SOFTWARE & SYSTEMS QUALITY CONFERENCES Germany | 2009

Information Leakage

Testing for information leakage from an attackers point of view

Dr. Alexander Schinner, CISSP, GCFA, GCIA

T-Systems

Agenda

Introduction

- Definition of Information Leakage
- Attackers point of View
- Security by Obscurity

Information Leakage

- Source Code
- Comments
- Internal Information
- Error Messages
- Names

Tools

- Server side
- Client Side

Conclusion

- Sanitize Output
- Filter Output
- Test Output

Testing for
Information
Leakage
from an
Attackers
Point of View

Information Leakage
Definition

- A system reveals some information to unauthorized parties.

Information Leakage
Definition

- A system reveals some information to unauthorized parties.

Information Leakage
Definition

- A system reveals some information to unauthorized parties.
- Every little piece of information will help the attacker!

Information Leakage
Definition

- A system reveals some information to unauthorized parties.
- Every little piece of information will help the attacker!

Attacker
Source Code
Comments
Error Message
SQL Injection

Attackers POV
Access to Secrets

Vulnerability

- “High” value information
- Unexpected access to secrets
  - Internal documentations
  - Default Passwords
  - Source Code
  - Configuration information

Exploit

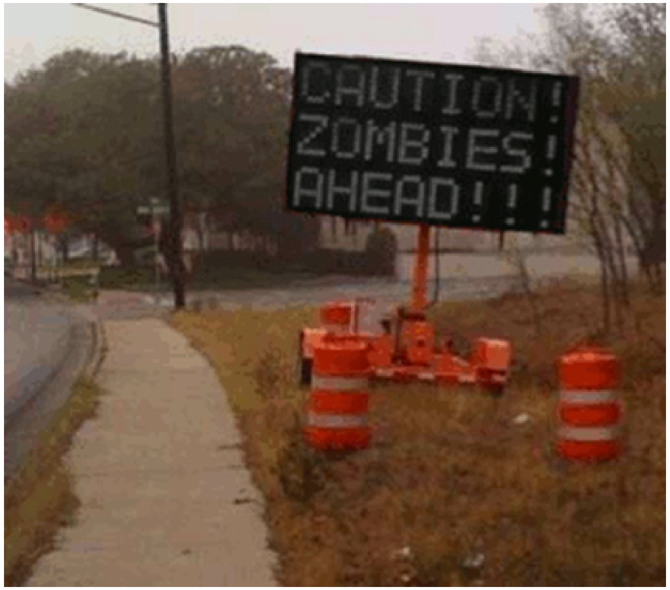
Attackers POV

Access to Secrets

Vulnerability

- “High” value information
- Unexpected access to secrets
  - Internal documentations
  - Default Passwords
  - Source Code
  - Configuration information

Exploit



Documentation with default passwords for these road signs appeared a few weeks before…

Attackers POV
Access to Secrets

Vulnerability

- "High" value information
- Unexpected access to secrets
  - Internal documentations
  - Default Passwords
  - Source Code
  - Configuration information

Exploit

- Tailored attacks
- Develop new attack vectors
- Free access

Documentation with default passwords for these road signs appeared a few weeks before…

Attackers POV
Reconnaissance

Vulnerability

- "Medium" value information
- Easier access to technical information
- Disclosure of
  - technical details
  - software versions
  - local architecture

Exploit

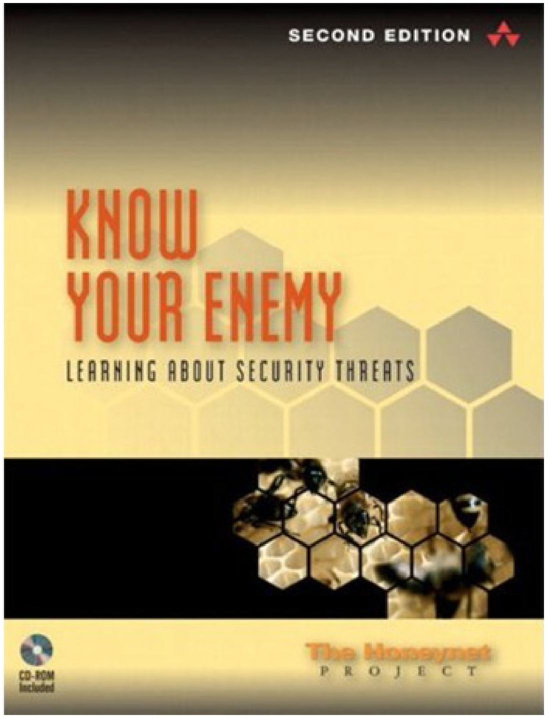
Attackers POV

Reconnaissance

Vulnerability

- “Medium” value information
- Easier access to technical information
- Disclosure of
  - technical details
  - software versions
  - local architecture

Exploit

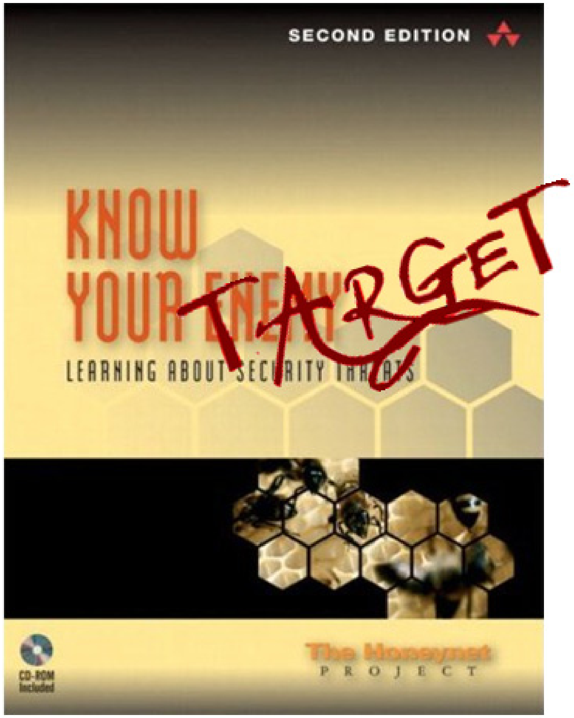


Attackers POV
Reconnaissance

Vulnerability

- "Medium" value information
- Easier access to technical information
- Disclosure of
  - technical details
  - software versions
  - local architecture

Exploit



Attackers POV

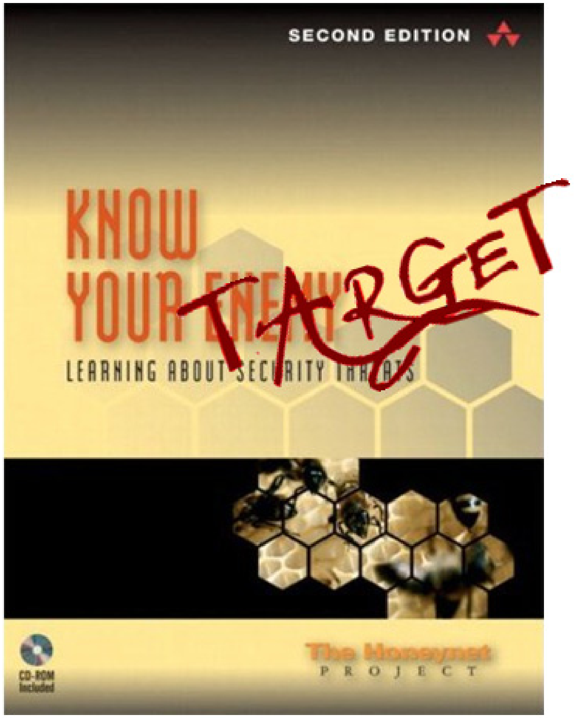
Reconnaissance

Vulnerability

- "Medium" value information
- Easier access to technical information
- Disclosure of
  - technical details
  - software versions
  - local architecture

Exploit

- Choose
  - valuable targets
  - vulnerable targets
  - correct exploit
  - attack vector
- Attacking is more comfortable



Attackers POV
Social Engineering

Vulnerability

- "Low" value information
- Whom do we trust?
  - People, pretending to be an "Official"
  - People, who ask for our help
  - People, who can "proof" their identity by "internal knowledge"

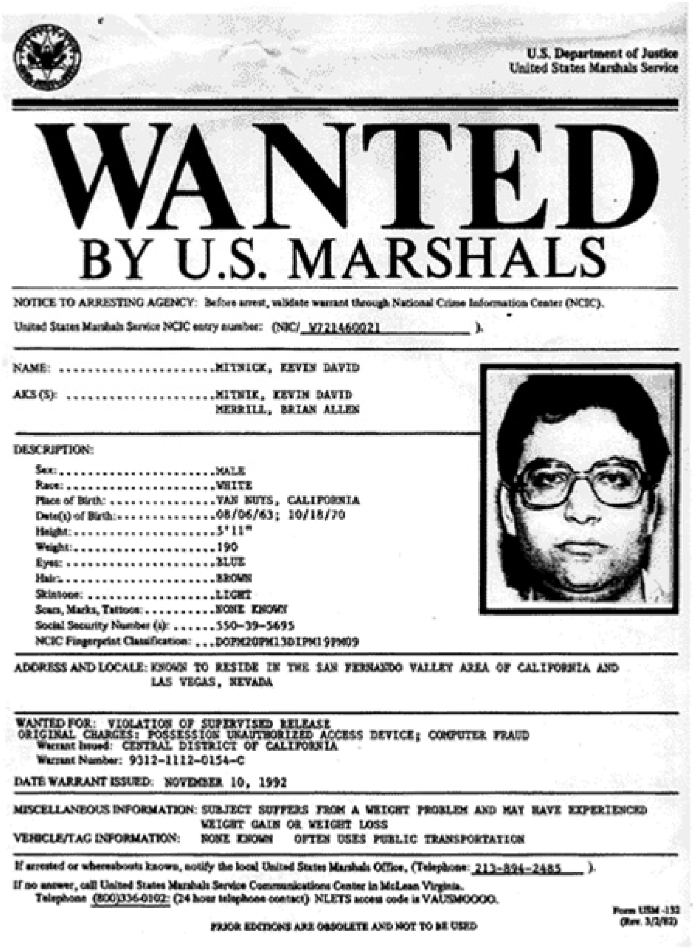
Exploit

Attackers POV
Social Engineering

Vulnerability

- "Low" value information
- Whom do we trust?
  - People, pretending to be an "Official"
  - People, who ask for our help
  - People, who can "proof" their identity by "internal knowledge"

Exploit



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM-132
(Rev. 3/2/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

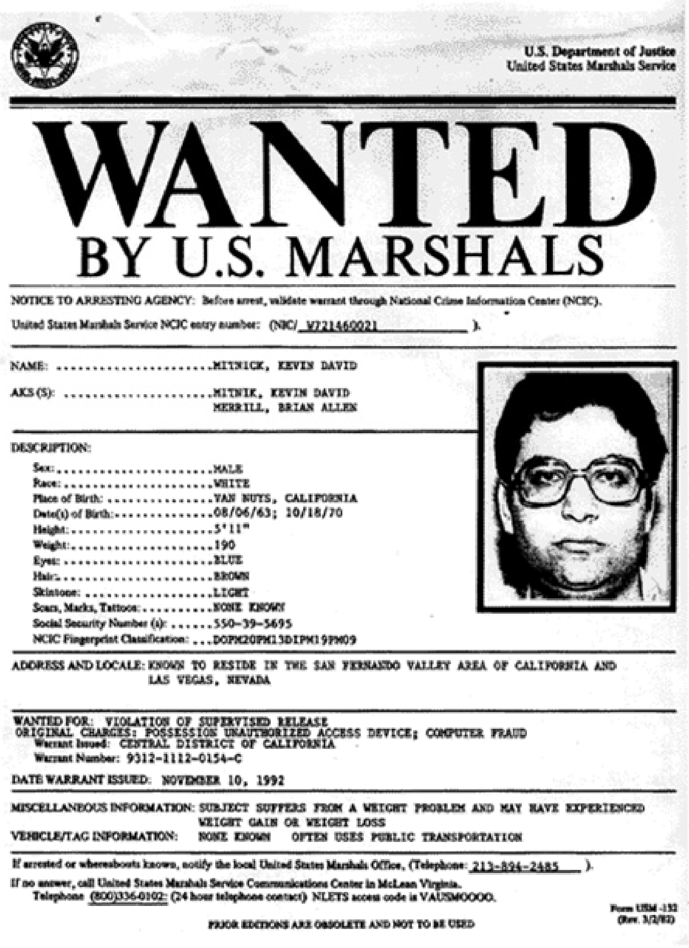
Attackers POV
Social Engineering

Vulnerability

- “Low” value information
- Whom do we trust?
  - People, pretending to be an “Official”
  - People, who ask for our help
  - People, who can “proof” their identity by “internal knowledge”

Exploit

- The clever manipulation of the natural human tendency to trust and help
- Most dangerous attack vector



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: ....MITNICK, KEVIN DAVID

AKS (S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: ....MALE
Race: ....WHITE
Place of Birth: ....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: ....5'11"
Weight: 190
Eyes: ....BLUE
Hair: ....BROWN
Skintone: ....LIGHT
Scars, Marks, Tattoos: ....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSMOOOO.

