

# Safeguarding Tax Information: Start By Covering Your Apps

Maribeth Anderson, Chief Information Officer

Federation of Tax Administrators 17<sup>th</sup> Annual Technology Conference  
August 14, 2001



## Agenda

- ☆ Understanding why network security is not enough
- ☆ Identifying the types of web application attacks
- ☆ Preventing application hacks
- ☆ Setting standards for web application developers



## Recent security news

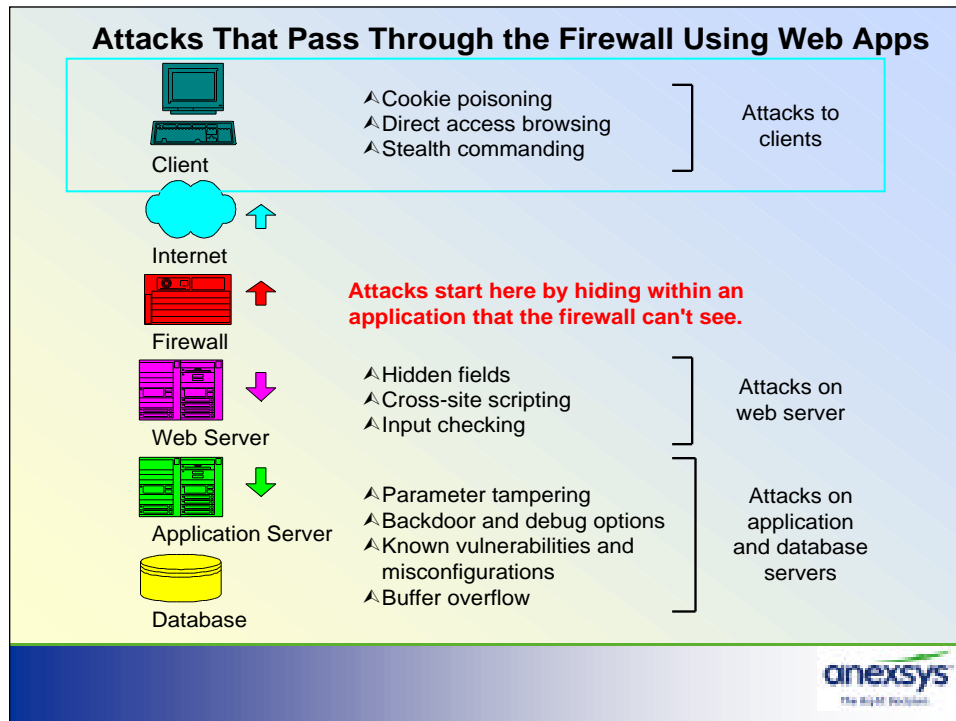
- ☆ Out of 3 million web sites tested world wide, 80 % have been given a thumbs down when it comes to security vulnerability *Source: Zdnet, May 03, 2001*
- ☆ According to the Computer Society Institute, one in every three intrusions occurs when a firewall is in place. *Source: Zdnet, May 03, 2001*
- ☆ **Bottom line:** If you can't point to the last detected hack attempt on your site then you're not secure. The hacks you don't see are the worst.



## Why is There a Trend Towards Hacking Into Applications?

- ☆ Applications are a neglected area and offer multiple entry points
- ☆ Network security is still a struggle
- ☆ It's difficult and firewall manufacturer's aren't addressing it
- ☆ Developers don't typically program with security in mind
- ☆ **Bottom line:** All that a hacker needs is a tiny hole in your code, a web browser mixed with malicious determination





## What is a cookie and why do I use them?

- ★ A flag or bookmark placed in browser to collect data
- ★ Cookie files are saved on the hard drive for next time's use
- ★ Data passes from page to page in your application
- ★ Improve user's experience

anexsys  
The Right Decision.

## Attacks to clients

### ☆ Cookie poisoning

- ◆ Definition: Refers to modifying data in a cookie and causing the return of unauthorized information and gaining access to accounts that aren't theirs.
- ◆ What happens: Cookie files previously stored are modified to pass different data at the next site visit.
- ◆ Defense tactics: Limit cookies to a client-side session ID and encrypt them. Associate the IP address with the cookie.



