Web Uygulamalarında Sık Karşılaşılan Güvenlik Problemleri ve İlginç Açıklar

Sertan Kolat

Peki ya diğer istatistikler?

- Mevcut durum
  - Türkiye
  - Dünya
- OWASP Top 10 ?
  - En kritik 10 web uygulama güvenlik riski
- WASC - Web Application Security Statistics
  http://bit.ly/WASCstats

id

- Sertan Kolat
- Kıdemli Güvenlik Danışmanı
- Avanteg – Yönetilen Servisler & Denetim Birimi Yöneticisi
- Penetration Tester
- CISSP, CISA, OSCP
- Blogger
  - SertanKolat.com
  - AutomatedScanning.blogspot.com

Ajanda

- Kapsam
- Veri İçeriği
- Web Uygulamalarında Sık Karşılaşılan Güvenlik Problemleri ve İlginç Açıklar

Kapsam

- Özel geliştirilmiş web uygulamaları, sayfalar, web servisleri
  - ASP, ASP.Net, ColdFusion, Java *, PHP
  - Flex, Flash

- Kapsam dışı
  - Hazır uygulamalardaki bilinen açıklar
  - Web sunucularındaki güvenlik açıkları
  - Sistem ve network güvenlik açıkları
  - Kullanıcı uygulamaları (desktop applications)
  - DNS, SSL güvenlik açıkları vd. konfigürasyon zaafiyetleri

