**IT210A Final Take-Home Exam (DO NOT DISTRIBUTE)**

*Instructor: Derek Hansen*

**Instructions**

You may use books, notes, class materials, the library, and Web resources to help you. You may NOT use other people to help (e.g., students, faculty, friends, family, discussion forums). Type your answers in this document using RED Color and upload your completed file as a .doc, .docx, or open office format to the Learning Suite site. Make sure the correct version of the file is uploaded and you get confirmation that it has been submitted.

Please note the number of points allocated for open questions (e.g. question 6). Be sure to answer the question deeply enough to justify the points being awarded.

**Question 1: GET & POST Comparison (10 points)**

1. (4) Give a line or two of html form syntax that shows how you can use the method POST to submit textual data to a PHP file called “submission.php”. Then give one line of PHP code that could retrieve that submitted data and display (i.e., print) it.

**<form method="post" action="submission.php">**

**<input id="pass" name ="pass"></input>**

**</form>**

**<?php echo $\_POST["pass"]; ?>**

1. (6) Describe at least 3 similarities and 3 differences between transmitting data by GET and POST.

**Similarities:**

* **Both are ways to submit form data to a server.**
* **Both are specified in an HTML form.**
* **When using HTTPS, both types of requests are encrypted in transit.**

**Differences:**

* **POST cannot be bookmarked, GET can be bookmarked.**
* **GET parameters are appended to the action url as query string parameters. POST parameters appear in the message body of the HTTP request.**
* **GET form data is restricted because a URL can only be a certain size. POST has no size restrictions.**

**Question 2: Command Line (9 points)**

A file in a Linux directory is currently listed as follows

-rw-r--r--@ 1 jimbo staff 108 Oct 13 21:28 coolstuff.o

Show the correct syntax for one or more command-line command(s) to do the following (making sure not to include any extraneous options):  
a. Change permissions so that ‘user’ can read/write/execute, ‘group’ can read/execute and ‘other’ can execute (assume you are not logged in as the root superuser and you are not user jimbo)

**sudo chmod 761 coolstuff.o**

b. Change ownership from ‘jimbo’ to ‘zanita’ (assume you are **not** logged in as the root superuser and you are not jimbo or zanita)

**sudo chown zanita coolstuff.o**

c. List all the .o files (and no other files) in this directory (assuming you are currently in the directory), making sure that the permission information for them is shown (as in the example above). This is useful when making sure that the file permission and ownership changes occurred as expected and that other files are unchanged.

**ls -l | grep \.o**

**Question 3: MySQL (4 points)**

Format an SQL statement (not the entire PHP code, just the SQL portion) that will query data from the following **table** called “userdata” in the “db\_band” **database** and return all of the users whose Favorite Band is “U2”, sorted in alphabetical order based on their username:

|  |  |  |
| --- | --- | --- |
| **userID** | **username** | **favoriteband** |
| 01 | joey | U2 |
| 02 | sammy | PinkFloyd |
| 03 | cathy | U2 |
| 04 | Jane | REM |
| … | … | … |

**SELECT username FROM db\_band.userdata WHERE  favoriteband = “U2” ORDER BY username;**

**Question 4: Web Architecture Scenarios (9 points)**

Give a scenario where you would reasonably do each of the following. For example, for part (a) the answer could be in the following format: a business is designing a website that needs to …, but doesn’t need to… In order to … they should [store data in a json file on the server] instead of [in a MySQL database]. Justify each scenario with 2 specific reasons why it makes sense, given your scenario (e.g., If they [stored data in a MySQL database] then they would… which would not work as well as if they [stored data in a json file on the server]. Also, if they did [stored json on a file on the server] they would be able to… more easily, since… compared to if they [stored it in a MySQL database]):

1. (3 points) Store data in a JSON file on the server instead of in a MySQL database.

**As the owner of a medium-sized business, I want to be able to keep track of links and the number of clicks on that link. In order to do this, I want to use a JSON file. JSON files are very lightweight and the data is so small so accessing them can be faster than with a MySQL database, and I don’t need to store anything sensitive so storing them in a file makes more sense than in a MySQL database.**

1. (3 points) Store data in local storage instead of in a cookie.

**As part of my business, I designed a small game that I want users to come back indefinitely and not lose their place. To do this, I want to use the localstorage because it will never expire while cookies do expire. Also, cookies are used to manage sessions and for the game a session is not needed so the localstorage is used instead.**

1. (3 points) Use PHP to perform some functionality instead of Javascript.

