CACS-205
Web Technology

(BCA, TU)

Ganesh Khatri
kh6ganesh@gmail.com

Chapter 4/5 : Tag Libraries

- a component of the web development platform
- Used to perform custom tasks like such as XML data processing, conditional execution, database access, loops.
- Java supports tag libraries.

Tag Libraries

- An example to make a tag library:

```
public class HelloTag extends SimpleTagSupport {
    Def:
        public void doTag() throws JspException, IOException {
                JspWriter out = getJspContext().getOut();
                out.println("Hello Custom Tag!");
        }
}
```

Tag Libraries

- Description:

```
<taglib>
      <tlib-version>1.0</tlib-version>
      <jsp-version>2.0</jsp-version>
      <short-name>Example TLD</short-name>
      <tag>
          <name>Hello</name>
          <tag-class>com.tutorialspoint.HelloTag</tag-class>
          <body-content>empty</body-content>
      </tag>
</taglib>
```

Tag Libraries

- Use:

```
<%@ taglib prefix="ex" uri="WEB-INF/custom.tld"%>
<html>
    <head>
        <title>A sample custom tag</title>
    </head>
    <body>
        <ex:Hello/>
    </body>
</html>
```

Anonymous Access

- An anonymous access/login is a process that allows a user to login to aan application anonymously, often by using "anonymous" as the username.
- In this case, the login password can be any text, but it is typically a user's email address.
- Users are able to access general services or public information by using anonymous logins.
- Anonymous Access is one of three authentication schemes for Microsoft Internet Information Services (IIS).
- Anonymous access allows anonymous users to gain access to Web content hosted on the IIS server by using the anonymous user account

Anonymous Access

- Anonymous logins are often used to provide users with easy access to multi-user chat rooms
- When users provide their emails for passwords during this process, they are normally only used for statistical purposes
- Critics of anonymous login claim that they can reduce overall Internet and network security because a secure authentication process is not part of the anonymous login process.
- In addition, user-specific pre-establishments are absent during anonymous logins, leaving critics warning that such logins might not be as anonymous as users would like because servers and IP addresses can be revealed

Authentication based on IP Address

- One way to secure a web-based application is to restrict access based on IP address
- We can block access to a specific address or range of addresses that you suspect belong to malicious individuals.
- The instance allows you to control access by IP address
- The system won't let you lock yourself out, so if you try to add a rule such that your current address would be locked out, the system warns you and refuses your insert.
- If you're inside of a corporate intranet, be very careful about setting up your IP rules.
- IP address you see on your own computer (like 10.10.10.25) generally bears no relationship to IP address you'll actually appear as out on the internet

Authentication based on IP Address

- A user whose access is restricted based on an access rule gets a 403 error on their browser.
- This feature does not supersede or override your existing access control rules if, for example, you're running a VPN to our data center.
- Allow rules always supersede deny rules. So if an address is both allowed (by one rule) and denied (by a second rule) it is, in fact, allowed.
- Asterisks and CIDR blocks are not currently supported.
- Regarding forwarded proxy addresses, the allow rules are applied to each address in the chain and then the deny rules are applied to each address in the chain if none of the allow rules matched
- Examples include intranet or internet access to specific IP addresses/MAC addresses

Integrated Windows Authentication

- Integrated Windows Authentication(IWA) is a term associated with Microsoft products that refers to the SPNEGO, Kerberos, and NTLMSSP authentication protocols with respect to SSPI functionality introduced with Microsoft Windows 2000 and included with later Windows NT-based operating systems
- The term is used more commonly for the automatically authenticated connections between Microsoft Internet Information Services, Internet Explorer, and other Active Directory aware applications
- IWA is also known by several names like HTTP Negotiate authentication, NT Authentication, NTLM Authentication, Domain authentication, Windows Integrated Authentication, Windows NT Challenge/Response authentication, or simply Windows Authentication.