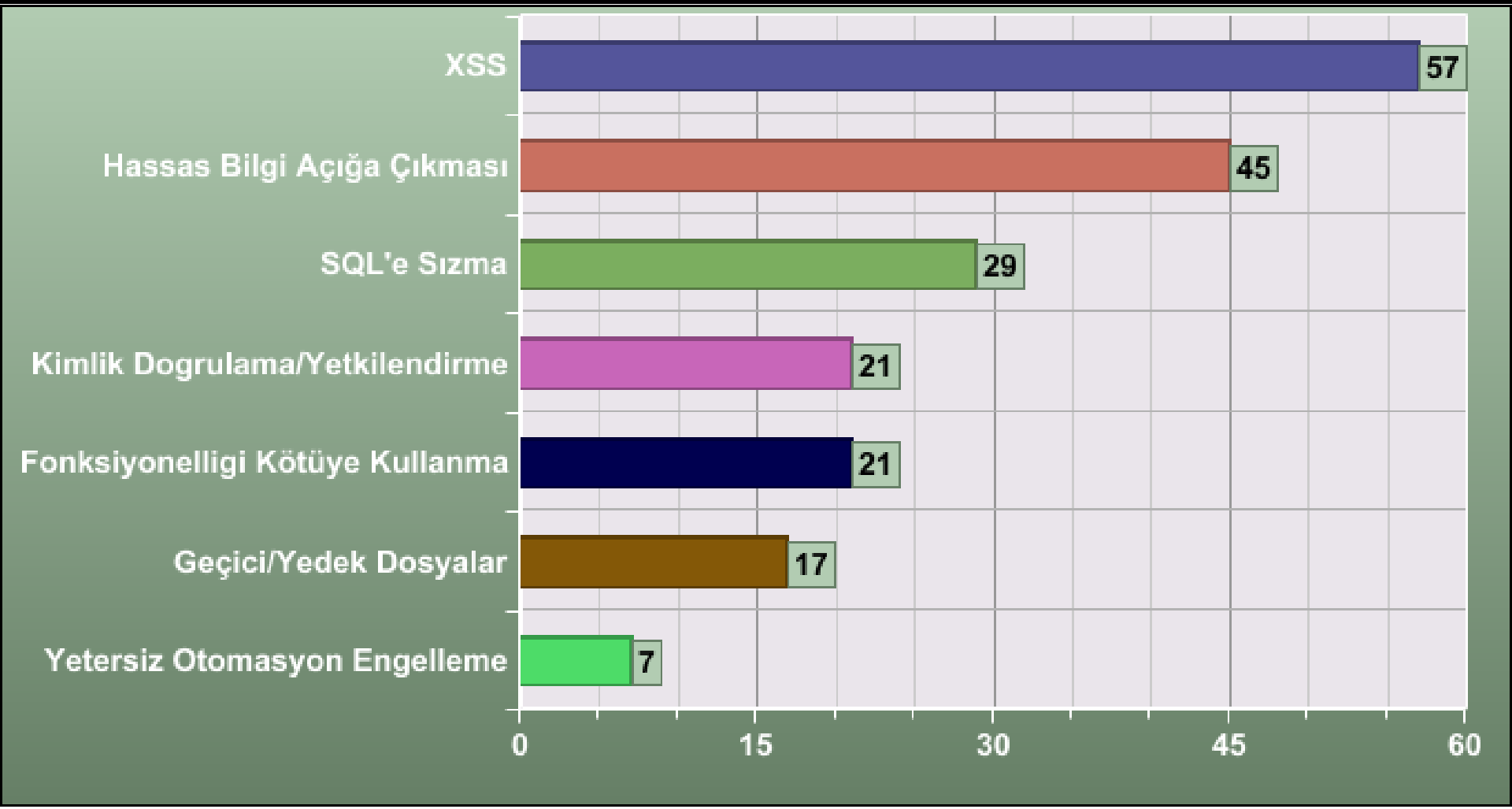
Veri İçeriği

- 1 Ocak – 31 Aralık 2010
- Sadece Türkiye'deki denetimler
- 100+ özel uygulama
- Tamamı doğrulanmış güvenlik açıkları

- Ekran görüntüleri veya istatistiklerde, herhangi bir firma, sektör, gerçek kişi vb. hakkında bilgi veya ipucu sunumda ve konuşmada bulunmamaktadır

Sık Karşılaşılan Güvenlik Açıkları

Denetlenen web uygulamalarının açığı bulundurma yüzdesi



Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

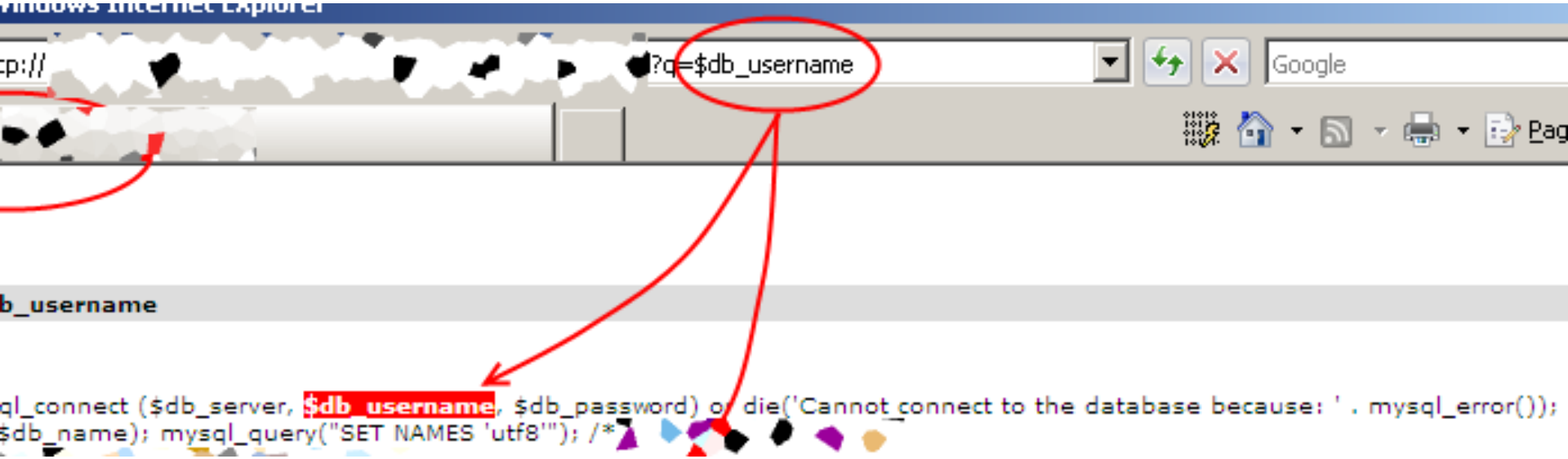
- XSS - Siteler Arası Kod Çalıştırma (%57)
  - Reflected (~ %90)
  - Stored (~ %10)
- SQL'e Sızma açığı olan her uygulamanın bir bölümünde XSS problemi bulundurduğu görülmüştür

