JTPD
JAVA TEKNOLOJİLERİ VE PROGRAMCILARI DERNEĞİ

Java™ Dergisi
Java ◆ Mimari ◆ Çevik Süreçler

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
- Blogger
  - 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

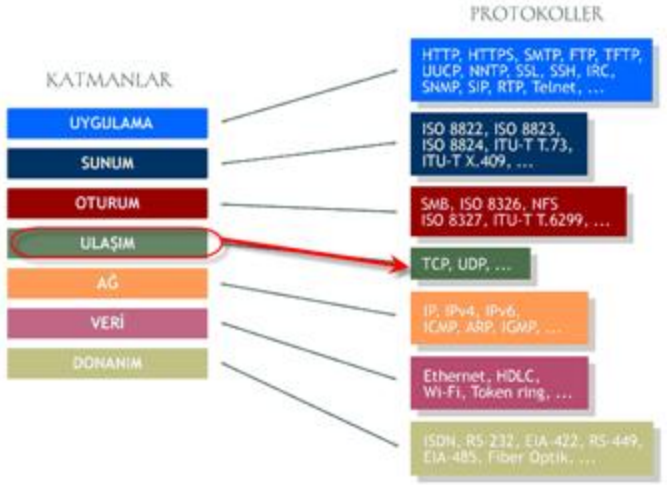
- Web uygulamaları günümüzü ve geleceğimizi kuşatmış durumda
  - Müzik dinleme:last.fm, fizy.org
  - Ofis Belgeleri için:Google Docs
  - Resim işleme amaçlı:Google Picasa, flickr
  - (A)Sosyal Hayat: Facebook, Friendfeed, twitter
  - Alışveriş, Para işleri:Paypal.com, online alışveriş siteleri
  - İletişim:E-posta->Webmail 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

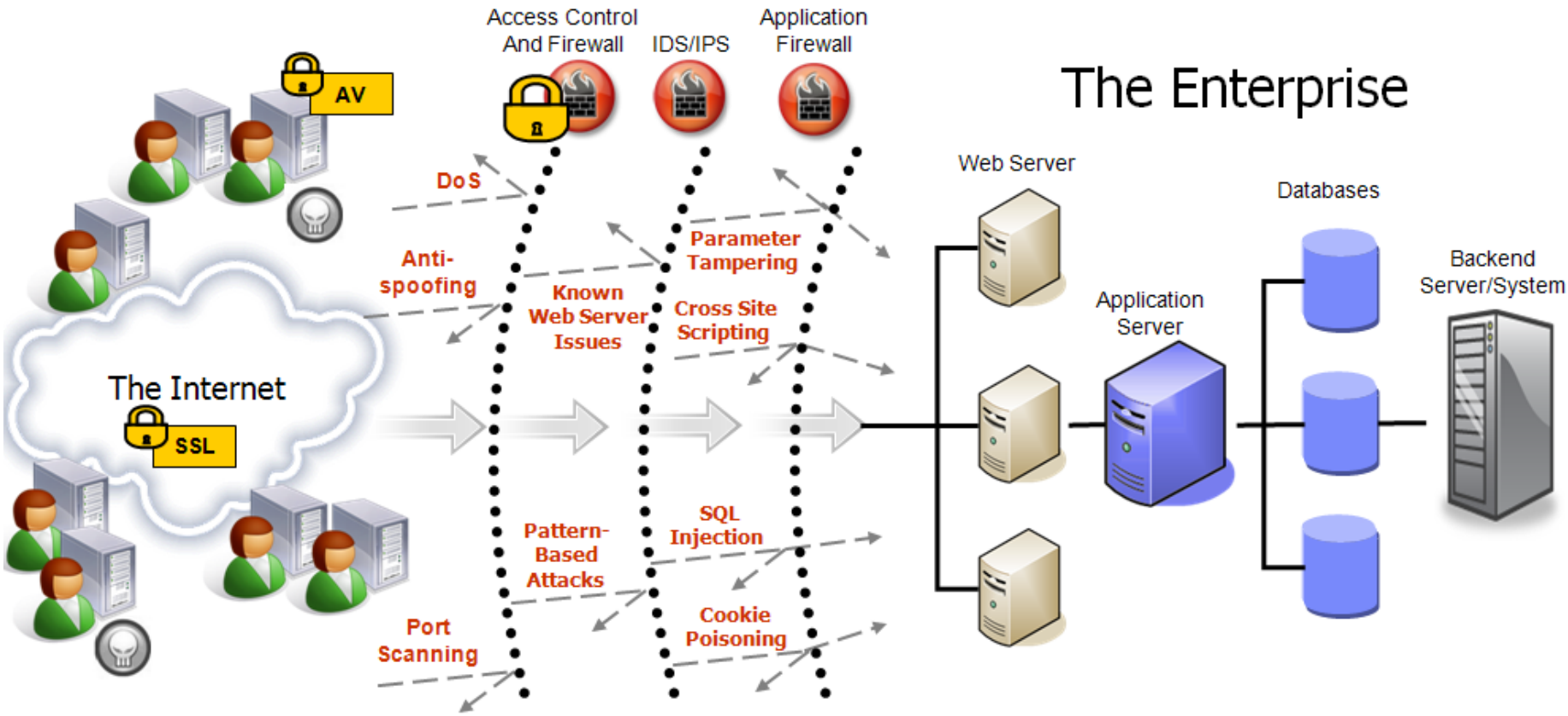
Geleneksel Güvenlik Yaklaşımı

- Henüz OSI 4. katmandan yukarı çıkamamıştır
- Network, işletim sistemi ve servis güvenliği
- Router(ACL), Firewall
  - Intrusion Detection System
    - Intrusion Prevention System
      - » ....

