

A photograph of a modern building facade with curved glass and metal structures, partially visible on the left side of the slide.

## Access Control Issues



## ▶ OWASP Top Ten

- 2004: Access Controls were the #2 issue
- 2007 (current): Access controls hold both the #4 and #10 spot

## ▶ WASC Security Statistics

- Two of the top four discovered vulnerabilities are related to access controls.

# An Overlooked Problem



September 6, 2000 11:40 AM PDT

## IKEA exposes customer information on catalog site

By Troy Wolverton  
Staff Writer, CNET News

Post a comment

February 11th, 2009

## Sage shows why bigcos can't be trusted with SaaS

Posted by Phil Wainewright @ 3:42 am

**Categories:** [Development](#), [ERP](#), [Europe](#), [Security](#), [Uncategorized](#)

**Tags:** [Security](#), [Accounting](#), [Software-as-a-service](#), [Software Company](#), [Sage Live.....](#)

6 T ADD YC

The first of  
David-and-

November 7, 2005 6:15 PM PST

## Pizza chain caught without fully baked security

By Joris Evers  
Staff Writer, CNET News

7 comments

### Related Stories

[Separating myth from reality in ID theft](#)  
October 24, 2005

[ChoicePoint: We're sorry for data leak](#)  
March 15, 2005

Papa John's has beefed up security for its Web-based e-mail system after the pizza chain learned that internal e-mail and customer data had been exposed.

The leak at the Louisville, Ky.-based pizza chain made internal corporate e-mail and thousands of customer comments available to anyone with a Web browser. The customer comments were submitted between Sept. 29 and Nov. 7 and included names, addresses, phone numbers and e-mail addresses of customers.

The furnishings retailer IKEA closed its online catalog order site last week after a privacy breach made the personal information of tens of thousands of its customers available online.

The information had been exposed since at least Monday morning, when an anonymous customer uncovered an unprotected database file containing customer records. The file, which was accessible until yesterday evening, contained the names, addresses, phone numbers and email addresses of customers who had ordered IKEA catalogs.

# Sage Software as a Service



Section Everyone Group - Windows Internet Explorer

[https://www.sagelive.co.uk/portal/server.pt?open=space&name=Tree&psname=CommunityEditor&psid=21&cached=true&in\\_hi\\_userid=712&subspace=EveryoneTreeSecurity11&control=StartTree&Root](https://www.sagelive.co.uk/portal/server.pt?open=space&name=Tree&psname=CommunityEditor&psid=21&cached=true&in_hi_userid=712&subspace=EveryoneTreeSecurity11&control=StartTree&Root)

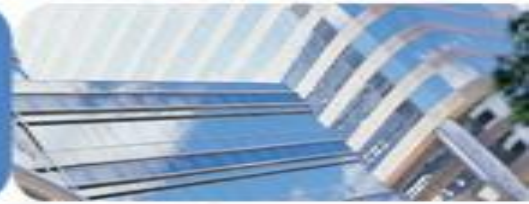
## Section Everyone Group

Search:  any object ▾ ▶

### Groups and Users in the Everyone Group.

- [-] Admin Objects Directory
  - [-] Active Directory
    - [-] Groups to Delete
  - [+] Administrative Resources
  - [+] Default Experience Definition
  - [-] Experience Definition Objects
  - [+] Portal Resources
  - [-] Publisher
    - [+] Published Content Portlets
  - [+] Roles and Users
  - [-] Sage
    - [-] Beta Test Users
    - [-] Common
      - [+] Images
      - [+] Templates
    - [-] Global

