



# Web Uygulama Güven(siz)liği 2.0

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

<http://www.bga.com.tr>

honal@bga.com.tr



*Güvenlik lüks değil, gereksinimdir!*

# Ben Kimim?

- Kıdemli bilgi güvenliği uzmanı (İş hayatı)
- Ağ güvenliği araştırmacısı/uzmanı/. (Gerçek hayat)
- Özgür yazılım destekçisi
- Bilgi Güvenliği AKADEMİSİ güvenlik eğitmeni
  - [www.bga.com.tr](http://www.bga.com.tr)
- Blogger
  - [www.lifeoverip.net](http://www.lifeoverip.net)



# Ajanda

- Siber dünyada web uygulamaları
- Neden web uygulama güven(siz)liği?
- Web uygulamalarında güvenliği etkileyen bileşenler
- Türkiye ve dünyadan web uygulama güven(siz)liği örnekleri
- Güvenlik dünyası ve web uygulamalarına bakışı
- Hacker(medya) camiası ve web uygulamalarına bakışı
- Günün sonunda kazanan kim? Skor tablosu



# İşleyiş

- Sıcak bir yaz akşamına uygun...
- Teknik detaylara boğmadan, uygulama güvenliğine yazılımcı olmayan birinin bakış açısı ve tecrübeleri...



# Siber Dünyada Web

- Web uygulamaları günümüzü ve geleceğimizi kuşatmış durumda
  - Müzik dinleme: last.fm, fizy.org
  - Ofis Belgeleri için: Google Docs
  - Resim işleme amaçlı: Google Picasa, flickr
  - (A)Sosyal Hayat: Facebook, Friendfeed, twitter
  - Alışveriş, Para işleri: Paypal.com, online alışveriş siteleri
  - İletişim: E-posta->Webmail hizmetleri
  - Oyun: Online oyunlar...
  - Televizyon: IP TV uygulamaları
- Yakın gelecekte web tabanlı işletim sistemleri...



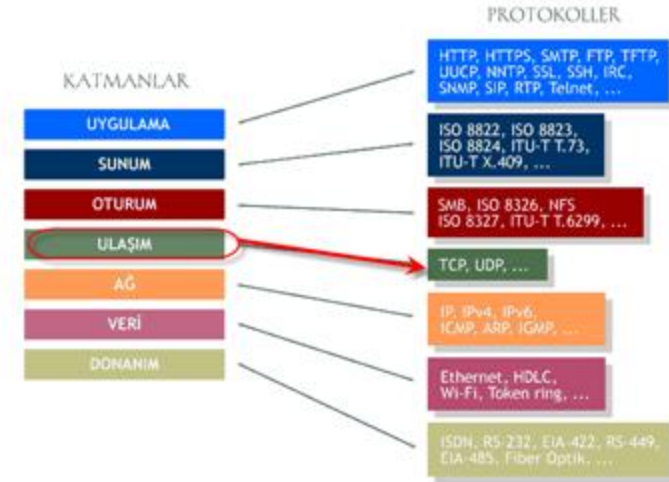
# Web'i Tanıyalım

- Web denilince artık akla iki üç sayfalık html+javascript karışımı sayfalar gelmiyor
- Web Uygulama Bileşenleri
  - Statik sayfalar
    - HTML
  - Dinamik sayfalar
    - CGI, ASP, PHP, Perl, Asp.net, JSP
  - Veritabanı
    - Mysql, MsSQL, Oracle, Sybase
  - Web servisleri
  - Kullanıcı browserları
  - Diğer bileşenler...
    - Ajax vs



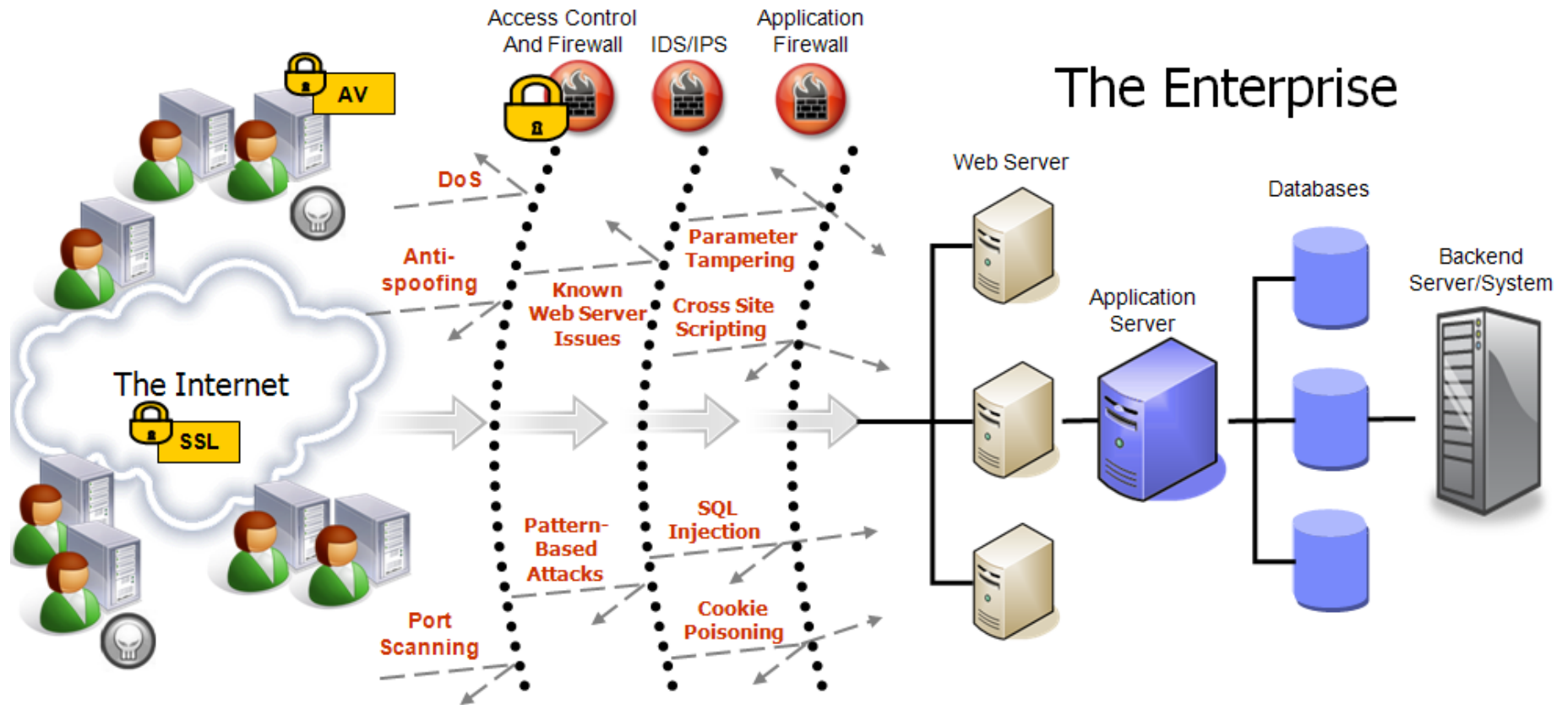
# Geleneksel Güvenlik Yaklaşımı

- Henüz OSI 4. katmandan yukarı çıkamamıştır
- Network, işletim sistemi ve servis güvenliği
- Router(ACL), Firewall
  - Intrusion Detection System
    - Intrusion Prevention System
  - » ....
- Ağırlık koruma tarafı için ayrılır
  - Güvenlikcilerin çoğu yeni saldırı yöntemlerinden habersizdir
- Web güvenliği tarihçesi
  - 2000~ web uygulamalarının yaygınlaşması
  - 2005~ Web uygulama güvenliği
  - 2009-2013 Web güvenliği altın çağı ☺



