

İÇİNDEKİLER

BÖLÜM 1: UYGULAMA GÜVENLİĞİ TEMELLERİ	1
Yazılım Güvenliği	2
Yazılım Güvenliği Olgunluk Modelleri	4
OpenSAMM	6
Tehdit Modelleme	7
Güvenli Kod Denetimi	8
Statik Kod Analizi	9
Sızma Testleri-Pentest	10
BÖLÜM 2: WEB STANDARDI	13
Ne Kadar Karmaşık Olabilir ki?	14
HTML Standardı	16
HTML Yapısı	16
HTML Kodlama (HTML Encoding)	18
DHTML	19
Javascript Dili	20
Document Object Model (DOM)	21
DOM Inspector	21
Anahtar Fonksiyonlar ve Önemli DOM API'ları	22
URL Standardı	23
URL Yapısı	23
URL Kodlama (URL Encoding)	24
HTTP Standardı	25
HTTP İstek Yapısı ve Çeşitleri	26
HTTP Cevap Yapısı ve Çeşitleri	27
HTTP Trafiği Yakalama	28
Firebug	29

Live HTTP Headers	30
Kişisel Vekiller (Proxy)	31
Amacı Ve Çalışma Prensipleri	31
OWASP ZAP	32
Same Origin Policy (Aynı Kaynak Politikası)	34
Tanımı ve Amacı	34
SQL	36
Tanımı ve Çeşitleri	36
Mantıksal İfadeler	39
İkili Arama Algoritması (Binary Search)	40
ASCII Tablosu	42
BÖLÜM 3: DOĞRULAMA EĞİLİMİ	45
Tanımı	46
2-4-6 Problemi	46
Şüpheli Yaklaşım	47
Tamsayı Taşması (Integer Overflow)	47
Tamsayı Taşması Java Uygulaması	48
BÖLÜM 4: WEB UYGULAMA GÜVENLİK TARAYICILARI	51
Tanım	52
Genel Çalışma Prensipleri	52
Girdi Keşfi	52
Zafiyet Bulma	53
Netsparker	54
Netsparker ile Hemen Taramaya Başlayın	57
Netsparker GUI	59
Custom Cookie Kullanımı	63
Encoder	64

BÖLÜM 5: GİRDİ NOKTALARI KEŞİF TEKNİKLERİ	67
Uygulamalar ve Girdi Noktaları	68
Firefox Web Developer Tool	68
Link Keşfetme Teknikleri (Crawling)	70
Paros	71
Owasp-Dirbuster	72
Web 2.0 Crawler Boy Ölçer (WIVET)	73
BÖLÜM 6: HTTP METOTLARI	75
HTTP Metot Tanımları	76
Bilgi Toplama	78
Sunucu Üzerinde Yönetim (WebDav)	78
BÖLÜM 7: KİMLİK DOĞRULAMA	85
Tanım	86
Kimlik Doğrulama Faktörleri	86
Kimlik Doğrulama Metotları	87
Kimlik Doğrulama Çeşitleri	87
Basic	87
DIGEST	90
Bütünleşik (Integrated) Windows Kimlik Doğrulama	92
Sertifika Tabanlı	93
Form Tabanlı	93
Kimlik Doğrulama Stratejileri	94
İstemci/Sunucu Tarafı Kimlik Doğrulama	94
Öntanımlı Kullanıcı Problemi	95
Kullanıcı Adı ve Parola Politikaları	95
Basit Uygulama Politikası (Kişisel Blog)	95
Karmaşık Uygulama Politikası (İnternet Bankacılığı)	96

Parola Depolama Politikası	97
Hashing	97
Sözlük Tabanlı Denemeler	98
Rainbow Tabloları	99
Parolaların Tuzlanması (Salt)	99
Parola Hash Değerlerinde İterasyon	100
Zayıf Hashing Algoritmaları	101
Güvenilir Parola Saklama Politikası	101
Parola Değiştirme Politikası	101
Kimlik Doğrulama Trafiğinin Güvenliği	102
Parola Kurtarma (Şifremi Unuttum) Operasyonları	102
Gizli Soru ve Cevaplar	103
Beni Hatırla (Remember Me)	104
Kayıt Tutma	105
Güvenli Çıkış	105
Kimlik Doğrulama Yöntemleri	107
Pozitif Kimlik Doğrulama	107
Negatif Kimlik Doğrulama	107
Kimlik Doğrulama Sonrası 200 vs. 302	108
Kimlik Doğrulama Mekanizmalarında Hata Yönetimi	109
BÖLÜM 8: DENEME YANILMA SALDIRILARI (BRUTE-FORCE)	113
Tanımı	114
Sözlük Tabanlı Saldırıları	114
Kaba Kuvvet Saldırıları	117
Yatay Yöntem	117
Dikey Yöntem	121