## Attacks to clients (continued)

### ☆ Direct access browsing

- ◆ Definition: Refers to accessing a web page directly without going through the required authentication
- ◆ What happens: The improper configuration gives access to URL's that might contain sensitive information or could be a source of lost revenue if the sight requires a subscription
- ◆ Defense tactics: Disallow bookmarks after authentication



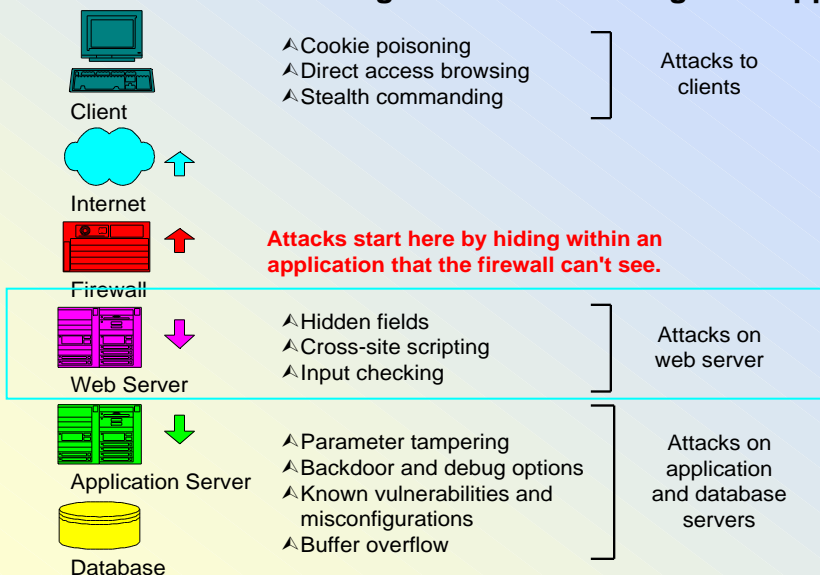
## Attacks to clients (continued)

### ★ Stealth commanding

- ◆ Definition: Planting Trojan horses in text fields that cause the web applications to perform commands you never intended
- ◆ What happens: A common result is site defacement or manipulation of the field parameters originally set
- ◆ Defense tactics: Program field validity checks. Prepare all database statements (eg. Insert, delete) in advance so that hackers can't append it.



## Attacks That Pass Through the Firewall Using Web Apps



## Attacks on web server

### ★ Hidden fields

- ◆ Definition: Refers to hidden HTML form fields containing system passwords or merchandise prices
- ◆ What happens: If fields aren't hidden then their source code can be viewed or modified. This can result in stolen passwords or changed pricing.
- ◆ Defense tactics: Do not use field tags for passwords or prices. Program the search to pull from the database and not the HTML form.



## Attacks on web server (continued)

### ★ Cross-site scripting

- ◆ Definition: Has many meanings. Generally speaking it is the process of adding code into pages sent by another source.
- ◆ What happens: A HTML form is presented and the user inputs code. When the server takes the data input it might execute the code if there aren't any input checks.
- ◆ Defense tactics: User code on the server side. Hide as much as possible from the client browser. Apply the patches specific to cross-site scripting hacks.