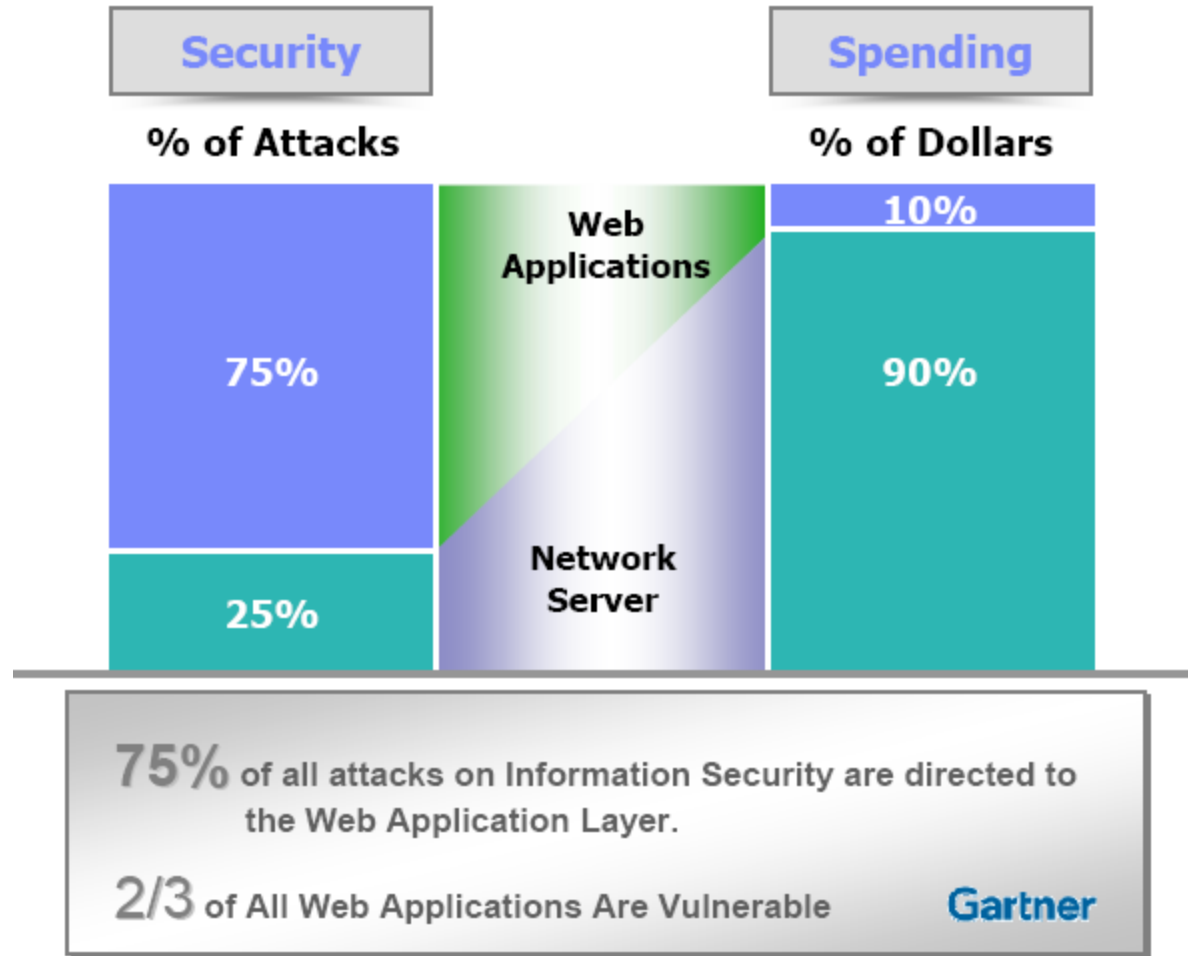


# Geleneksel Güvenlik Yaklaşımı-II



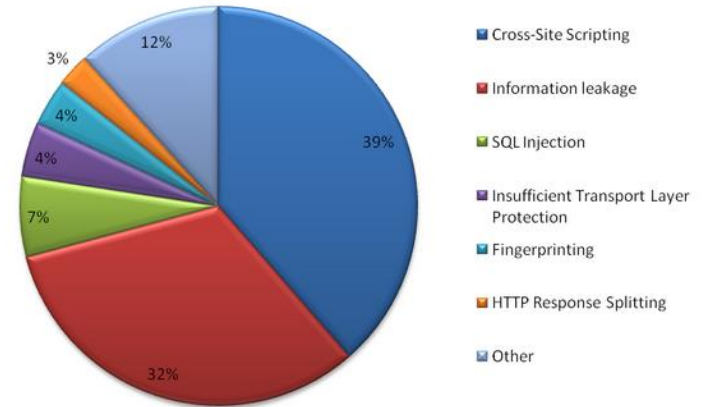


# Geleneksel Güvenlik Anlayışının Göstergesi



# Neden Uygulama/WEB Güvenliği?

- Web=Giriş kapısı
- Sınır güvenliğinin en zayıf noktalarından
- Güvenlikte en büyük problem: çözümü başka yerde aramak!
  - IPS ile spesifik uygulamalara yönelik atakları engellemeye çalışma
  - Çözüm kendi içinde 😊
- Hizmet veren herşey bir yazılımdır
- Problemi temelinden çözmek varken....



# Neden Web Güvenliği-II

## LexisNexis Data Breach

— Washington Post, Feb 17, 2008

**IndiaTimes.com Malware**  
— InformationWeek, Feb 17, 2008

**Mac blogs defaced by XSS**  
• The Register, Feb 17, 2008

**Chinese hacker steals 18M identities**  
— HackBase.com, Feb 10, 2008

**Hacker breaks into Ecuador's presidential website**

— The Indian, Feb 11,

**Greek Ministry websites hit by hacker intrusion**

— eKathimerini, Jan 31, 2008

**Hacker steals Davidson Cos client data**  
— Falls Tribune, Feb 4 2008

**200 Your Free MacWorld Expo Platinum Pass**

— CNet, Jan 14, 2008

**Hacking Stage 6**

— Wikipedia, Feb 9 2007

**Hacker takes down Pennsylvania gvm**

— AP, Jan 6, 2008

**Drive-by Pharming in the Wild**

— Symantec, Jan 21 2008

**Italian Bank hit by XSS fraudsters**

— Netcraft, Jan 8 2008

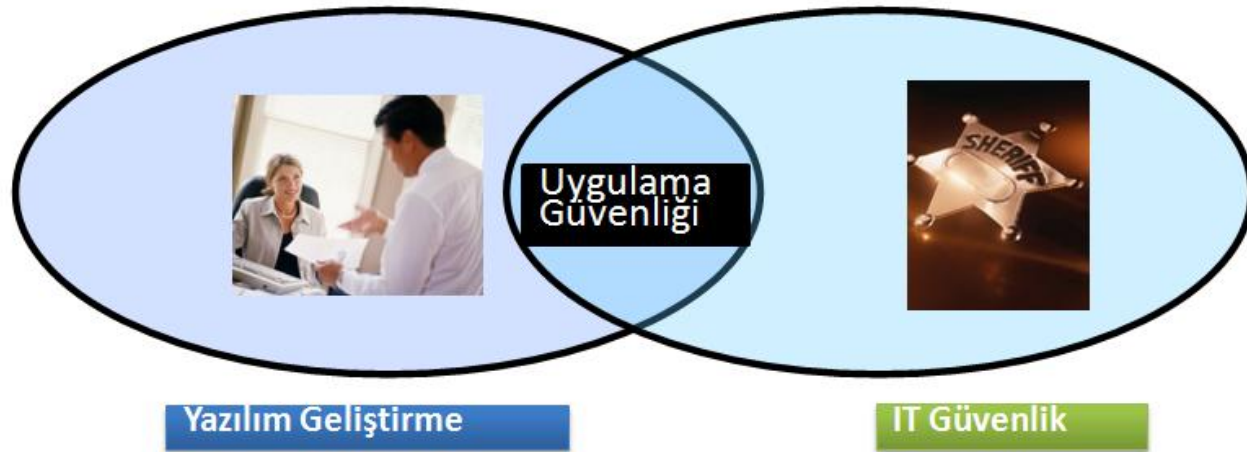
**RIAA wiped off the Net**

— TheRegister, Jan 20 2008



# Uygulama Güvenliđi Tanımı

- Yazılım geliřtiriciler en kısa sürede ortaya ürün çıkarma peřindeler.
- Güvenlik uzmanları yoğunlukla altyapı güvenliđine yönelmiřlerdir
- Uygulama Güvenliđi: Üretilen yazılımın fonksiyonlarını yitirmeden güvenli bir řekilde geliřtirilmesini sađlama.