Sık Karşılaşılan Güvenlik Açıkları

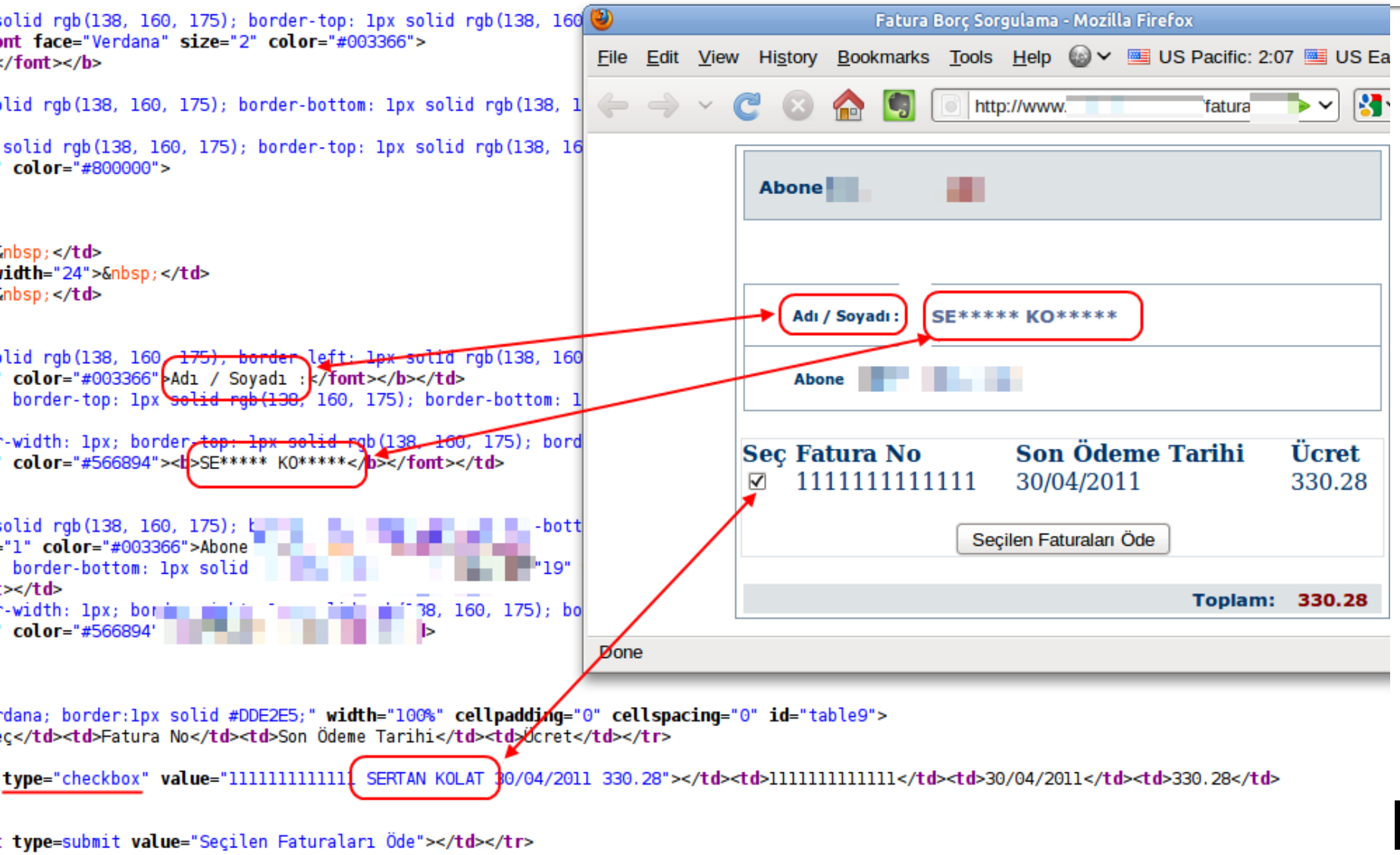
Diğer istatistikler…

- Hassas Bilgilerin Açığa Çıkması (%45)
  - Hata mesajları (fiziksel klasör, iç IP yapısı, veritabanı bilgileri)
  - HTML yorum satırlarındaki bilgiler <!-- comments --> (include dosyaları, url rewrite ayarları, güvenlik açığı bulunan eski sayfaların adresleri)
  - Kullanıcı adı, email adresi gibi bilgileri ele verme
  - Yardım dosyaları (Uygulama hakkında detaylı bilgi)