Form USM-132
(Rev. 3/2/93)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

Security by Obscurity

Isn‘t information hiding equal to „Security by Obscurity“?

Yes, because

- Violation of Kerckhoffs' doctrine from 1883
- Indicator for Snakeoil
- Typical wording
  - This information will help nobody to...
  - Nobody will find this hidden entry point...

Security by Obscurity

Isn‘t information hiding equal to „Security by Obscurity“?

Yes, because

- Violation of Kerckhoffs' doctrine from 1883
- Indicator for Snakeoil
- Typical wording
  - This information will help nobody to…
  - Nobody will find this hidden entry point…

No, because

- Military notion: Loose Lips sink Ships
- Should never be used as a primary security measure
- You are not obligated to help attacker

Security by Obscurity

Isn‘t information hiding equal to „Security by Obscurity“?

Yes, because

- Violation of Kerckhoffs' doctrine from 1883
- Indicator for Snakeoil
- Typical wording
  - This information will help nobody to…
  - Nobody will find this hidden entry point…

No, because

- Military notion: Loose Lips sink Ships
- Should never be used as a primary security measure
- You are not obligated to help attacker

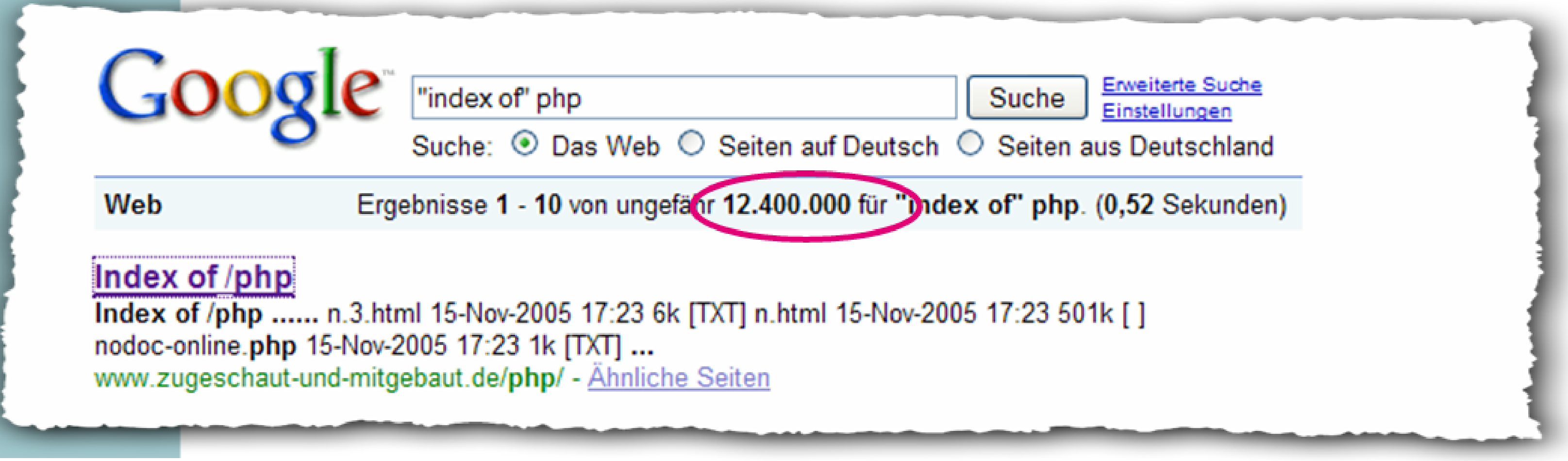
→Should be part of “Defense in Depth”
→Buys you time

Source Code

Introduction

How to leak

- Directory listings followed by direct download



Suche: ● Das Web ○ Seiten auf Deutsch ○ Seiten aus Deutschland

Web Ergebnisse **1** - **10** von ungefähr **12.400.000** für **"index of" php**. (**0,52** Sekunden)

Index of /php

Index of /php ...... n.3.html 15-Nov-2005 17:23 6k [TXT] n.html 15-Nov-2005 17:23 501k [ ] nodoc-online.**php** 15-Nov-2005 17:23 1k [TXT] **...**

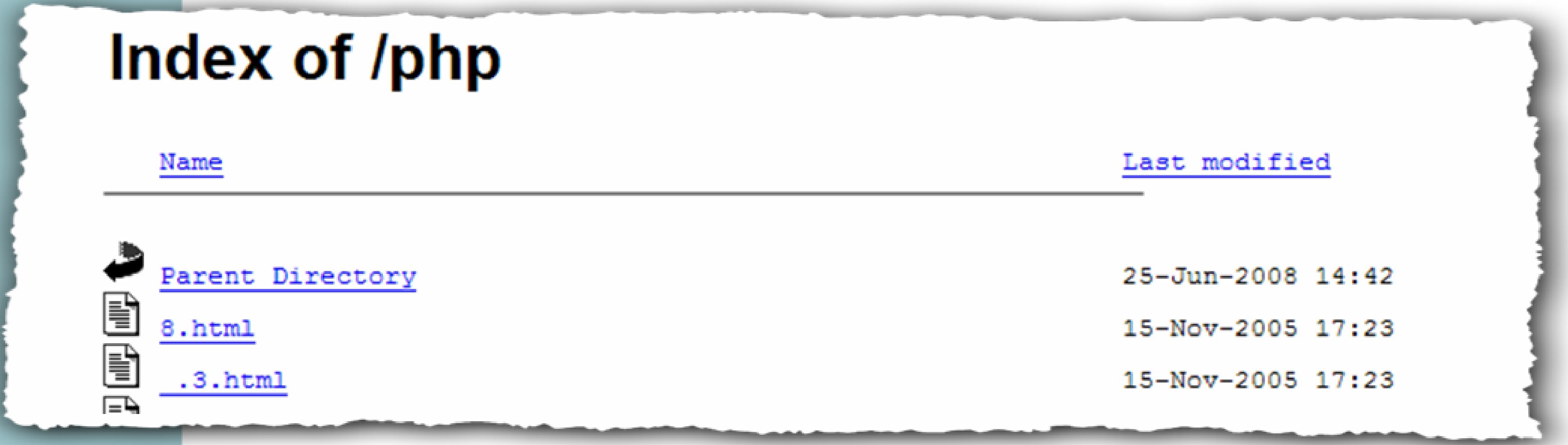
www.zugeschaut-und-mitgebaut.de/**php**/ - Ähnliche Seiten

Source Code

Introduction

How to leak

- Directory listings followed by direct download



Index of /php

```
    Name                                   Last modified

    Parent Directory                       25-Jun-2008 14:42
    8.html                                 15-Nov-2005 17:23
     .3.html                               15-Nov-2005 17:23
```

Source Code
Introduction

How to leak

- Directory listings followed by direct download
- Bug in Web-/Application Server

- Bugtraq ID 14764: Microsoft IIS WebDAV HTTP Request Source Code Disclosure Vulnerability
- Bugtraq 20001121 Disclosure of JSP source code with ServletExec AS v3.0c + web instance

Source Code

Introduction

How to leak

- Directory listings followed by direct download
- Bug in Web-/Application Server
- Filename guessing

- Include files: `header.inc, footer.inc, db.inc`
- Backup files: `index.bak, index.old, index.php~`
- Log-/Debug files: `debug.log, nohup.out, 1`

Source Code
Introduction

How to leak

- Directory listings followed by direct download
- Bug in Web-/Application Server
- Filename guessing

How to use

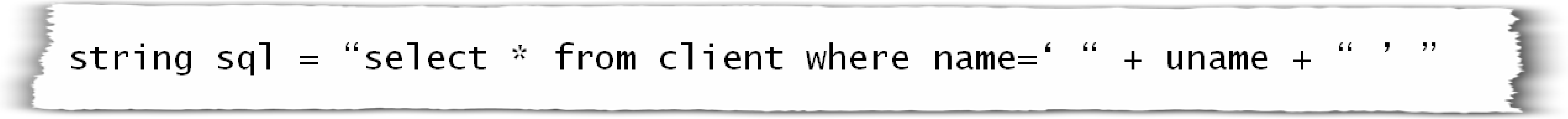
- Search for vulnerabilities

Source Code

Exploit

SQL Injection

- Search for database commands



```
string sql = “select * from client where name=‘ “ + uname + “ ’ ”
```

Source Code
Exploit

SQL Injection

- Search for database commands

```
string sql = “select * from client where name=‘ “ + uname + “ ’ ”
```

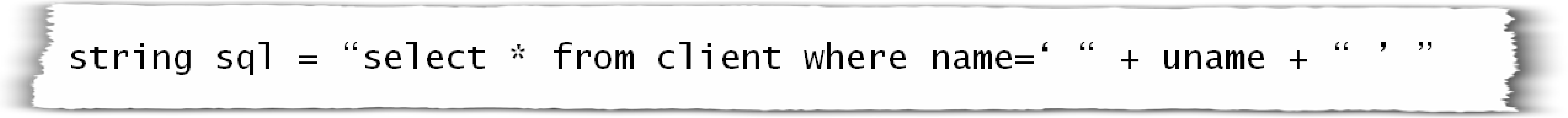
- User enters uname: “Schinner”. Effective command is

```
string sql = “select * from client where name=‘Schinner’
```

Source Code
Exploit

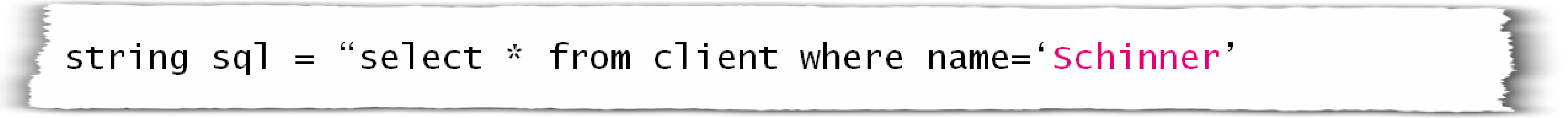
SQL Injection

- Search for database commands



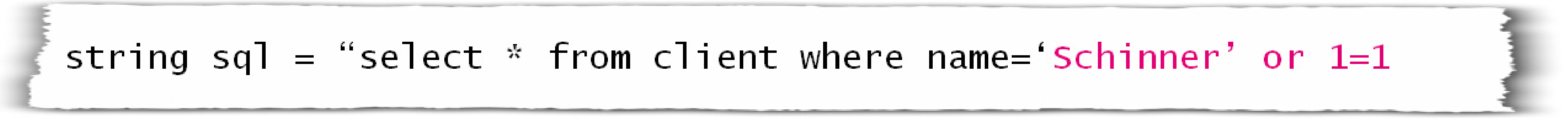
```
string sql = “select * from client where name=‘ “ + uname + “ ’ ”
```

- User enters uname: “Schinner”. Effective command is



```
string sql = “select * from client where name=‘Schinner’
```

- User enters uname: “Schinner’ or 1=1”. Effective command is

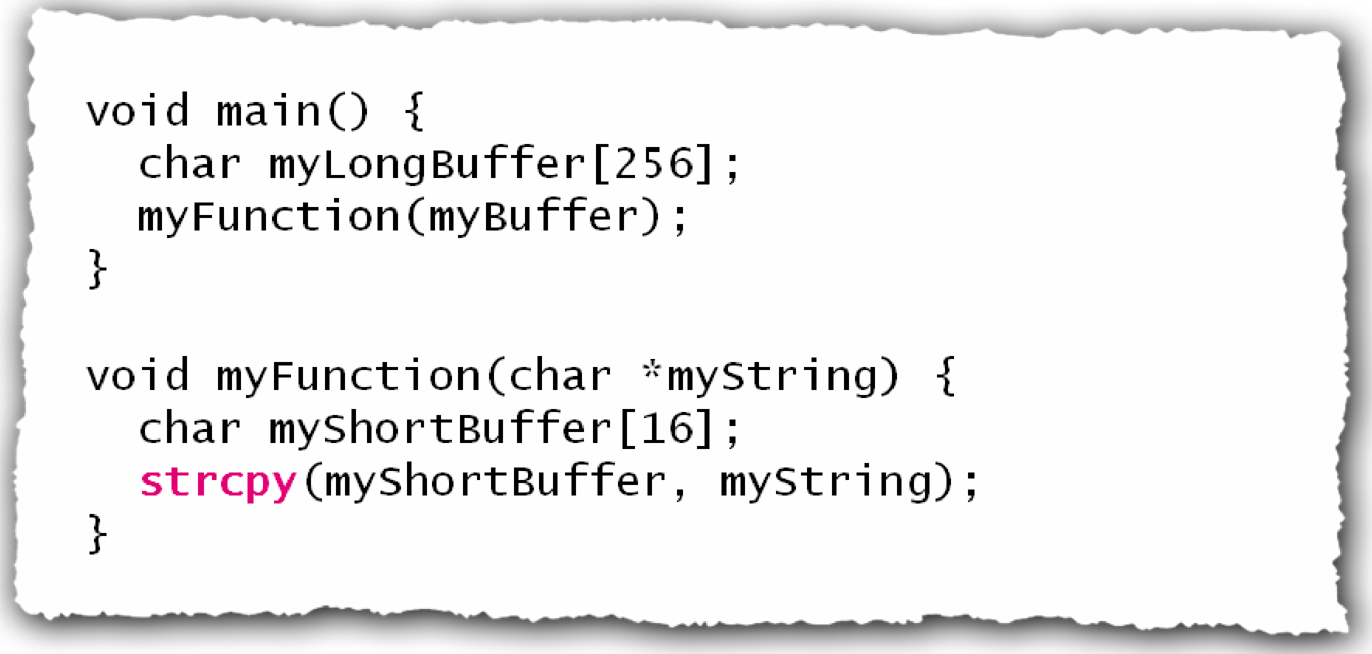


```
string sql = “select * from client where name=‘Schinner’ or 1=1
```