**As part of my business, I want people to be able to login and authenticate. In order to do that, they should use PHP to talk with a database instead of Javascript.  PHP talks with a database much easier than JavaScript does because JavaScript requires a server side language like PHP to do it. PHP can also encrypt passwords and such so that it is more secure as well.**

**Question 5:** **Information Assurance (9 points)**

Use the MSRQ cube to analyze the following scenario. Make sure to explain (a) which **Security Service(s)** were compromised and which were not (explain each of the 5 security services, don’t just list them), and (b) which **Information State(s)** are relevant and which were not (again, take a sentence or two to explain why for each of the 3 states). Also, (c) provide **one** **Security Countermeasure** that would solve this problem, making sure to identify which type of countermeasure it is (i.e., technology, policy and practice, people) (if it has to do with more than one then list which ones and explain). Three points are awarded for correct answers to (a), (b), and (c).

*Scenario: A Hacker uses SQL Injection to delete a table that stores data on users, their credit card information, and their past purchases.*

a) **Availability- the timely, reliable access to data and information services for authorized users. Availability is compromised because users can no longer access information, it is not available anymore.**

**Integrity - Protection against unauthorized modification or destruction of information. Integrity was compromised because someone deleted something that they should not have been able to delete.**

**Authentication - designed to establish the validity of a transmission, message, or a user's authorization to receive specific information. Authentication was not compromised**

**Confidentiality - assurance that information is not disclosed to unauthorized persons. Confidentiality was not compromised because, even though the table contained credit card information, it was not stolen, just deleted which means no one has the information who should not.**

**Non-repudiation - The assurance that the sender is provided with proof of delivery and the recipient is provided with proof of the sender's identity. Non-repudiation was compromised because the past-purchase information was deleted, so there is no proof of who bought things.**

b) **Transmission - While the data is being moved between the client and server. This is not relevant to the situation.**

**Storage - Time during which the data is on a hard drive or storage device. This is relevant because the table that was deleted was in a database on a storage device.**

**Processing - Time during which the data is actually being modified in a processing step. This is not relevant because the data that was hacked was not being processed, it was stored.**

c) **When allowing people to submit data to a server, any data that they submit should be screened so as to make sure that there are no SQL commands and necessary characters in what is submitted or by making sure that only correct people can make changes. This can be fixed by pattern checking, or by limiting database permissions. This is a Technology countermeasure.**

**Question 6:** **Life-long learning: (8 points)**

(a) What process do you use to discover resources to learn new technologies for this class? Describe the process. (b) Explain the criteria that you use to ensure that you are finding good quality and relevant information. (c) Share one lesson you have learned to be more effective at finding, understanding, and/or using the information you find.

a). **The first thing I did for this class when learning new technologies, take PHP for example, was to go to Codecademy.com and take the PHP lesson. This allowed me to get a good understanding of syntax and of what the technology was capable of. Next, I went to my older brother, a source of authority because he is a web developer for a school district, and would pose my questions to him. This allowed me to broaden my understanding of what the technology could be used for. Then, when I was trying to figure something out for a lab, I would search for it on the internet to try and find a good source that I could try or I would ask a friend who was working on the same thing to work with me on it.**

b). **When searching for information, I would use two criteria. 1) Easily understandable. If I was able to read the code and know what it was going to do either because of comments or by programming style, then it passed. 2) It had been confirmed as a solution by other sources. This was important so that I knew that I would be trying something that worked for others. I would first try and find information that satisfied both criteria, and only if I was stuck would I try something that was verified to work but that I did not understand very well. I would not try anything that was not verified to work.**

c). **When searching for information, it is extremely important to read the comments that people leave. Most of the time they will leave comments about why code isn’t working and even give alternative ideas that work better. This is especially true for using Stack Overflow.**

**Question 7: CSS: (4 points)**

Consider the following html code fragment. Add any necessary CSS to this page in just one place so that all the content of the paragraph tags (and only the paragraph tags) display in Arial sans-serif format. Show the CSS code clearly (**bold** or color it) and make sure it is inserted into the correct place in the document for it to work correctly.

