

CSC368 Systems Programming Languages

IA Projects given to students:

1. Encryption/Decryption program in Perl - Students have to write a program to encrypt a file and another program to decrypt a file.

2. Management of cookies and web files in PHP - In lecture only.

Semester Offered: Fall 2008

Some snapshots:

The screenshot shows a Microsoft Internet Explorer browser window with the following details:

- Title Bar:** Blackboard Academic Suite - Internet Explorer provided by Dell
- Address Bar:** http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fau...
- Toolbar:** Includes links for Google, Bookmarks, Popups okay, Check, AutoLink, AutoFill, Send to, Settings, and several other icons.
- Menu Bar:** File, Edit, View, Insert, Format, Tools, Help.
- Content Area:**
 - Header:** University of Illinois at Springfield (UIS)
 - Main Navigation:** My UIS, Courses, Library, System Admin.
 - Left Sidebar:** Announcements, Course Information, Lecture Slides, Communication, Tools, Course Resources, Projects, Exam Center.
 - Tools:** Communication, Course Tools, Course Map, Control Panel, Quick Unenroll, Refresh.
 - Central Content:**
 - Section:** 2. Encryption/Decryption Program:
Write a program in Perl that can do encryption and decryption programs. An example of encryption program is that "a" becomes "z", and "b" becomes "y" and so on, or whatever shifting algorithm you devise. The input file is any readable text file that is to be encrypted. When this input file is run against the encryption program, it encrypts the file with the use of your encryption algorithm and saves the processed file to an encrypted file with same file name but with an extension of ".inc".
When you run the decryption program, it reads the encrypted file and decrypt (or reverse) it and save to same filename but with an extension of ".dec" which stands for decrypted file. The contents of the decrypted file should be same as the input file.
This has some practical application like sending sensitive file through email. The sender can use the encryption program before sending a sensitive information and then the recipient can use the decryption program to be able to read the file.
For example:
Input File: OriginalFile.txt
To run the encryption program: ./encryption.pl OriginalFile.txt
Its output will be: OriginalFile.inc
To run the decryption program: ./decryption.pl OriginalFile.inc
Its output will be: OriginalFile.dec
Please execute: chmod 711 filename to make your program not readable to others.
 - Item List:** 4 items, one of which is "Midterm Exam".
- Bottom Status Bar:** Done, Internet | Protected Mode: On, 100%, 5:13 PM.

Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fau...

Google

Bookmarks Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Web Search Bookmarks Settings Finance Messenger Mail MySpace News

Blackboard Academic Suite Home Feeds () Print Page Tools

University of Illinois at Springfield UIS

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map

Control Panel Quick Unenroll

Refresh Detail View

General Guidelines Setting a Cookie (1)

- If the cookie should last as long as the user browses through the site, don't set expiration time.
- If the cookie should continue to exist after the user has closed and reopened their browser, set an expiration time that's months in the future.
- If the cookie can constitute a security risk, set an expiration time of an hour or a fraction thereof so that the cookie doesn't continue to exist too long after a user has left the browser.
- The expiration time is set based on the server's time zone, but the browser may delete the cookie based on the client's time zone. Some browsers do automatically correct the time difference between the server and Web browser.

Cookies/Sessions, Functions, File/Dir, Databases

Internet | Protected Mode: On 100% 4:06 PM

A screenshot of an Internet Explorer window displaying the Blackboard Academic Suite interface. The title bar reads "Blackboard Academic Suite - Internet Explorer provided by Dell". The address bar shows the URL "http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fau...". Below the address bar is a toolbar with various icons for Google, Bookmarks, and system functions. The main content area shows the "General Guidelines Setting a Cookie (1)" page from the University of Illinois at Springfield. To the left is a sidebar with links like Announcements, Course Information, and Communication. The bottom of the screen shows the Windows taskbar with multiple open application icons and the system clock at 4:06 PM.

Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fau...

Google

Bookmarks Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Web Search Bookmarks Settings Finance Messenger Mail MySpace News

Blackboard Academic Suite Home Feeds () Print Page Tools

University of Illinois at Springfield UIS

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map

Control Panel Quick Unenroll Refresh Detail View

General Guidelines Setting a Cookie (2)

- For security purposes, set a five or ten-minute expiration time on a cookie and have the cookie re-sent with every new page the user visits. This way, the cookie will continue to persist as long as the user is active but will automatically die five or ten minutes after the user's last action.
- Setting the cookie's path to '/' makes the cookie accessible within an entire Web site.
- If the Web application involves sensitive information such as online banking or e-commerce, set up an SSL (Secure Sockets Layer) connection so that cookies can be sent securely.