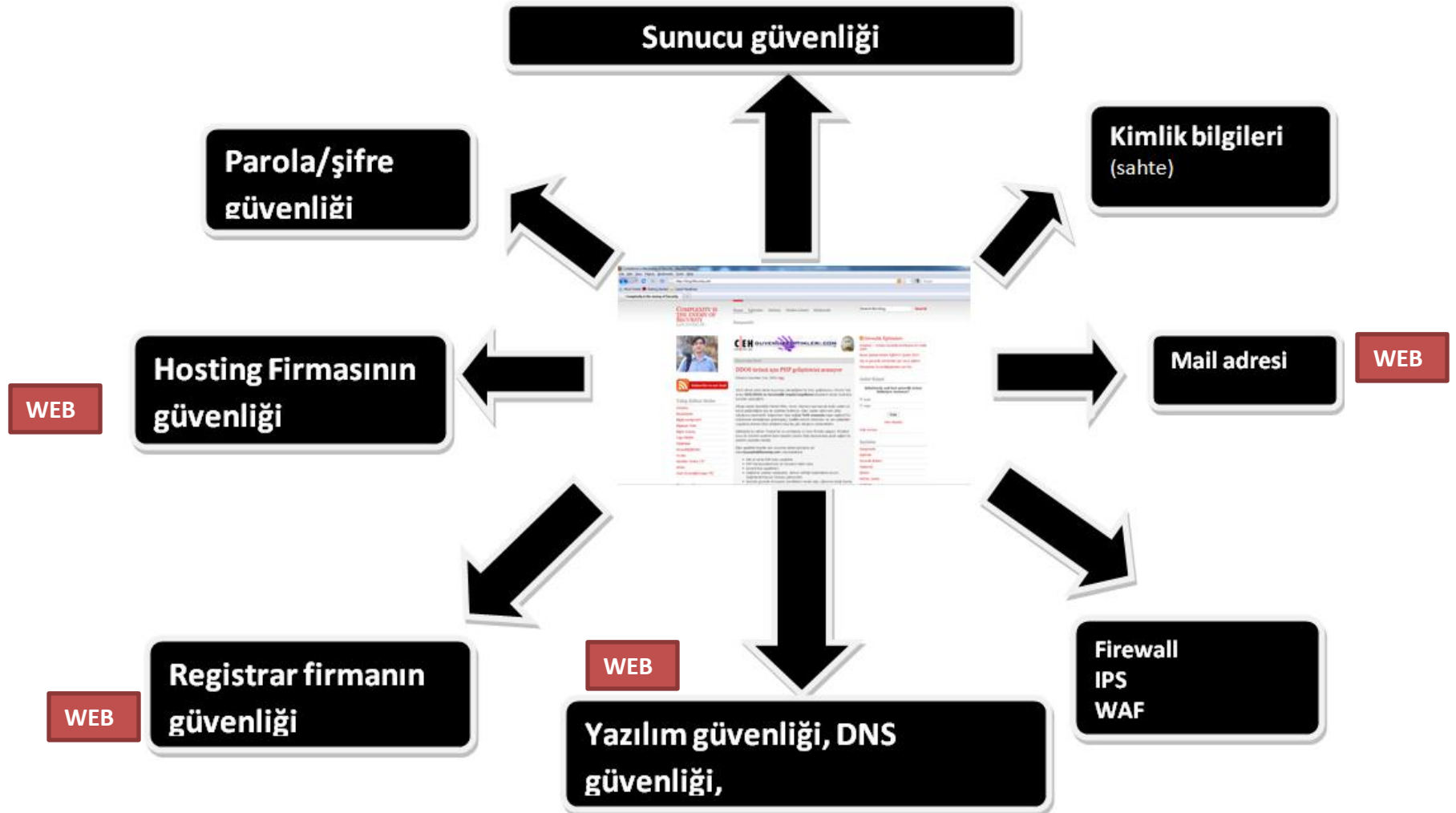


# Uygulama Güvenliği Sorunları

- Güvenli kod geliştirme için oturmuş bir standart yok
- Yazılım geliştirme süreçlerinde güvenlik bileşeni unutulur
- Geliştirme dilleri hala büyük açıklıklar içerebiliyor
- Denetim eksikliği
  - Güncellenen kodlar daha farklı açıklıklar içerebiliyor.
- Geliştiriciler üzerinde ciddi baskılar var
  - Gelişim sürecinde güvenlik için ek zaman düşünülmez
  - Yeterli eğitim/bilinç(güvenlik açısından) eksik



# Web/Uygulama Herşey mi?





# Hacker / Güvenlik Uzmanı

- Güvenlik uzmanları prosedürel hareket ettiği için hackerlara göre bir adım geriden gelir.
- Güvenlik uzmanları için koruma bir meslek, hackerlar için bu korumaları aşmak bir zevktir.
- Hacker için bilgi güvenliği diye bir kavram yoktur, sadece aşılması gereken engel vardır!
- Hackerların mesaisi, sayısı ve motivasyonu farklıdır...
  - Siber dünyada gece gündüz kavramları yoktur
  - 7/24 mesai yaparlar!
- Örnek: Wordpress açıklığı



# Bakış Açısı

- Her iki dünyanın kendine özgü bakış açısı vardır
- Bakış açısı örnekleri...

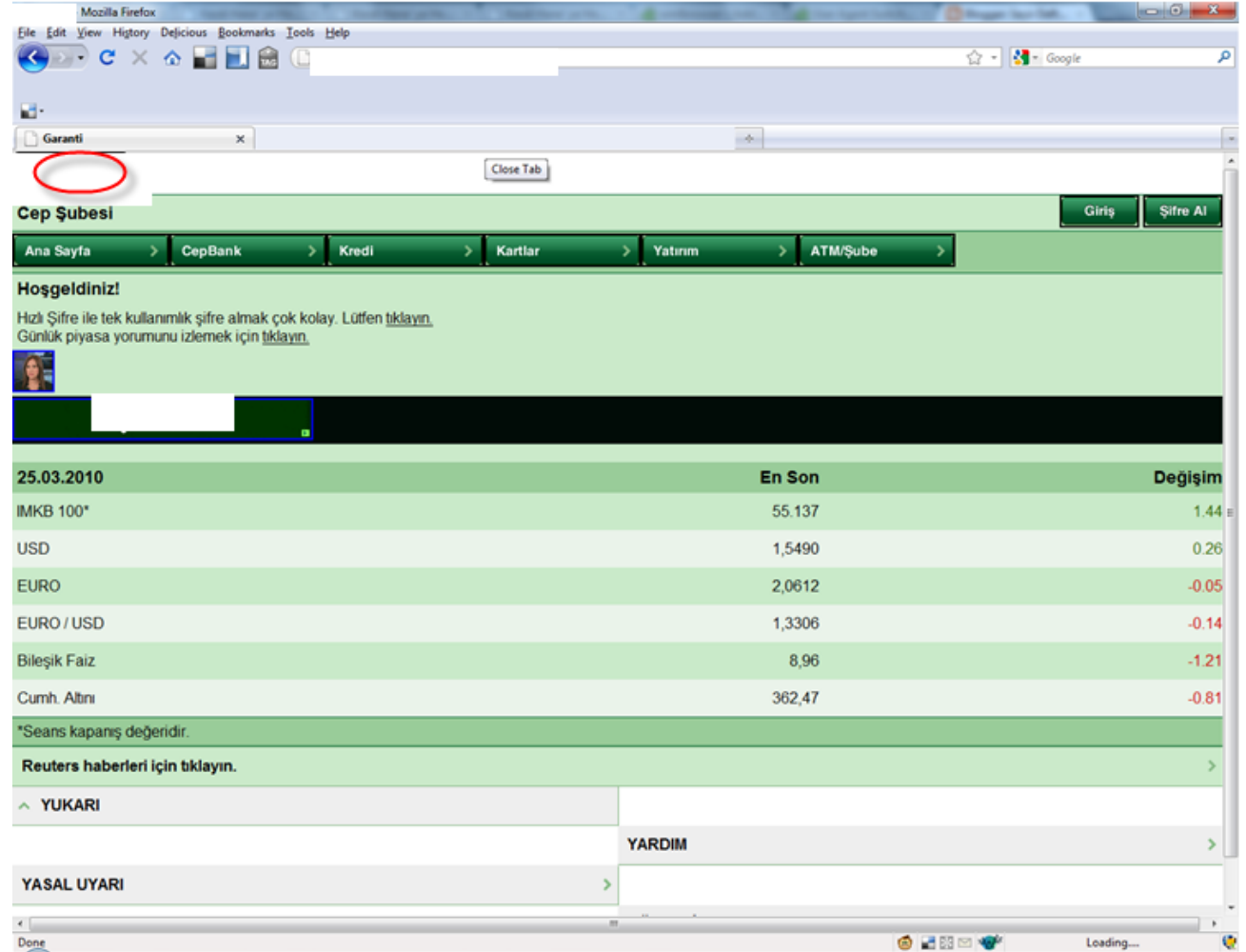


# BA-I:User-Agent Kontrolünü Aşma

EFT Ücreti:2.5 TL  
WAP üzerinden  
yapılan EFT'lerde  
ücret alınmıyor.

Firefox plugini  
kullanarak User-  
Agent mobil cihaz  
gibi gösterilip WAP  
sayfasından ücretsiz  
EFT işlemi yapılabilir

Nasıl engellenebilir?



# BA-II:Bankacılık Uygulamaları IP Kısıtlama



## Re: [netsec] Bankaların CEP telefonu ile internet bankacılığı uygulaması

Selamlar,

Konu acilmisken aklima gelen bir soruyu sorayım.

Bankacılık uygulamalarında IP kısıtlaması yapabiliyoruz. Sadece su ISP, su IP blogu gibi. Ancak son zamanlarda denemedim ama, cep telefonundaki uygulamalar aracılığı bile bankacılık işlemlerini yapabiliyoruz. Yani bu durumda, User-Agent bilgisini, mobil bir telefona ait User-Agent ile değiştirirsek, o zaman banka için girdiğimiz IP kısıtlamasının bir anlamı kalmıyor.

Hatta simdi denedim, bankacılık web arayüzünden daha önce bazı IP adresleri tanımlamış olmama rağmen, cep telefonuma yüklediğim uygulama ile bankaya bağlanabildim.

Simdi, Firefox umun User-Agent ini mobile bir telefon olarak değiştirdim ve <https://wap....com.tr> adresinden ilgili bankanın, web arayüzünden giriş yaptım. Süper. IP kısıtlaması var diye seviniyordum ama anlaşılan yokmuş. Arkadaşlar sizde kendi kullandığınız bankaların arayüzlerini bu şekilde denermisiniz.

Bilgisayarıma bir şekilde virus bulaştı diyelim ve girişte kullandığım kullanıcı adı vs bilgilerim çalındı. Ancak ben IP ayarı yaptığımdan dolayı girememelerini beklerken, wap aracılığı ile girip işlem yapabilirler. Bu durumda kimin hatası olur? Mahkeme durumları olursa, hangi taraf haklı olur?

Ben şimdi, ilgili bankanın iletişim kısmına yazacağım. Bakalım ne cevap verecekler.Cevap geldiğinde sizinle paylaşacağım.