Source Code
Exploit

Buffer Overflow

- Search for typical commands e.g. strcpy

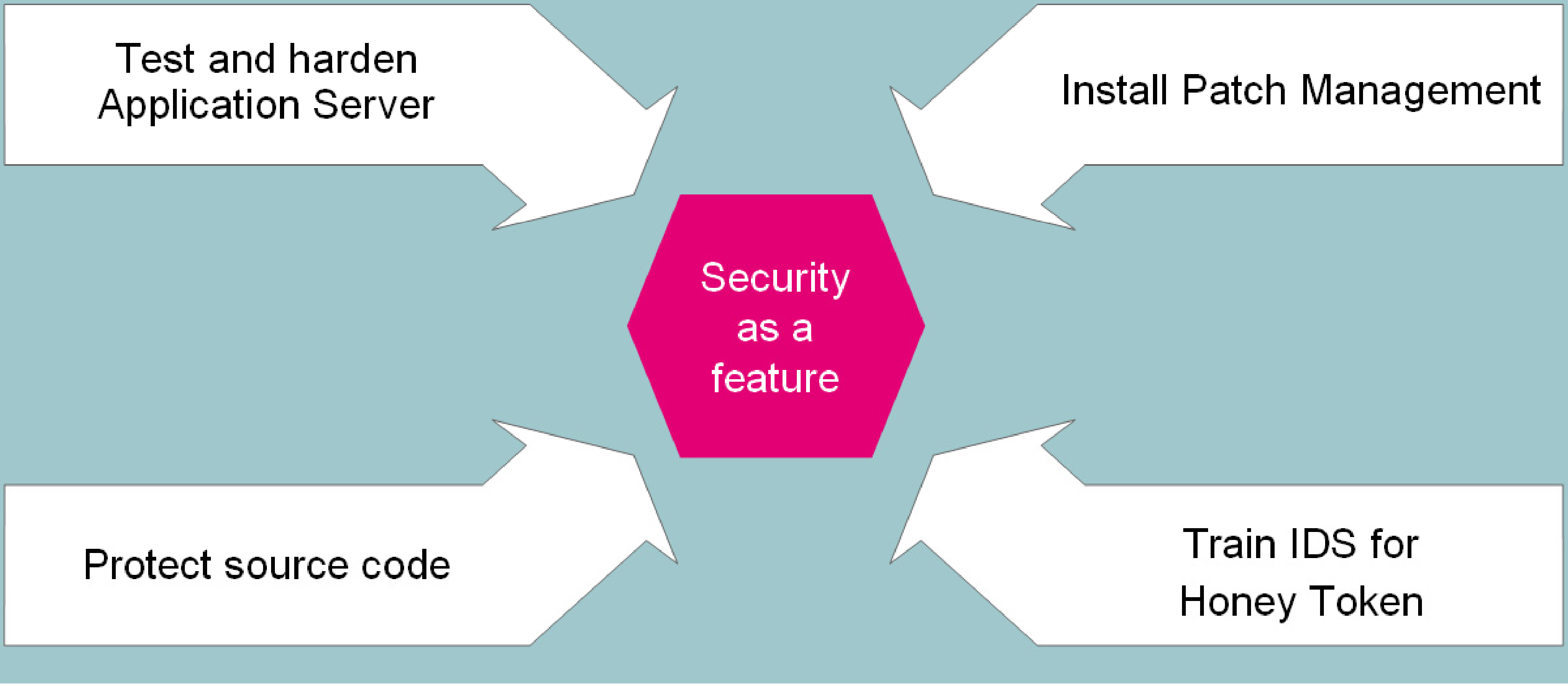


```
void main() {
  char myLongBuffer[256];
  myFunction(myBuffer);
}

void myFunction(char *myString) {
  char myShortBuffer[16];
  strcpy(myShortBuffer, myString);
}
```

- What happen, if `myString` is longer than 16 charactes?

Source Code
Prevention



Test and harden Application Server

Install Patch Management

Security as a feature

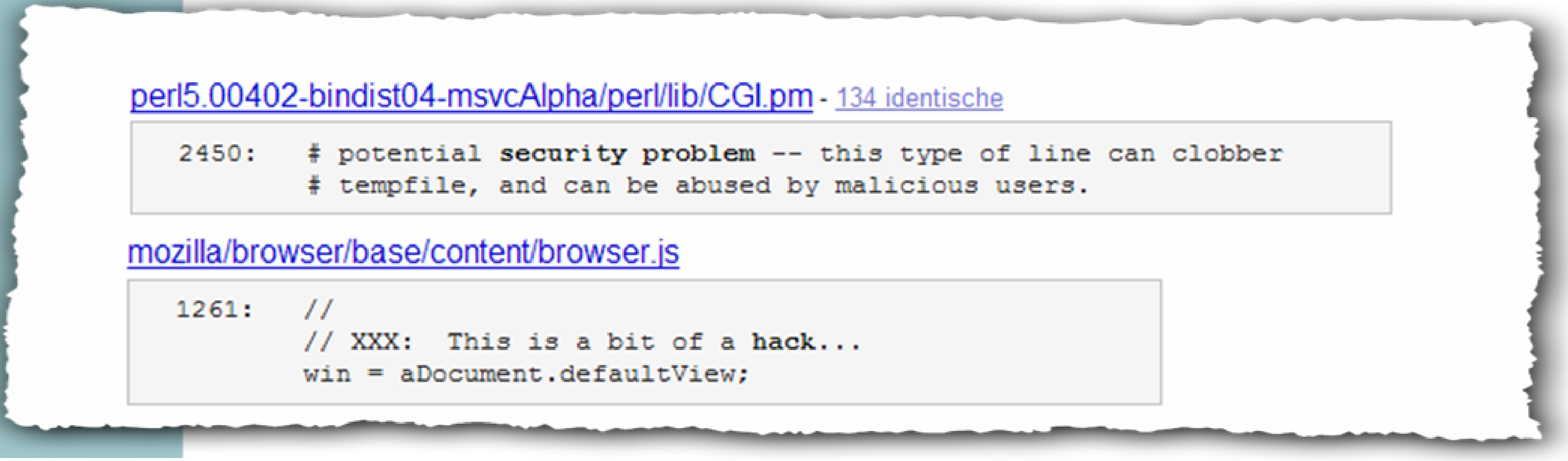
Protect source code

Train IDS for Honey Token

Comments
Introduction

How to leak

- Application source code



perl5.00402-bindist04-msvcAlpha/perl/lib/CGI.pm - 134 identische

```
  2450:   # potential security problem -- this type of line can clobber
          # tempfile, and can be abused by malicious users.
```

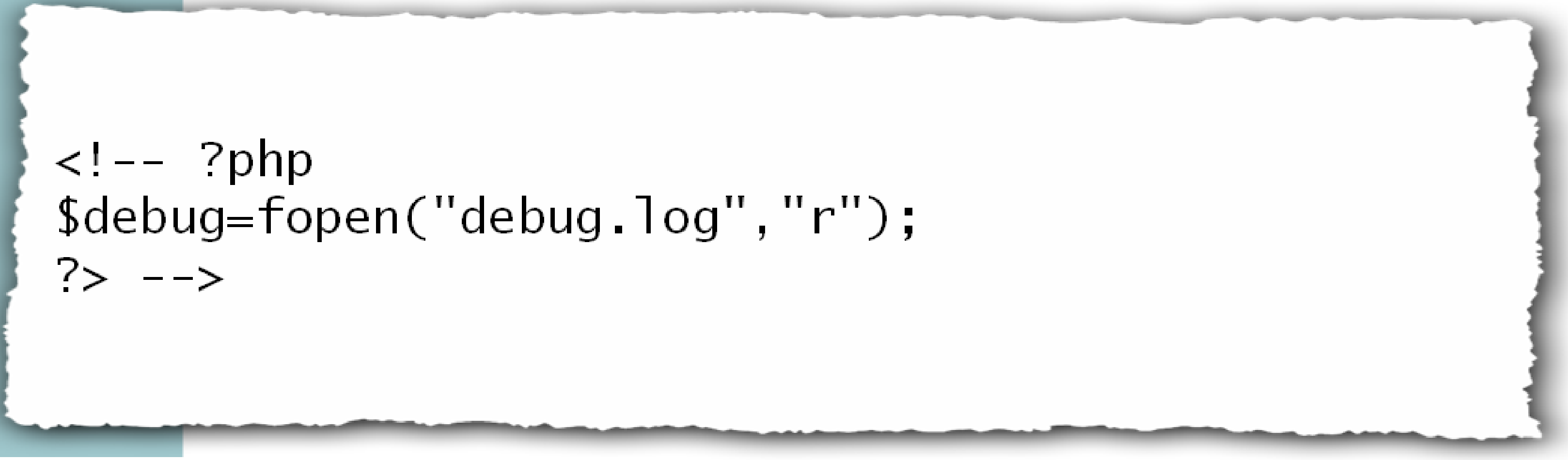
mozilla/browser/base/content/browser.js

```
  1261:   //
          // XXX:  This is a bit of a hack...
          win = aDocument.defaultView;
```

Comments
Introduction

How to leak

- Application source code
- HTML source code



```
<!-- ?php
$debug=fopen("debug.log","r");
?> -->
```

Comments
Introduction

How to leak

- Application source code
- HTML source code
- Internet discussion forum

- Usenet
- Developer lists
- Social networks

Comments
Introduction

How to leak

- Application source code
- HTML source code
- Internet discussion forum

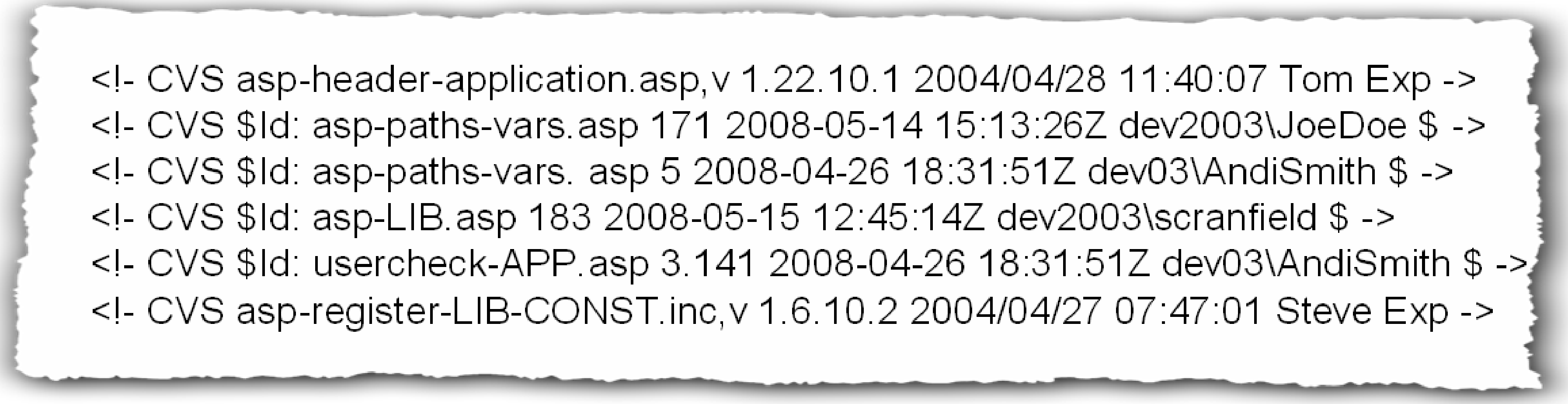
How to use

- Search for vulnerabilities
- Social engineering

Comments

Exploit

What would Kevin Mitnick do?