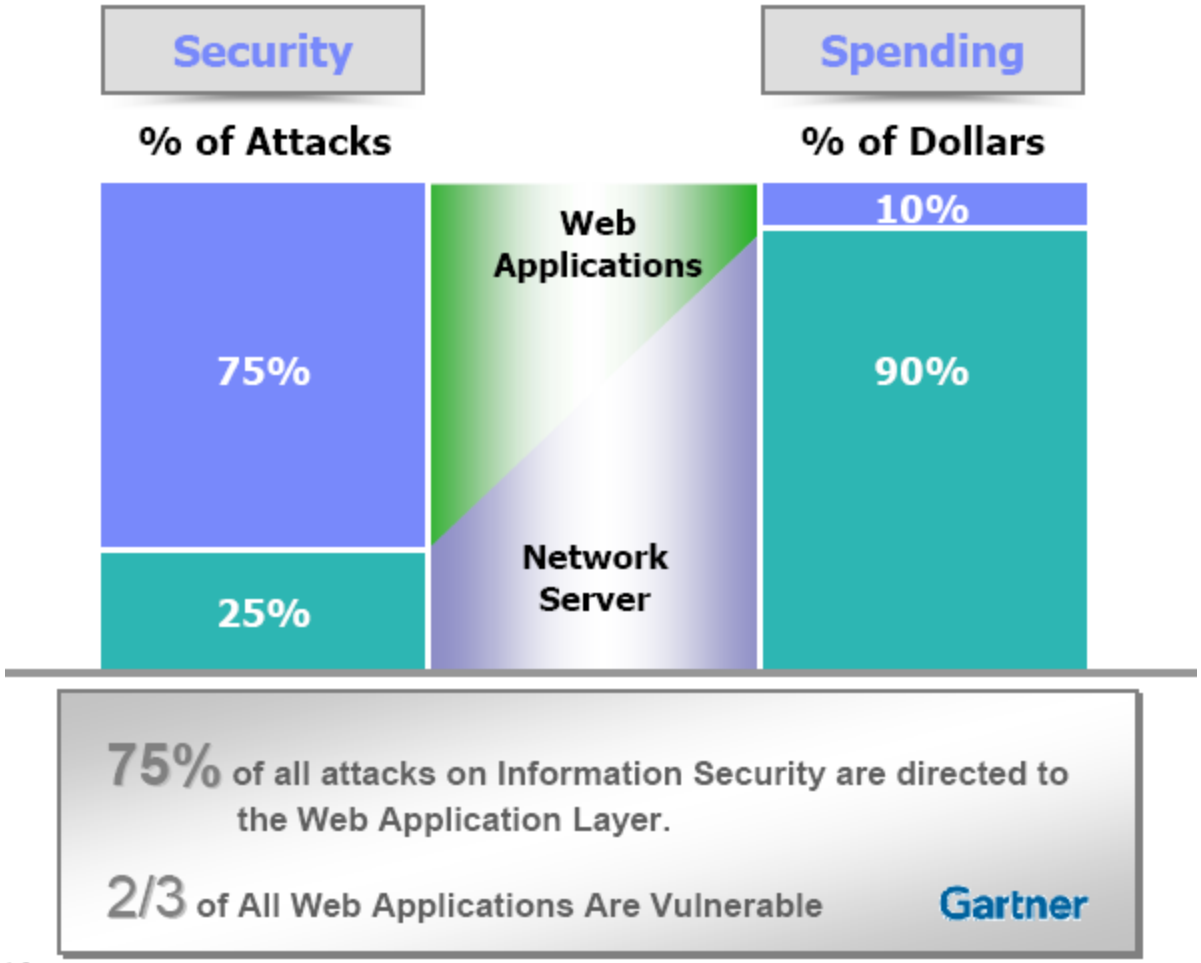


- Ağırlık koruma tarafı için ayrılır
  - Güvenlikcilerin çogu yeni saldırı yöntemlerinden habersizdir
- Web güvenliği tarihçesi
  - 2000~ web uygulamalarının yaygınlaşması
  - 2005~ Web uygulama güvenliği
  - 2009-2013 Web güvenliği altın çağı ☺

Geleneksel Güvenlik Yaklaşımı-II

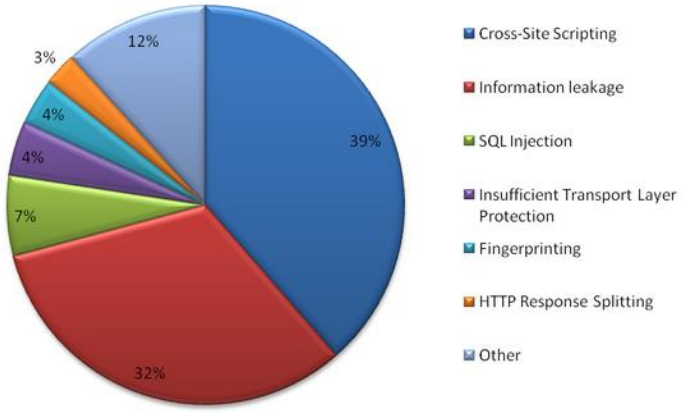


Geleneksel Güvenlik Anlayışının Göstergesi



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 Pos'
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
— T' ·indian, Feb 11, 200

Greek Ministry websites hit by hacker intrusion
— eKathimerini, Jan 31,2008

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

Your Free MacWorld Expo Platinum Pass
— CNet, Jan 14, 2008

Hacking Stage 6
— Wikipedia, Feb 9 2007

Hacker takes down Pennsylvania gvmt
— AP, Jan 6, 2008

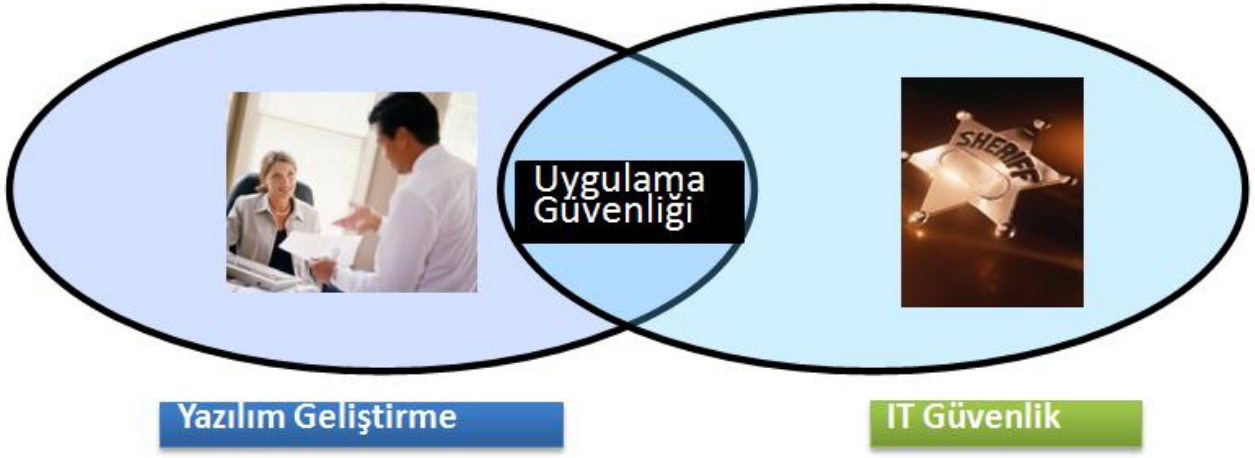
RIAA wiped off the Net
— TheRegister, Jan 20 2008

Italian Bank hit by XSS fraudsters
— Netcraft, Jan 8 2008

Drive-by Pharming in the Wild
— Symantec, Jan 21 2008

Uygulama Güvenliği Tanımı

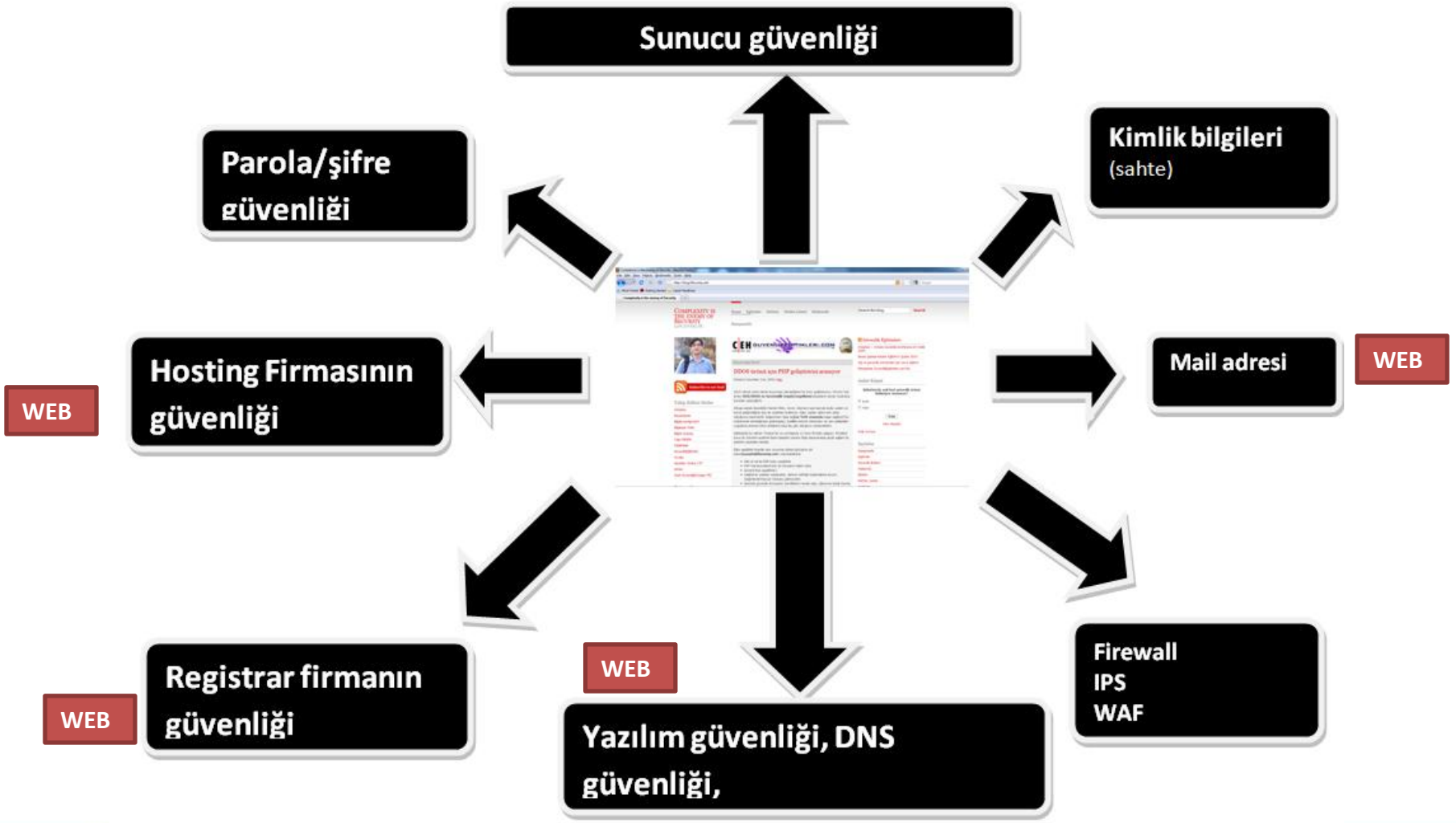
- Yazılım geliştiriciler en kısa sürede ortaya ürün çıkarma peşindeler.
- Guvenlik uzmanları yoğunlukla altyapı güvenliğine yönelmişlerdir
- Uygulama Güvenliği: Üretilen yazılımın fonksiyonlarını yitirmeden güvenli bir şekilde geliştirilmesini sağlama.