Cookies/Sessions, Functions, File/Dir, Databases 10

Internet | Protected Mode: On 100% 4:07 PM

Done

Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fmain

Google

Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Web Search Bookmarks Settings Finance Messenger Mail MySpace News

Blackboard Academic Suite Home Feeds Print Page Tools

University of Illinois at Springfield UIS

Home Help Logout

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map Control Panel Quick Unenroll Refresh Detail View

Example of Cookie's Expiration Date

```
<?php

// Address error handling.
ini_set ('display_errors', 1);
error_reporting (E_ALL & ~E_NOTICE);

$cookies = FALSE; // Cookies have not been sent.

// Handle the form if it has been submitted.
if (isset ($_POST['submit'])) {
    // Send the cookies.
    setcookie ('bg_color', $_POST['bg_color'], time() +1000000, '/', 0);
    setcookie ('font_color', $_POST['font_color'], time() +1000000, '/', 0);
    $cookies = TRUE; // Cookies have been sent.

} // End of submit IF.

?>
```

Cookies/Sessions, Functions, File/Dir, Databases

Internet | Protected Mode: On

100% 4:08 PM

A screenshot of an Internet Explorer window displaying a PHP script. The title bar says "Blackboard Academic Suite - Internet Explorer provided by Dell". The address bar shows the URL "http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fmain". The page content is a code editor with the following PHP code:

```
<?php

// Address error handling.
ini_set ('display_errors', 1);
error_reporting (E_ALL & ~E_NOTICE);

$cookies = FALSE; // Cookies have not been sent.

// Handle the form if it has been submitted.
if (isset ($_POST['submit'])) {
    // Send the cookies.
    setcookie ('bg_color', $_POST['bg_color'], time() +1000000, '/', 0);
    setcookie ('font_color', $_POST['font_color'], time() +1000000, '/', 0);
    $cookies = TRUE; // Cookies have been sent.

} // End of submit IF.

?>
```

The code is intended to demonstrate how to set and handle cookies in PHP. The browser interface includes toolbars for navigation, search, and settings, along with a status bar showing "Internet | Protected Mode: On" and the time "4:08 PM".

Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fmain

Google

Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Web Search Bookmarks Settings Finance Messenger Mail MySpace News

Blackboard Academic Suite Home Feeds Print Page Tools

University of Illinois at Springfield UIS

Home Help Logout

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map Control Panel Quick Unenroll Refresh Detail View

File Permissions (1)

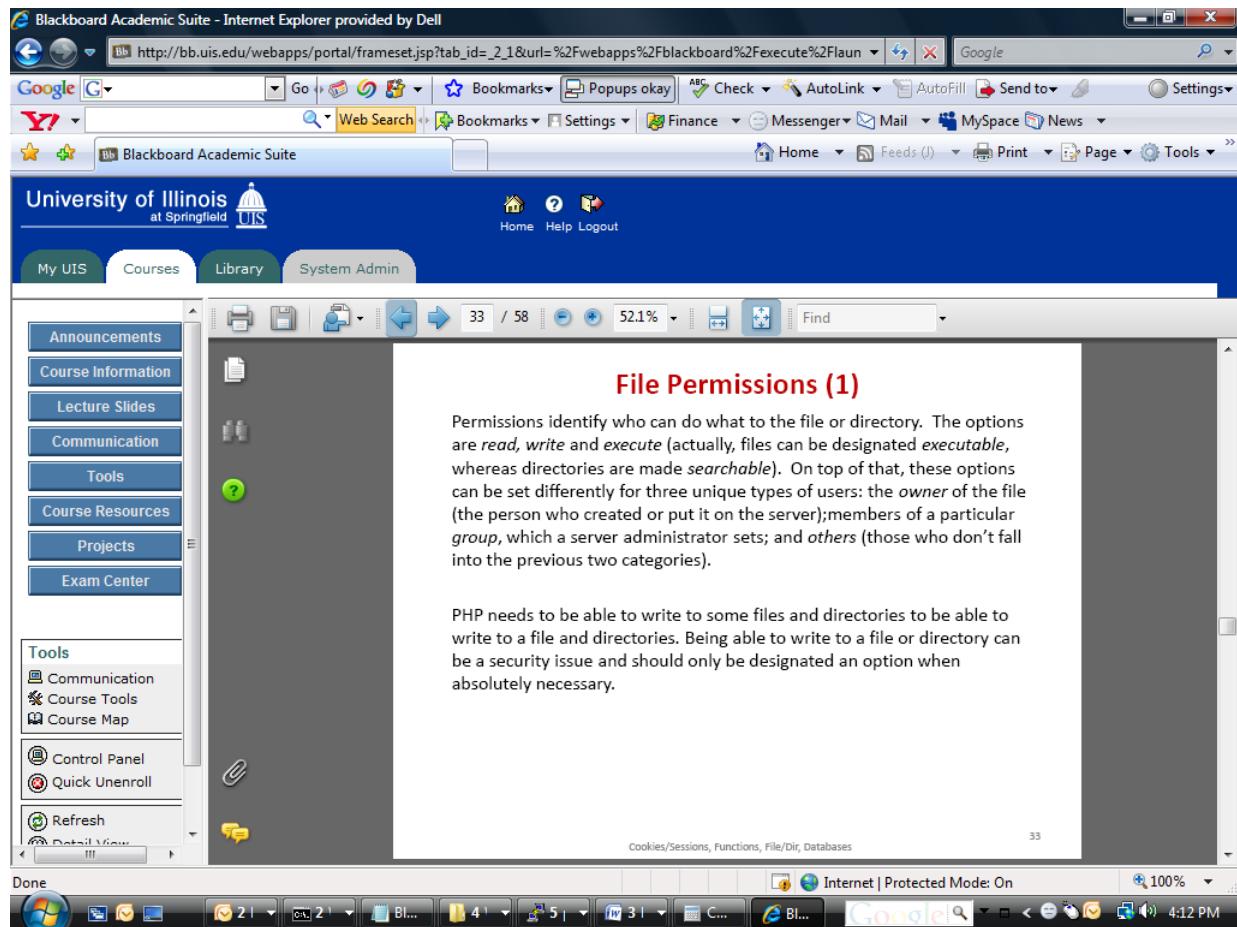
Permissions identify who can do what to the file or directory. The options are *read*, *write* and *execute* (actually, files can be designated *executable*, whereas directories are made *searchable*). On top of that, these options can be set differently for three unique types of users: the *owner* of the file (the person who created or put it on the server); members of a particular *group*, which a server administrator sets; and *others* (those who don't fall into the previous two categories).