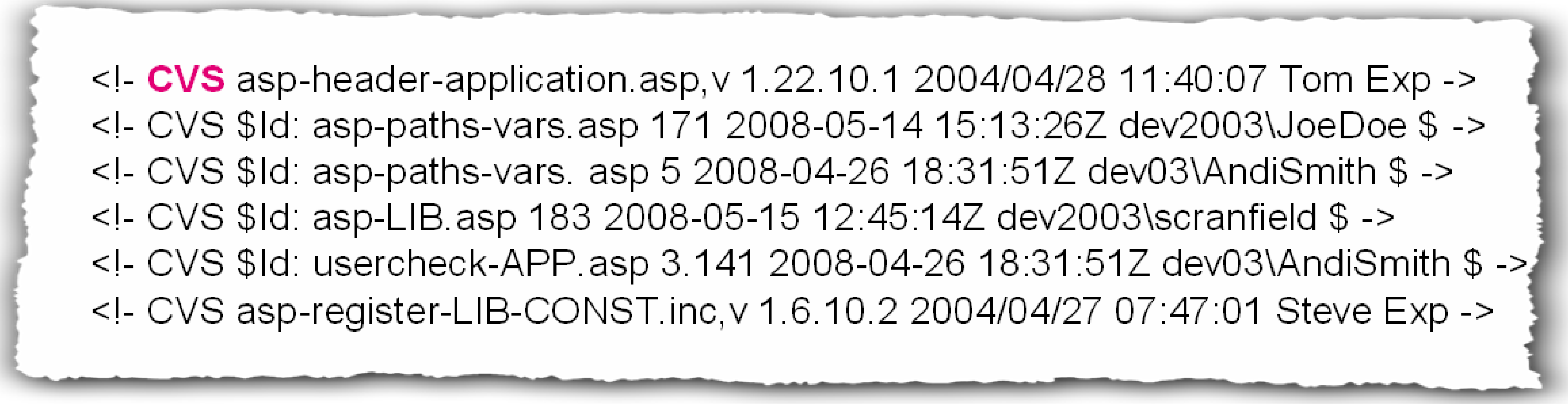


```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

Comments

Exploit

What would Kevin Mitnick do?

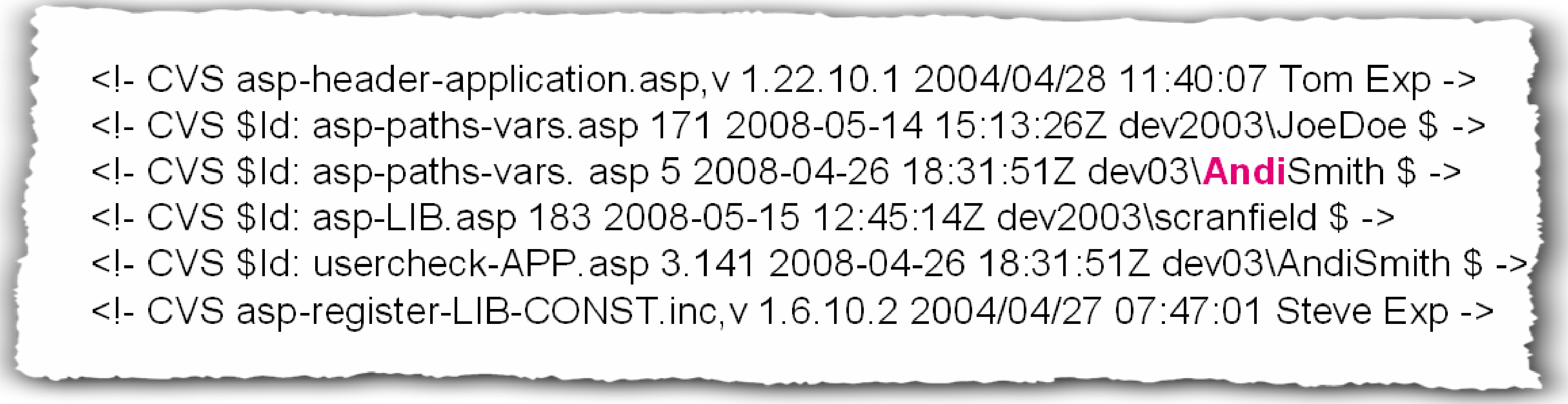


```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS …*

Comments
Exploit

What would Kevin Mitnick do?



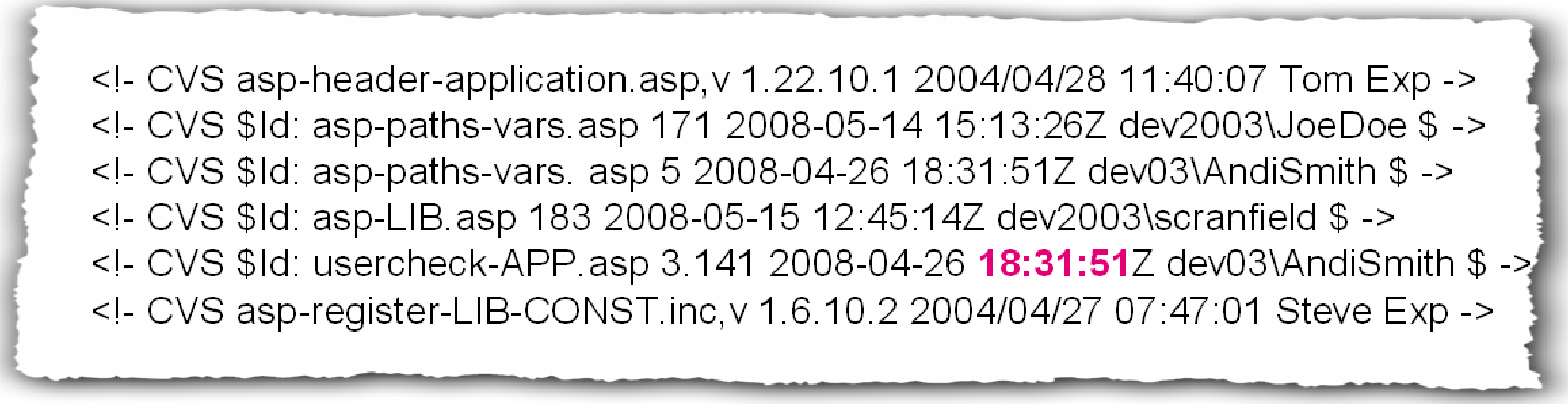
```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS check in Andi*

Comments

Exploit

What would Kevin Mitnick do?



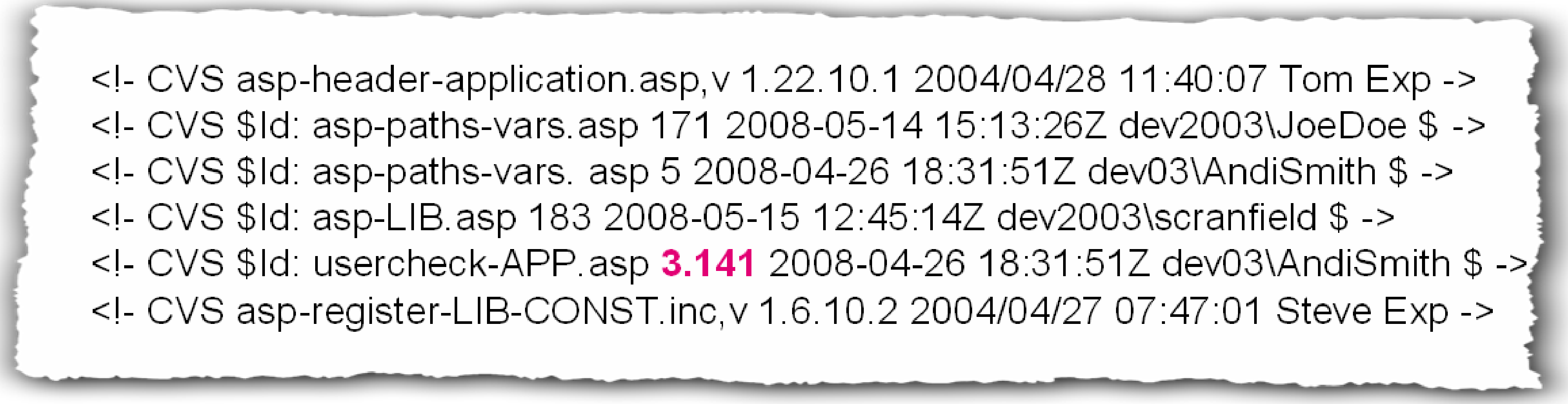
```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS check in Andi did in the evening.*

Comments

Exploit

What would Kevin Mitnick do?



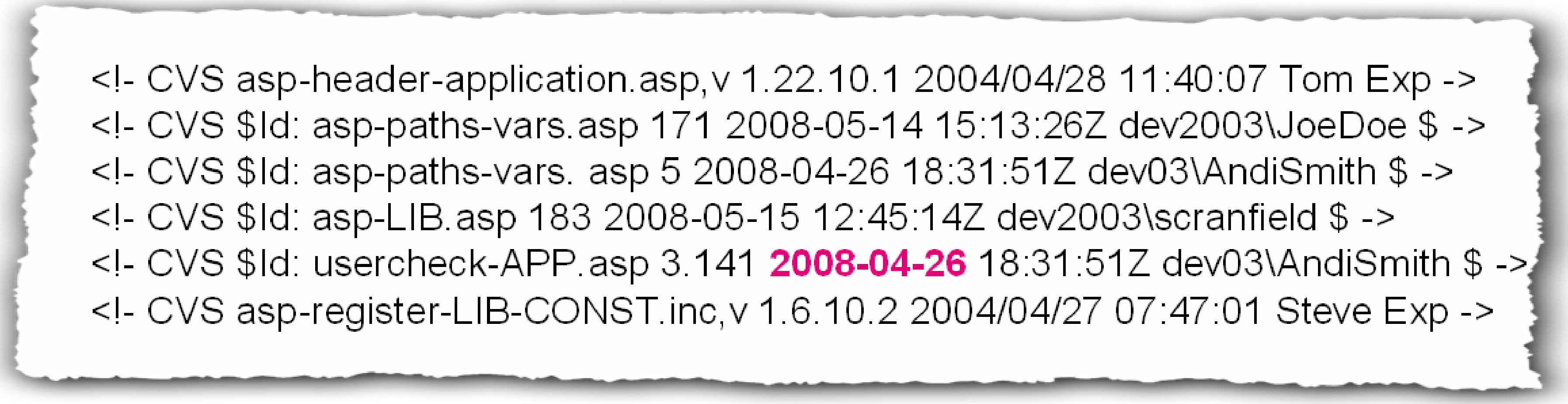
```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS check in Andi did in the evening. We had a crash and now we get only scrambled data from the CVS. Can you mail me version 3.141*

Comments

Exploit

What would Kevin Mitnick do?



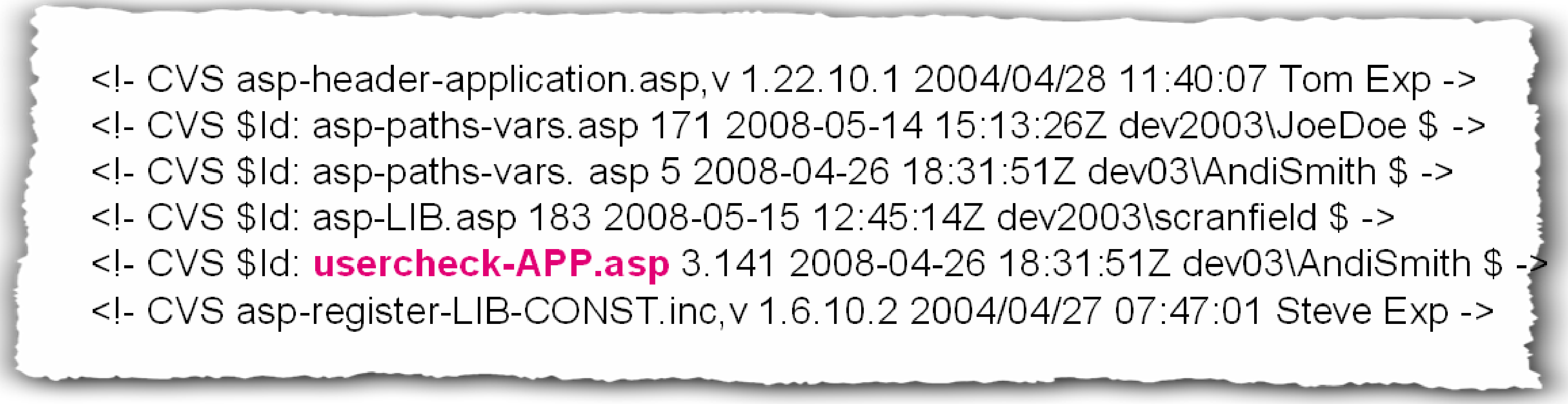
```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS check in Andi did in the evening. We had a crash and now we get only scrambled data from the CVS. Can you mail me version 3.141 from 26th of April*