Hassas Bilgilerin Açığa Çıkması 1



Hassas Bilgilerin Açığa Çıkması 2



Hassas Bilgilerin Açığa Çıkması 3

```
144
145 <script type="text/javascript">
146
147     document.getElementById('email').setAttribute('value',
    '                    ');
148     document.getElementById('password').setAttribute('value', '
149
150     document.getElementById('login_screen').setAttribute('style', 'disp
151     document.getElementById('copyright').setAttribute('style', 'display
152
153     document.getElementById('submit').click();
154
155 </script>
156 </body>
157 </html>
```

Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

- SQL'e Sızma (SQL Injection) (%29)
  - Veritabanından veri okunabilmesi/yazılabilmesi (Blind SQL Injection, UNION, OOB kanalı)
  - Sistem üzerinde komut çalıştırma
  - Kimlik doğrulamanın aşılabilmesi
  - SQL hata mesajının görüntülenebildiği durumlar azalıyor

Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

- Kimlik Doğrulama/Yetkilendirme Problemleri (%21)
  - Anti-otomasyon mekanizmasının olmayışı
  - Zayıf şifreler
  - Şifreli bölümlere şifresiz erişim
  - Beni hatırla özelliği
  - Diğer kullanıcıların bilgilerine erişme

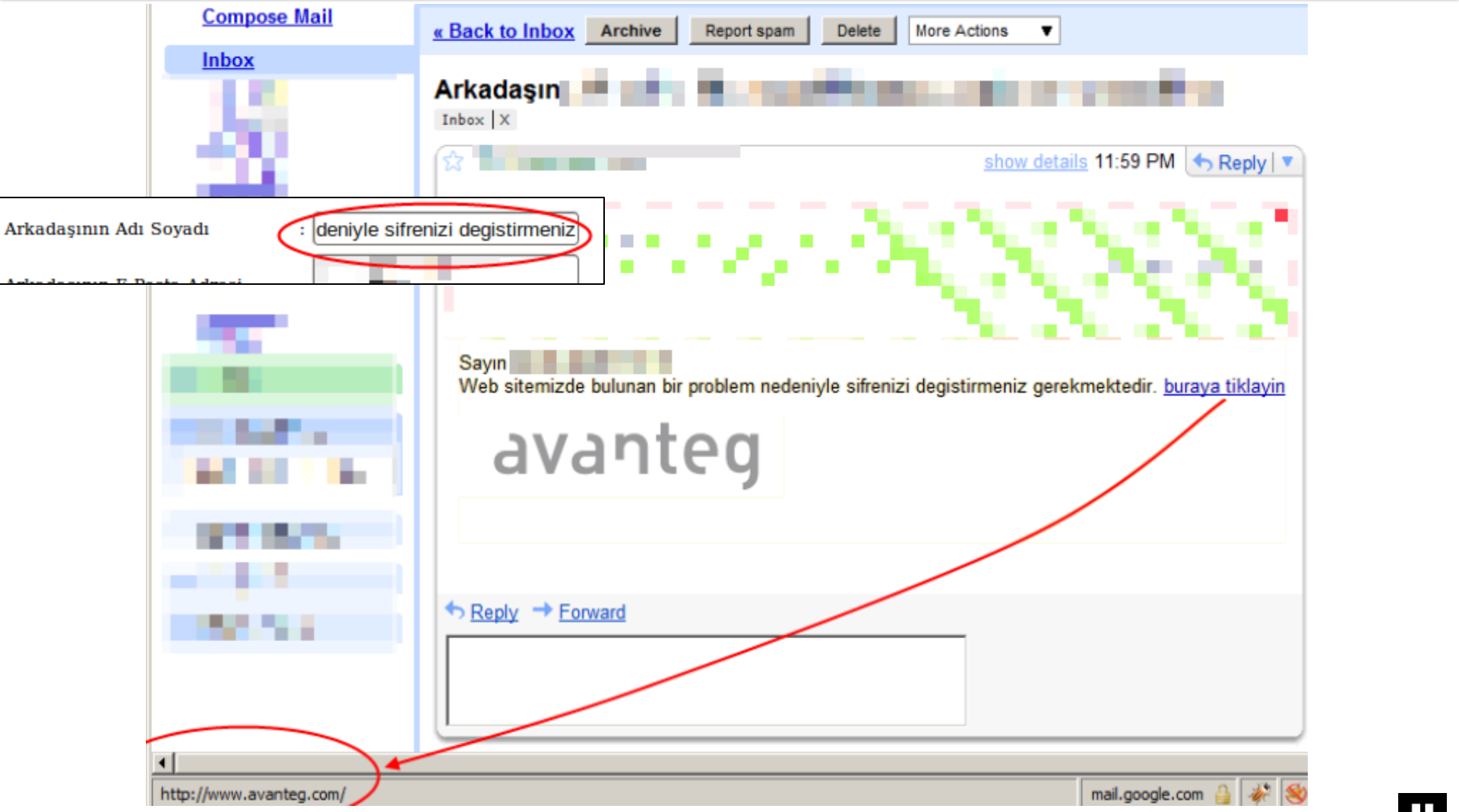
Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