Integrated Windows Authentication

- IWA uses the security features of Windows clients and servers.
- Unlike Basic or Digest authentication, initially, it does not prompt users for a user name and password
- current Windows user information on the client computer is supplied by the web browser through a cryptographic exchange involving hashing with the Web server.
- If the authentication exchange initially fails to identify the user, the web browser will prompt the user for a Windows user account user name and password

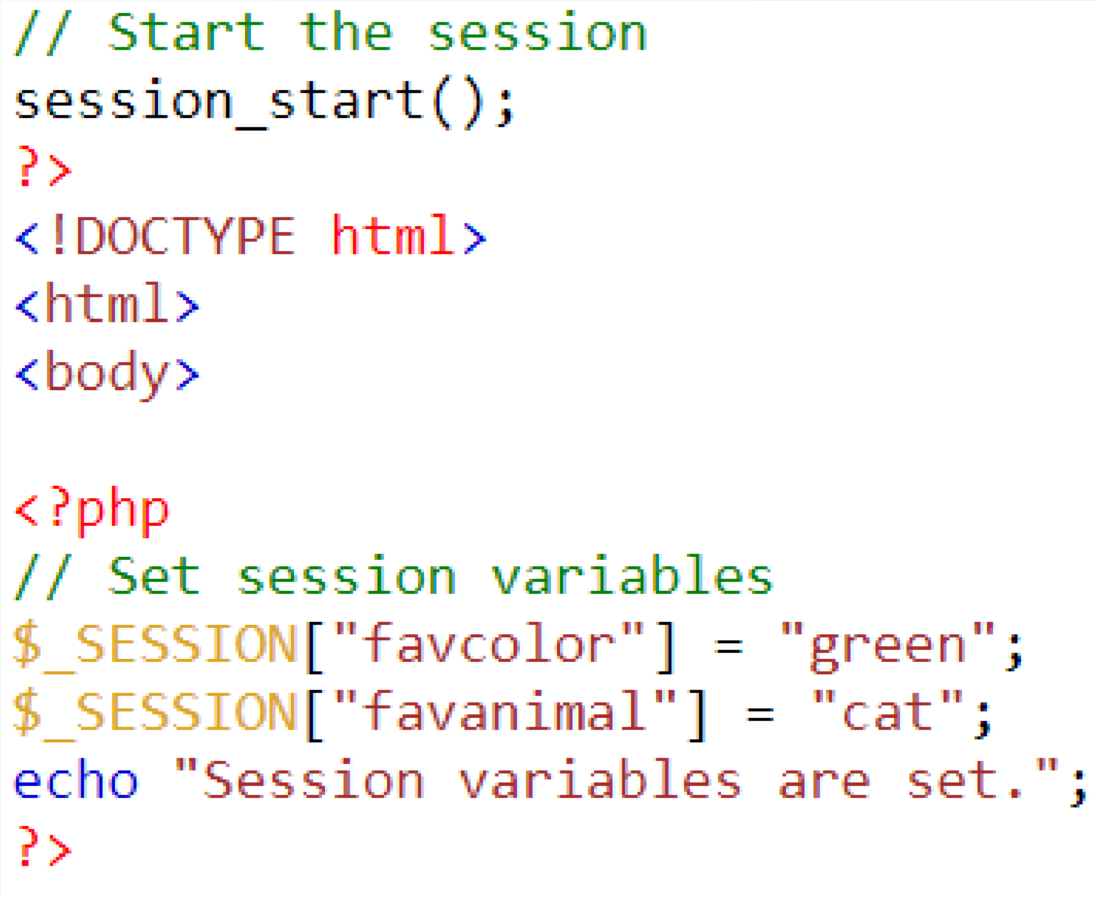
PHP Sessions

- A session is a way to store information (in variables) to be used across multiple pages
- When you work with an application, you open it, do some changes, and then you close it. This is much like a Session. The computer knows who you are. It knows when you start the application and when you end. But on the internet there is one problem: the web server does not know who you are or what you do, because the HTTP address doesn't maintain state.
- Session variables solve this problem by storing user information to be used across multiple pages (e.g. username, favorite color, etc). By default, session variables last until the user closes the browser

- When you work with an application, you open it, do some changes, and then you close it. This is much like a Session. The computer knows who you are. It knows when you start the application and when you end. But on the internet there is one problem: the web server does not know who you are or what you do, because the HTTP address doesn't maintain state.
- Session variables solve this problem by storing user information to be used across multiple pages (e.g. username, favorite color, etc). By default, session variables last until the user closes the browser

Start a PHP Session

- A session is started with the session_start() function.
- Session variables are set with the PHP global variable: $_SESSION
- Note: The session_start() function must be the very first thing in your document. Before any HTML tags.