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

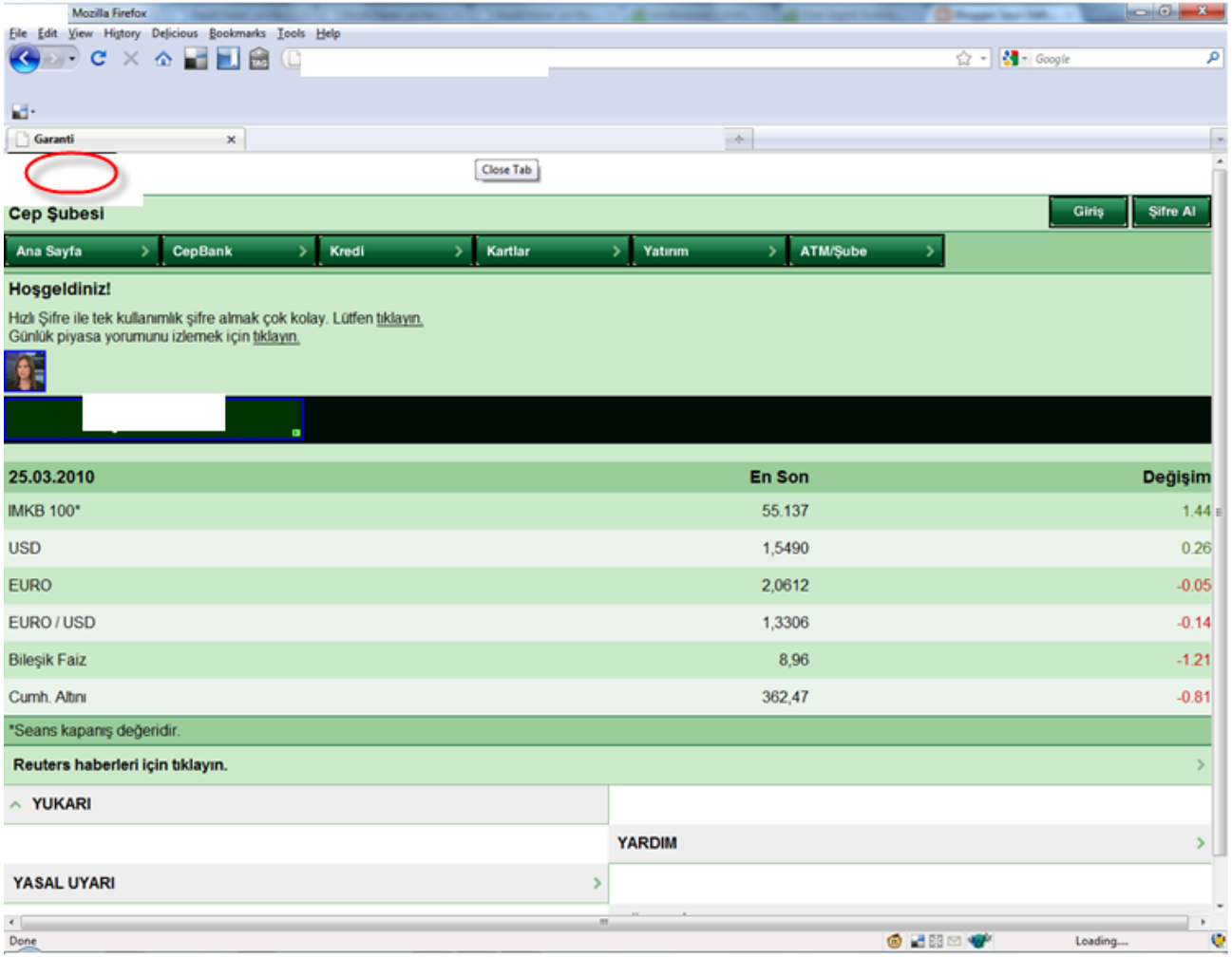
- Her iki dünyanın kendine özgü bakış açısı vardır
- Bakış açısı örnekleri...

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

Gmail

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 müdahele 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!

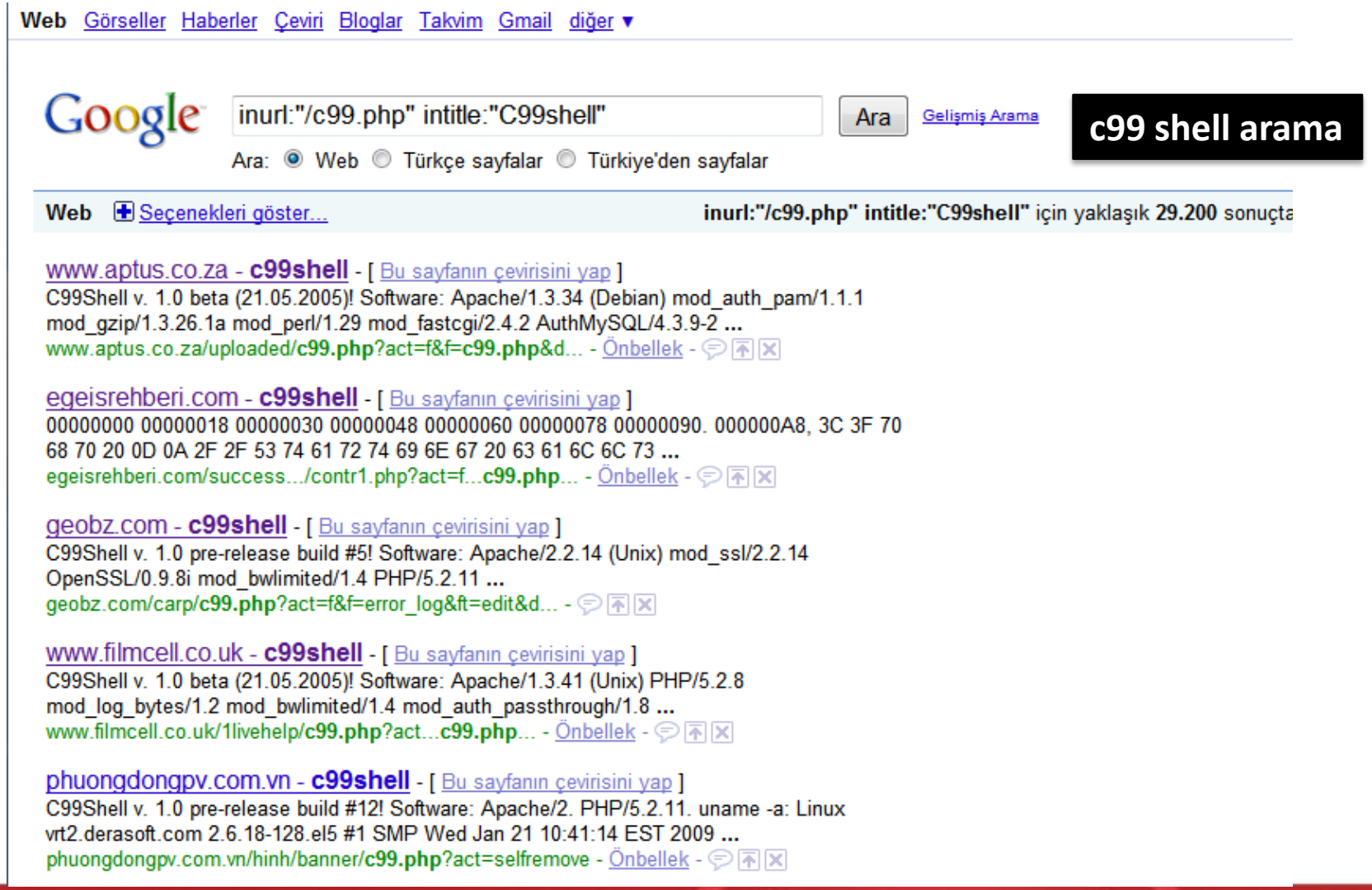
Google Üzerinden Açıklık Arama

```
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
```

