University *of* Dayton
Department of Computer Science

CPS 475/575
Secure Application Development

Lecture 20 –Session Protection

Phu Phung
4/2/2020

Review: Lab 6

Lab instructions: http://bit.ly/secad-s20-lab6

- Task 1: Data Protection and HTTPS
  - Follow Lecture 18 to setup HTTPS for your web server
  - Copy Lab 5 code and deploy as Lab 6
- Task 2: Secure Session Authentication
  a. Revised Login System with Session Management (Lecture 19)
  b. Session Hijacking - Broken authentication (Lecture 19)
  c. Session Protection (Session Hijacking prevention) - today
- Task 3: Secure Database Modification
  - Lecture 21

Today's Agenda

- Review:
  - Broken Session Authentication: Session Hijacking Attacks
- Session Protection

Review: Revised index.php – all code together

```php
<?php
    session_start();
    if (isset($_POST["username"]) and isset($_POST["password"]) ){
        if (securechecklogin($_POST["username"],$_POST["password"])) {
            $_SESSION["logged"] = TRUE;
            $_SESSION["username"] = $_POST["username"];
        }else{
            echo "<script>alert('Invalid username/password');</script>";
            session_destroy()
            header("Refresh:0; url=form.php");
            die();
        }
    }
    if (!isset($_SESSION["logged"] ) or $_SESSION["logged"] != TRUE) {
        echo "<script>alert('You have not login. Please login first');</script>";
        header("Refresh:0; url=form.php");
        die();
    }
?>
    <h2> Welcome <?php echo htmlentities($_SESSION["username"]); ?> !</h2>
    <a href="logout.php">Logout</a>
<?php
```

Revision