

SPAM



A really good system
with a really dumb name!

SPAM

- Security, Privileges and Access Management
 - Lesson 1: Don't even *think* of suggesting funny names for your new system

Protecting web pages

- **Grant access to application**
- **Grant access level to application**
 - **Basic**
 - **Maintenance**
- **Build pages depending on level**

<cf_authorize>

- ColdFusion custom tag
- One line of code to protect page
- All the work done by the tag and the system of pages behind it

<cf_authorize>

- **Login/password management**
 - State-issued passwords expire every 90 days
 - Passwords reset to 'changeme' by Help Desk if necessary
 - 'changeme' passwords expire immediately
 - Last login date/time stored in pw table

<cf_authorize>

- **How it works**

- Page calls tag

- Tag checks to see if logged in

- If not logged in, calls login page

- User attempts login. If fails, rerouted to login failure page.

- If password expired, user changes password

- Privileges copied to daily table

- Calling page called, and we start over

<cf_authorize>

- If logged in, tag looks up access level in daily privileges table
 - If not found, reroutes user to access failure page
 - If found, returns level, user ID and SSN to calling page
 - Calling page is displayed

<cf_authorize> features

- **Level**
 - can return level
 - can require a match with level
 - can require a level greater than or equal to specified value
 - can require a level less than or equal to specified level

<cf_authorize> features

- **Background**

- Can pass a background image so the login screen matches your application

`<cf_authorize>` features

- **Access failure page**
 - Can send your visitor to an application-specific failure page or simply use the default
 - For example, may want to send unauthorized users back to the main menu of the application, rather than to a generic page.

<cf_authorize> features

- **Returns level, user ID and SSN**
 - **Developer's page is not required to use them, but many pages need one of these values to work properly**

Issues: Login IDs for visitors

- How do we give IDs to visitors?
 - Generate an ID?
 - Let them pick their own?
 - Let them pick one, but translate internally to our scheme?
- What privileges do we grant automatically?
 - Specify exam sign-up?
 - Generic web app application group?

Issues: What if they forget?

- How do we get them the information they need to log in?
- Do we grant them an ID if they don't have e-mail?
- If they give their SSN and last name, is that enough to let them in or give them the uid/pw?

The Process

- **User attempts to log in**
 - **Enters uid/pw correctly**
 - **pw is 'changeme'**
 - User must change password
 - **pw has expired**
 - User must change password
 - **otherwise**
 - User successfully logs in

The Process

- **User attempts to log in**
 - **User enters wrong uid/pw**
 - **User is redirected to the login failure page**

The Process

- **User clicks “Don’t know your password?”**
 - **User enters uid**
 - **Hint is displayed**
 - **User enters correct password**
 - **Successful: check for ‘changeme’ and expiration**

The Process

- **User clicks “Don’t know your password?”**
 - **User enters SSN and Last Name**
 - **SSN/Last Name match our files**
 - Application resets password to ‘changeme’
 - User has e-mail address
 - User ID e-mailed to user
 - User has no e-mail address
 - Application prepares letter
 - Help Desk prints and sends letter

The Process

- **User clicks “Don’t know your password?”**
 - **User enters SSN and Last Name**
 - **SSN/Last Name do not match**
 - **User informed we have no match**
 - **User will not be able to enter the application**

The Process

- **User clicks on “Need a Civil Service ID?”**
 - **SPAM provides form to collect required information**
 - **User fills out form, including SSN, proposed user ID, password, and hint**
 - **User submits**
 - **Information is missing or invalid**
 - **User must correct and re-submit**

The Process

- **User clicks on “Need a Civil Service ID?”**
 - **User submits**
 - **Information is valid and complete**
 - **SSN already on file**
 - **user is informed Department already has issued an ID for that SSN**
 - **user is prompted to correct SSN or enter existing user ID**
 - **SSN not on file**
 - **Record information**

The Process

- **User clicks on “Need a Civil Service ID?”**
 - **SSN not on file**
 - **Save information**
 - **User ID is not unique**
 - User Enters a new ID
 - User enters application
 - **User ID is Unique**
 - User enters application

Other Features

- **Information changes, such as personal information, are e-mailed to the person as confirmation**
- **E-mail changes are sent to the old AND new e-mail addresses**

Lessons Learned

- **Lesson 2: Choosing the right words can save a lot of headaches**
 - **Asking for Civil Service ID reduced calls by 50%.**
 - **Telling people not to bookmark eliminated a whole class of calls**

The Screen

Department of Civil Service - Web Login test

Do not bookmark this page! Please complete the login process before bookmarking any pages.



Please enter your **Civil Service** User ID and Password to access this **Secure Site**.

Civil Service User ID:

Password:

Click here if you: [Need a **Civil Service** ID?](#) or [Don't know your password?](#)

Is it your:

[About cookies](#) | [About logging in](#)

© 2001 New York State Department of Civil Service

Lessons Learned

- **Lesson 3: Users will read, but not too much**
 - **Users will yell at you for not telling them things you did tell them, but they didn't read.**
 - **First time users think they know enough not to click the First Time Users button.**
 - **Users will not necessarily read your explicit error messages.**

Lessons Learned

- **Lesson 4: You can't make your system foolproof, because fools are so ingenious.**
 - Users will try things you never even considered.
 - Users will try things your four-year-old wouldn't even consider.

Lessons Learned

- **Lesson 5: Despite your best efforts to make the system self-sufficient, your Help Desk will be critical**

Lessons Learned

- **Lesson 6: Users on the other end of the telephone do not always tell you the truth.**

Lessons Learned

- **Lesson 7: Implementing in-house may be more difficult than implementing for the public.**

Lessons Learned

- **Lesson 8: Watch out for the back button -- it can be deadly.**