Comments

Exploit

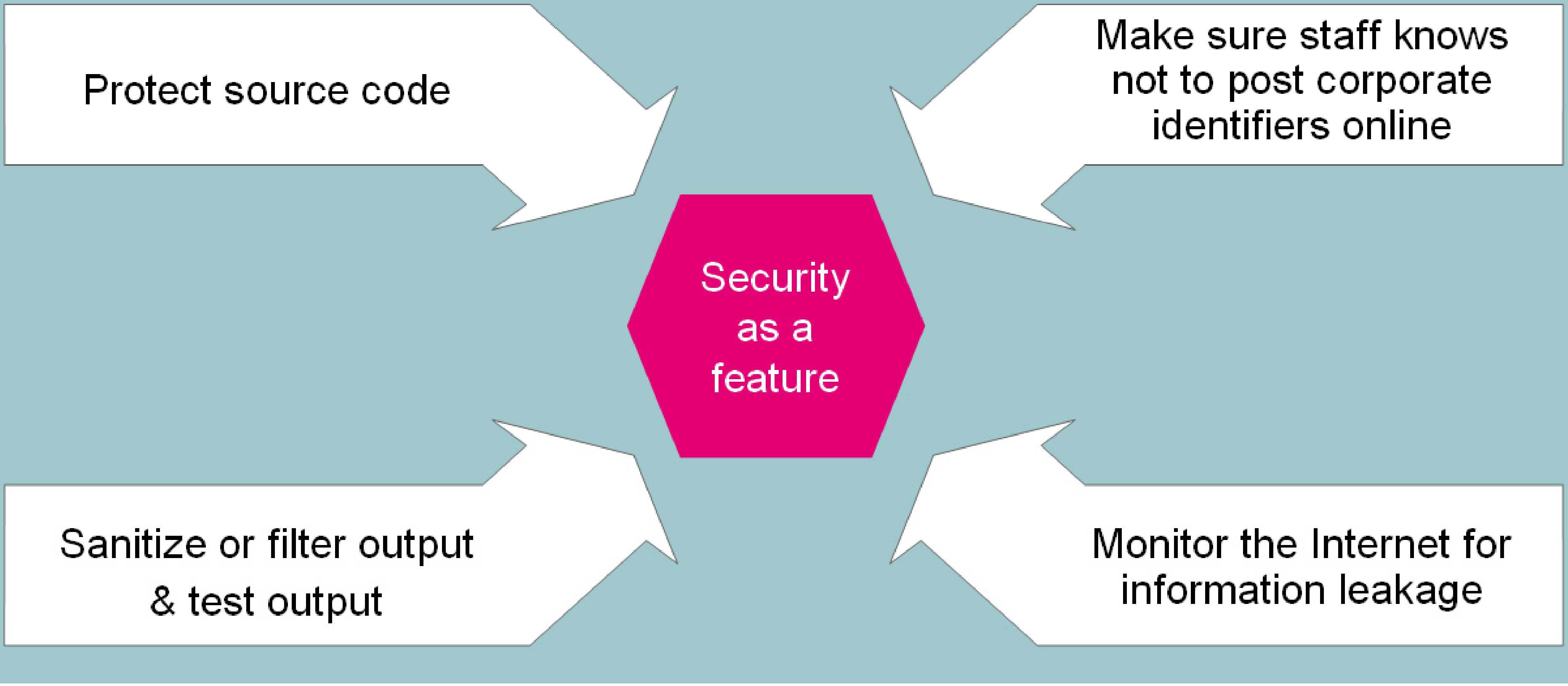
What would Kevin Mitnick do?



```
<!- CVS asp-header-application.asp,v 1.22.10.1 2004/04/28 11:40:07 Tom Exp ->
<!- CVS $Id: asp-paths-vars.asp 171 2008-05-14 15:13:26Z dev2003\JoeDoe $ ->
<!- CVS $Id: asp-paths-vars. asp 5 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS $Id: asp-LIB.asp 183 2008-05-15 12:45:14Z dev2003\scranfield $ ->
<!- CVS $Id: usercheck-APP.asp 3.141 2008-04-26 18:31:51Z dev03\AndiSmith $ ->
<!- CVS asp-register-LIB-CONST.inc,v 1.6.10.2 2004/04/27 07:47:01 Steve Exp ->
```

- *Hi, this is Kevin from web server operations. We have a big problem with the latest CVS check in Andi did in the evening. We had a crash and now we get only scrambled data from the CVS. Can you mail me version 3.141 from 26th of April of usercheck-APP.asp?*

Comments
Prevention



Protect source code

Make sure staff knows not to post corporate identifiers online

Security as a feature

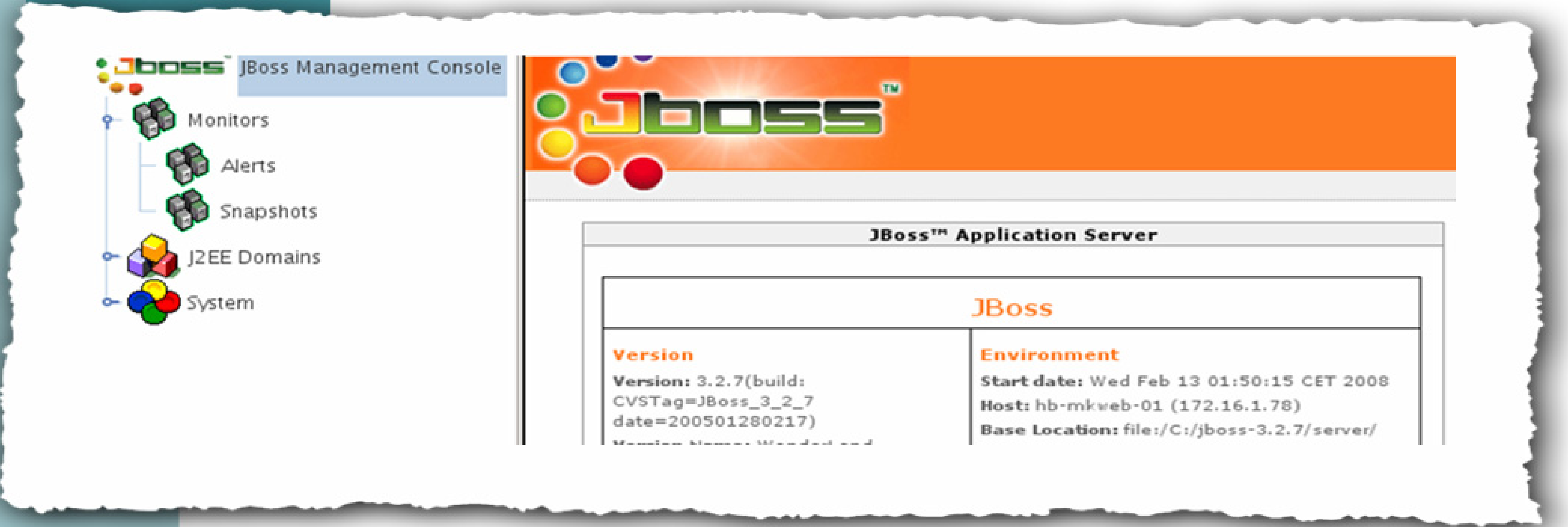
Sanitize or filter output & test output

Monitor the Internet for information leakage

Internal Information
Introduction

How to leak

- Misconfigured application server



JBoss™ Application Server

JBoss

Version

Version: 3.2.7(build: CVSTag=JBoss_3_2_7 date=200501280217)

Version Name: Wonderland

Environment

Start date: Wed Feb 13 01:50:15 CET 2008

Host: hb-mkweb-01 (172.16.1.78)

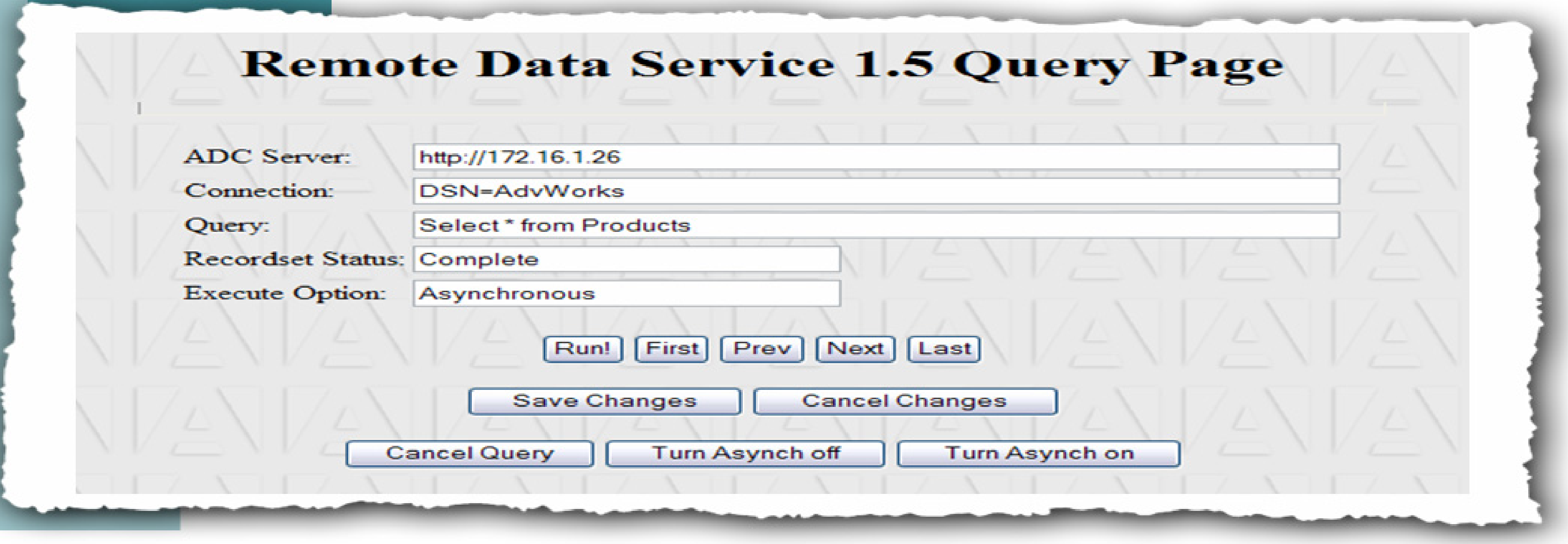
Base Location: file:/C:/jboss-3.2.7/server/

T · · Systems

Internal Information
Introduction

How to leak

- Misconfigured application server
- “Hidden” debug pages



Remote Data Service 1.5 Query Page

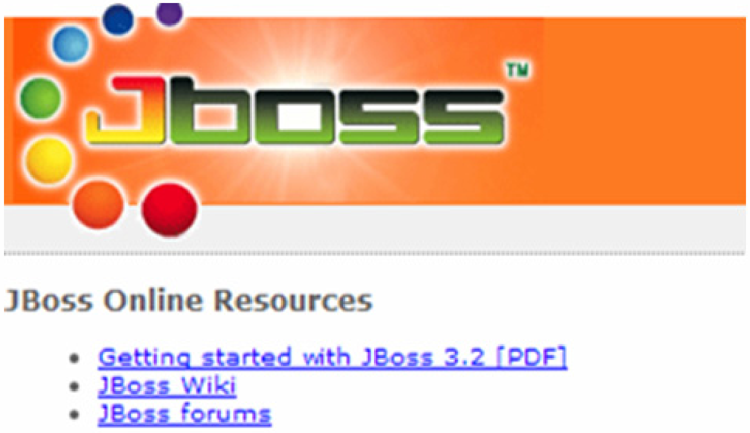
ADC Server: http://172.16.1.26
Connection: DSN=AdvWorks
Query: Select * from Products
Recordset Status: Complete
Execute Option: Asynchronous