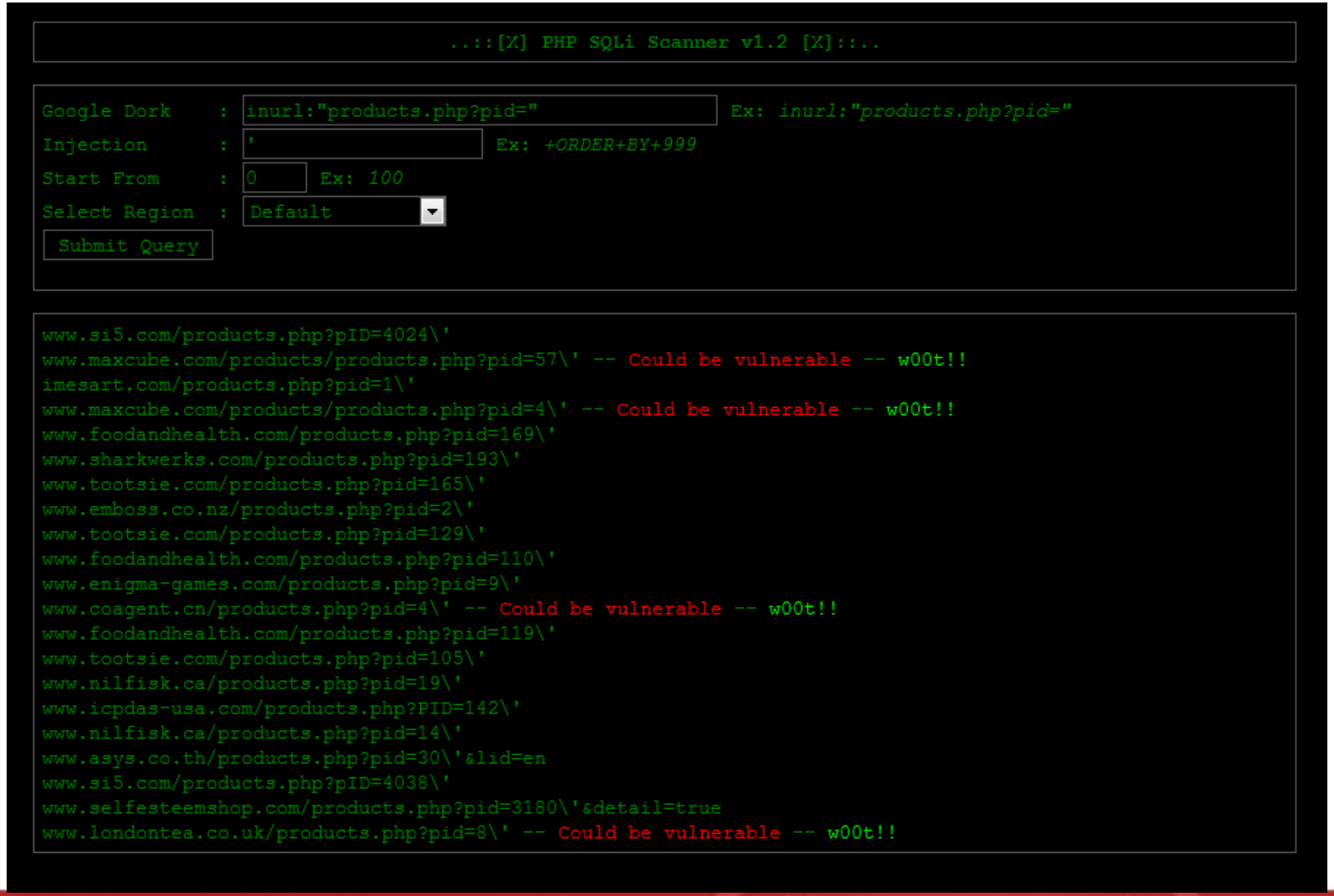
```
inurl:/modules/coppermine/themes/default
/theme.php?THEME_DIR=

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=
```