Necati Ersen ŞİŞECİ



# Web Uygulamalarının Güvensizliği

- Web uygulamalarında amaç herkese hizmet verebilmektir
  - Internette en fazla açık port 80/443'tür
- Uygulama geliştirme için bir standart henüz yerleşmediği için yazılımı geliştirenler kolay hata yapabilir
- Web uygulamalarında yapılan hatalar daha fazla dikkat çeker ve saldırıya açıktır
- Birilerinin sizi takip etmesine gerek yok
  - Google üzerinden aramalarla sayfalarınız hacklenebilir



# Web Uygulamalarının Güvensizliği-II

- Koruma amaçlı geliştirilen yazılımlar stabil değil
  - Fazla müdahale istiyor(WAF sistemleri)
- Geliştirme aşamalarında güvenlik önemsenmiyor
- Üst yönetim Web'i 10 sene önceki haliyle biliyor
  - Web = bizi tanıtan sayfa
- Güvenlikcilerin çoğu web/uygulama dünyasına yabancı





# Sık Rastlanan Web Açıklıkları

## Owasp Top10 -2010

**A1: Injection**

**A2: Cross Site Scripting (XSS)**

**A3: Broken Authentication and Session Management**

**A4: Insecure Direct Object References**

**A5: Cross Site Request Forgery (CSRF)**

**A6: Security Misconfiguration**

**A7: Failure to Restrict URL Access**

**A8: Unvalidated Redirects and Forwards**

**A9: Insecure Cryptographic Storage**

**A10: Insufficient Transport Layer Protection**



# Açıklık Arama Yöntemleri

- Google'dan önce, Google'dan sonra olmak üzere ikiye ayrılır
- Eski yöntem: Site bulunur üzerinde açıklık aranır
- Yeni yöntemler: Açıklık belirlenir, Google vs üzerinden hangi sitelerde açıklık olduğu otomatik belirlenir!



# Google Üzerinden Açıklık Arama

```
download c99.php
inurl:c99.php
inurl:c99.php
allinurl: c99.php
inurl:c99.php
allinurl: c99.php
inurl: "/c99.php"
allinurl: c99.php
inurl:c99.php
inurl: "c99.php" c99shell
inurl:c99.php uid=0(root)
c99shell powered by admin
c99shell powered by admin
inurl: "/c99.php"
inurl:c99.php
```

```
inurl:/modules/coppermine/themes/default
/theme.php?THEME_DIR=
```

```
inurl:/modules/agendax/addevent.inc.php?agendax_path=
```

```
inurl:/ashnews.php?pathtoashnews=
```

```
inurl:/eblog/blog.inc.php?xoopsConfig[xoops_url]=
```

```
inurl:/pm/lib.inc.php?pm_path=
```

```
inurl:/b2-tools/gm-2-b2.php?b2inc=
```

```
inurl:/modules/mod_mainmenu.php?mosConfig_absolute_path=
```

```
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:historialeer.php?num=
inurl:reagir.php?num=
inurl:Stray-Questions-View.php?num=
inurl:forum_bds.php?num=
inurl:game.php?id=
inurl:view_product.php?id=
```



# Google Üzerinden Hazır Sistem Bulma

Web Görseller Haberler Çeviri Bloglar Takvim Gmail diğer ▼



inurl:"/c99.php" intitle:"C99shell"

Ara

Gelişmiş Arama

c99 shell arama

Ara: ☒ Web ☐ Türkçe sayfalar ☐ Türkiye'den sayfalar

Web [Seçenekleri göster...](#)

inurl:"/c99.php" intitle:"C99shell" için yaklaşık 29.200 sonuçta

[www.aptus.co.za](http://www.aptus.co.za) - **c99shell** - [ [Bu sayfanın çevirisini yap](#) ]

C99Shell v. 1.0 beta (21.05.2005)! Software: Apache/1.3.34 (Debian) mod\_auth\_pam/1.1.1  
mod\_gzip/1.3.26.1a mod\_perl/1.29 mod\_fastcgi/2.4.2 AuthMySQL/4.3.9-2 ...

[www.aptus.co.za/uploaded/c99.php?act=f&f=c99.php&d...](http://www.aptus.co.za/uploaded/c99.php?act=f&f=c99.php&d...) - [Önbellek](#) - [Yeni](#) [Görüntüle](#) [Sil](#)

[egeisrehberi.com](http://egeisrehberi.com) - **c99shell** - [ [Bu sayfanın çevirisini yap](#) ]

00000000 00000018 00000030 00000048 00000060 00000078 00000090. 000000A8, 3C 3F 70  
68 70 20 0D 0A 2F 2F 53 74 61 72 74 69 6E 67 20 63 61 6C 6C 73 ...

[egeisrehberi.com/success.../contr1.php?act=f...c99.php...](http://egeisrehberi.com/success.../contr1.php?act=f...c99.php...) - [Önbellek](#) - [Yeni](#) [Görüntüle](#) [Sil](#)

[geobz.com](http://geobz.com) - **c99shell** - [ [Bu sayfanın çevirisini yap](#) ]

C99Shell v. 1.0 pre-release build #5! Software: Apache/2.2.14 (Unix) mod\_ssl/2.2.14  
OpenSSL/0.9.8i mod\_bwlimited/1.4 PHP/5.2.11 ...

[geobz.com/carp/c99.php?act=f&f=error\\_log&ft=edit&d...](http://geobz.com/carp/c99.php?act=f&f=error_log&ft=edit&d...) - [Yeni](#) [Görüntüle](#) [Sil](#)

[www.filmcell.co.uk](http://www.filmcell.co.uk) - **c99shell** - [ [Bu sayfanın çevirisini yap](#) ]

C99Shell v. 1.0 beta (21.05.2005)! Software: Apache/1.3.41 (Unix) PHP/5.2.8  
mod\_log\_bytes/1.2 mod\_bwlimited/1.4 mod\_auth\_passthrough/1.8 ...

[www.filmcell.co.uk/1livehelp/c99.php?act...c99.php...](http://www.filmcell.co.uk/1livehelp/c99.php?act...c99.php...) - [Önbellek](#) - [Yeni](#) [Görüntüle](#) [Sil](#)

[phuongdongpv.com.vn](http://phuongdongpv.com.vn) - **c99shell** - [ [Bu sayfanın çevirisini yap](#) ]


C99Shell v. 1.0 pre-release build #12! Software: Apache/2. PHP/5.2.11. uname -a: Linux  
vt2.derasoft.com 2.6.18-128.el5 #1 SMP Wed Jan 21 10:41:14 EST 2009 ...

[phuongdongpv.com.vn/hinh/banner/c99.php?act=selfremove](http://phuongdongpv.com.vn/hinh/banner/c99.php?act=selfremove) - [Önbellek](#) - [Yeni](#) [Görüntüle](#) [Sil](#)



# Otomatik SQLi Bulucu

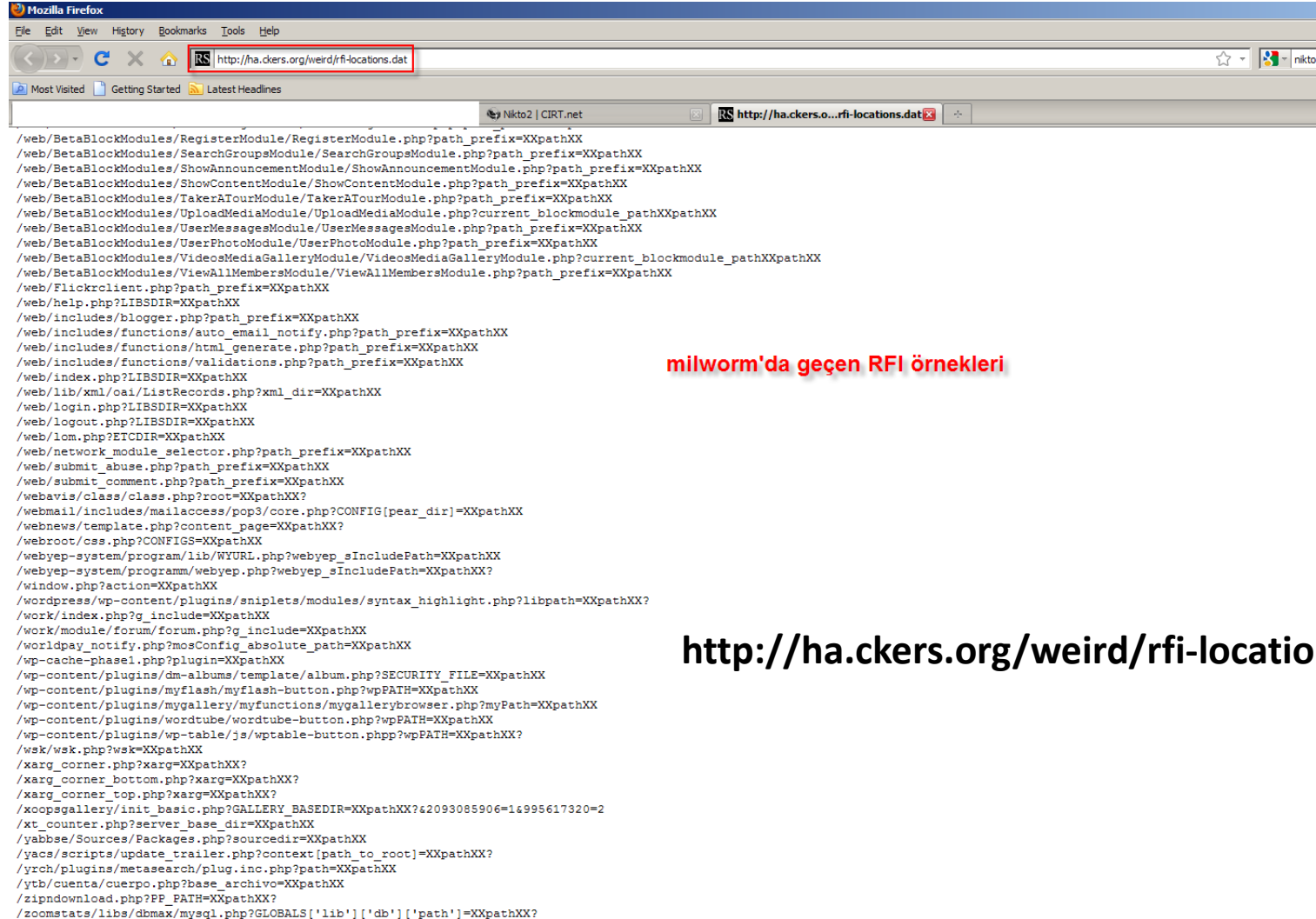
...:[X] PHP SQLi Scanner v1.2 [X]:...