Internal Information

Introduction

How to leak

- Misconfigured application server
- “Hidden” debug pages
- Help pages



JBoss Online Resources

- Getting started with JBoss 3.2 [PDF]
- JBoss Wiki
- JBoss forums

Internal Information

Introduction

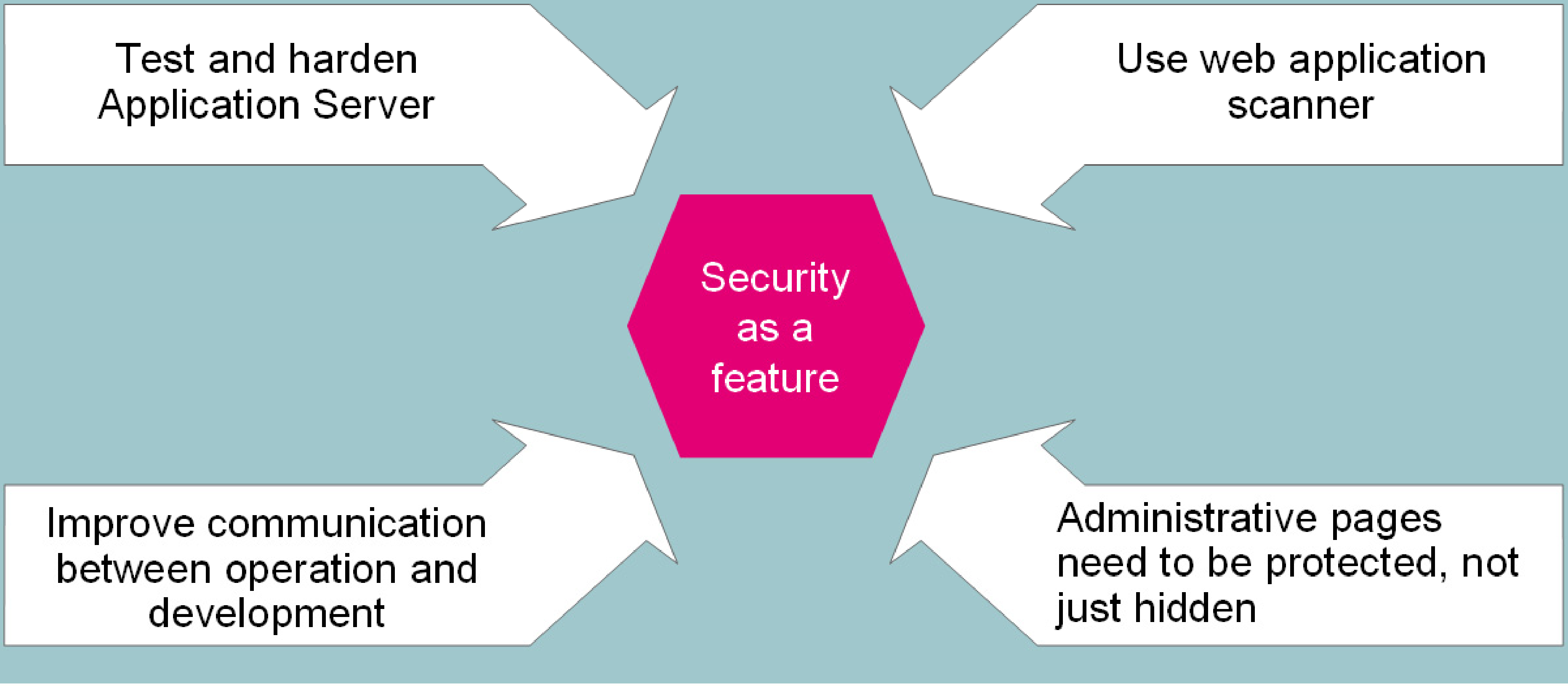
How to leak

- Misconfigured application server
- “Hidden” debug pages
- Help pages

How to use

- Preparation of attacks

Internal Information
Prevention



Test and harden Application Server

Use web application scanner

Security as a feature

Improve communication between operation and development

Administrative pages need to be protected, not just hidden

Error Massages

Introduction

How to leak

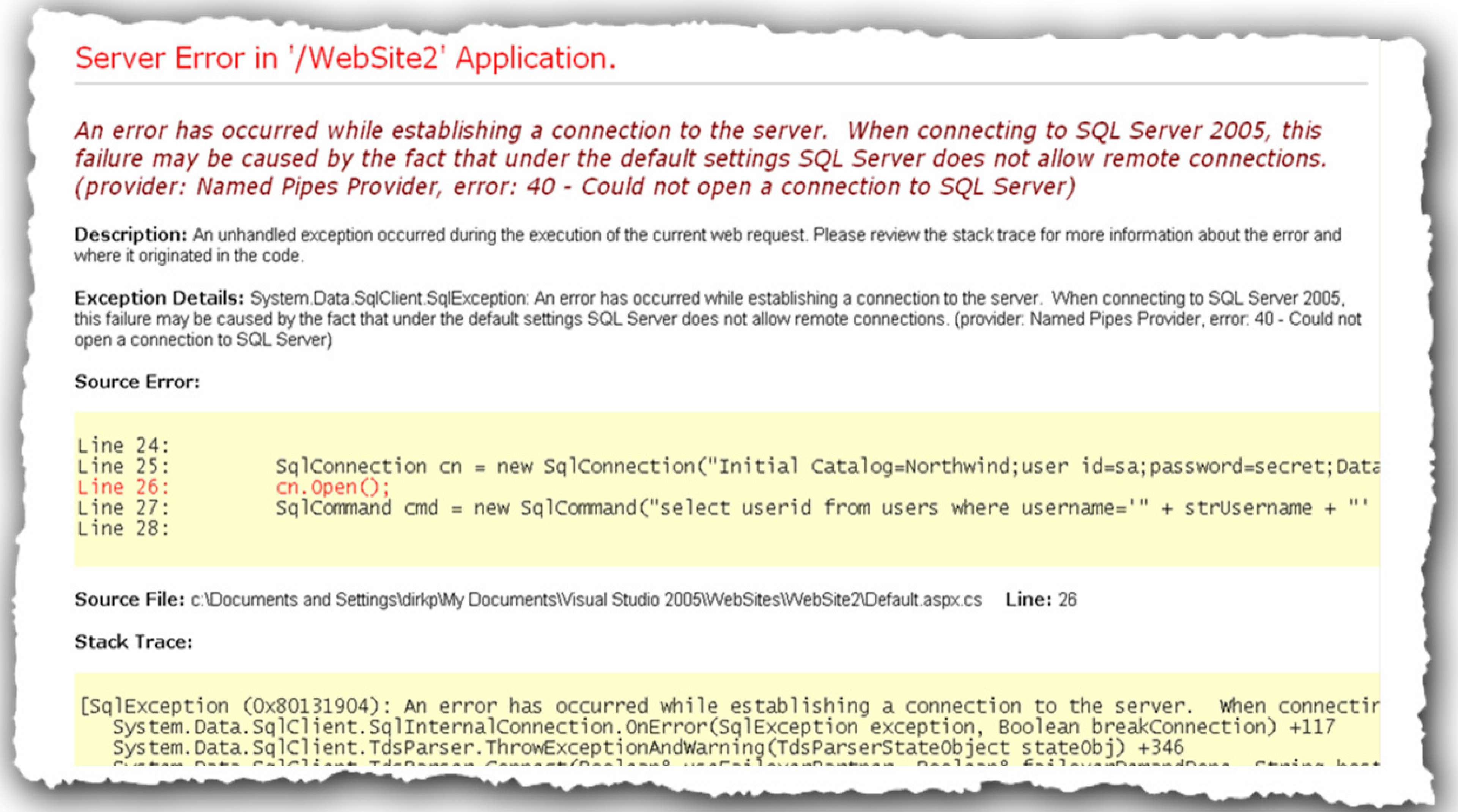
- Provoke error

How to use

- Deduce internal states
- Username brute force
- Parts of source code

Error Massages

Exploit



Server Error in '/WebSite2' Application.

An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Source Error:

```
Line 24:
Line 25:        SqlConnection cn = new SqlConnection("Initial Catalog=Northwind;user id=sa;password=secret;Data
Line 26:        cn.Open();
Line 27:        SqlCommand cmd = new SqlCommand("select userid from users where username='" + strUsername + "'
Line 28:
```

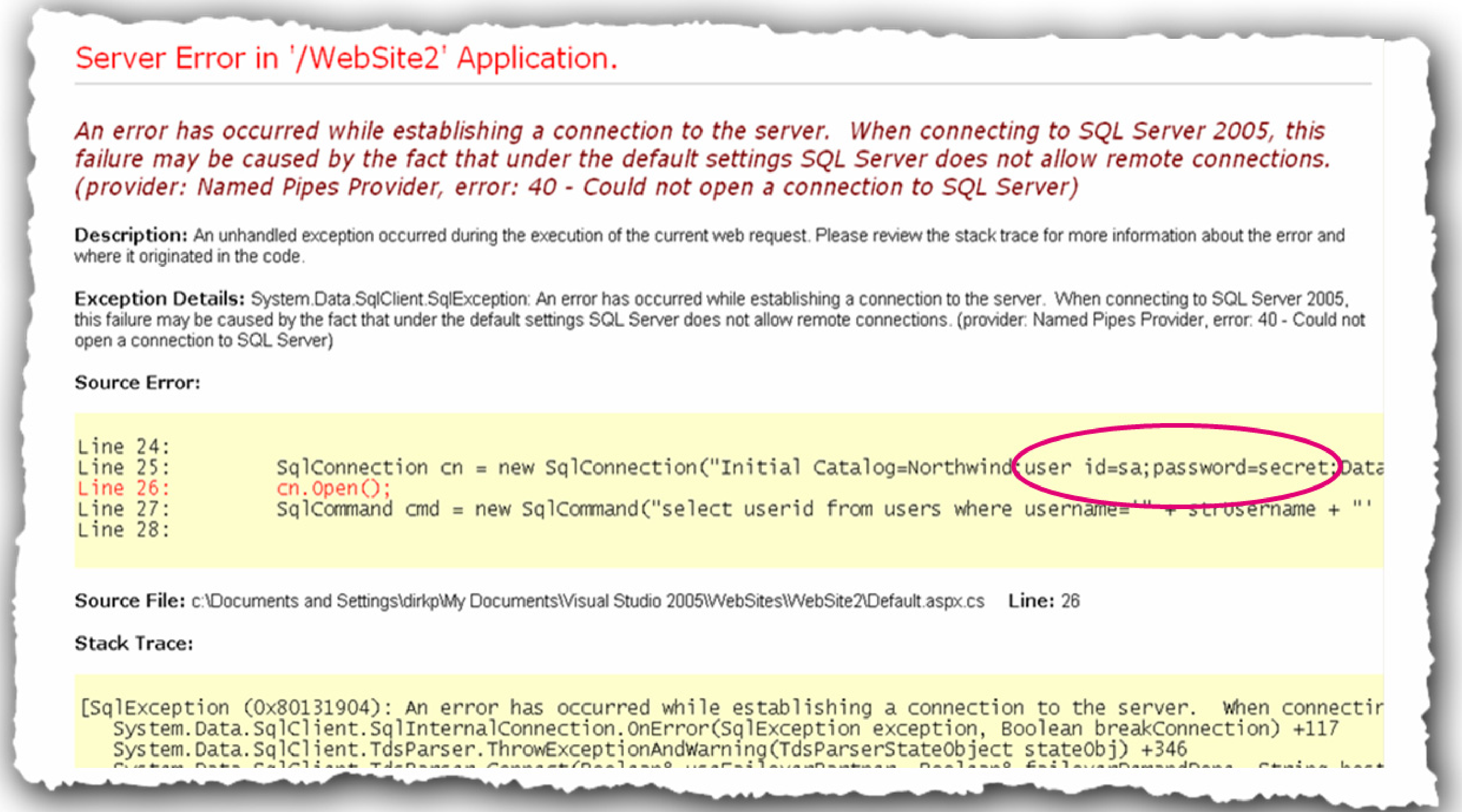
Source File: c:\Documents and Settings\dirkp\My Documents\Visual Studio 2005\WebSites\WebSite2\Default.aspx.cs **Line:** 26

Stack Trace:

```
[SqlException (0x80131904): An error has occurred while establishing a connection to the server.  When connectin
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +117
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +346
```

Error Massages

Exploit



Server Error in '/WebSite2' Application.

An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Source Error:

```
Line 24:
Line 25:        SqlConnection cn = new SqlConnection("Initial Catalog=Northwind;user id=sa;password=secret;Data
Line 26:        cn.Open();
Line 27:        SqlCommand cmd = new SqlCommand("select userid from users where username='" + strUsername + "'
Line 28:
```

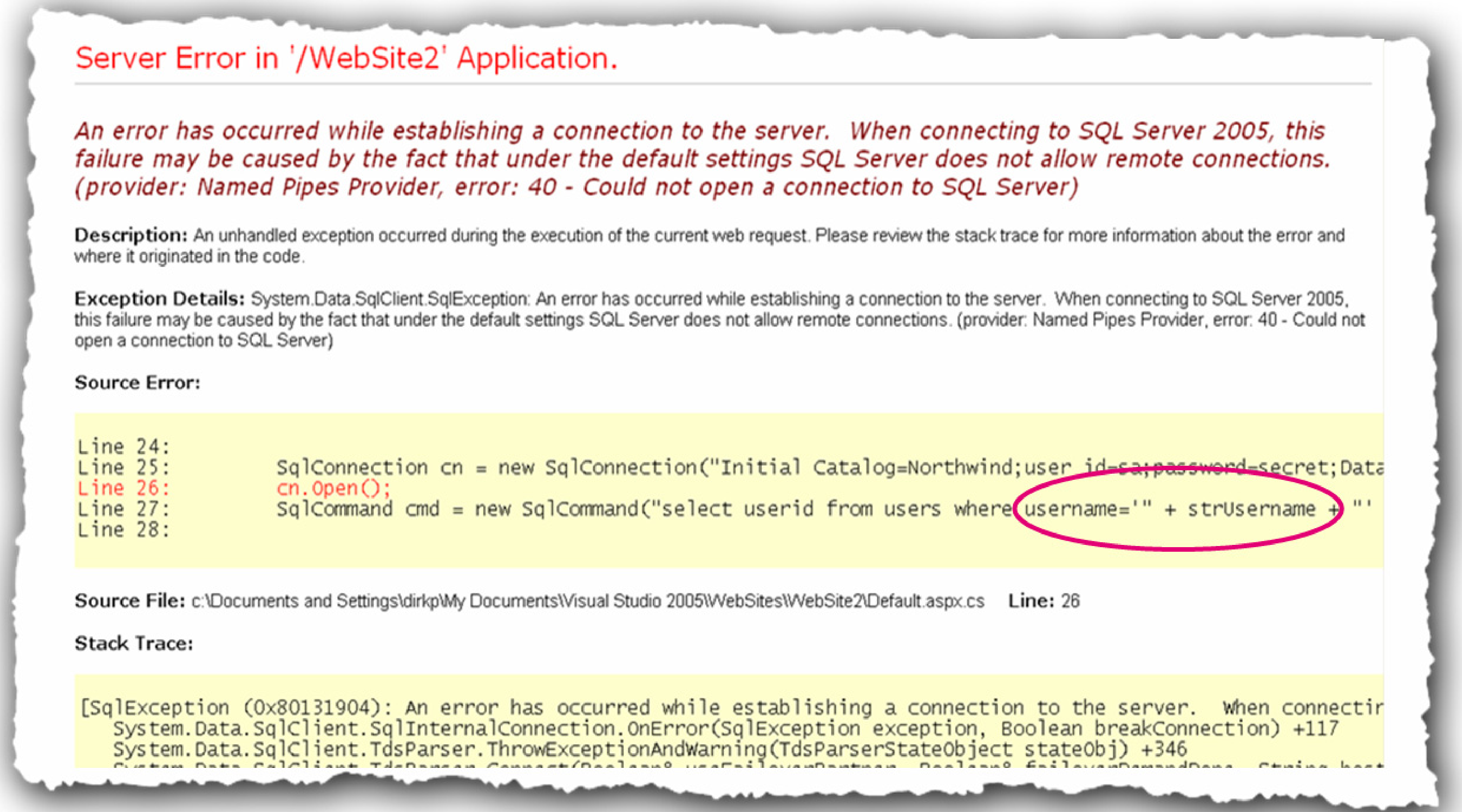
Source File: c:\Documents and Settings\dirkp\My Documents\Visual Studio 2005\WebSites\WebSite2\Default.aspx.cs **Line:** 26

Stack Trace:

```
[SqlException (0x80131904): An error has occurred while establishing a connection to the server.  When connectin
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +117
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +346
   System.Data.SqlClient.TdsParser.Connect(Boolean& useFailoverPartner, Boolean& failoverDemandDone, String host
```

Error Massages

Exploit



Server Error in '/WebSite2' Application.

