

WEB UYGULAMA GÜVENLİĞİ VE HACKING YÖNTEMLERİ

ERHAN SAYGILI

İÇİNDEKİLER

BÖLÜM 1: Giriş	1
Sektörden Temel Bilgiler	2
Hacker	2
Siyah Şapkalı Hacker	3
Gri Şapkalı Hacker	3
Beyaz Şapkalı Hacker	3
Hacktivist	3
Vulnerability (Güvenlik Açığı)	3
Penetrasyon Testi	4
Penetrasyon Test Çeşitleri	4
White Box	4
Black Box	4
Gray Box	4
Penetrasyon Test Türleri	4
Ağ Penetrasyon Testi	4
Web Uygulama Penetrasyon Testi	5
Mobil Uygulama Penetrasyon Testi	5
Sosyal Mühendislik Penetrasyon Testi	5
Fiziksel Penetrasyon Testi	5
Penetrasyon Test Adımları	5
Bilgi Toplama	6
Ağ Haritasının Çıkartılması	6
Zafiyet Tarama	6
Sisteme Sızma	6
Yetki Yükseltme	7
Başka Ağlara Sızma	7

Erişimi Koruma/Kalıcı Hale Getirme	7
İzleri Temizleme	7
Raporlama	7
Neler Öğrendik?	7
BÖLÜM 2: TEMEL PROGRAMLAR VE İŞLETİM SİSTEMİ KURULUMU	9
VirtualBox	10
VirtualBox Kurulum Aşamaları	10
Parrot Security OS	11
Parrot Security OS Kurulum Aşamaları	12
WampServer	22
WampServer Kurulum Aşamaları	22
WampServer'da Farklı Bir Port Kullanmak	27
WampServer ile Local Ağda Yayın Yapmak	28
Neler Öğrendik?	29
BÖLÜM 3: TEMEL LINUX KOMUTLARI	31
Linux	32
\$	32
#	32
~	33
Linux Dosya/Dizin Hiyerarşisi	33
Genel Amaçlı Komutlar	39
man Komutu	39
apropos Komutu	39
halt Komutu	40
reboot Komutu	40
help, h Komutu	41
type Komutu	41

exit Komutu	42
su Komutu	42
pwd Komutu	43
history Komutu	43
Dosya Komutları	44
ls Komutu	44
cd Komutu	45
sort Komutu	46
mkdir Komutu	48
rm Komutu	48
cp Komutu	49
mv Komutu	49
wc Komutu	50
ln Komutu	50
touch Komutu	51
cat Komutu	52
echo Komutu	54
more Komutu	54
head Komutu	55
tail Komutu	55
chmod Komutu	56
gzip Komutu	57
gunzip Komutu	57
alias Komutu	58
Sistem Komutları	58
date Komutu	58
uptime Komutu	59
cal Komutu	59

df Komutu	60
du Komutu	61
free Komutu	61
whereis Komutu	62
which Komutu	62
uname Komutu	62
w Komutu	64
whoami Komutu	64
hostname Komutu	65
time Komutu	65
who Komutu	66
lsmod Komutu	66
cat /proc/cpuinfo Komutu	67
cat /proc/meminfo Komutu	67
Proses Yönetimi Komutları	68
ps Komutu	68
top Komutu	69
kill Komutu	70
pidof Komutu	70
pgrep Komutu	70
pstree Komutu	71
write Komutu	72
last Komutu	72
Arama Komutları	73
grep Komutu	73
find Komutu	74
Network Komutları	74
ping Komutu	74
traceroute Komutu	75