Google Dork :  Ex: *inurl:\"products.php?pid=\"*  
Injection :  Ex: *+ORDER+BY+999*  
Start From :  Ex: *100*  
Select Region :  

```
www.si5.com/products.php?pID=4024\'
www.maxcube.com/products/products.php?pid=57\' -- Could be vulnerable -- w00t!!
imesart.com/products.php?pid=1\'
www.maxcube.com/products/products.php?pid=4\' -- Could be vulnerable -- w00t!!
www.foodandhealth.com/products.php?pid=169\'
www.sharkwerks.com/products.php?pid=193\'
www.tootsie.com/products.php?pid=165\'
www.emboss.co.nz/products.php?pid=2\'
www.tootsie.com/products.php?pid=129\'
www.foodandhealth.com/products.php?pid=110\'
www.enigma-games.com/products.php?pid=9\'
www.coagent.cn/products.php?pid=4\' -- Could be vulnerable -- w00t!!
www.foodandhealth.com/products.php?pid=119\'
www.tootsie.com/products.php?pid=105\'
www.nilfisk.ca/products.php?pid=19\'
www.icpdas-usa.com/products.php?PID=142\'
www.nilfisk.ca/products.php?pid=14\'
www.asys.co.th/products.php?pid=30\'&lid=en
www.si5.com/products.php?pID=4038\'
www.selfesteemshop.com/products.php?pid=3180\'&detail=true
www.londontea.co.uk/products.php?pid=8\' -- Could be vulnerable -- w00t!!
```



# RFI Arama Örnekleri



milworm'da geçen RFI örnekleri

```
/web/BetaBlockModules/RegisterModule/RegisterModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/SearchGroupsModule/SearchGroupsModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/ShowAnnouncementModule/ShowAnnouncementModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/ShowContentModule/ShowContentModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/TakerATourModule/TakerATourModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/UploadMediaModule/UploadMediaModule.php?current_blockmodule_pathXXpathXX
/web/BetaBlockModules/UserMessagesModule/UserMessagesModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/UserPhotoModule/UserPhotoModule.php?path_prefix=XXpathXX
/web/BetaBlockModules/VideosMediaGalleryModule/VideosMediaGalleryModule.php?current_blockmodule_pathXXpathXX
/web/BetaBlockModules/ViewAllMembersModule/ViewAllMembersModule.php?path_prefix=XXpathXX
/web/Flickrclient.php?path_prefix=XXpathXX
/web/help.php?LIBSDIR=XXpathXX
/web/includes/blogger.php?path_prefix=XXpathXX
/web/includes/functions/auto_email_notify.php?path_prefix=XXpathXX
/web/includes/functions/html_generate.php?path_prefix=XXpathXX
/web/includes/functions/validations.php?path_prefix=XXpathXX
/web/index.php?LIBSDIR=XXpathXX
/web/lib/xml/oai/ListRecords.php?xml_dir=XXpathXX
/web/login.php?LIBSDIR=XXpathXX
/web/logout.php?LIBSDIR=XXpathXX
/web/lom.php?ETCDIR=XXpathXX
/web/network_module_selector.php?path_prefix=XXpathXX
/web/submit_abuse.php?path_prefix=XXpathXX
/web/submit_comment.php?path_prefix=XXpathXX
/webavis/class/class.php?root=XXpathXX?
/webmail/includes/mailaccess/pop3/core.php?CONFIG[pear_dir]=XXpathXX
/webnews/template.php?content_page=XXpathXX?
/webroot/css.php?CONFIGS=XXpathXX
/webweyep-system/program/lib/WYURL.php?webyep_sIncludePath=XXpathXX
/webweyep-system/programm/webweyep.php?webyep_sIncludePath=XXpathXX?
/window.php?action=XXpathXX
/wordpress/wp-content/plugins/snippets/modules/syntax_highlight.php?libpath=XXpathXX?
/work/index.php?g_include=XXpathXX
/work/module/forum/forum.php?g_include=XXpathXX
/worldpay_notify.php?mosConfig_absolute_path=XXpathXX
/wp-cache-phase1.php?plugin=XXpathXX
/wp-content/plugins/dm-albums/template/album.php?SECURITY_FILE=XXpathXX
/wp-content/plugins/myflash/myflash-button.php?wpPATH=XXpathXX
/wp-content/plugins/mygallery/myfunctions/mygallerybrowser.php?myPath=XXpathXX
/wp-content/plugins/wordtube/wordtube-button.php?wpPATH=XXpathXX
/wp-content/plugins/wp-table/js/wptable-button.php?wpPATH=XXpathXX?
/wsk/wsk.php?wsk=XXpathXX
/xarg_corner.php?xarg=XXpathXX?
/xarg_corner_bottom.php?xarg=XXpathXX?
/xarg_corner_top.php?xarg=XXpathXX?
/xoopsgallery/init_basic.php?GALLERY_BASEDIR=XXpathXX?&2093085906=1&995617320=2
/xt_counter.php?server_base_dir=XXpathXX
/yabbse/Sources/Packages.php?sourcedir=XXpathXX
/yacs/scripts/update_trailer.php?context[path_to_root]=XXpathXX
/yrch/plugins/metasearch/plug.inc.php?path=XXpathXX
/ytc/cuenta/cuerpo.php?base_archivo=XXpathXX
/zipndownload.php?FP_PATH=XXpathXX?
/zoomstats/libs/dbmax/mysql.php?GLOBALS['lib']['db']['path']=XXpathXX?
```





# Basit (!) Bir Web Zaafiyeti Nelere Yol Açabilir?



Video



# Web Shell

- Hacklenen sunucuları daha kolay yönetmek için yazılmış web uygulamalarıdır
- Her dil için özel yazılmış web shell bulunmaktadır
  - Asp shell, php shell, jsp shell, perl shell vs
- Hackerların işini oldukça kolaylaştırır, birçok işi otomatikleştirir
- Detay Linux/UNIX bilgisi gerektirmez, birden fazla siteyi aynı anda deface etmeye yarar, kolaylıkla yakalanmaz(IPS'ler tarafından).
- Bypass özellikleri vardır




# Sık kullanılan Shell isimleri

- R57, c99, cmd.asp, zehir shell vs
- jsp-reverse.jsp, php-backdoor.php, perlcmd.cgi
- <http://www.wtfchan.org/~evil1/Web-Shells-rev2.pdf>



# R57 Shell

Lord-Voldemort [ No-LimitD.us ] Lord-Voldemort -->

 ascrimez 3.5

15-02-2008 17:42:12 phpinfo() php.ini cpu mem users tmp delete  
safe\_mode: OFF\_not\_secure PHP version: 4.4.4-8+etch4 cURL: OFF MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF  
Disable functions : NONE  
Free space : 3.26 GB Total space: 4.55 GB

uname -a : Linux dnsl 2.6.18-5-686 #1 SMP Mon Dec 24 16:41:07 UTC 2007 i686 GNU/Linux  
sysctl :  
\$OSTYPE : linux-gnu  
Server : Apache/2.2.3 (Debian) PHP/4.4.4-8+etch4 mod\_perl/2.0.2 Perl/v5.8.8  
id : uid=33(www-data) gid=33(www-data) groups=33(www-data)  
pwd : /var/www (drwxr-xr-x)

Executed command: ls -lia

```
total 232
234237 drwxr-xr-x  9 root root  4096 Feb 11 18:00 .
196609 drwxr-xr-x 14 root root  4096 Jan  9 22:56 ..
234351 -rw-r--r--   1 root root    165 Feb 10 18:16 .htaccess
234435 -rw-r--r--   1 root root  4223 Jan 30 18:33 ...es.php
248449 drwxr-xr-x 10 root root  4096 Jan  9 23:39
234428 -rw-r--r--   1 root root  2358 Jan 30 18:33 ...k.php
234405 drwxr-xr-x  3 root root  4096 Jan 12 18:46 ...s
234216 -rw-r--r--   1 root root  3976 Jan 30 16:59 ...ns.php
234386 -rw-r--r--   1 root root  2104 Jan 26 12:53 ...php
234387 -rw-r--r--   1 root root  2102 Jan 26 12:53 ...php
234388 -rw-r--r--   1 root root  2246 Jan 30 19:14 ...php
234218 -rw-r--r--   1 root root  1995 Jan 19 19:58 ...ain.php
234239 -rw-r--r--   1 root root  7157 Jan 30 18:17 ...hp
278537 drwxr-xr-x  3 root root  4096 Jan 12 18:46 ...flux
234240 -rw-r--r--   1 root root    0 Jan  9 17:43 ...3.html
```

:: Execute command on server ::

Run command ▶

Work directory ▶ /var/www

:: Edit files ::

File for edit ▶ /var/www

:: Aliases ::

Select alias ▶ find suid files

:: Find text in files ::

Find text ▶ text

In dirs ▶ /var/www



- Video..



# Dünyadan Örnekler





# Meşhur Türk Hackerlar(?)😊

## My School Rooted [www.usep.edu.ph](http://www.usep.edu.ph)

November 9, 2008

have you ever wanted to hack your school's website, well i just r00ted my almamater

sorry sir val you server pawned, sooner or later turks will deface it so put checks on your security and monitor logs

R00T!