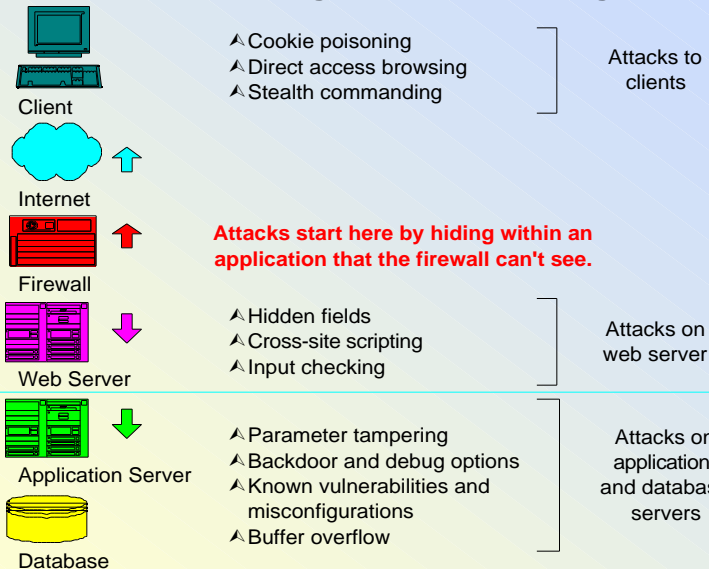
## Attacks on web server (continued)

### ☆ Input checking

- ◆ Definition: Ability to run system commands by manipulating input in HTML forms processed by a Command Gateway Interface (CGI) script.
- ◆ What happens: A client form is populated with a malicious command to execute something. The query, executed by CGI attacks data on the server or results in the retrieval of sensitive data.
- ◆ Defense tactics: CGI is old school programming and full of holes. Avoid it. Program validity checks.



### Attacks That Pass Through the Firewall Using Web Apps



## Attacks on application and database servers

### ☆ Parameter tampering

- ◆ Definition: Manipulating URL strings and their embedded SQL in an attempt to gain access to information the user should not see
- ◆ What happens: Hackers change the SQL query to broaden access to data.
- ◆ Defense tactics: Program field validity checks. Prepare all database statements in advance so that hackers cannot append it. If the data does not match a set criteria within your database table the SQL will not be completed.



## Attacks on application and database servers

### ☆ Backdoors and debug options

- ◆ Definition: Areas left open (debugging left on) to facilitate troubleshooting and administering applications during development.
- ◆ What happens: If left in the production application, then a user can login or obtain a URL that allows them direct access to the application configuration.
- ◆ Defense tactics: Execute internal programming with care



## Attacks on application and database servers (continued)

### ★ Buffer overflow

- ◆ Definition: Sending too much data in a request to the application
- ◆ What happens: It attacks internally or third party developed code
- ◆ Defense tactics: Install software updates that replace exploitable software; implement a proxy which does buffer length checking. Implement non-executable stack on servers. If you are using your own code check the source data lengths when copying data into a variable.



## Attacks on application and database servers (continued)

### ★ Known vulnerabilities and misconfigurations

- ◆ Definition: Vulnerabilities include bugs and security holes in operating systems and third party components (e.g. web and database servers)
- ◆ What happens: Insecure default settings and misconfigurations are published on hacker sites to attack.
- ◆ Defense tactics: Apply patches and keep them updated; regularly check for exploits occurring. Hide operating system versions from outside.