# Why Do They Show Up So Frequently?

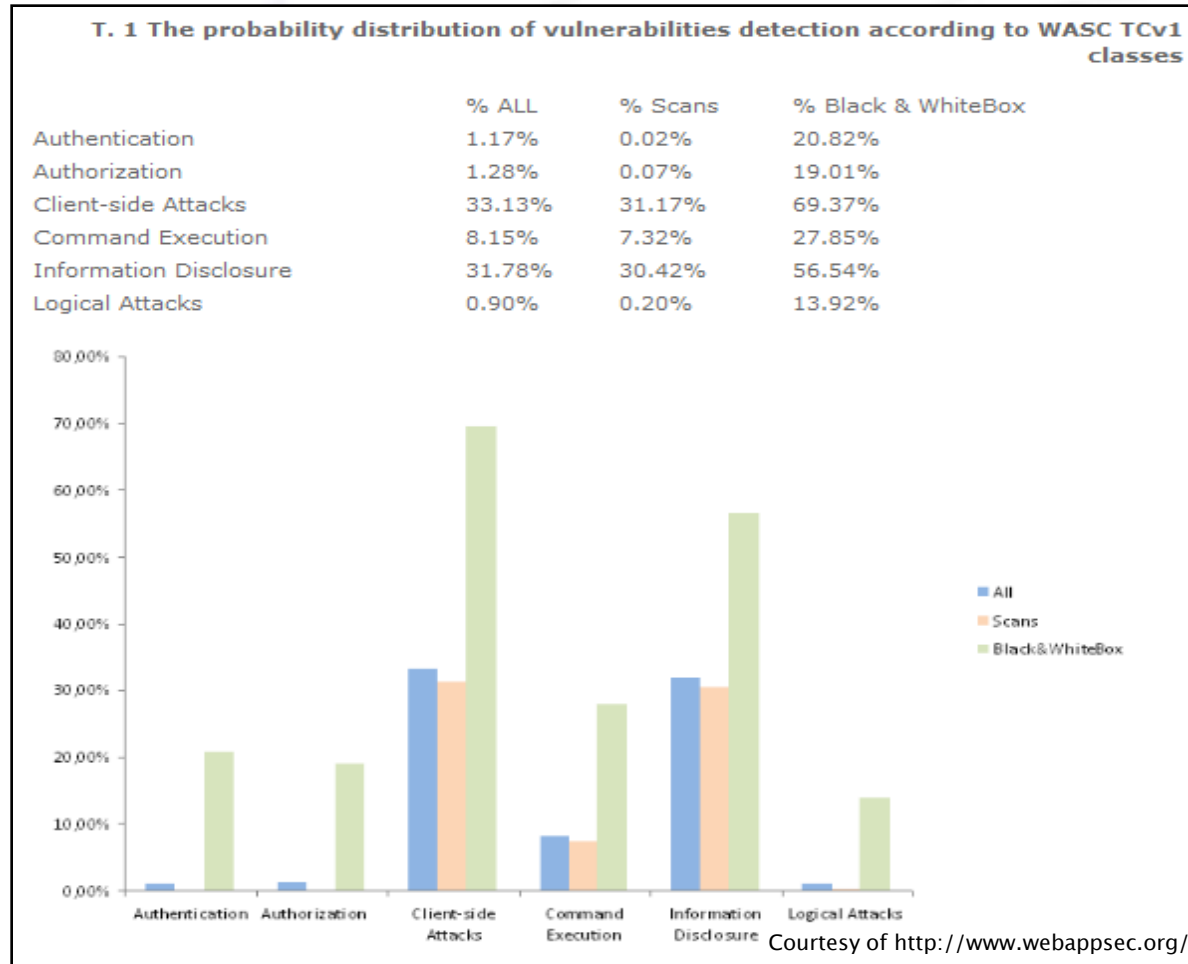


- ▶ **Wide range of possible vulnerabilities and practices**
  - Horizontal permission boundaries
  - Vertical permission boundaries
  - Static file access
  - Cross domain request permissions (crossdomain.xml)
  - Application resource rights
  - Use case access controls – date, IP address, location, etc.

# Why Do They Show Up So Frequently?



## ▶ Application scanners can't detect them



# Why Do They Show Up So Frequently?



## ▶ Manual Detection

- Parameter manipulation
- Flow-based manipulation
  - ▶ GET vs. POST
  - ▶ Step retracing
  - ▶ State machines
- Static file access

## ▶ Solutions cannot be ad hoc

- Global framework
- Documented, repeatable processes

# In-Depth: Parameter Manipulation



Browser address bar: `http://www.bustedbank.com/onlinebanking/ViewStatement.aspx?accountnum=12342`