<html xmlns="http://www.w3.org/1999/xhtml">   
<head>

**<style>**

**p**

**{**

**font-family: Arial;**

**}**

**</style>**

<title>Sample HTML Page</title>   
</head>   
<body>  
 <h1><a href="index.htm">Jump to Barzoom</a></h1>  
 <p>This is a page with links to places and people in the magical country of Barzoom. </p>  
 <p>Barzoom has lots of people and lots of places and the links below show you lists of all the wonderful people. Some of the people aren’t really people, they’re more goblins and dwarfs and trolls and things, but hey! We did say this is a magic kingdom</p>  
 <br />  
 <h3>The Lists of People and Places</h3>  
 <ul>  
 <li><a href="places.htm">Sites</a></li>   
 <li><a href="people.htm" >Topics</a></li>  
 </ul>  
 <p>That’s all folks</p>  
</body>  
</html>

**Question 8: Sources of Delay (9 points)**

(a) (6 points) Visit the following website: <http://www.taboradelaide.edu.au/> List, *in your own words*, 3 things the webmaster of the site could do to decrease the load time. Justify your recommendations with concrete evidence. You may use tools that help identify problems, measure the size of the page elements, and/or look at the page’s source code (search for “speed up website online tool” or related terms). However, your explanations of what to change must be your own (i.e., don’t just copy and paste recommendations from a website). Make sure and include recommendations that will make the most difference. (6pts)

(b) (3 points) Ping the website listed above. Also Ping <http://www.uvu.edu/>. Report the average latency for each website and the amount of packet loss. Explain why they are similar or different.

**a). According to Yslow, one of the things the webmaster could do is put the JavaScript at the bottom of the page. Many browsers make 2-8 connects to a server at the same time, this parallel approach speeds up pages. However, when JavaScript is encountered, these parallel downloads are blocked and new downloads cannot start until the JavaScript is loaded.**

**Another thing they could do is Make the JavaScript and CSS external instead of loading them in document body. The reason for this is caching. If your site uses the same things over and over, you can set the server to cache those files, making it so a visitor doesn’t download the same files over and over, making the HTML page load faster.**

**They could also make sure that they remove duplicate JavaScript and CSS. Whenever there is more than one of the same thing, the browser has to load both of them and then evaluate the script each time. Removing duplicates means the server has fewer requests to load the page, thus allowing it to load faster.**

**b). I pinged msu.ru, Moscow State University because the site given was unavailable.**

**20 packets sent**

**20 packets received**

**0.0% packet loss.**

**Average round-trip: 180.647 ms**

**Pinging uvu.edu**

**20 packets sent**

**20 packets received**

**0.0% packet loss.**

**Average round-trip: 9.704 ms.**

**UVU.edu’s latency is much lower than MSU.ru because UVU is so much closer. Latency is the literal wait time for the packet to get there and come back. The packets don’t need to travel across the world. One would expect more packet loss as well because the packet has to travel across the world and there is much more chance of it getting lost along the way but that did not happen in this case, but there was an obvious difference in latency.**

**Question 9: Encryption (6 points)**

In class we discussed 3 main cryptographic algorithms types: secret key (symmetric) cryptography, public key (asymmetric) cryptography, and hash functions. For each of the 3 cryptographic algorithm types, describe how it can (in principle) be used to provide **one** specific information security service (Integrity, Authentication, Confidentiality, or Non-Repudiation). Be specific. (For example, for symmetric and asymmetric, make sure you discuss how keys work, who has them, and how they are used.).

**Secret Key (Symmetric) Cryptography: This could be used to provide Confidentiality assurance. This helps keep anyone who doesn’t have the secret key from being able to decrypt and see the sensitive material. Both parties but have the same key in order to encrypt and decrypt the message. An example of this would be using a book cypher. Even if someone knew what book you were using, unless they knew the key they would never be able to break it, or vice versa. The tricky part is exchanging the key in a secure way.**

**Public Key (Asymmetric) Cryptography: This could be used to provide Authentication assurance. This uses a public and a private key and one can decode the other and vice versa, but knowing one does not give you access to the other key. That way, you can keep the private key to yourself, and then give out the public key, and no one but you or the person you send a message to can decrypt it because one will encrypt and the other will decrypt. An example of this could be with sending private emails or messages. You give out a public key so someone can send you a message encrypted, and no one else will be able to read it because they don't have the corresponding key pair. That way Authentication happens.**

**Hash Functions: These can be used to provide Integrity assurance. Since a password can be hashed, it will have turned into some crazy combination of characters. The actual password is not given out, so even if someone gets ahold of the hash and they know what algorithm was used, there is no way of knowing what the password was that was used to make the hash since hash functions are one way. That way, you can compare hashes of passwords and it is still secure so that you can make sure that only someone who can provide the right hash has access to something important. An example of this is logging on to a website. If the hash that they give you does not match one you have on file, then they are not able to log on.**