...sooner or later turks will deface it



# Apache Projesi

## What Happened?

On April 5th, the attackers via a compromised [Slicehost](#) server opened a new issue, INFRA-2591. This issue contained the following text:

ive got this error while browsing some projects in jira <http://tinyurl.com/XXXXXXXXXX> [obscured]

Tinyurl is a URL redirection and shortening tool. This specific URL redirected back to the Apache instance of JIRA, at a special URL containing a [cross site scripting \(XSS\) attack](#). The attack was crafted to steal the session cookie from the user logged-in to JIRA. When this issue was opened against the Infrastructure team, several of our administrators clicked on the link. This compromised their sessions, including their JIRA administrator rights.

At the same time as the XSS attack, the attackers started a brute force attack against the JIRA login.jsp, attempting hundreds of thousands of password combinations.

On April 6th, one of these methods was successful. Having gained administrator privileges on a JIRA account, the attackers used this account to disable notifications for a project, and to change the path used to upload attachments. The path they chose was configured to run JSP files, and was writable by the JIRA user. They then created several new issues and uploaded attachments to them. One of these attachments was a JSP file that was used to browse and copy the filesystem. The attackers used this access to create copies of many users' home directories and various files. They also uploaded other JSP files that gave them backdoor access to the system using the account that JIRA runs under.

By the morning of April 9th, the attackers had installed a JAR file that would collect all passwords on login and save them. They then sent password reset mails from JIRA to members of the Apache Infrastructure team. These team members, thinking that JIRA had encountered an innocent bug, logged in using the temporary password sent in the mail, then changed the passwords on their accounts back to their usual passwords.

One of these passwords happened to be the same as the password to a local user account on brutus.apache.org, and this local user account had full sudo access. The attackers were thereby able to login to brutus.apache.org, and gain full root access to the machine. This machine hosted the Apache installs of JIRA, Confluence, and Bugzilla.

Once they had root on brutus.apache.org, the attackers found that several users had cached Subversion authentication credentials, and used these passwords to log in to minotaur.apache.org (aka people.apache.org), our main shell server. On minotaur, they were unable to escalate privileges with the compromised accounts.

About 6 hours after they started resetting passwords, we noticed the attackers and began shutting down services. We notified Atlassian of the previously unreported XSS attack in JIRA and contacted SliceHost. Atlassian was responsive. Unfortunately, SliceHost did nothing and 2 days later, the **very** same virtual host (slice) [attacked Atlassian directly](#).

We started moving services to a different machine, thor.apache.org. The attackers had root access on brutus.apache.org for several hours, and we could no longer trust the operating system on the original machine.

By April 10th, JIRA and Bugzilla were back online.

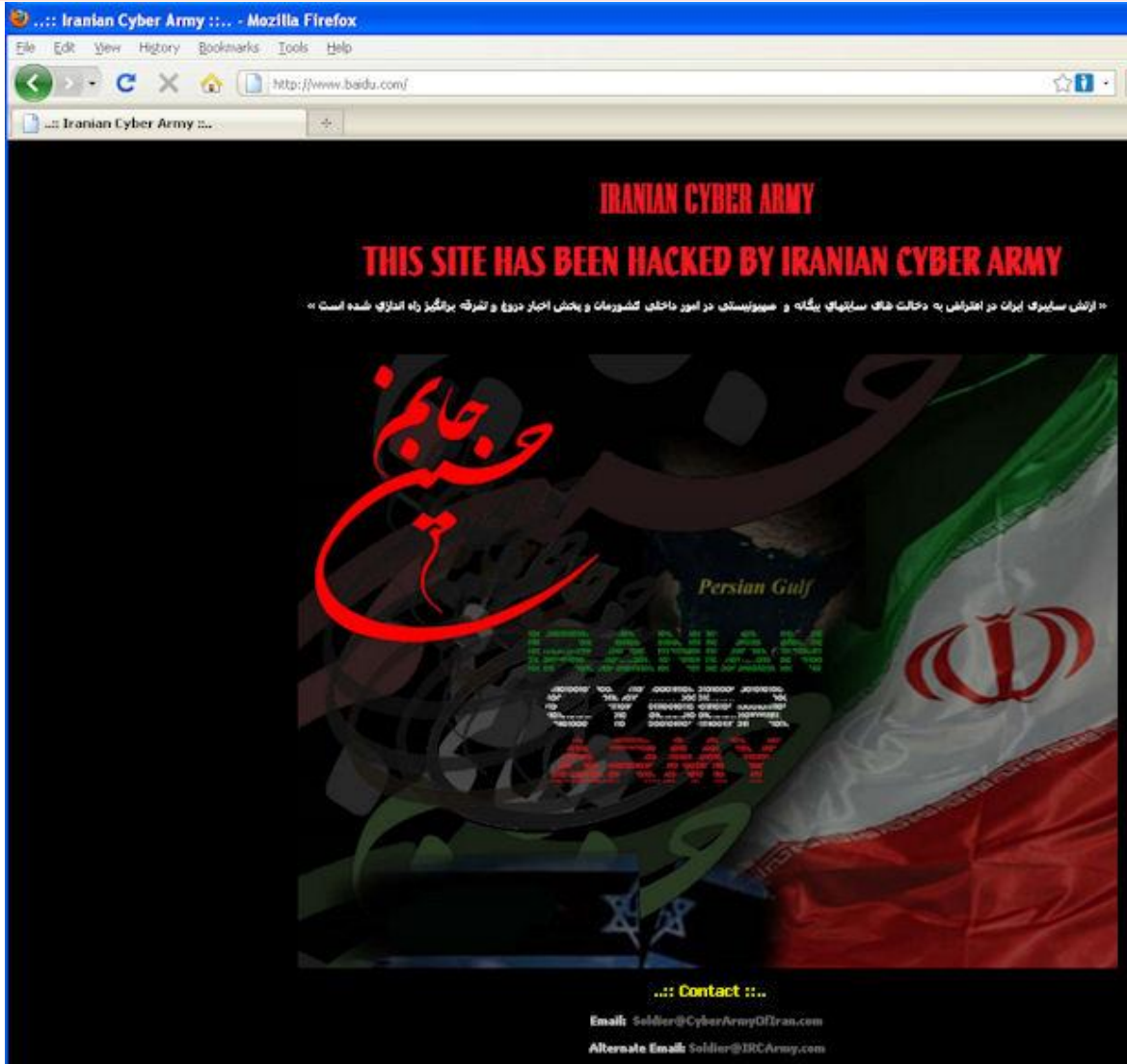


# SQLi ☺





# Baidu.com



- Neden?
- Nasıl?



# Intel.com

Intel® Driver Update Utility for Intel® wireless adapters - Check for the latest driver - Windows Internet Explorer

http://www.intel.com/support/wireless/detect.htm

Sık Kullanılanlar Önerilen Siteler Web Slice Galerisi

Intel® Driver Update Utility for Intel® wireless adapt...

Advanced Search  
Contact Support

Search  
Support & Downloads

☐ All of Support  
☒ This Category

Search

Did you find this information to be helpful?

☐ Yes ☐ No

If you have additional feedback, please let us know.

Remaining Characters: 300

Submit

We appreciate all feedback, but cannot reply or give product support. Please do not enter contact information. If you require a response, contact us.

The Intel® Driver Update Utility keeps your Intel® wireless adapter driver and Intel® PROSet/Wireless software up-to-date. It detects which updates are relevant, then helps you install them quickly and easily.

Related topics:

- Scan your entire system
- Manually search Download Center for drivers and software

•Neden?  
•Nasıl?

Başlat Intel Driver Update sitesi... Intel® Driver Update ...