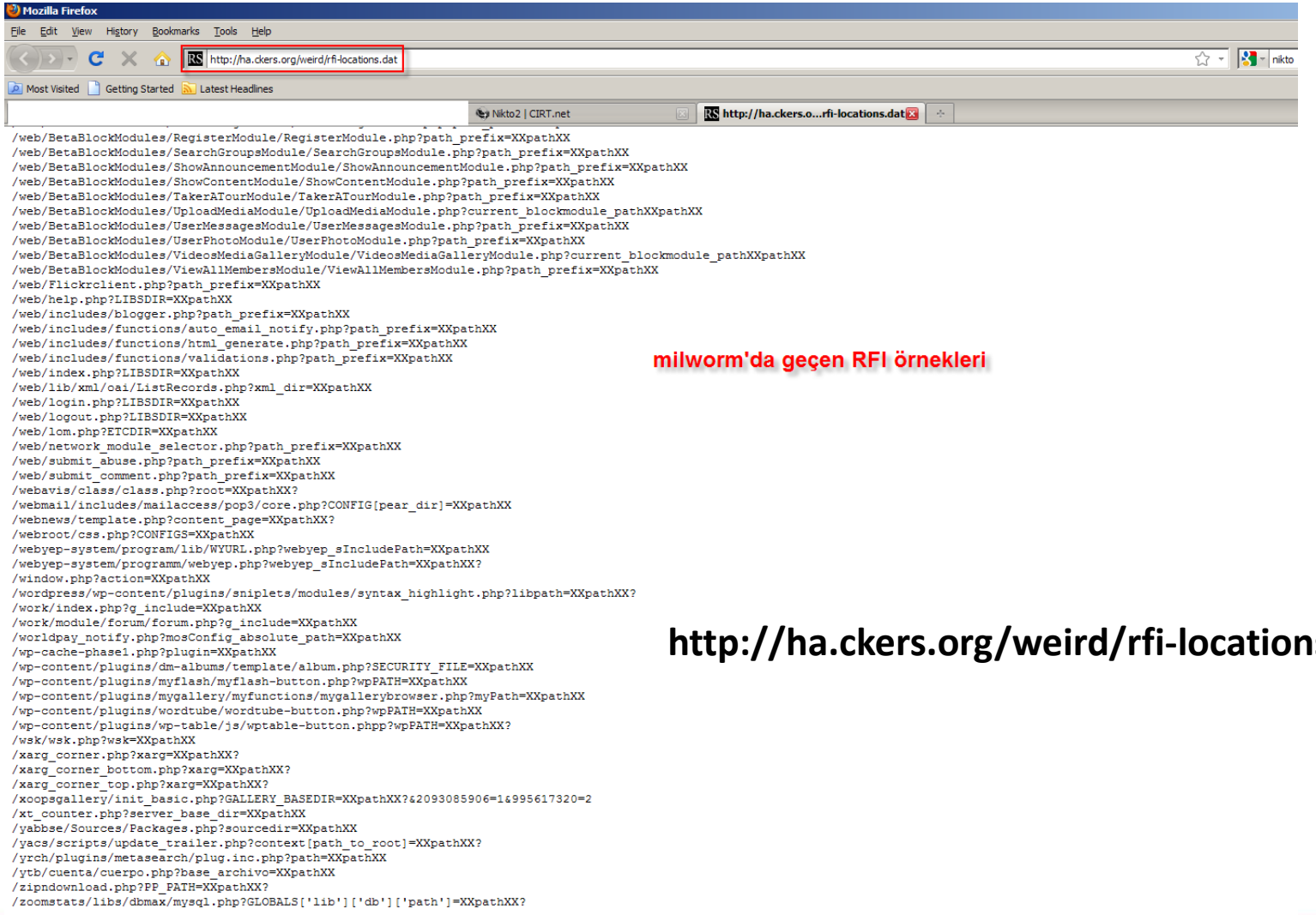

Google Üzerinden Hazır Sistem Bulma



Otomatik SQLi Bulucu



RFI Arama Örnekleri



milworm'da geçen RFI örnekleri

http://ha.ckers.org/weird/rfi-locations.dat

Basit (!) Bir Web Zaafiyeti Nelere Yol Açabilir?

Video

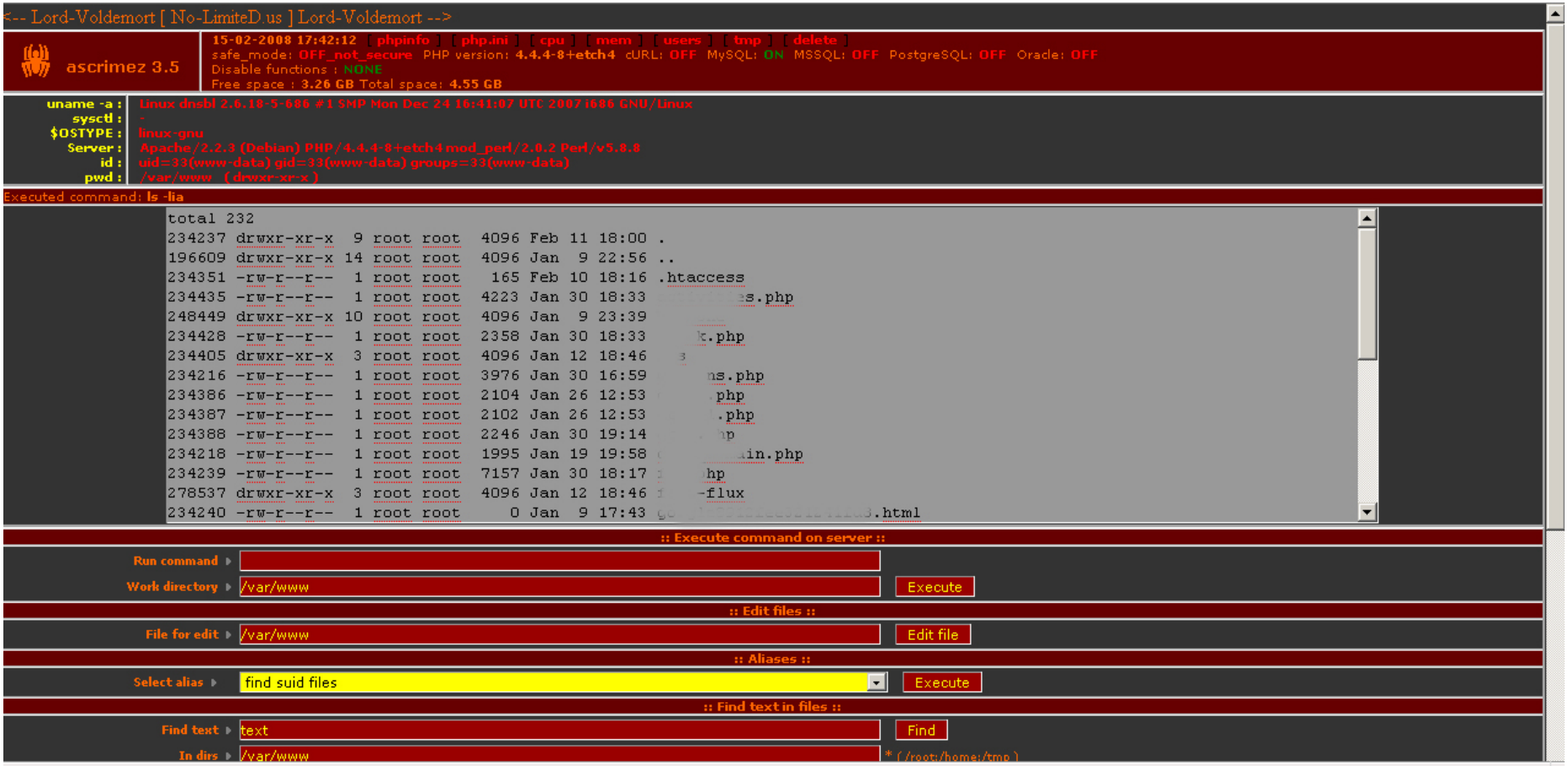
Web Shell

- 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-LimiteD.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 dnsbl 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
248449 drwxr-xr-x 10 root root 4096 Jan 9 23:39
234428 -rw-r--r-- 1 root root 2358 Jan 30 18:33
234405 drwxr-xr-x 3 root root 4096 Jan 12 18:46
234216 -rw-r--r-- 1 root root 3976 Jan 30 16:59
234386 -rw-r--r-- 1 root root 2104 Jan 26 12:53
234387 -rw-r--r-- 1 root root 2102 Jan 26 12:53
234388 -rw-r--r-- 1 root root 2246 Jan 30 19:14
234218 -rw-r--r-- 1 root root 1995 Jan 19 19:58
234239 -rw-r--r-- 1 root root 7157 Jan 30 18:17
278537 drwxr-xr-x 3 root root 4096 Jan 12 18:46
234240 -rw-r--r-- 1 root root 0 Jan 9 17:43
:: Execute command on server ::
Run command
Work directory /var/www Execute
:: Edit files ::
File for edit /var/www Edit file
:: Aliases ::
Select alias find suid files Execute
:: Find text in files ::
Find text text Find
In dirs /var/www

- Video..

Dünyadan Örnekler

Meşhur Türk Hackerlar(?)☺

My School Rooted 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/XXXXXXXXX [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 administators 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.