Page title: `ViewStatement.aspx?accountnum=12342`

**Busted Bank**  
Not a Member FDIC

PERSONAL | SMALL BUSINESS | CORPORATE | ABOUT BUSTED BANK | CONTACTS

Site Search

To Account Name/#	From Account Name/#	Amount	Date
12343	12342	11/13/2006 6:07:11 PM	1.0000
12342	12343	11/13/2006 6:07:16 PM	2.0000
12343	12342	2/2/2007 9:56:39 AM	100000.0000
12342	12343	2/2/2007 10:02:47 AM	1000000000.0000
12343	12342	2/2/2007 10:03:27 AM	1000000000.0000
12343	12342	11/13/2006 6:06:28 PM	1540.0000
12343	12342	11/13/2006 6:06:28 PM	4130.0000
12343	12342	11/13/2006 6:06:28 PM	3261.0000
12342	12343	11/13/2006 6:06:28 PM	3871.0000
12343	12342	11/13/2006 6:06:28 PM	1109.0000
12342	12343	11/13/2006 6:06:28 PM	4635.0000
12342	12343	11/13/2006 6:06:28 PM	1511.0000
12342	12343	11/13/2006 6:06:28 PM	1259.0000

Download Statement

- > Accounts
- > Online Bill Pay
- > Logout
- > Open a New Account
- > Customer Service

# In-Depth: Parameter Manipulation



ViewStatement.aspx?accountnum=12354

**Busted Bank**  
Not a Member FDIC

PERSONAL | SMALL BUSINESS | CORPORATE | ABOUT BUSTED BANK | CONTACTS

Site Search

To Account Name/#	From Account Name/#	Amount	Date
12355	12354	11/13/2006 6:06:29 PM	970.0000
12354	12355	11/13/2006 6:06:29 PM	4685.0000
12355	12354	11/13/2006 6:06:29 PM	1859.0000
12355	12354	11/13/2006 6:06:29 PM	3770.0000
12354	12355	11/13/2006 6:06:29 PM	1060.0000
12354	12355	11/13/2006 6:06:29 PM	2985.0000
12354	12355	11/13/2006 6:06:29 PM	4778.0000
12354	12355	11/13/2006 6:06:29 PM	4561.0000