## Preventing application attacks

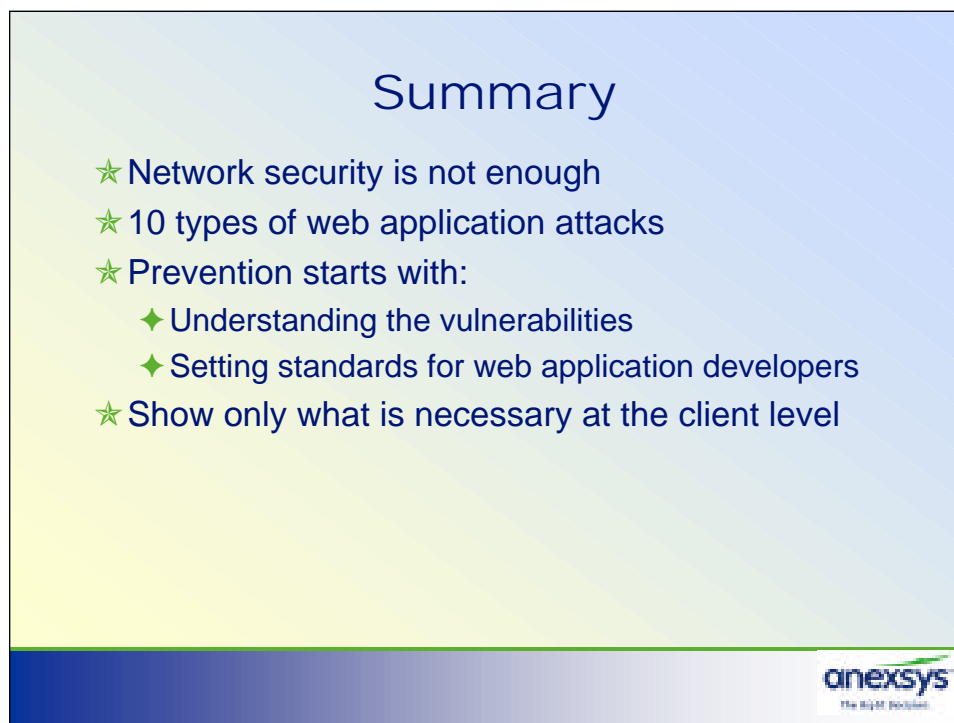
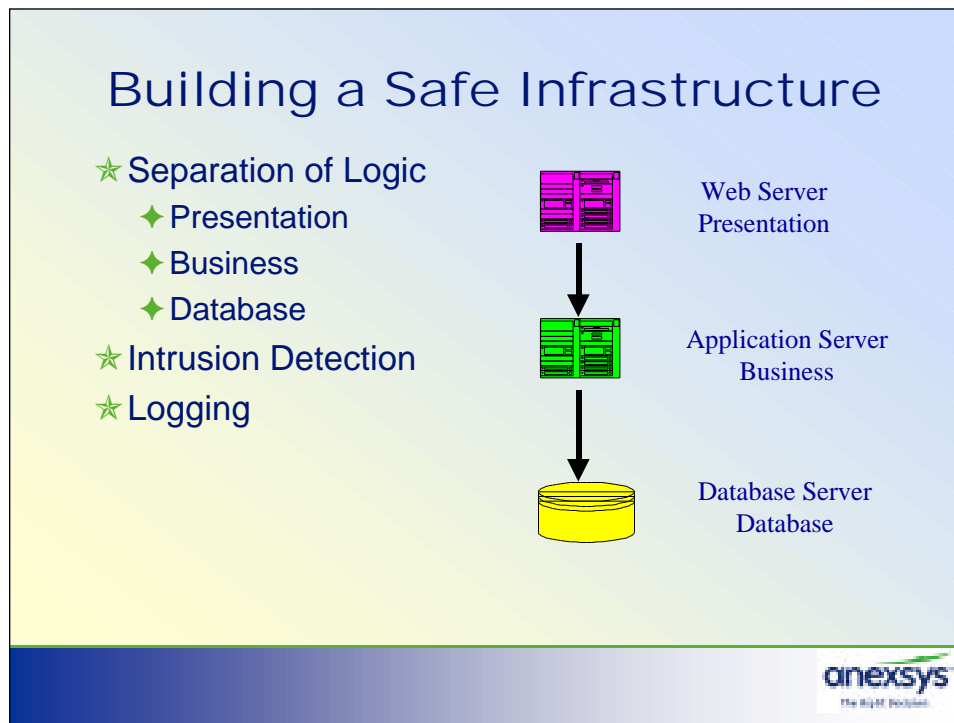
- ★ Education
  - ◆ Developers
  - ◆ Management
  - ◆ Standards Usage
- ★ Constant vigilance
- ★ Build security into all phases
- ★ Investigate tools and applications to help audit and secure web applications



## Setting Application Standards

- ★ When to use.....and how to use...
  - ◆ Encryption
  - ◆ Cookies
  - ◆ Access control
  - ◆ Email
  - ◆ HTML





To receive a PDF copy of this presentation please visit [www.anexsys.com](http://www.anexsys.com). Click on "About Anexsys" and then visit the "News and Events Section".

