OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

January Examination 2012

Third Year Computer Science
Visiting European Students

CS3511 Web Security

Professor J. Bowen
Dr. S.N. Foley

Answer *all* questions

1.5 Hours

1. a) Why is it considered good practice for a web server to limit information in the `Server` and `X-Powered-By` attributes in its HTTP responses? (*6 marks*)

   b) Why is it dangerous to configure PHP with `Register Globals` enabled? (*6 marks*)

   c) What is `Magic Quotes` and why is dangerous to rely on it in PHP? (*6 marks*)

   d) Why shouldn't a web-site administrator store the password file (eg `.htpasswd`) used by HTTP Basic authentication under the document root? (*6 marks*)

   e) Give an example of a Semantic URL attack. (*6 marks*)

   f) A website form is used to obtain sensitive password data from a visitor. Should the data be requested using HTTP GET or HTTP POST? Explain your answer. (*6 marks*)

   (*Total 30 marks*)

2. A home broadband user can configure his router/broadband box by visiting a web-based configuration application hosted at `192.168.1.1` within his home network. The web server uses HTTP Basic Authentication to authenticate the user. For convenience, the application provides a one-click security-disable feature which can be used to turn off all security controls on the router and is useful when testing network connectivity:

```
<form method="GET" action="192.168.1.1/disableSec.php">
  <p><input type="submit" value="Disable"></p> </form>
```

   a) Even though the web-server at `192.168.1.1` is not visible to the external Internet, outline how an external attacker on the Internet might be able to disable the security controls on this router by using a *cross-site request forgery*. Explain with the help of PHP code fragments how this vulnerability might be mitigated by using synchronizer tokens. (*15 marks*)

   b) Suppose that the programmer decides to replace the HTTP Basic Authentication by a dedicated `login.php` script whereby session state is managed for visitors authenticated against a user/password database. Explain a *session fixation attack* and whether or not this application is vulnerable to such an attack. (*10 marks*)

   (*Total 25 marks*)

3. A radio station sets up a competition website: a visitor who correctly answers a series of multiple-choice questions is requested to submit their name and telephone number using form:

```
<form action="http://radio.com/correct.php" method="get" />
<p>Name: <input type="text" name="namenum" /><br />
<input type="submit" value="Name and number" /></p></form>
```

   The following code at `http://radio.com/correct.php` adds the listener to a database:

```
$listener = $_GET['namenum'];
//.. set up connection to database $db
$sqli = "INSERT INTO 'correctListeners' VALUES ('$listener')";
mysql_query($sqli, $db);
```

   The radio station uses `http://radio.com/select.php` (authentication required) to select a random listener from the database and display as the winner.

   a) Describe how the radio station website may be subjected to a cross-site scripting attack. Describe the changes necessary in order to avoid this attack. Would setting the `HTTPonly` flag in the response header avoid this attack? Explain your answer. (*15 marks*)

   b) Explain how the website may be subject to a SQL injection attack and describe the changes that should be made in order to avoid this attack. (*10 marks*)

   (*Total 25 marks*)