dig Komutu	76
wget Komutu	76
ifconfig Komutu	77
host Komutu	78
Paket Kurulum Komutları	78
dpkg Komutu	78
apt-get Komutu	79
Neler Öğrendik?	80
BÖLÜM 4: AKTİF VE PASİF BİLGİ TOPLAMA TEKNİKLERİ	83
Hedef Sistem Hakkında Bilgi Toplama Yöntemleri	84
whois	84
ping	85
theharvester Aracının Kullanımı	86
Dmitry Aracının Kullanımı	88
Fierce Aracının Kullanımı	90
URLcrazy Aracının Kullanımı	92
wafw00n Aracının Kullanımı	92
WhatWeb Aracının Kullanımı	94
IPS-IDS Tespiti	94
Nmap ile Firewall Kontrolü	95
Hedef Sistem Hakkında İnternet Ortamında Bilgi Toplama	96
robtex.com	96
bing.com	96
serversnif.net	97
centralops.net	97
web.archive.org	97
netcraft.com	97
pipl.com	97

sitedigger	97
whois.net	97
ripe.net ve arin.net	97
mxtoolbox.com	97
Google Hacking	98
Bazı Arama Operatörleri ve Kullanım Şekilleri	98
site Operatörü	98
filetype Operatörü	98
" " Operatörü	98
- Operatörü	99
.. Operatörü	99
+ (And) Operatörü	99
(Or) Operatörü	99
link Operatörü	99
related Operatörü	100
info Operatörü	100
allintitle Operatörü	100
intitle Operatörü	100
allinurl Operatörü	101
inurl Operatörü	101
cache Operatörü	102
intext Operatörü	102
mail Operatörü	102
Neler Öğrendik?	102

BÖLÜM 5: WEB TABANLI UYGULAMALAR VE TEMEL BİLGİLER	105
Web Tabanlı Uygulama	106
Web Tabanlı Uygulama Örnekleri	106
Web Tabanlı Uygulamalarının Çalışma Prensipleri	106
Web Tabanlı Uygulama Geliştirme	107
Web Uygulama Güvenliği	107
HTTP ve HTTPS	107
HTTP ile HTTPS Arasındaki Farklar	108
HTTP Başlıkları	108
HTTP Başlık Analizi	109
HTTP Request	113
HTTP Response	114
HTTP Metotları	115
GET	115
POST	116
HEAD	117
TRACE	118
OPTIONS	119
PUT	120
DELETE	120
CONNECT	120
HTTP Durum Kodları	120
En Sık Karşılaşılan Durum Kodları	121
200 OK	121
206 Partial Content (Kısmi İçerik)	121
302 (or 307) Moved Temporarily & 301 Moved Permanently	121
401 Unauthorized (Yetkisiz)	122
403 Forbidden (Yasak)	122

404 Not Found	122
500 Internal Server Error (Dahili Sunucu Hatası)	123
HTTP İsteklerindeki Genel HTTP Başlık Parametreleri	123
Host	123
User-Agent	123
Accept	123
Accept-Language	124
Accept-Encoding	124
If-Modified-Since	124
Cookie	125
Referer	125
Authorization	125
HTTP Yanıtlarında Bulunan HTTP Başlık Parametreleri	127
Cache-Control	127
Content-Type	128
Content-Length	129
Etag	130
Last-Modified	130
Location	130
Set-Cookie	132
www-Authenticate	134
Content-Encoding	136
Server	136
Date	136
Keep-Alive	136
Connection	136
URL	137
URL Encoding	137
Neler Öğrendik?	139

BÖLÜM 6: VERİTABANI 141

SQL	142
SQL Deyimleri	144
Create	144
Use	148
Insert Into	148
Select	149
Where	150
Delete	151
Update	151
Alter Table	151
And/Or	152
Limit	153
In	154
Between	155
Like	155
Order By	157
Union	158
Drop	158
Join	159
Neler Öğrendik?	159

BÖLÜM 7: WEB GÜVENLİK ZAFİYETLERİNDE KULLANILAN PROGRAM VE ARAÇLAR161

Burp Suite	162
Firefox'u BurpSuite ile Çalışacak Şekilde Yapılandırma	162
Tarayıcı Proxy Yapılandırmasını Denetleme	164
Firefox'a Burp Suite CA Sertifikasını Yükleme	165