PHP needs to be able to write to some files and directories to be able to write to a file or directories. Being able to write to a file or directory can be a security issue and should only be designated an option when absolutely necessary.

Cookies/Sessions, Functions, File/Dir, Databases

Internet | Protected Mode: On

100% 4:12 PM



Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fmain

Google Y! Web Search Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Blackboard Academic Suite Home Feeds Print Page Tools

University of Illinois at Springfield UIS Home Help Logout

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map Control Panel Quick Unenroll Refresh Detail View

Click to go to the next page in the document

File Permissions (2)

- Most OS have no PHP users. Instead, the PHP user is essentially the Web user application (example Apache, PWS, or IIS) is running as. On the Unix family, Apache often runs as *nobody*. On Windows, the Web server frequently runs as the same user who is logged in (and who probably created the file), meaning there be no need to alter a file's permissions.
- In Unix, Linux or Mac, *chmod 761 filename*, the 7 means *write* (2) plus *read* (4) plus *execute* (1) permission to the *owner*; the 6 means *write* (2) plus *read* (4) permission to the *group*; the 1 means *execute* (1) permission to *others*.
- PHP has several functions for changing a file or directory's permissions, including *chgrp()*, *chown()*, and *chmod()*. However, they will work only if PHP already has permission to modify the file or directory in question.

Cookies/Sessions, Functions, File/Dir, Databases

Internet | Protected Mode: On 100% 4:13 PM

Blackboard Academic Suite - Internet Explorer provided by Dell

http://bb.uis.edu/webapps/portal/frameset.jsp?tab_id=_2_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Fmain

Google

Bookmarks Popups okay Check AutoLink AutoFill Send to Settings

Web Search Bookmarks Settings Finance Messenger Mail MySpace News

Blackboard Academic Suite Home Feeds Print Page Tools

University of Illinois at Springfield UIS

Home Help Logout

My UIS Courses Library System Admin

Announcements Course Information Lecture Slides Communication Tools Course Resources Projects Exam Center

Tools Communication Course Tools Course Map Control Panel Quick Unenroll Refresh Detail View

A More Secure File Structure

Having writable files and directories on the server is a bit of a security risk. If the Web server (and everyone else) can write to the file or directory, then malicious users can hack the system using this same gateway.

The best security measure to take in such instance is to place the writable files and directories outside of the Web directory. For example:
/home/netid/public_html/sites/

The sites directory is where the writable files are stored. If possible give permission only to the locally running PHP program but not to others over the Internet.

Cookies/Sessions, Functions, File/Dir, Databases 35

Internet | Protected Mode: On 100% 4:13 PM