



Bir Güvenlik Açığının Bulunması

Fatih Özavcı

Bilgi Güvenliği Danışmanı

fatih.ozavci@gamasec.net



Sunum İeriđi



- Gvenlik Aıđı ve İstismar Tanımı
- Gvenlik Aıđı Trleri
- Gvenlik Aıđının Bulunması ve Aralar
 - Gvenlik Aıđının Keşfi
 - Kullanım Yntemlerinin Araştırılması
 - Etki Dzeyi ve Elde Edilenler
- Gvenlik Aıđı Yayınlama Sreci



Kaşık YOK !



Güvenlik Açığı



- Sistemlerin sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksiklikler
- Nedenler
 - Yetersiz Programlama
 - Yapılandırma Hataları
 - Teknoloji Yorumlamaları
- Sonuçlar
 - Sistemde Komut Çalıştırılması
 - Servisin Engellenmesi
 - Güvenlik Kontrollerinin Aşılması
 - İstemcilerin Yanıltılması

Nedenler



- Programlama
 - Yetersiz Programlama
 - Yetersiz Güvenlik Kontrolleri
 - Ortak Kütüphanelerdeki Genel Hatalar
- Yapılandırma
 - Yönetim Arabirimleri
 - Depolama Seçimleri
 - Şifre Seçimleri
- Teknoloji
 - TCP/IP Protokol Oyunları
 - Dil Kodlamaları
 - Kriptolama

* Açıklar birinden veya daha fazlasının kombinasyonundan da oluşabilir.

Yetersiz Programlama

➤ Girdi Doğrulama

- SQL Sorguları Değiştirilmesi ' OR 1='1
- Komut Sorguları Çalıştırılması ; dir c:\
- Tampon Bellek Taşmaları AAAAA...AAAA
- Heap Taşmaları AAAAA...AAAA
- Format String Açıkları %s %n %x
- Farklı Dil Kodları Kullanımı %c0%af %u0061

➤ Asenkron İletişim / Erişim

- Race Condition Yazma/Okuma Zamanı

➤ Kriptolama

- Zayıf Kripto Seçimi Şifrelerin Metin Olarak Saklanması

.....

Yetersiz Güvenlik Kontrolleri

- Kara Liste Yaklaşımı
\' 'SEL'+ 'ECT' concat(char(59),char(21)) FROM XXX WH/**/ERE id=1
- Değişkene Boyut Sınırı Belirtilmemesi
AAAAA...AAA 1938741923478691238746
- Değişkene Tür Sınıfı Belirtilmemesi
int -> AAA string -> '<script>%x || && -- ;
- Sıkıştırma/Kodlama Algoritmaları Kullanımı
Base64 Gzip Zip Tar Rar
- Farklı Dil Kodlarının Hatalı Çevrimi
%c0%af %u0061
- Oturum Yönetim Sorunları
Cookie yetersizlikleri, Kullanıcı/Şifre kontrolleri
Oturumun belleğe veya diske erişim kontrolsüz kaydedilmesi