Diagonal (Çapraz) Yöntem	121
Üç Boyutlu Yöntem	122
Uygulama Kullanıcı Adı Listesi Çıkartılması	122
Burp Intruder ile Farklı Senaryolar	127
Kaba Kuvvet Saldırılarına Karşın Önlemler	129
Form Otomasyonlarına Karşın Önlemler	129
Kimlik Doğrulama İşlemlerine Gecikme Süresi Ekleme	132
Detaylı Hata Mesajları	133
Doğru Bilinen Yanlıřlar	133
BÖLÜM 9: CAPTCHA	135
Tanımı	136
Kullanım Alanları	136
Güvensiz Captcha Uygulamaları ve Zafiyetleri	137
Aritmetik Captcha	137
Metin Tabanlı Captcha	138
İstemcide Saklanan Captcha Cevapları	139
İstemci Tarafalı Captcha Kontrolleri	140
Zayıf Captcha Resimleri	141
Tekrarlama Saldırıları	142
CAPTCHA Resmi Kirma Teknikleri	144
İnsan Kaynağı	144
OCR ve Tesseract	145
Güvenli Captcha Kullanımı	148
Güvenli Tasarım	148
Güvenli Resim	149
reCAPTCHA	149

BÖLÜM 10: BAĞLANTI GÜVENLİĞİ SSL	153
Tanım	154
SSL Tokalaşması ve Kimlik Denetimi	154
Dijital Sertifikalar	155
Intranet ve Self-Signed Sertifikaları	157
SSL Sürümleri	158
SSL Saldırıları	158
BasicConstraints ile MITM Saldırısı	158
Renegotiation Saldırısı	158
Beast	160
SSL Güvenliğini Test Etme	161
SSL Zayıf Şifreleme Algoritmaları Kontrolü	161
SSL/TLS Sürüm Kontrolü	162
Renegotiation Kontrolü	164
Dijital Sertifika Kontrolü	165
Ssl Güvenli Yapılandırma	165
Apache Web Sunucusu	165
Iis Web Sunucusu	166
BÖLÜM 11: OTURUM YÖNETİMİ	169
Tanım	170
Oturum Anahtarı	171
Zayıf Oturum Anahtarları	171
Güvenli Oturum Anahtarları	175
Cookie	175
Cookie'lerin Özellikleri	175
Güvenli Cookie	177

BÖLÜM 12: OTURUM SABİTLEME (SESSION FIXATION)	179
Hırsızlığa Karşı Alınması Gereken Önlemler	180
Oturum Sabitleme (Session Fixation)	180
Cookie Oluşturma Yöntemleri	183
URL ile Cookie Oluşturma	183
Javascript ile Cookie Oluşturma	183
Meta Etiketleri ile Cookie Oluşturma	184
HTTP Cevap Başlığı ile Cookie Oluşturma	184
Oturum Sabitleme Saldırılarına Karşın Önlemler	185
BÖLÜM 13: SİTELER ARASI İSTEK SAHTECİLİĞİ (CSRF)	189
CSRF Nedir?	190
CSRF Tuzakları Hazırlama	192
Owasp CSRF Tester	194
CSRF Saldırılarına Karşın Önlemler	195
Owasp CSRFguard (Java)	196
PHP'de CSRF Saldırılarından Korunma	200
Asp.net'de CSRF Saldırılarından Korunma	202
ViewState	202
AntiForgeryToken	205
BÖLÜM 14: DİZİN GEZİNİMİ	209
Tanımı	210
Şüpheli Noktalar	211
Uygulamaya Yönelik Dizin Gezinimi Saldırıları	212
İşletim Sistemine Yönelik Dizin Gezinimi ve Saldırıları	213
Dizin Gezinimi Saldırılarının Otomatize Edilmesi	215
Dizin Gezinimi Saldırılarına Karşın Önlemler	219

BÖLÜM 15: KOD/DOSYA ENJEKSİYONU (RFI/LFI)	223
Tanımı	224
Dosya Dâhil Etme (File Inclusion) Saldırıları	224
RFI (Remote File Inclusion)	225
PHP Uygulamalarında RFI	226
JAVA/JSP Uygulamalarında RFI	228
ASP.Net Uygulamalarında RFI	231
LFI (Local File Inclusion)	232
PHP Uygulamalarında LFI İstismarı	233
Java/JSP Uygulamalarında LFI	238
ASP.Net Uygulamalarında LFI	240
Kod/Dosya Dâhil Etme Saldırılarına Karşın Önlemler	241
BÖLÜM 16: İŞLETİM SİSTEMİ KOMUT ENJEKSİYONU	245
Tanımı	246
İşletim Sistemi Komut Çalıştırma Enjeksiyonu Örnekleri	247
PHP	247
.NET	249
JAVA	252
İşletim Sistemi Komut Enjeksiyonuna Karşın Önlemler	253
BÖLÜM 17: XSS (CROSS SITE SCRIPTİNG)	257
Tanım	258
Yansıtılmış (Reflected) XSS	259
Depolanmış (Stored/Persistent) XSS	264
Birinci Kademe Depolanmış XSS	264
İkinci Kademe Depolanmış XSS	265
Dom Tabanlı XSS	266

