Brenton Grundman
8129460164
CS356 H10

Chapter 11 Review questions 11.5 and 11.9 and 11.12.

Chapter 22 Review questions 22.4 and 22.6

Chapter 23 Review questions 23.1, 23.4, 23.11

11.5 State the similarities and differences between command injection and SQL injection attacks.

Similarities:

- Both are “injection” attacks from an outward-facing web interface
- To defend against them, you must verify that the input you get is input you’d expect

Differences:

- SQL injection is exclusive to databases
- Command injections are executed by the system with privileges of the web server

11.9 Define input fuzzing. State where this technique should be used.

Input fuzzing is a software testing technique that essentially tests the robustness of software by generating random input data in order to determine whether the software responds appropriately to the input values. It should be used to determine reliability as well as potential security deficiencies.

11.12 Identify several concerns associated with the use of environment variables by shell scripts.

Environment variables provide another path for untrusted or incorrect data to enter a program. This could be used to use a program that has increased privileges to run the attacker’s code. Because PATH can be altered, an attacker can feed it their own sed and grep programs. Further, the PATH variable could use a known default value by the script, which is now vulnerable because of the IFS variable. The IFS determines how words are separated in a line of commands, but can be set to any string of characters. It is essentially impossible to stop this form of attack (omg wtf).

22.4 What is DKIM?

DomainKeys Identified Mail is how to cryptographically sign emails. A signing domain claims responsibility of a message in a mail stream. This can be used to verify that a message came from a specific person.

22.6 What is the difference between and SSL connection and an SSL session?

Connection:

A connection is part of one session, is transient, and is peer-to-peer (in TLS)

Session:

Association between client and server that are created by the Handshake Protocol. They define security parameters which can be shared amongst multiple connections. So basically they’re the airport for the flights that are the connections (because you have one security setup for all the flights)

23.1 What are the principal elements of a Kerberos system?

Authentication Server – knows all the passwords of clients

Data Encryption Standard – shares a unique secret encryption key with each server

Ticket-Granting Ticket and Session Key – encrypted using the user's password, and sent to the user. The user is then prompted for a password. The correct password decrypts these both, which allows them to connect to the server using the ticket granted by the ticket-granting ticket and the session key.

The user ID and password of all participating users in its database

Must share a secret key with each server

23.4 What is X.509?

Certificate used in most network security applications

23.11 What are some key problems with current public key infrastructure implementations?

- reliance on user to make an informed decision when there is a problem verifying a certificate
- assumption of all CAs in the "trust store" are equally trusted
- different implementations in different browsers use different trust stores
- various other issues