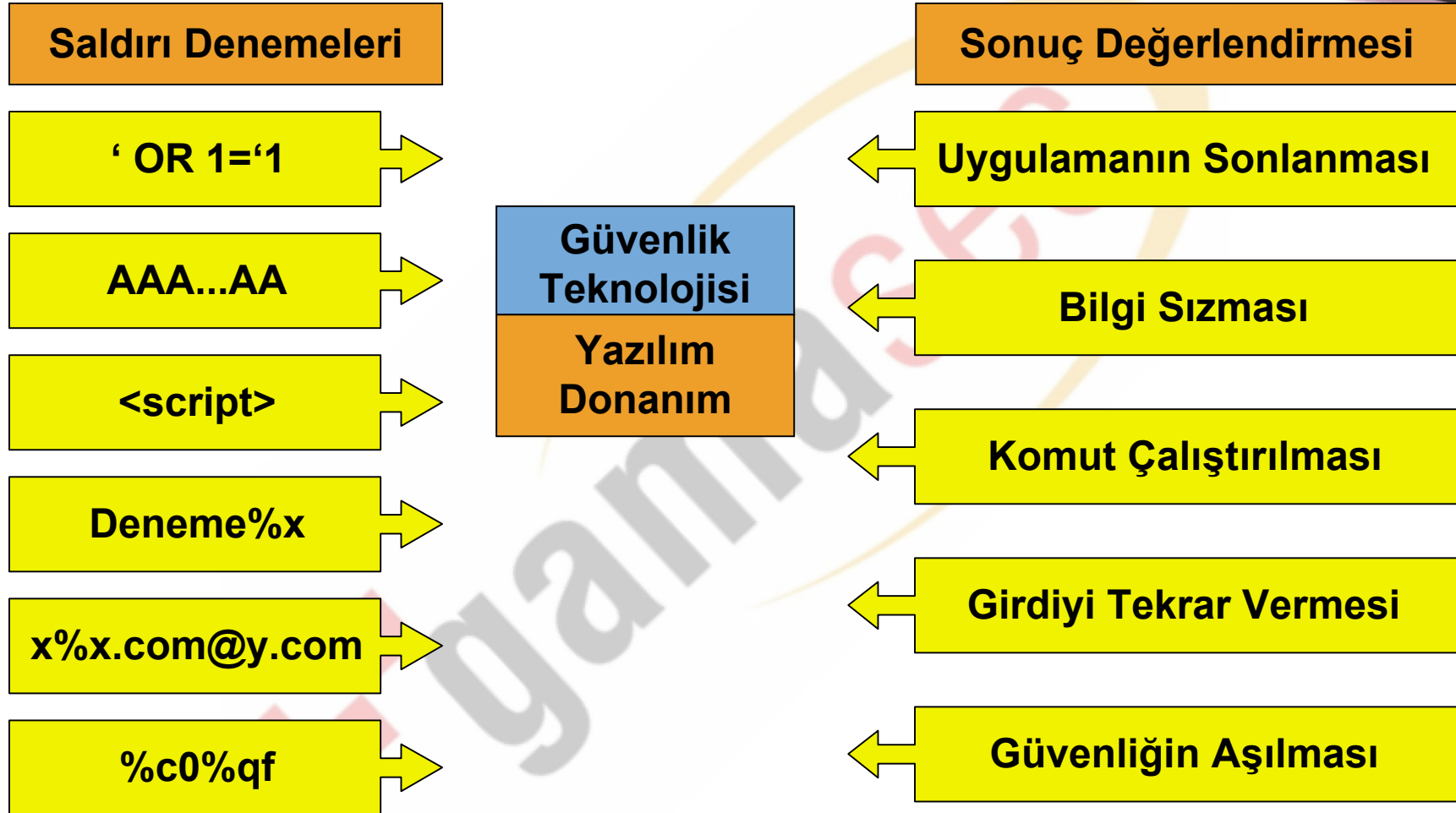
.....

TCP/IP Oyunları



- Proxy Özelliği
 - Farklı Protokol veya Sürüm Kullanımı
 - Tünelleme Kullanımı
 - Kriptolu İletişim Kullanımı
- Erişim Denetimi
 - IP/ARP/DNS Sahteciliği
 - IP/TCP Paket Parçalama
 - TCP Bayrakları veya Seçenekler ile Oynama
- IPS/IDS Saldırısı/Kabuk Kodu İmzası Farklılaştırma
 - Açığın Farklı Kullanımları ..%c0%af.. veya ..%c0%qf..
 - Kodlama %u0061 Base64 XOR

Kapalı Kutu Analizi



* Test esnasında yazılımın kendisinden önce, güvenlik teknolojisinin açığı bulunabilir

Açık Kod Analizi



Karıştırıcılar/Deneyiciler



- Uygulamaya belirlenen girdi türleri veya işlemlerin, istenen biçimde ve ardışık olarak gönderilmesini sağlayan betikler/yazılımlar

220 SMTP Sunucusuna Hosgeldiniz

helo deneme.com

250 x.y.com

mail from: x@x.com

250 2.1.0 Ok

rcpt to: x@y.com

250 2.1.5 Ok

data

354 End data with <CR><LF>.<CR><LF>

deneme

.

250 2.0.0 Ok: queued as 64516D0013

```
for t in 513xA 1025xA %x
```

```
do
```

```
echo "helo $t" | nc -vw3 x.com 25 >> cikti
```

```
done
```

İzleyici / Hata Ayıklayıcı



- İzleyici : Bir uygulamayı çalışmasından sonlanmasına kadar izleyen ve yapılan işlemleri çıktı olarak üreten yazılımlar
- Hata Ayıklayıcı : Bir uygulamanın veya bir alt bileşenin hata oluşturup sonlanması durumunda oluşan çıktıyı analiz eden yazılımlar
- Kapalı kutu analizlerinde, uygulamanın çalışma sürecinde yaptıklarının, uygulamanın sonlanma sebebinin, bellekteki yerleşiminin, sorunlu fonksiyon ve sonuçlarının öğrenilmesi için kullanılırlar