Burp Suite Menüleri	166
Target	167
Proxy	167
Spider	168
Scanner	168
Intruder	169
Repeater	169
Sequencer	170
Decoder	170
Comparer	170
Extender	171
Project Options	171
Alerts	171
Burp Suite ile Brute Force Saldırısı	172
Sqlmap	177
Windows'a Sqlmap Kurulumu	177
Python Kurulumu	177
Sqlmap Kurulumu	179
Sqlmap Parametreleri	181
Options	182
Target	183
Request	184
Optimization	190
Injection	191
Detection	193
Techniques	195
Fingerprint	196
Enumeration	196

Brute Force	202
User-Defined Function Injection	203
File System Access	203
Operation System Access	204
Windows Registry Access	205
General	206
Miscellaneous	209
Sqlmap Kullanımı	211
Crunch Aracının Kullanımı	219
hash-identifier Aracının Kullanımı	223
Findmyhash Aracının Kullanımı	224
Nikto Aracının Kullanımı	224
Dirbuster Aracının Kullanımı	226
Wapiti Aracının Kullanımı	227
Uniscan Aracının Kullanımı	227
Neler Öğrendik?	229
BÖLÜM 8: OWASP, WAF VE BAZI WEB GÜVENLİK ZAFİYETLERİ	231
OWASP	232
WAF	232
Command Injection	233
SQL Injection	237
Veri Giriş Alanlarının Belirlenmesi	238
Veri Akışı	240
SQL Injection Tespiti	241
SQL Injection'u Sonlandırma	241
Dize Birleştirme	243
SQL Injection Sırasında Veri Akışı	244

SQL Injection Türleri	245
Error-based SQL Injection	245
Union-based SQL Injection	246
Kolon Sayısının Tespiti	247
MySQL Versiyonunun Tespiti	251
Veritabanında Bulunan Tablo Adlarının Tespiti	252
Veritabanında Bulunan Bir Tabloya Ait Kolonlarının Tespiti	254
Tablo ve Kolon İsimleri Tespit Edilen Veri Tabanından Veri Çekme	256
Blind SQL Injection	258
Boolean-Based (Content-Based) Blind SQL Injection	258
MySQL Versiyon Tespiti	260
Veri Tabanı İsmi'nin Uzunluğunun Tespiti	261
Veritabanı İsmi'nin Tespiti	262
Tablo İsimlerinin Tespiti	267
Kolon İsimlerinin Tespiti	274
Tablo ve Kolon İsmi Tespit Edilen Veritabanından Veri Çekme	279
Time-Based Blind SQL Injection	283
MySQL Versiyon Tespiti	285
Veritabanı İsmi'nin Tespiti	285
Tablo İsimlerinin Tespiti	286
Kolon İsimlerinin Tespiti	287
Tablo ve Kolon İsmi Tespit Edilen Veritabanından Veri Çekme	291
Zamana Dayalı Saldırıların Avantaj ve Dezavantajları	293
XSS (Cross Site Scripting)	293
Kullanıcıdan Alınan Verilerin Bazı Kullanım Alanları	295
XSS Zafiyetinin Verebileceği Zararlar	295
Çerez Hırsızlığı	295
Kimlik Hırsızlığı	296
Keylogger Ekleme	296

XSS Türleri	296
Stored XSS	296
Reflected XSS	298
DOM XSS	301
CSRF (Cross Site Request Forgery)	303
CSRF Zafiyetine Karşı Alınabilecek Önlemler	306
File Upload	307
File Inclusion	312
Local File Inclusion	312
Remote File Inclusion	312
File Inclusion Zafiyeti Nasıl Oluşur?	313
File Inclusion Zafiyetine Karşı Alınabilecek Güvenlik Önlemi	314
php.ini ile Web Shell Script'lerinin Etkisizleştirilmesi	315
Neler Öğrendik?	315
Dizin	317



Kitap içerisinde anlatılan konular; sadece meraklılarına ve bu alanda uzmanlaşmak isteyen kişilere bilgi vermek amacıyla hazırlanmıştır. Anlatılan konular ve yöntemler ile kişilerin, başkalarına zarar verebilecek davranışlarından dolayı yazar kesinlikle yasal bir sorumluluk kabul etmemektedir...