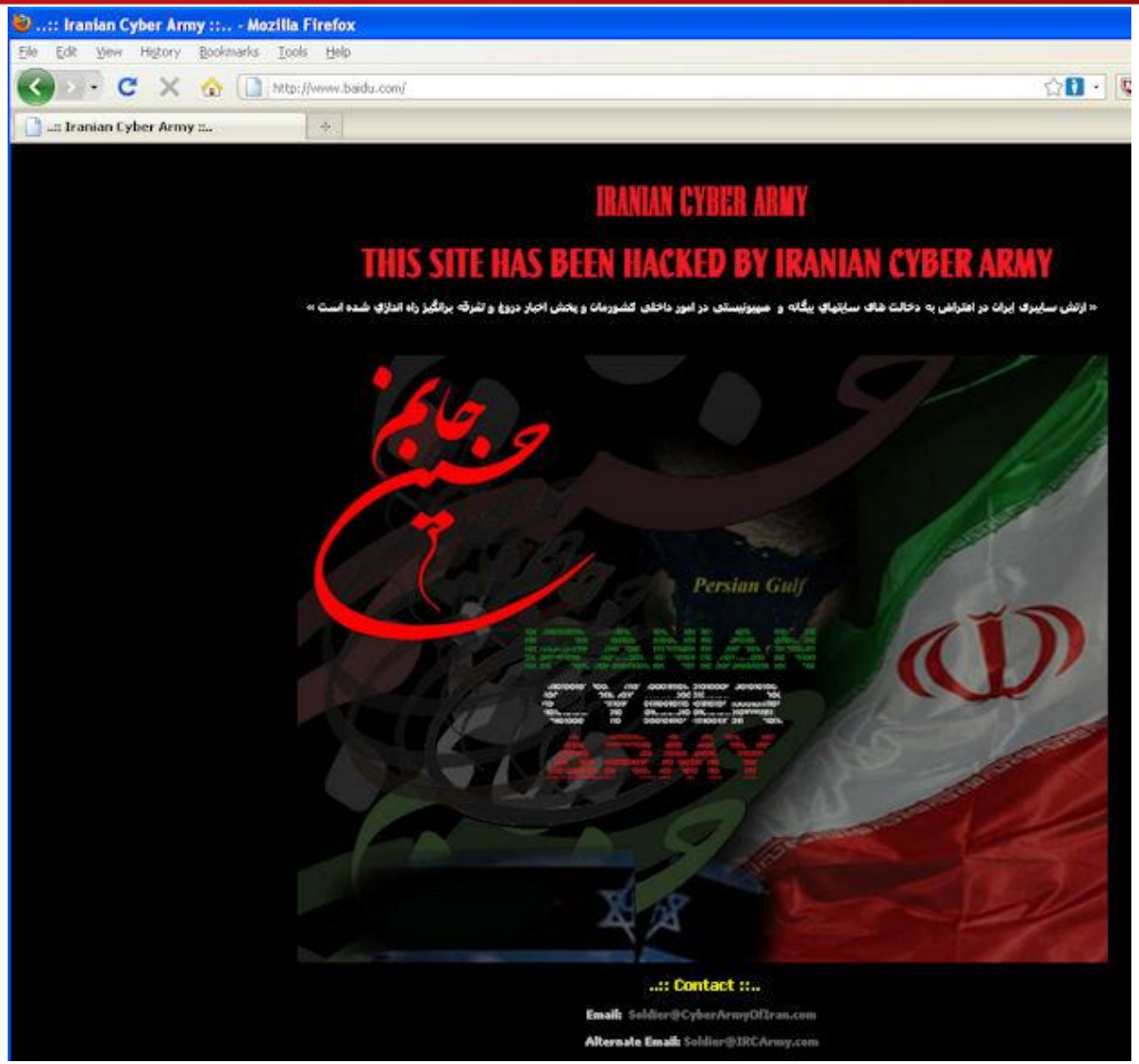
About 6 hours after they started resetting passwords, we noticed the attackers and began shutting down services. We notified Atlassian of the previously unreported XSS attack in JIRA and contacted SliceHost. Atlassian was responsive. Unfortunately, SliceHost did nothing and 2 days later, the **very** 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.

