

Module 2 - Lecture 9

Data Security



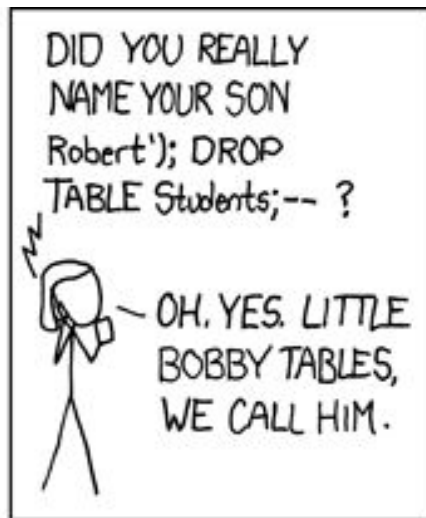
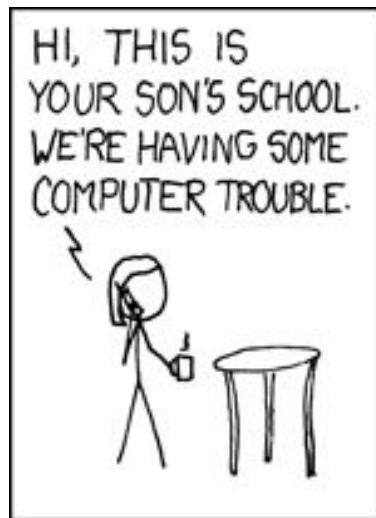
REVIEW

- What is Integration Testing?
- What are 3 attributes of a good test?
- Where to host the database?
- What to do with the data to enable repeatability?



Open Web Application Security (OWASP)





SQL Injection Attacks



Practice Safe Computing

- **Parameterized queries:** when done consistently, SQL injection attacks will not be possible.
- **Input validation:** limit the number of acceptable values.
- **Limit database user privileges:** the user that your application is accessing your database with should be given the least permissions necessary to function. This is called *Principle of Least Privilege*.



Securing Passwords / Secrets



Securing Passwords / Secrets

- We need to be able to verify a password, not see the password.
- A system administrator with full access to the credential database should not be able to see your password.
- A hacker that stole the credential database should not be able to see your password.
- Even with supercomputing power, no one should be able to uncover the data in a reasonable amount of time.



HASHING



HASHING

- A one way function to obfuscate the data.
- This is used prior to storage of the password.
- To verify the password, the same function is used to re-generate the hash and that is what is compared against the database.
- Passwords should also be salted prior to hashing. This will make it take even longer for someone to crack.



What makes a good hashing function?

- Inputs and outputs are constrained
- Relationship between inputs and outputs appears random
- Inputs should be evenly distributed over outputs
- Some degree of efficiency that does not sacrifice collision resistance
- Examples of hashing functions:
 - Message Digest (**MD5** - cracked via Birthday Attack)
 - Secure Hash Algorithm (**SHA-512**)



ENCRYPTION



Securing data at rest

- Data at rest can use a form of encryption called **symmetric key encryption**. Symmetric because the key works for both encrypting and decrypting.
- Requires both parties to use the key to encrypt and decrypt data.
- Any party possessing the key can read the data.
- Has difficulties of securing the symmetric key amongst multiple parties.



Securing data in transit

- Data in transit is often secured using **asymmetric encryption**.
- Asymmetric algorithms allow us to create a **public key** and a **private key**.
 - The public key is distributed freely.
 - The private key is kept to ourselves.



HTTPS & SSL/TLS

- TLS and SSL are recognized as protocols to provide secure HTTP(S) for internet transactions. It supports authentication, encryption, and data integrity.
- What are Digital Certificates?
- What is a Man-in-the-Middle Attack?
- High-level, how is data secured during a web-browsing session?



QUESTIONS?