An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

Source Error:

```
Line 24:
Line 25:        SqlConnection cn = new SqlConnection("Initial Catalog=Northwind;user id=sa;password=secret;Data
Line 26:        cn.Open();
Line 27:        SqlCommand cmd = new SqlCommand("select userid from users where username='" + strUsername + "'
Line 28:
```

Source File: c:\Documents and Settings\dirkp\My Documents\Visual Studio 2005\WebSites\WebSite2\Default.aspx.cs **Line:** 26

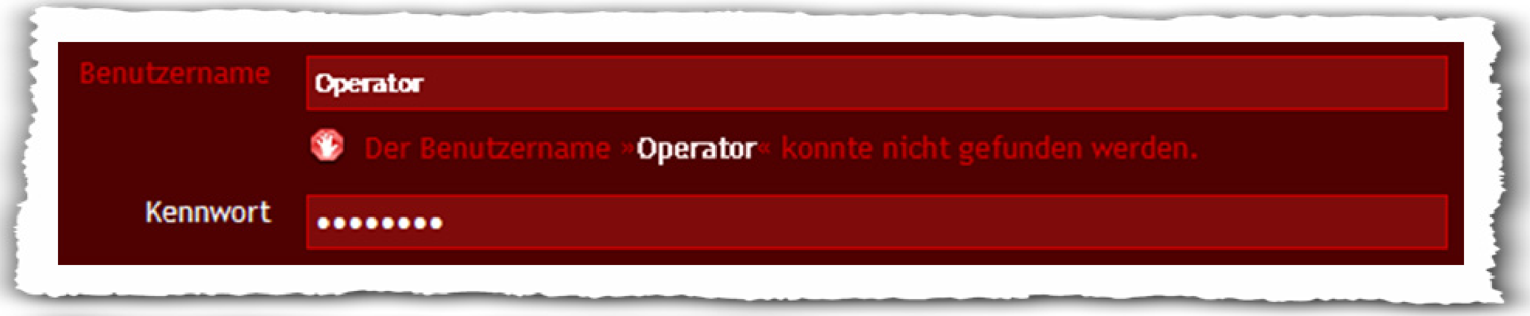
Stack Trace:

```
[SqlException (0x80131904): An error has occurred while establishing a connection to the server.  When connectir
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +117
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +346
   System.Data.SqlClient.TdsParser.Connect(Boolean& useFailoverPartner, Boolean& failoverDemandDone, String host
```

Error Massages

Exploit

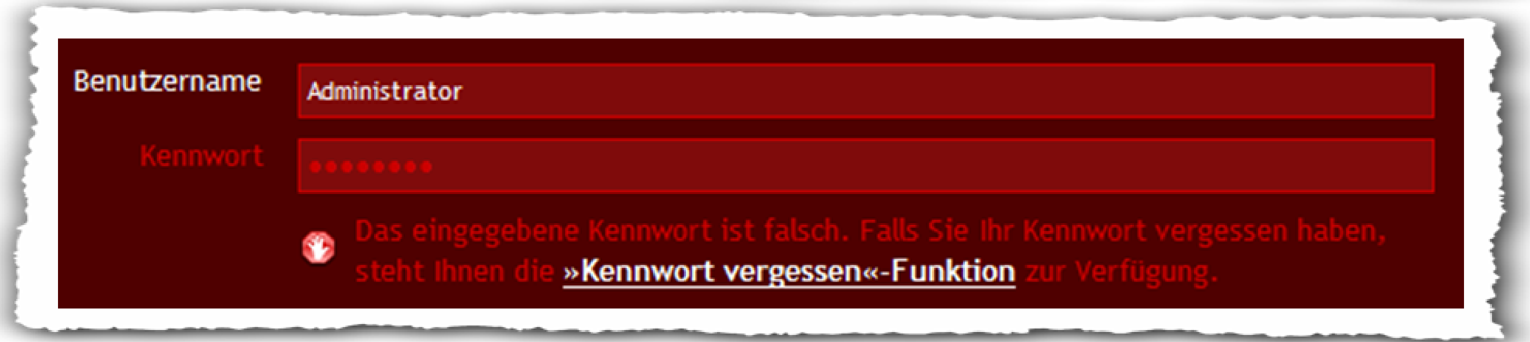
Username brute force



Benutzername Operator

Der Benutzername »Operator« konnte nicht gefunden werden.

Kennwort ••••••••



Benutzername Administrator

Kennwort ••••••••

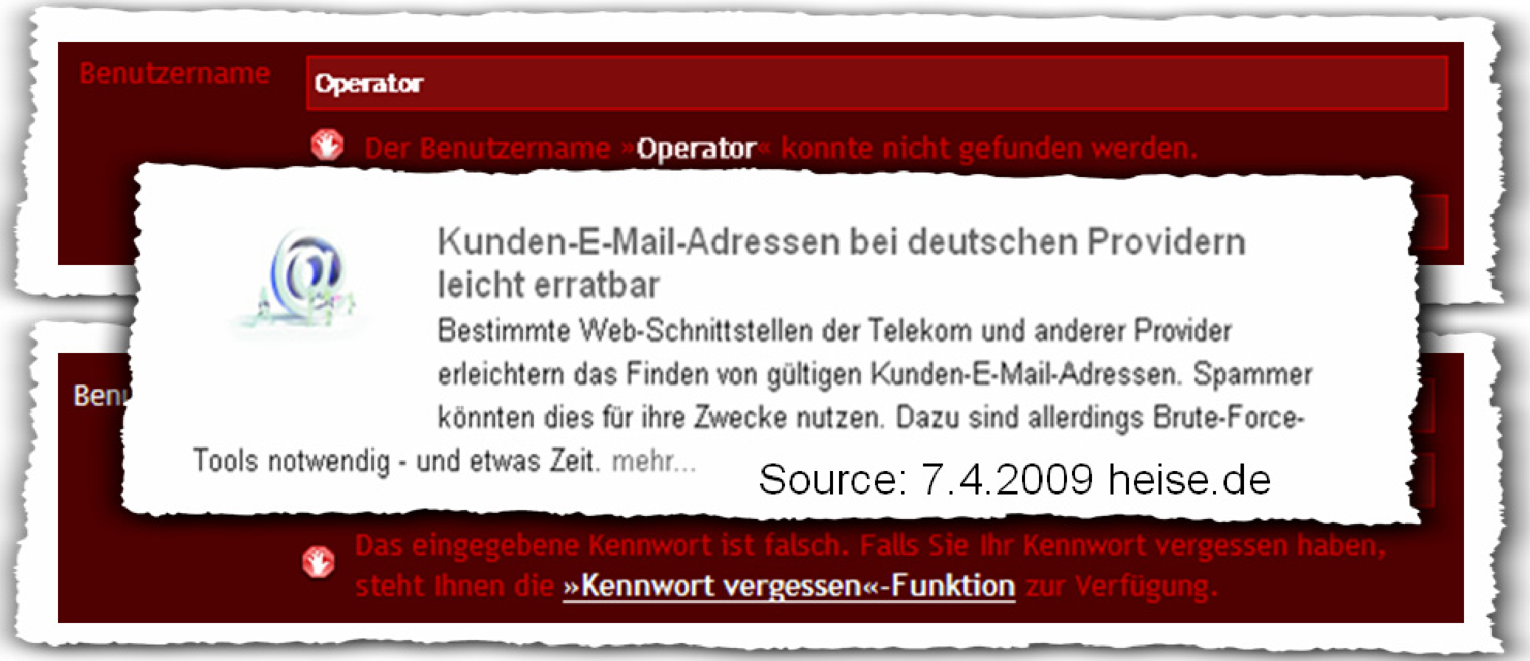
Das eingegebene Kennwort ist falsch. Falls Sie Ihr Kennwort vergessen haben, steht Ihnen die »Kennwort vergessen«-Funktion zur Verfügung.

- Identify user
- Trace target people

Error Massages

Exploit

Username brute force



Operator

Der Benutzername »Operator« konnte nicht gefunden werden.

Kunden-E-Mail-Adressen bei deutschen Providern leicht erratbar

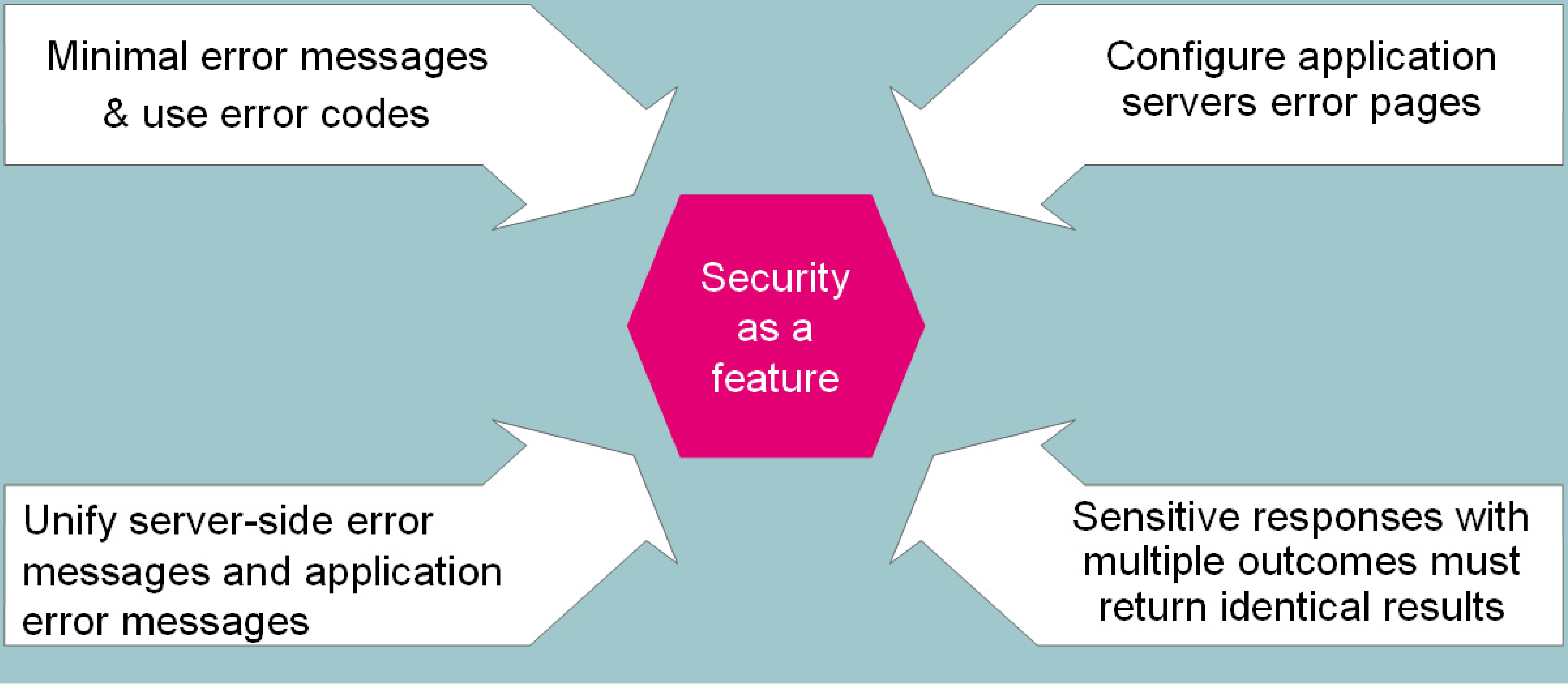
Bestimmte Web-Schnittstellen der Telekom und anderer Provider erleichtern das Finden von gültigen Kunden-E-Mail-Adressen. Spammer könnten dies für ihre Zwecke nutzen. Dazu sind allerdings Brute-Force-Tools notwendig - und etwas Zeit. mehr...