TR 17:22

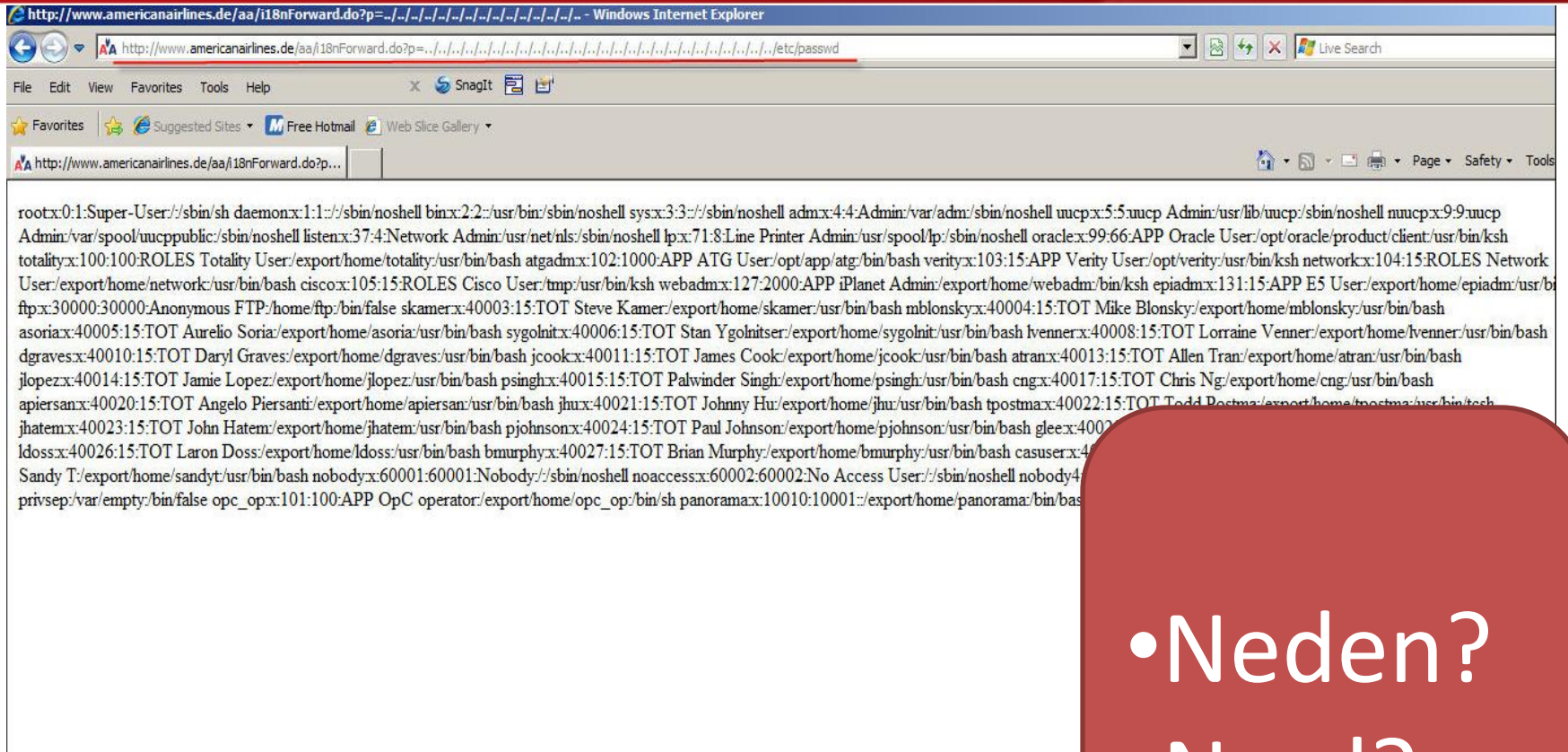


Downloaded from <http://ajphaphysocpharm.sagepub.com/> at 11:01 11 November 2014





# American Airlines



- Neden?
- Nasıl?





# Türkiye'den Örnekler...



# Wordpress Türkiye



## Duyuru

Merhaba arkadaşlar,

Önceki gün ufak bir ele geçirme olayı yaşadık. Konuyu detaylı bir şekilde incelemeden bir duyuru yapmış olmanın bilinen bir açık olmadığını sizinle paylaşmak isteriz.

Test sonuçlarına göre bir dizi güvenlik tedbirleri alınmış; wordpress-tr kullanıcı yetkileri üzerinde değişiklikler alınana kadar wordpress kurulum dosyalarının değiştirilmiş olabileceği kanısı bizde kalmıştır. Wordpress 3.0 kurulumu yaptıysanız tavsiyemiz aşağıdaki yöntemleri kullanarak düzenleme

görmekte olduğunuz ekranda yer alan güncelleme ekranından, WordPress 3.0 Türkçe paketi var olan kurulumunuz

wordpress-tr.TR.zip adresinde yer alan Türkçe paketi edinin, ftp ile dosyaları sisteminize yükleyerek, var olan kurulumu güncelleyebilirsiniz.

WordPress Türkiye Ekibi tarafından hazırlanmış bulunmaktadır. Bu kararları da şu şekilde sıralayabiliriz;

1. wordpress.org adresinden indirilecektir. Otomatik güncellemeler zaten bu adresi kullanıyor.

2. İsteyenler de bu adrese yönlendirileceklerdir.

3. Altyapının güncellenmesi ve yapılacak değişikliklerin uygulanması için bir süreliğine

wordpress.org üzerinden Türkçe pakete ulaşılabilir.

4. Güvenli bir şekilde kullanılabilmesi için editör ve forum yöneticisi alımları yapılacaktır.

Bizden esirgemeyen WordPress Türkiye kullanıcılarına, dostlarımıza ve üstün hizmet anlayışıyla çalışmalarına teşekkür ederiz.

WordPress Türkiye Ekibi

### WordPress Türkçe Paket

tr.wordpress.org'dan indirmek için tıklayın.  
md5: 9057cdb06cafd3b0bb6cf84c684092ef



Söylentilere göre  
15.000 web sayfası  
bu ele geçirme  
olayından etkilendi!

- Neden?
- Nasıl?



# Alınacak Dersler

- Web açıklıkları basit ama etkili açıklıklardır
- Güvenlikte zaafiyetin riski bulunduğu yere göre değişir
  - Basit(!) bir XSS açıklığı tüm sistemlerinizin ele geçirilmesine neden olabilir
- İnsan faktörü hala güvenlik zincirinin en zayıf halkası
  - Sektörün devamı için şart 😊
- Zaafiyeti analiz edip yayınlamak erdemdir 😊



# Web Sunuculara Yönelik DOS Saldırıları

- Ya benimsin ya toprağın mantığı
- Bilgi güvenliğini tam anlayamamış kurumların dikkat etmedikleri bir konu
- Web uygulamaları&sunucuları en kritik bileşenlerdir
  - Online bankacılık sitesi çalışmayan bir bankanın zararı?
  - Onlien oyunlar? E-ticaret siteleri?
- Diğer DDOS saldırılarına oranla çok daha kolaydır
  - Aynı şekilde engellemesi de kolaydır
- Spoof edilmiş ip adreslerinden yapılamaz
  - HTTP isteği için TCP'de üçlü el sıkışma tamamlanması gerekir



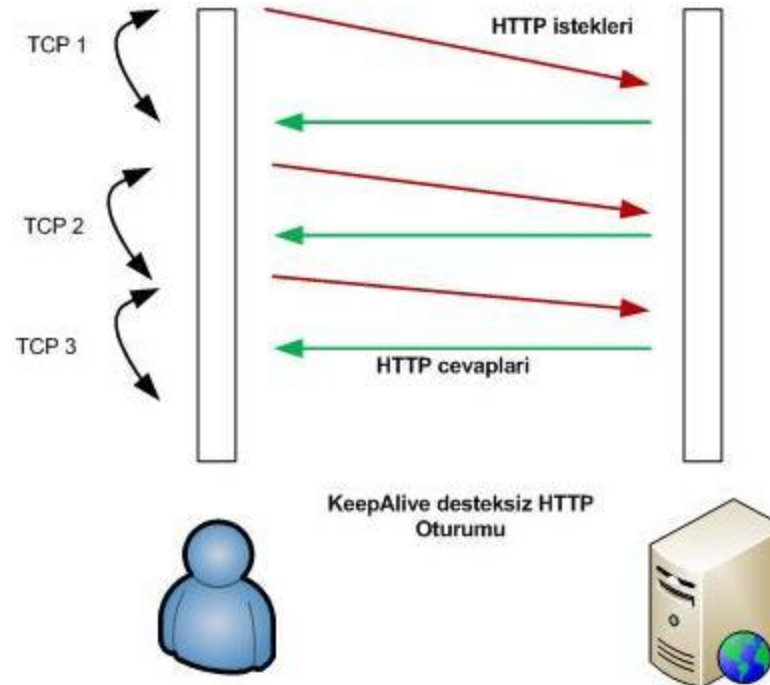
# HTTP ve TCP ilişkisi

- HTTP TCP kullanan bir protokoldür.
  - Her HTTP bağlantısı öncesinde mutlaka TCP bağlantısı kurulmalıdır
- Basit bir hesapla her HTTP bağlantısı için ortalama 10 adet TCP paketi gerekir (3 adet TCP bağlantı başlangıcı, 4 adet TCP bağlantı koparılması, 2-3 adet de HTTP isteği ve buna dönecek cevap paketlerinin taşındığı TCP paketleri).
- Günümüzde normal bir haber portalının yüklenmesi için ortalama 40-50 HTTP GET isteği gönderilmektedir
  - Portal sayfasının açılması için ortalama  $50 \times 10 = 500$  TCP paketinin gidip gelmesi gerekir



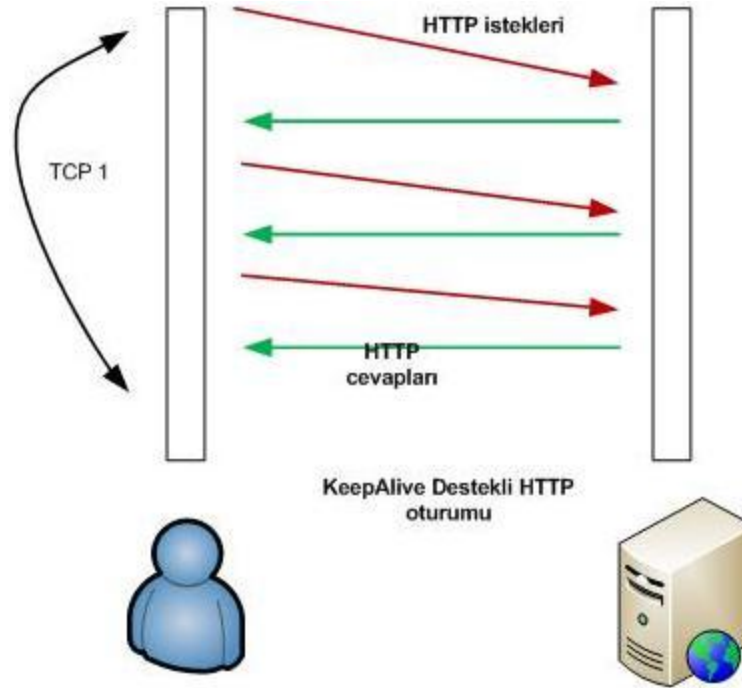
# Klasik HTTP oturumu

- Her HTTP bağlantısı için TCP bağlantısı gerekir.