Download Statement

- Accounts
- Online Bill Pay
- Logout
- Open a New Account
- Customer Service

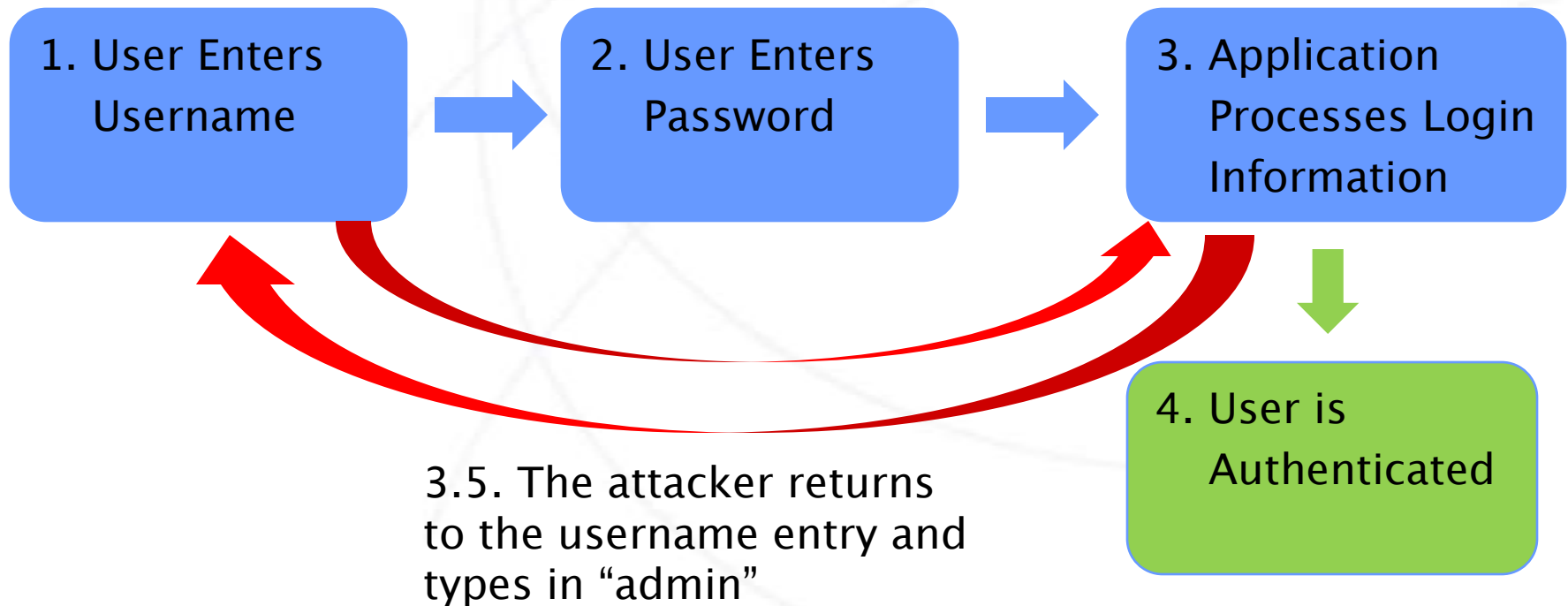


## ► GET vs. POST

```
protected void Page_Load(object sender, EventArgs e)
{
    if (!Page.IsPostBack)
    {
        check_access();
        ... application logic ...
    }
    else
    {
        check_access();
        ... logic to execute on PostBack ...
        ... logic to execute on PostBack ...
    }
}
```



## ► Step Retracing



# In-Depth: Static File Access



Busted Bank

Not a Member FDIC

- PERSONAL
- SMALL BUSINESS
- CORPORATE
- ABOUT BUSTED BANK
- CONTACTS



- > Accounts
- > Online Bill Pay
- > Logout
- > Open a New Account
- > Customer Service

Site Search

To Account Name/#	From Account Name/#	Amount	Date
12343	12342	11/13/2006 6:06:28 PM	1109.0000
12343	12342	11/13/2006 6:07:11 PM	1.0000
12342	12343	11/13/2006 6:07:16 PM	2.0000
12343	12342	2/2/2007 9:56:39 AM	100000.0000
12342	12343	2/2/2007 10:02:47 AM	1000000000.0000
12343	12342	2/2/2007 10:03:27 AM	1000000000.0000
12342	12343	11/13/2006 6:06:28 PM	4635.0000
12342	12343	11/13/2006 6:06:28 PM	1511.0000
12343	12342	11/13/2006 6:06:28 PM	1540.0000
12343	12342	11/13/2006 6:06:28 PM	4130.0000
12343	12342	11/13/2006 6:06:28 PM	3261.0000
12342	12343	11/13/2006 6:06:28 PM	1259.0000
12342	12343	11/13/2006 6:06:28 PM	3871.0000

```
<input id="file" name="file" type="text" value="/tmp/12343.txt" />  
<input id="ctl00_mainContent_Men_Download" type="button" value="Download Statement" />
```

/tmp/12343.txt

# In-Depth: Static File Access



**Busted**  
Not a

PERSONAL | SMALL

- > Accounts
- > Online Bill Pay
- > Logout
- > Open a New Account
- > Customer Service

Opening 12350.txt

You have chosen to open

**12350.txt**  
which is a: Notepad++ Document  
from: http://www.bustedbank.com

What should Firefox do with this file?

**Open with:** Notepad++ : a free (GNU) source code... ▼

**Save File**

Do this **automatically** for files like this from now on.

OK Cancel

<input id="ctl00\_btnSearch" name="ctl00\$btnSearch">

			Date
12343	12342	11/13/2006 6:06:28 PM	1109.0000
12343	12342	11/13/2006 6:06:28 PM	1.0000
12342	12343	11/13/2006 6:06:28 PM	2.0000
12342	12343	11/13/2006 6:06:28 PM	100000.0000
			1000000000.0000
			1000000000.0000
			4635.0000
			1511.0000
			1540.0000
			4130.0000
			3261.0000
			1259.0000
			3871.0000

<input id="file" name="file" /tmp/12343.txt

<input id="ctl00\_mainContent\_btn\_Download" name="ctl00\$mainContent\$btn\_Download">

Download Statement

## How Do We Fix It?

- ▶ **Global unified framework**
- ▶ **Accountability**
- ▶ **Appropriate security exercises**
- ▶ **Documentation!**

A photograph of a modern glass skyscraper with curved architectural elements, viewed from a low angle looking up.

# Discussion