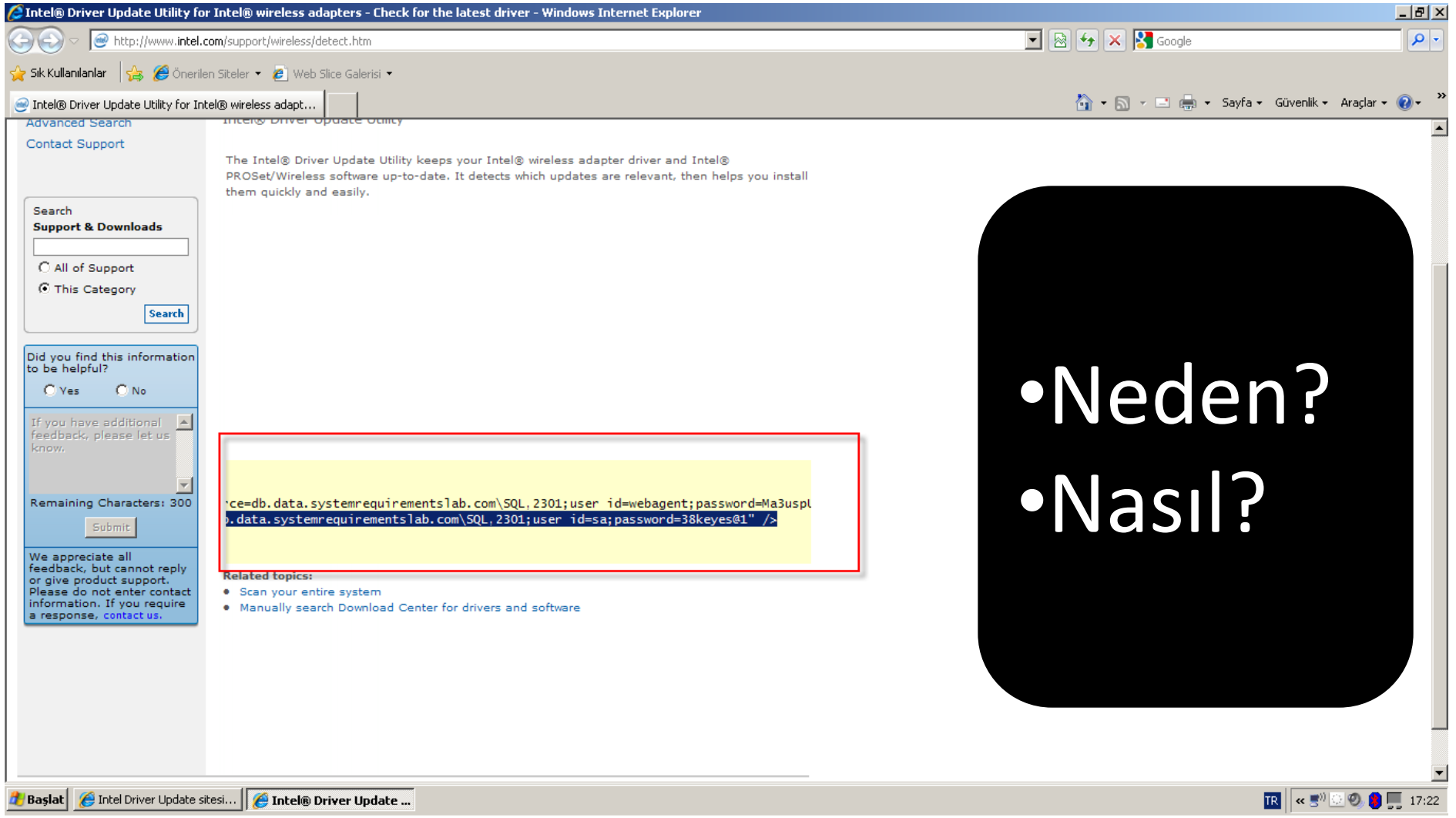
SQLi ☺

Baidu.com



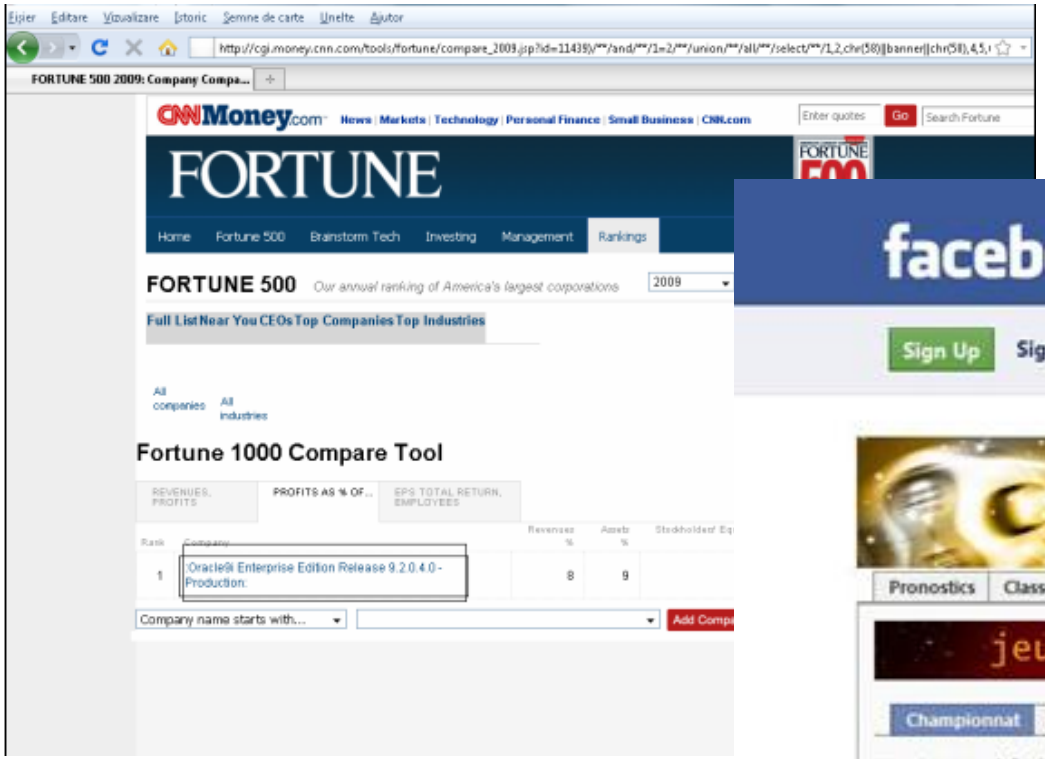
- Neden?
- Nasıl?

Intel.com

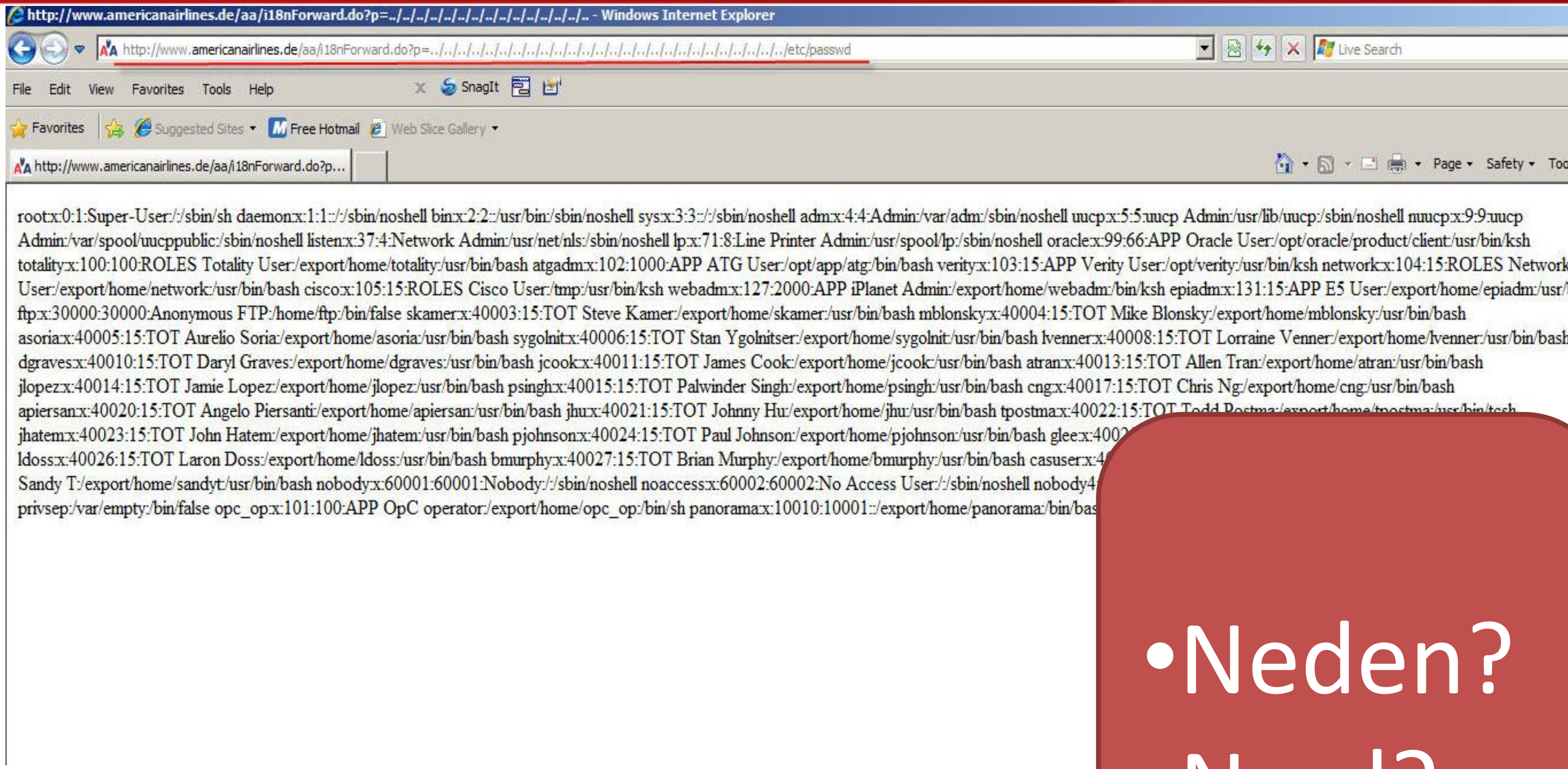


- Neden?
- Nasıl?