Exploit



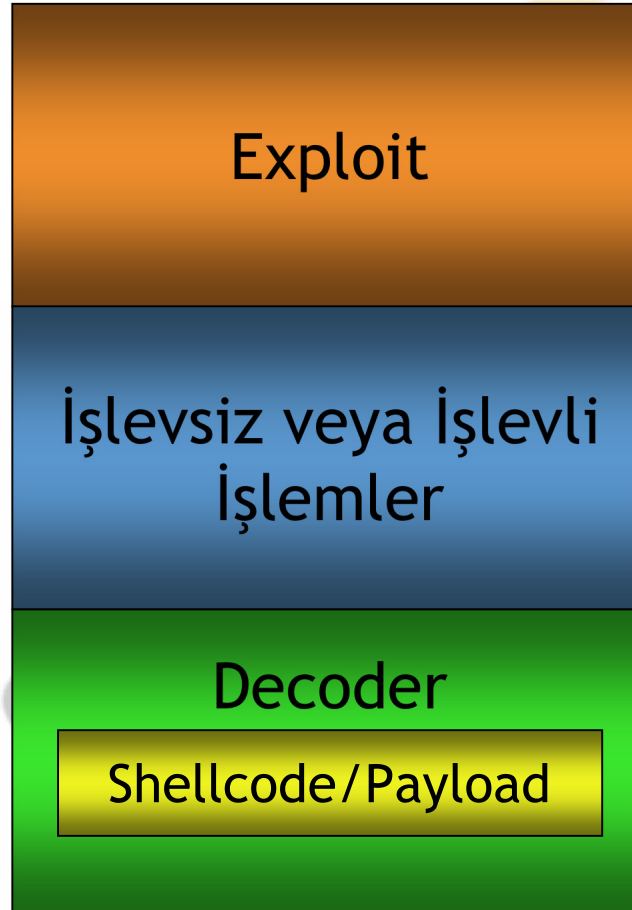
Bir güvenlik açığını kullanarak normal-dışı bir işlem yapılmasını sağlayan yöntem veya yazılım

- <http://sunucu/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir>
- <http://sunucu/login.asp?uid=' OR 1='1>

Diğer Kavramlar

- Payload
 - Exploit sonrası çalıştırılacak ve normal-dışı işlemi yapacak içerik
- Shellcode
 - Exploit sonrası çalıştırılacak platforma özel binary'ler
- NOP
 - “Not Operation”, işlevsiz veya bellek yeri öğrenme amaçlı bellek dolduran bitler
- Encoder
 - Çalıştırılacak Shellcode’u değiştiren ve IDS/IPS’ler tarafından yakalanmasını önleyen yazılımlar

Exploit Yapısı



Yardımcı Araçlar

- Açık Bulunan Yazılımın Örneği !?
- Exploit Geliştirme Ortamı
- Karıştırıcılar / Deneyiciler (Fuzzer)
- Kodlayıcılar (Encoder)
- İkilik Editörler (Hex Editor)
- İzleyiciler (Tracer)
- Hata Ayıklayıcılar (Debugger)
- Paket Yakalayıcılar (Sniffer)
- Protokol Çözümleyiciler
- Yorumlayıcılar / Derleyiciler (Interpreter/Compiler)
- Kabuk Kodları (Shellcode)
- SQL Sorguları

Exploit Geliştirme Ortamları

- Exploit ve Payload ayrımı
- Hazır ve kodu açık Exploit'ler
- Binary analizi için yardımcı araçlar
- Hazır Payload veya Agent'lar
- Grafik arabirim ile "tıkla ve gir" kolaylığı
- Hazır fonksiyonlar ile daha az Exploit kodu
- Kategorizasyon ve analiz arabirimleri
- Hazır Recon'lar ile bilgi toplama
- Yerel, yetki yükseltimi amaçlı Exploit'ler
- 0 gün Exploit'leri

Güvenlik Açığı Yayınlama Süreci



- Bir denetim esnasında sadece o kuruma özel bir uygulamada saptanan güvenlik açığının yayınlanması etik değildir
- Bir denetim veya test ortamında genel kullanıma açık ve yaygın kullanılan uygulamalarda ;
 - Üretici ile temasa geçilmeli, yayınlama için en az 2 hafta beklenmelidir
 - Üreticinin açığı önemsememesi veya çok uzun süre bekleyeceğini belirttiği durumlarda beklemek gerekmeyebilir
 - Açık kaynaklı uygulamalarda; mümkünse üretici/geliştirici ile doğrudan irtibata geçerek bir yama eşliğinde yayınlama yapılmalı
- Açık yayınlamalarında, kurumların zarar görmemesi için gerekli tüm önlemler alınmalı, mümkünse yama veya alternatif çözüm önerilmeli, gerekirse sadece örnek amaçlı ve kısıtlı bir açık istismarı açıklanmalıdır

Bağlantılar ve Referanslar



- GamaLAB
<http://www.gamasec.net/gamalab.html>
- Enderunix - Belgeler
<http://www.enderunix.org/?lng=tr&page=papers>
- Solar Eclipse - Exploit Code Development
<http://www.phreedom.org/solar/exploits/exploit-code-development/>
- OWASP
<http://www.owasp.org>
- Polymorphic Buffer Overflow
http://www-static.cc.gatech.edu/classes/AY2003/cs6265_fall/pallavi.ppt
- Thermoptic Camouflage
<http://www.metasploit.org/confs/blackhat2006/blackhat2006-thermoptic.pdf>
- Metasploit Framework
<http://www.metasploit.org>



Teşekkürler....