- Fonksiyonelliği Kötüye Kullanma (%21)
  - Mail ile gönderme özelliği
  - URL yönlendirme
  - eShoplifting (sadece para değil, ödül puanı kullanılan uygulamalarda da karşılaşılmaktadır)

Fonksiyonelliği Kötüye Kullanma

Fonksiyonelliği Kötüye Kullanma

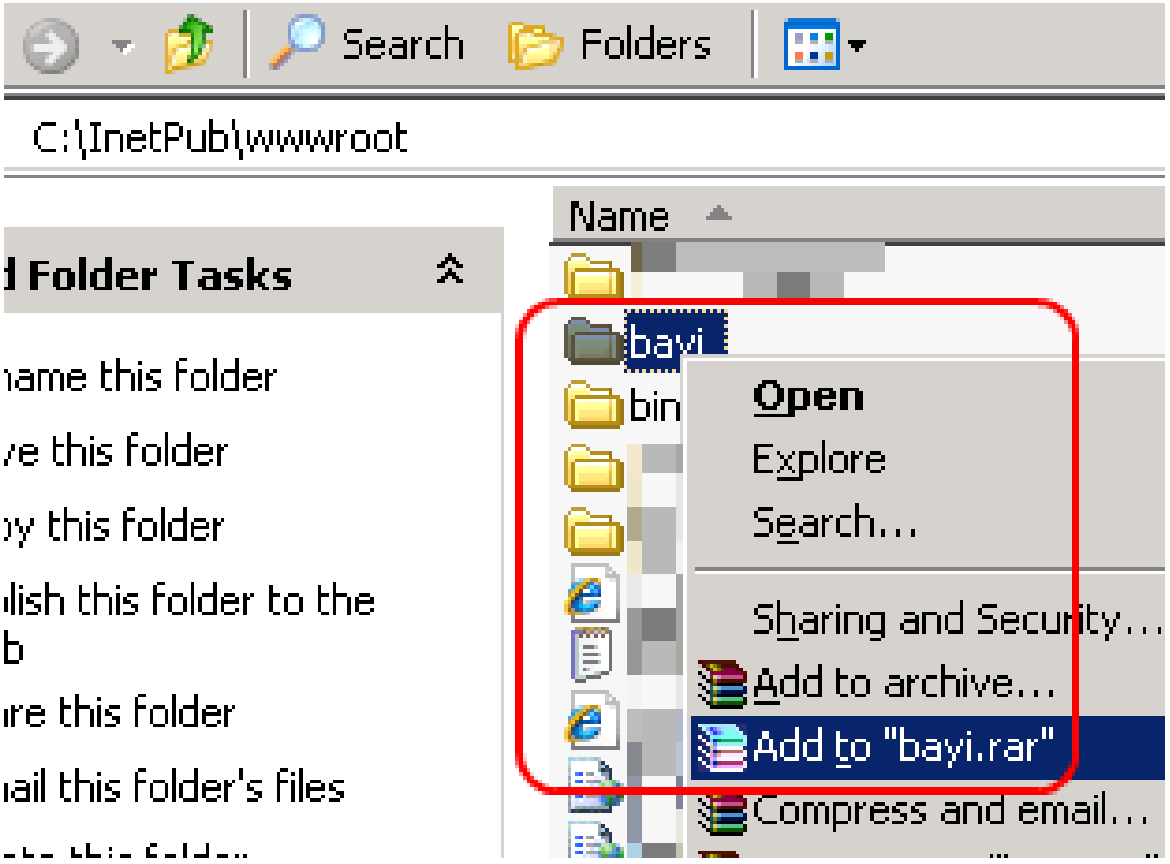


Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

- Geçici/Yedek Dosyalar (%17)
  - Sıkıştırılmış klasörler (klasör.rar, klasör.zip)
  - Değiştirilmeden önce yedeklenen dosyalar (Copy of …, Kopya …, .old, .orig, .bak)
  - Test dosyaları (phpinfo, odbc kontrol sayfaları vd)