CNN & Facebook



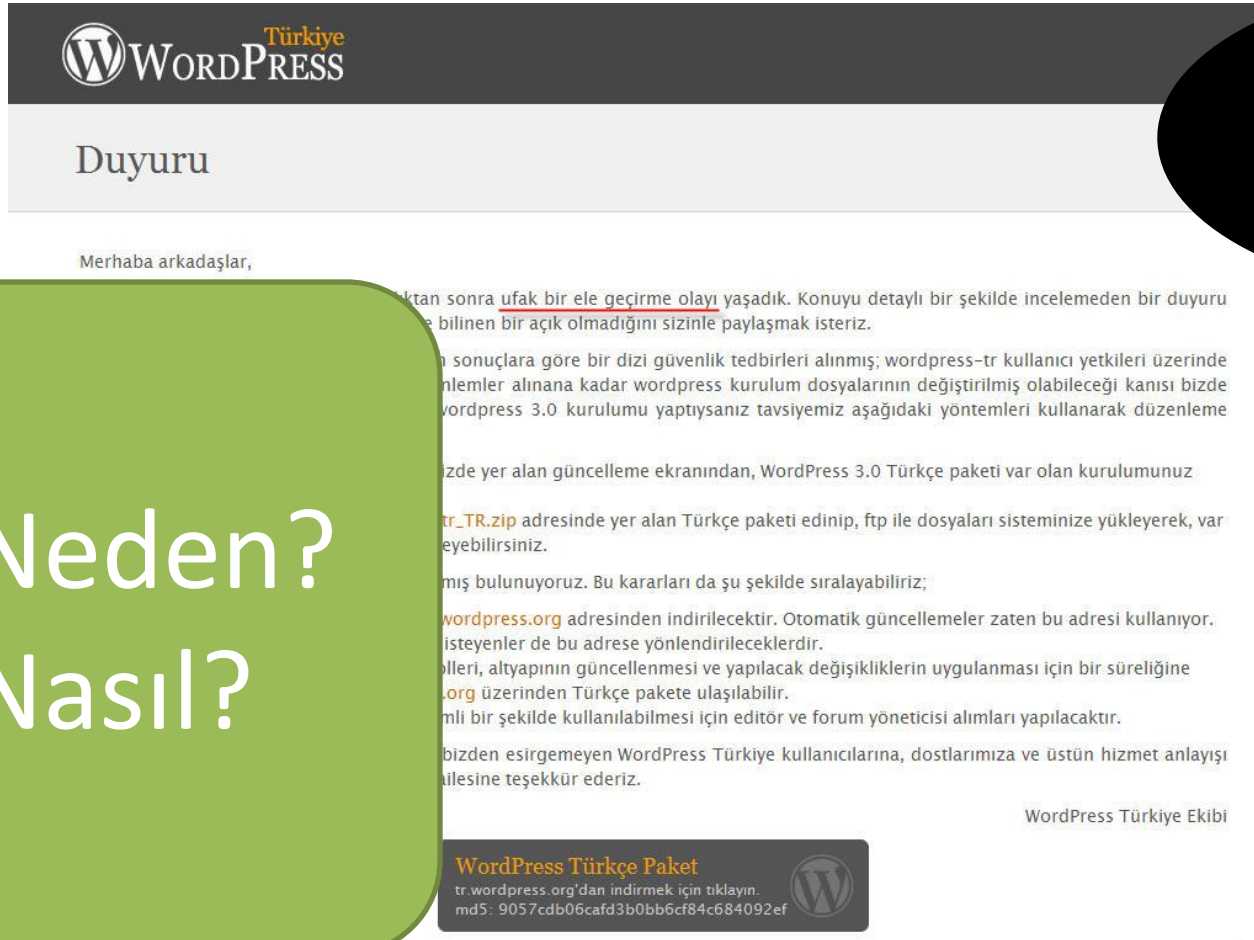
American Airlines



- Neden?
- Nasıl?

Türkiye’den Örnekler...

Wordpress Türkiye



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

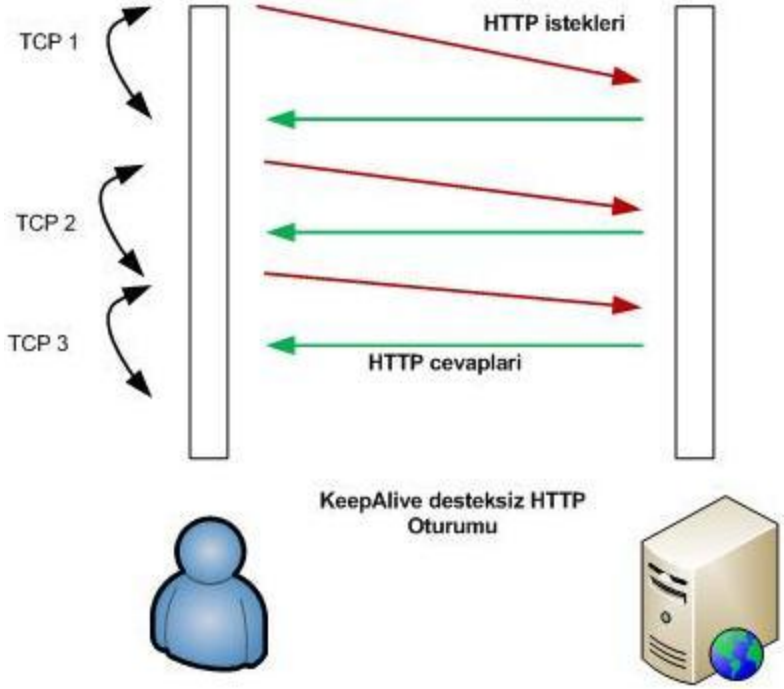
- Ya benimsin ya toprağın mantığı
- Bilgi güvenliğini tam anlayamamış kurumların dikkat etmedikleri bir konu
- Web uygulamaları&sunucuları en kritik bileşenlerdir
  - Online bankacılık sitesi çalışmayan bir bankanın zararı?
  - Onlien oyunlar? E-ticaret siteleri?
- Diğer DDOS saldırılarına oranla çok 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 50X10=500 TCP paketinin gidip gelmesi gerekir

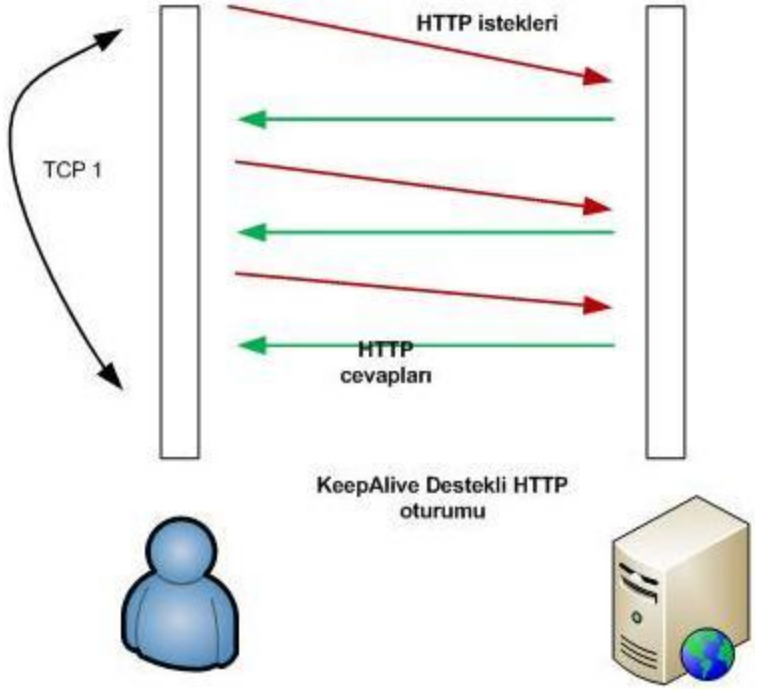
Klasik HTTP oturumu

- Her HTTP bağlantısı için TCP bağlantısı gerekir.



HTTP KeepAlive

- HTTP KeepAlive(persistent connection): her HTTP isteği için ayrı bir TCP bağlantısı açmak yerine bir adet TCP bağlantısı içerisinden belirli sayıda (5, 10, ..) HTTP isteğinin aktarılabilmesini sağlar.

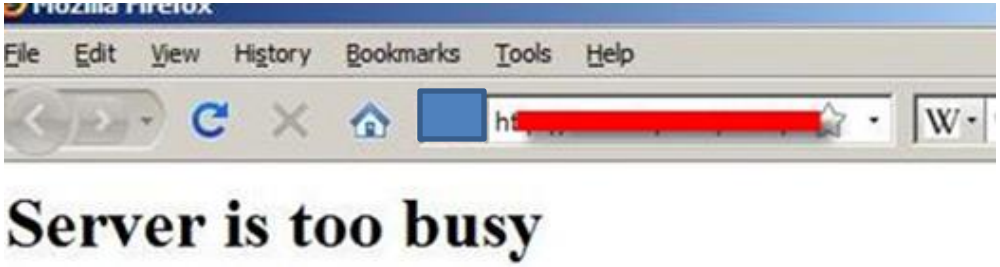


Http Pipelining

- 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



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 b
  adresinden gönderilebilir

Web Uygulama Güvenliği Testleri

Türkçe Web Güvenliği Kaynağı:OWASP Türkiye

www.lifeoverip.net/netsec-listesi/

NetSec
Ağ ve Bilgi Güvenliği Topluluğu

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 amaci, benzer pozisyonlarda calisan bilisimciler arasinda bilgi paylasimini artirmak ve guvenlik konusunda referans olabilecek kaynaklar olusturmaktir.
Ag ve guvenlik amacli kullanilabilecek her tur ticari ve acik kaynak kodlu yazilimin tanitiminin yapilmasi (kuru reklama kesinlikle izin verilmeyecektir) serbesttir. Boylece farkli urunleri kullanan bilisim profesyonellerine alternatif urunleri tanima firsati verilmis olacaktir.
Listenin Genel icerigi asagidaki konulardan olusmaktadir;

* Güvenlik Duvarlari
* Saldiri Tespit ve Engelleme Sistemleri
* Kablosuz Aglarda Guvenlik
* Yerel Aglarda Guvenlik
* Web Uygulama Guvenligi
* VPN Uygulamalari
* Trafik Analizi
* Adli Bilişim Analizi
* Tuzak Sistemler
* Linux/UNIX/Windows isletim sistemlerinde Guvenlik

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...