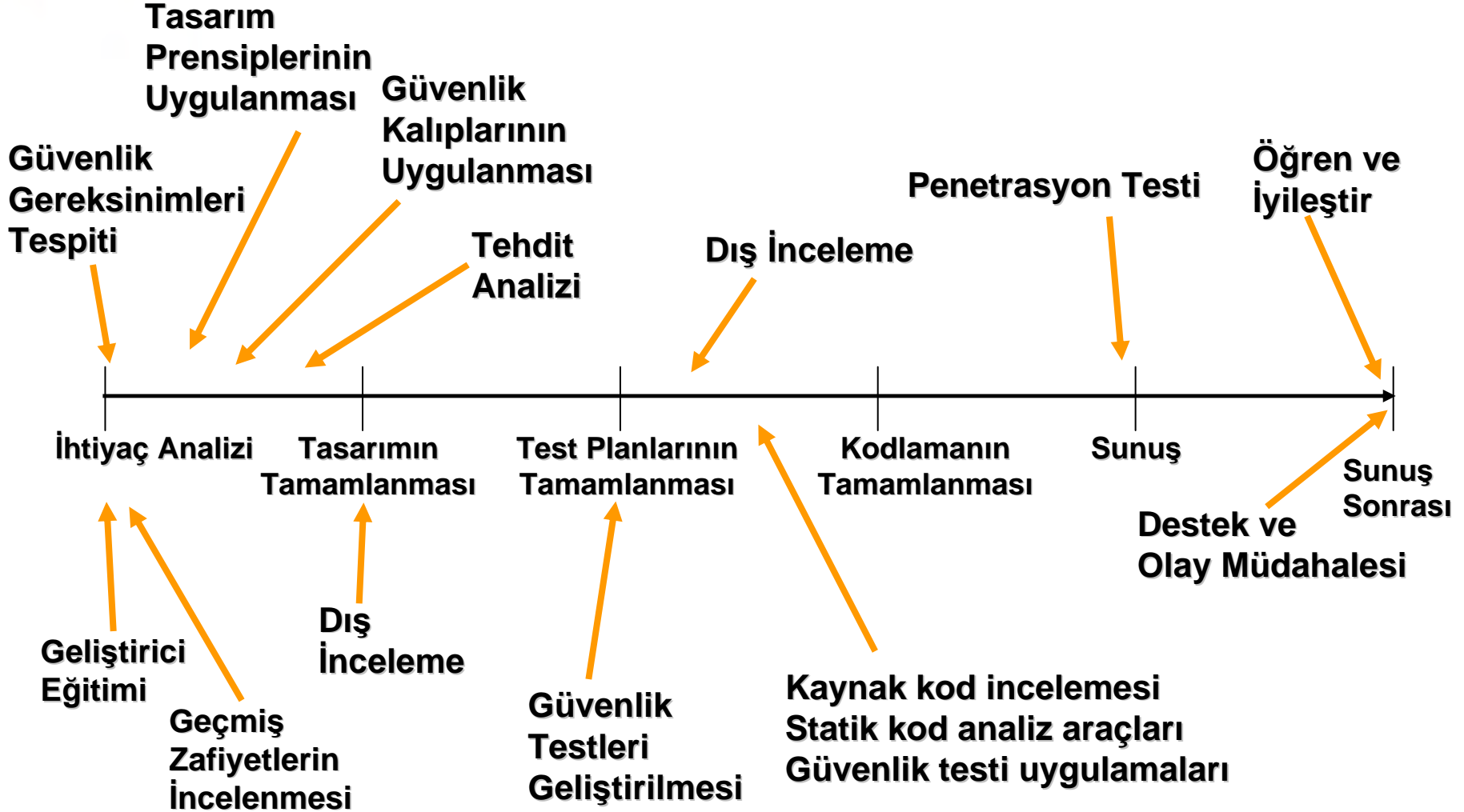
Çalışanlar için self-
servis portalleri

İş ortağı ve tedarikçi
bağlantıları





Güvenli Geliştirme Süreci





Geliştirme Süreci Modelleri

- Üç ana geliştirme süreç modeli
 - OWASP: Comprehensive Lightweight Application Security Process (CLASP)
 - Microsoft: Security Development Lifecycle (SDL)
 - Cigital: 7 Touchpoints



PCI ve Geliştirme Süreci

- Gereksinim 6: Güvenli Sistem ve Uygulamalar Geliştirin ve İşletin
 - Değişiklik ve konfigürasyon yönetimi
 - Geliştirme, test ve üretim ortamı ayrışımı
 - Geliştirme ortamında gerçek verilerin kullanılmaması
 - Üretim ortamına almadan önce kod incelemesi
 - Güvenli programlama teknikleri kullanımı
 - Uygulama güvenlik duvarı kullanımı ya da kaynak kod inceleme hizmeti alınması (Haziran 2008)



PCI ve Geliştirme Süreci

- Gereksinim 11.5:
 - Kritik dosyalar için bütünlük denetimi
- Payment Application Best Practices (PABP):
 - Visa en-iyi uygulaması
 - 2008 içinde bir PCI standardı olacak (PA-DSS)



PABP Gereksinimleri

1. Kart bilgisi saklamayın
2. Depolanan bilgileri koruyun
3. Güvenli parolalar kullanın
4. Uygulama hareketlerini kaydedin
5. Güvenli uygulamalar geliştirin
6. Kablosuz iletişimlerini koruyun
7. Zafiyetler için uygulamaları test edin
8. Güvenli ağlar kurun
9. Kart bilgileri Internet'e bağlı bilgisayarlarda kesinlikle depolanması
10. Uzaktan güvenli yazılım güncellemeleri kullanın
11. Uygulamalara uzaktan güvenli bağlantılar sağlayın
12. Kamusal ağlar üzerinde hassas bilgileri şifreleyin
13. Konsoldan yapılmayan yönetici girişlerini şifreleyin
14. Kullanıcılar, satıcılar ve entegratörler için eğitsel belgeler hazırlayın



Pro-G Çözümleri

- Yazılım Güvenliđi Eđitimleri
- Geliřtirme Süreci Danıřmanlıđı
- Uygulama Penetrasyon Testleri
- Kaynak Kod İncelemesi
- Statik Kod Analizi Araçları (Fortify ürünleri)
- Bütünlük Denetim Araçları (Ares-Integrity)
- PABP Denetimleri (Trustwave ile)



Güvenliğiniz Geleceğinizdir...



7 Touchpoints