Source: 7.4.2009 heise.de

Das eingegebene Kennwort ist falsch. Falls Sie Ihr Kennwort vergessen haben, steht Ihnen die »Kennwort vergessen«-Funktion zur Verfügung.

- Identify user
- Trace target people

Error Massages
Prevention



Minimal error messages & use error codes

Configure application servers error pages

Security as a feature

Unify server-side error messages and application error messages

Sensitive responses with multiple outcomes must return identical results

Names
Introduction

How to leak

- Names:
  - Filenames
  - URLs
  - Variables and Parameters
- Problem: names must be delivered

How to use

- Filename guessing
- Supporting Trojans, phishing
- Manipulating application state
- Captchas

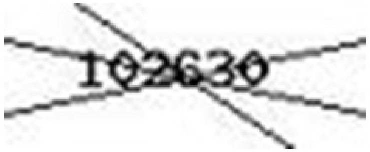
Names

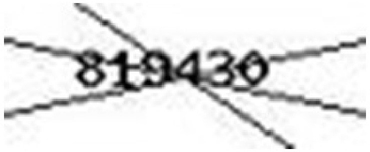
Example

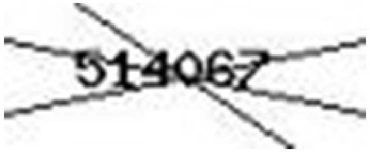
Captchas

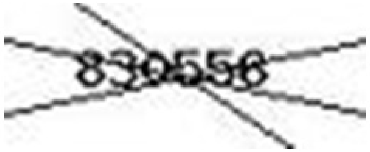
*A **Captcha** (IPA: /kæptʃə/) is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.*

wikipedia.org







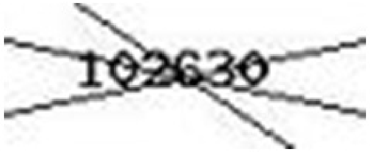


Names
Example

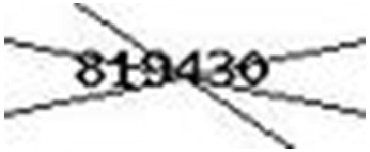
Captchas

*A **Captcha** (IPA: /kæptʃə/) is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.*

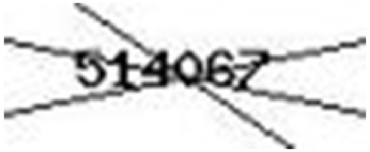
wikipedia.org



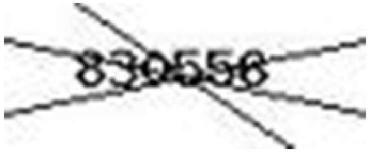
qpwzep.jpg



iqorep.jpg



tqrpzu.jpg



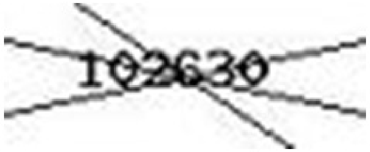
iepttz.jpg

Names
Example

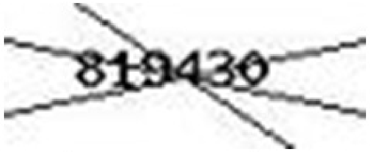
Captchas

A ***Captcha*** *(IPA: /kæptʃə/) is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.*

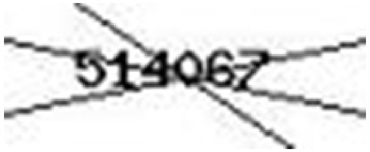
wikipedia.org



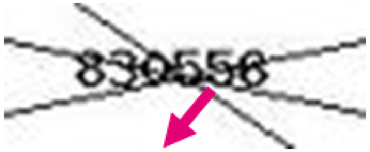
qpwzep.jpg



iqorep.jpg



tqrpzu.jpg



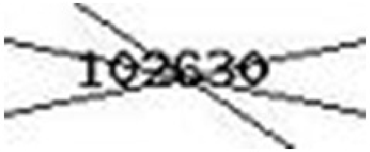
iepttz.jpg

Names
Example

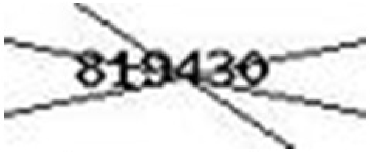
Captchas

*A **Captcha** (IPA: /kæptʃə/) is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.*

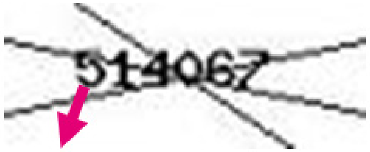
wikipedia.org



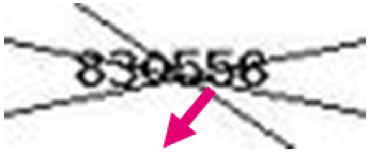
qpwzep.jpg



iqorep.jpg



tqrpzu.jpg



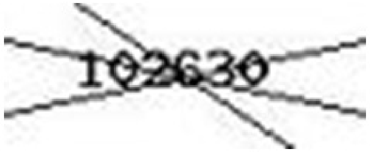
iepttz.jpg

Names
Example

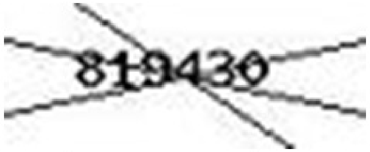
Captchas

*A **Captcha** (IPA: /kæptʃə/) is a type of challenge-response test used in computing to ensure that the response is not generated by a computer.*

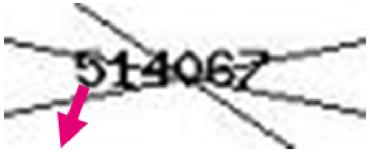
wikipedia.org



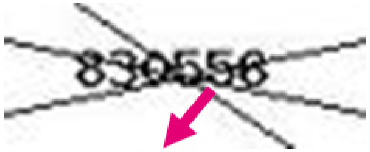
qpwzep.jpg



iqorep.jpg

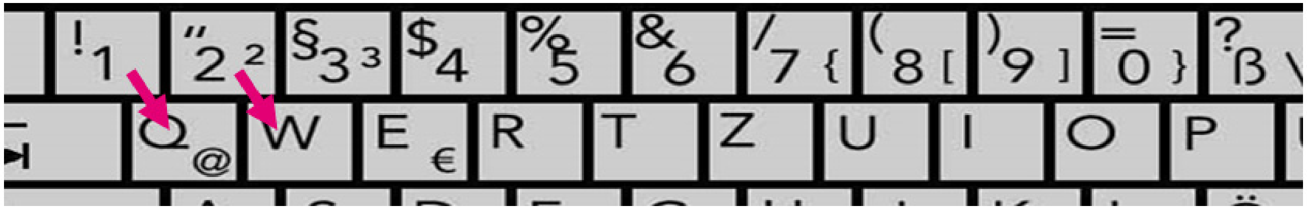


tqrpzu.jpg



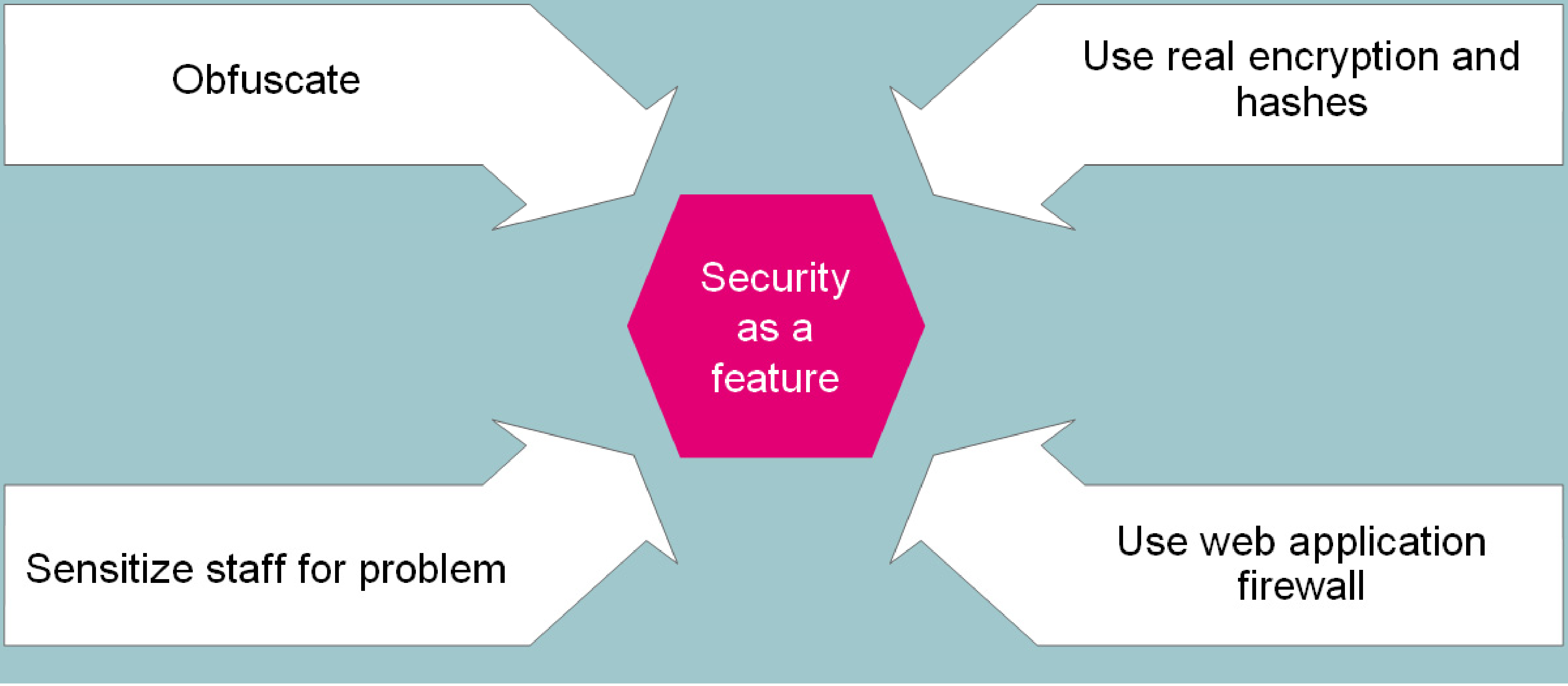
iepttz.jpg

- Filenames are encrypted content of Captcha:



Names

Prevention


Obfuscate

Use real encryption and hashes

Security as a feature

Sensitize staff for problem

Use web application firewall

Short test plan

Short test plan

1. Mirror website
2. Search in pages for:
    - HTML & application comments
    - IP-addresses and domain names
    - email addresses
    - SQL / database keywords
3. HTTP banner grabbing
4. Provoke error messages
5. Generate site map, than guess name
6. Search for downloadable scripts
7. Check for sample scripts left from default installations

Testing
Server Side – Test Tools

ModSecurity

- Web Application Firewall
- Works between the Apache server process and the client
- Operation is controlled by robust rule processing including regular expression pattern matching
- Analyzes request and response data, blocks transmission, logs transactions for analysis

Testing
Server Side – Test Tools

ModSecurity

- Web Application Firewall
- Works between the Apache server process and the client
- Operation is controlled by robust rule processing including regular expression pattern matching
- Analyzes request and response data, blocks transmission, logs transactions for analysis

snort

- free and open source network intrusion detection system
- packet logging
- real-time traffic analysis on IP networks
- Simple rule syntax

```
▪alert tcp $WEBSERVER 80 -> any any (content „<!--"; msg: „Comment";)
▪alert tcp $WEBSERVER 80 -> any any (content „Andi Smith"; msg: „Person";)
```

Testing
Client Side – Test Tools

Web application vulnerability assessment proxy

- Paros proxy, BurpSuite,WebScarab
- Typical features:
  - editing/viewing HTTP/HTTPS messages on-the-fly
  - change items such as cookies and form fields
  - traffic recorder, web spider

Testing
Client Side – Test Tools

Web application vulnerability assessment proxy

- Paros proxy, BurpSuite,WebScarab
- Typical features:
  - editing/viewing HTTP/HTTPS messages on-the-fly
  - change items such as cookies and form fields
  - traffic recorder, web spider

PAROS

Web scanner nikto

- Nikto is a tool for web scanner, originally written by Rain Forest Puppy
- Find default web files
- CGI security
- Can evade Intrusion detection systems
- Not a silent tool, may crash the server
- Command line tool

Take-home message

Attackers point of view

- Every little piece of information is valuable
- Combination of information provides insight
- One can find information everywhere

Service providers point of view

- Every little piece of information is valuable – treat it accordingly !
- Combination of information provides insight – prevent it !
- One can find information everywhere – hide it !
- Don’t support the attacker – test for information leakage!

Take-home message

Attackers point of view

- Every little piece of information is valuable
- Combination of information provides insight
- One can find information everywhere

Information Leakage Prevention will
•**not** protect you but
•will buy you time

cordingly !

- ombination of information provides insight – prevent it !
- One can find information everywhere – hide it !
- Don’t support the attacker – test for information leakage!

Thank you for your attention! Questions?