# HTTP KeepAlive

- HTTP KeepAlive(persistent connection): her HTTP isteđi için ayrı bir TCP bađlantısı açmak yerine bir adet TCP bađlantısı içerisinde belirli sayıda (5, 10, ..) HTTP isteđinin aktarılabilmesini sađlar.





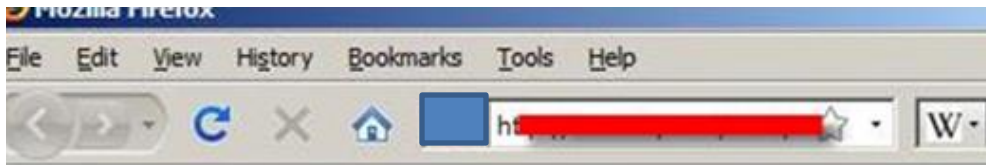
# Http Pipelining

- Pipelining http isteklerinin eş zamanlı olarak gönderilmesi işlemidir(KeepAlive ile karıştırılır)
- Klasik http bağlantılarında önce istek gönderilir, cevap beklenir, sonra tekrar istek gönderilir, cevabı beklenir
- Pipelining kullanıldığında cevapları beklemeksizin birden fazla http isteği eş zamanlı olarak gönderilebilir
- KeepAlive özelliği kullanılarak her istek için ek bir TCP bağlantısı açılmaz.

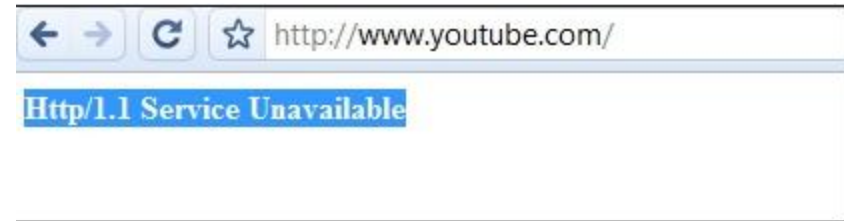


# Web Sunuculara Yönelik DOS Saldırıları

- Amaç sayfanın işlevsiz kalması ve o sayfa üzerinden verilen hizmetlerin kesintiye uğratılmasıdır.
- Web sunuculara yönelik yapılacak DOS saldırıları temelde iki türden oluşur;
  - Kaba kuvvet saldırıları (Flood)
  - Tasarımsal/yazılımsal eksikliklerden kaynaklanan zaafiyetler

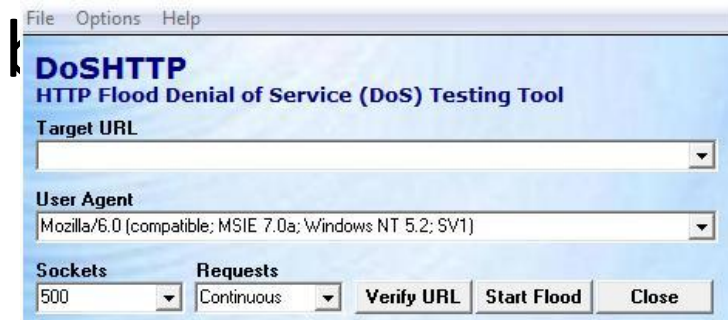


**Server is too busy**



# Kaba kuvvet DOS/DDOS Saldırıları

- Literatürde adı “GET Flood”, “POST Flood” olarak geçer
- Eş zamanlı olarak binlerce istek gönderilir ve sunucunun kapasitesi zorlanır.
- İstekler tek bir ip adresinden gönderilebilir
  - Bir IP adresinden saniyede 1000 HTTP isteği gönderilebilir
- İstekler bir botnet kullanılarak IP adresinden gönderilebilir



# Web Uygulama Güvenliği Testleri

**mavitunasecurity**  
web application security experts

NETSPARKER PRICING DOWNLOAD BLOG SUPPORT ABOUT CONTACT

## False-Positive **Free**

Web Application Security Scanner  
find and exploit vulnerabilities in web applications

**Netsparker**

[BUY NOW!](#) See our competitive pricing and licensing options.

[REQUEST DEMO](#) Request an evaluation version of Netsparker.



**PRODUCT TOUR VIDEO**  
click here to start watching

**netsparker®**  
web application security scanner

“ Netsparker found both bugs and security problems within the first five minutes! It's great to have this safety net as we continue to code -- it's like having automated unit tests for security with almost no effort.

Jason Cohen, [Smart Bear Software](#)

### Free - Netsparker Community Edition

We are proud to announce [Free Netsparker® Community Edition](#). It's a free edition of our False Positive Free scanner Netsparker for the community so you can start securing your website now. It's user friendly, fast, smart and as always **False Positive Free**.

[Download now for free](#), No registration, no data collection, no strings attached.



**free**  
COMMUNITY  
EDITION  
is out!  
[DOWNLOAD](#)



# Türkçe Web Güvenliği Kaynağı:OWASP Türkiye

Web Güvenlik Topluluğu  
http://www.webguvenligi.org



[Ana Sayfa](#) [E-Dergi](#) [OWASP-TR ve WGT](#) [Projeler](#) [Belgeler](#) [Çeviriler](#) [Etkinlikler](#) [Sözlük](#)

[in](#) [ff](#) [tw](#) [bilgi at webguvenligi.org](#)

JSecureImage v2 - Güvenli Resim Upload1st Jul, 2010

JSecureImage, java ortamında güvenli resim upload'ı için kullanılabilecek bir kütüphanedir. Upload edilen resimlerin bazı özelliklerini kontrol eden JSecureImage hatalı veya güvensiz resimleri reddeder. Standard Java ImageIO API'ini kullanan JSecureImage, küçük bozuklukları olan bazı resimlerde hatalı sonuç vermekteydi. Bu hatayı kütüphanenin kullandığı işletim sisteminde JDK üzerine JAI ImageIO kütüphanesini kurarak çözebilirsiniz.

[https://jai-imageio.dev.java.net/binary-builds.html#Release\\_builds](https://jai-imageio.dev.java.net/binary-builds.html#Release_builds)

Ayrıca yeni JSecureImage kütüphanesini indirip resim dosya upload özelliği bulunan kendi J2EE web uygulamanızı da güvenli hale getirebilirsiniz.

No Comments yet... | [Read More »](#)


Yeni Bir Teknik - BSQli Optimizasyonu7th Jun, 2010

```
terminal
Dosya Düzen Görünüm Uçbirim Yardım
hcr@world:~/desktop/pentest/mydocs$ php bsqli.php
Start @ 00:40:08
Total Request: 10
Result: abhkz
Finish @ 00:41:04
hcr@world:~/desktop/pentest/mydocs$
```

Teknik, blind sql injection saldırılarında tek bir karakteri minimum istek ile elde etmek için yeni bir optimizasyondur. Zaman tabanlı kör sql enjeksiyonlarına getirdiği yeni soluk MOD fonksiyonu ile bekleme zamanını düşürmektedir.

Canberk Bolat (canberk.bolat[-AT-]gmail[-DOT-]com)'ın geliştirdiği ve MySQL için tecrübe ettiği yol kullandığı fonksiyonlar itaban ile diğer veritabanları için de gerçekleştirilebilir.

En Son YazılarPerembe, 29 Temmuz 2010



Tag Bulutu



En Sevilen Projeler

CAMMP (3,394)

SecureTomcat (3,092)

WIVET (2,914)

Jarvinen (2,781)

Çeviri (2,748)

MSALParser (2,627)

SecureImage (2,606)

Gözet

Monthly Archives

Search

Bilgi Güvenliği Akademisi  
www.guvenlikegitimleri.com



**Ağ ve Bilgi  
Güvenliği  
Listesine  
Hoşgeldiniz**

Netsec, Türkiye’de sistem, ağ ve güvenlik birimlerinde çalışan bilişimcilere yönelik hizmet veren Türkiye’nin en geniş katılımlı e-posta listesidir.

Listenin amacı, benzer pozisyonlarda çalışan bilişimciler arasında bilgi paylaşimini artırmak ve güvenlik konusunda referans olabilecek kaynaklar olusturmaktır.

Ağ ve güvenlik amaçlı kullanılacak her tür ticari ve açık kaynak kodlu yazılımın tanıtımının yapılması (kuru reklama kesinlikle izin verilmeyecektir) serbesttir. Böylece farklı ürünleri kullanan bilişim profesyonellerine alternatif ürünleri tanıma fırsatı verilmiş olacaktır.

Listenin Genel içeriği aşağıdaki konulardan oluşmaktadır;

- \* Güvenlik Duvarları
- \* Saldırı Tespit ve Engelleme Sistemleri
- \* Kablosuz Ağlarda Güvenlik
- \* Yerel Ağlarda Güvenlik
- \* Web Uygulama Güvenliği
- \* VPN Uygulamaları
- \* Trafik Analizi
- \* Adli Bilişim Analizi
- \* Tuzak Sistemler
- \* Linux/UNIX/Windows işletim sistemlerinde Güvenlik





# Sonuç

- İnsan faktörü hala güvenlikteki en büyük sıkıntı!
- Web uygulama geliştirme süreci standartlara bağlandıkça ve diller daha güvenli yazılım geliştirmeye olanak verene kadar tehdit sıralamasında en üstlerde yer almaya devam edecek
- Güvenliği hafife almamak, işi ehline bırakmak gerekir
- Herkes kendi payına düşen güvenlik miktarını bilmeli😊





# Teşekkürler...