Sıkıştırılmış Klasör



Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

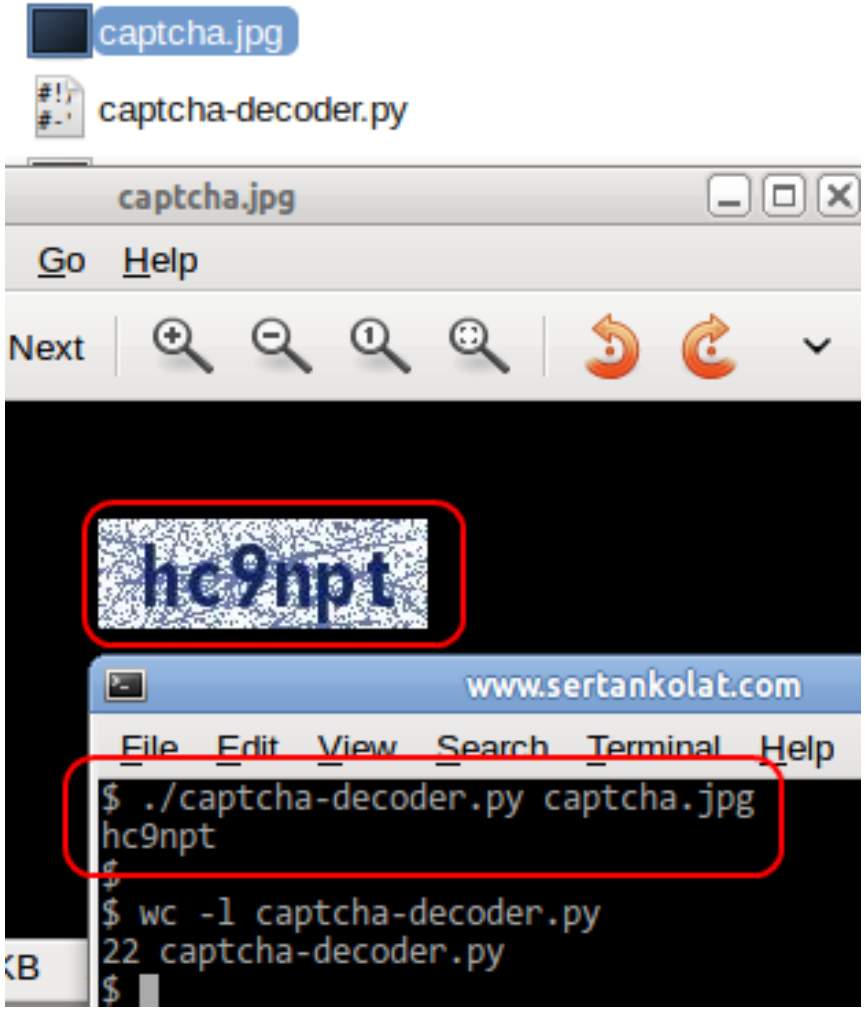
- Yetersiz otomasyon engelleme (%7)
  - Zayıf CAPTCHA implementasyonları

Zayıf CAPTCHA


```
$ ./decode_captcha https://www.[redacted].asp
[redacted]  86x21x24
```

CAPTCHA icerigi: O51041

Zayıf CAPTCHA



hc9npt

Sık Karşılaşılan Güvenlik Açıkları

Diğer istatistikler…

- Diğer güvenlik problemleri, her biri ayrı ayrı tüm denetlenen uygulamalarda %7 altında
  - File Inclusion (< %7)
  - CSRF – Cross Site Request Forgery (< %7)
  - XPath Injection (< %7)
  - İzinsiz dosya okuma (< %7)
  - File upload fonksiyonlarındaki zaafiyetler (<%7)
  - Diğer güvenlik problemleri (<%7)

Teşekkürler!

İletişim

Sertan Kolat

sertan@gmail.com

sertankolat.com

twitter: @warex

avanteg

www.avanteg.com

denetim@avanteg.com