William Weiskopf November 16, 2011

Web Programming

Unit 12: Security and Sessions

Chapter 15:

1. Read pages 342-350. List two points that you think are important to remember.
   1. Remove unnecessary services from the server to reduce the number of weak points
   2. Assumptions made by developers, though perhaps true, are best to be avoided and/or heavily tested.
2. Explain briefly how private key and public key encryption schemes work.

Private key: A key used to encrypt and decrypt, it is kept amongst those trusted with the information and secret from everyone else.

Public key: A key known to everyone is used to encrypt a message, but that message cannot be decrypted through the use of the same public key. To decrypt the message the recipient uses their own private key, kept secret from everyone else.

1. Explain the purpose of the hash function when using digital signatures.

A hash function is used to quickly generate a small “digest” of the message. Every time the function is run on the same content it will produce the same result. But if the content has been altered at all, then the digest will be different. This way a hash can be generated and encrypted for a message. The recipient can check the encrypted hash and ensure that the hash of the message still matches the original hash and thus the message has not been tampered with.

Chapter 16:

1. If your web page contains code that limits the user’s choices (e.g., radio buttons, select statements etc. that force the user to pick a predefined option, such as male or female), can a php form assume that the data is valid? Explain.

No, forms are submitted as a text message to the server, thus someone could send such a message with entirely absurd values and if you never checked, you would never know. Verify that the data received is within a range that you expect.

1. What additional security advantage does mysqli include when executing a query?

mysqli only allows one statement to be executed by a query passed to it. Thus reducing the potential of many harmful statements being executed.

1. What is the purpose of htmlspecialchars?

To replace “<”, “>”, and “&” (and optionally single and double quotes) with the equivalent html entity, a character sequence that represents a special character we don’t want to have considered as part of the code, but as part of the content.

1. Describe an alternative to placing database name and password information in the .php file that is processed in response to a user request.

The username and password are placed in a file not on the document root of the web site and then that file is included or required when the code in the document root needs that information.

1. What potential problem exists with user input that contains a back quote?

Back quotes are used to execute arbitrary commands in a command shell. Because we definitely don’t want users executing commands to the server it is best to restrict all use of the back quote.

1. New software versions are thoroughly tested by the vendor, so it’s safe to install directly on your production system. True or false?

False, always start by installing on a test system

1. List four things to consider regarding security when evaluating commercials hosts for your website.
2. Complete support documentation
3. Access to entire directory trees, not just document root
4. Find out the php.ini settings and check that they are safe
5. Up to date software versions

Chapter 23:

1. Describe the parameters for a cookie.

Name: cookie name

Value: value stored in cookie

Expires: date that the cookie expires

Path and Domain: specify the URL(s) for which the cookie is relevant

Secure: The cookie will not be sent over a plain HTTP connection

1. What are the security risks if you set the session\_use\_trans\_sid in php.ini.

Session IDs can be communicated, posted, or otherwise become public knowledge

1. What is the purpose of strip\_tags()?

By stripping out HTML and PHP tags from a string users are prevented from planting malicious scripts.