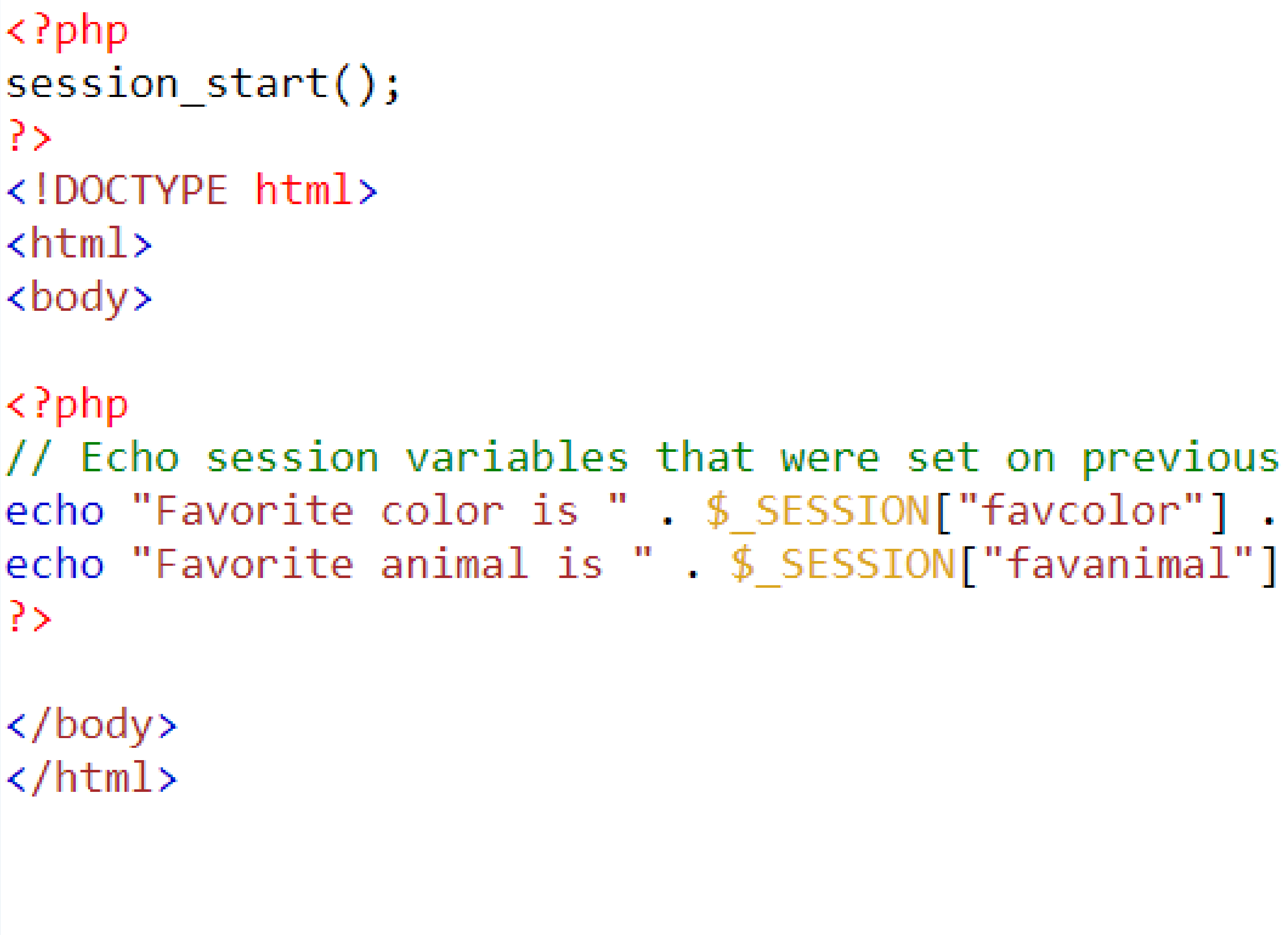


```
// Start the session
session_start();
?>
<!DOCTYPE html>
<html>
<body>

<?php
// Set session variables
$_SESSION["favcolor"] = "green";
$_SESSION["favanimal"] = "cat";
echo "Session variables are set.";
?>
```

Get PHP Session Variable Values

- Notice that session variables are not passed individually to each new page, instead they are retrieved from the session we open at the beginning of each page (session_start()).
- Also notice that all session variable values are stored in the global $_SESSION variable:



```
<?php
session_start();
?>
<!DOCTYPE html>
<html>
<body>

<?php
// Echo session variables that were set on previous
echo "Favorite color is " . $_SESSION["favcolor"] .
echo "Favorite animal is " . $_SESSION["favanimal"]
?>

</body>
</html>
```