Phishing	269
XSS Zafiyetinin Çözümü	272
Microsoft Anti-XSS (.Net)	273
Owasp-Esapı (Java)	281
PHP'de XSS Önlemi	287
Dom Tabanlı XSS Önlemi-Jquery.Encoder	292
BÖLÜM 18: SQL ENJEKSİYONU	297
Tanımı	298
SQL Enjeksiyonu Zafiyeti Çeşitleri	301
Genel SQL Enjeksiyonu	301
Union Tabanlı (Union Based) SQL Enjeksiyonu	303
Hata Tabanlı (Error Based) SQL Enjeksiyonu	308
Kör (Blind) SQL Enjeksiyonu	310
Zaman Tabanlı (Time Based) SQL Enjeksiyonu	314
Farklı SQL İfadelerinde SQL Enjeksiyon Zafiyeti	319
İleri Seviye SQL Enjeksiyon Zafiyeti Çeşitleri	323
İşletim Sistemi Etkili	323
Kanal Dışı	325
İkinci Kademe	326
Fonksiyonaliteye SQL Enjeksiyonu ile Saldırı	327
SQL Enjeksiyonu ile Giriş Sayfası İstismarı	327
SQL Enjeksiyonu ile Parolamı Unuttum Formu İstismarı	330
SQL Enjeksiyonu Zafiyetinin Otomatizasyonu	331
SQLMap	331
SQL Enjeksiyonu Zafiyetinin Çözümü	332

BÖLÜM 19: HTTP BAŞLIK MANİPÜLASYONU	335
Tanım	336
HTTP Başlık Enjeksiyonu	336
HTTP Başlık Enjeksiyonu ile Oturum Sabitleme	337
HTTP Başlık Enjeksiyonu ile Siteler Arası Betik Çalıştırma	338
HTTP Cevap Bölme (Http Response Splitting)	338
Web Önbellek Zehirleme (Web Cache Poisoning)	340
HTTP Başlık Manipülasyonu Önleme	342
BÖLÜM 20: İŞ MANTIĞI PROBLEMLERİ	345
Tanım	346
Bir Proje Hikâyesi	346
Yaygın İş Mantığı Zafiyetleri	347
Şifremi Unuttum	347
Finansal Algoritmalar	348
Teknik Olmayan Hizmet Dışı Saldırıları	348
İstemci Tarafı Veri Kontrolü	348
Time of Check, Time of Use	350
Google Hesap Yönetimi	350
BÖLÜM 21: HAK YÜKSELTME (YETKİLENDİRME EKSİKLİKLERİ)	353
Tanım	354
Dikey ve Yatay Hak Yükseltme	354
Örnek Uygulamalar	355
Otomatize Test Yöntemleri (Karşılaştırma Yöntemi)	356

BÖLÜM 22: YAYINLANMIŞ ZAFİYET ARAMA TEKNİKLERİ	363
Tanım	364
Uygulama Sürüm Bilgisi Belirleme	364
Yayınlanmış Açıklık İçin Exploit Arama	366
Exploit'in Uygulanması	366
WhatWeb	368
BÖLÜM 23: GOOGLE HACKING	371
Google Nasıl Çalışır?	372
Google Arama Teknikleri	373
Bilgi Toplama	374
Kurban Arama	376
SiteDigger	379
BÖLÜM 24: WEB SERVİSLERİ GÜVENLİĞİ	381
Tanım	382
Klasik Web Servisleri	382
Web Apı Web Servisleri	387
Web Servisi Güvenlik Testleri ve Saldırıları	388
Bilgi Toplama	388
Güvensiz Tasarım	390
Parsing Saldırıları	397
Referans Saldırıları	399
Web Servisi Saldırılarına Karşın Önlemler	402
BÖLÜM 25: HİZMET DIŞI BIRAKMA SALDIRILARI (DOS)	405
Tanım	406
Kullanıcı Hesap Kilitleme	406
Otomatik Form Gönderme	408

Veri Tabanı Wildcard Sorguları (Arama Tabanlı Dos)	410
Limitsiz Dosya Yükleme	413
Veritabanı Bırakılmayan Kaynaklar	415
Son Kullanıcı Kontrollü Parametreler	418
Uygulama Dışı Servislerin Kesintisi	419
HTTP Protokolü Kaynaklı Servis Kesintisi Saldırıları	419
Slow Headers (Slowlories)	420
Slow POST	421
GET Flood	422
POST Flood	422
HashDoS	423