### **Part 1: Q&A**

#### **The URL Cruise Missile**

1. Which part of the URL can be manipulated by an attacker to exploit a vulnerable back-end database system?

Answer: Parameter

1. Which part of the URL can be manipulated by an attacker to cause a vulnerable web server to dump the /etc/passwd file? Also, name the attack used to exploit this vulnerability.

Answer:Path

1. Name three threat agents that can pose a risk to your organization.

Answer:hacktivists, nation states, insider threat

1. What kinds of sources can act as an attack vector for injection attacks?

Answer:Email,post requests and or parameters

1. Injection attacks exploit which part of the CIA triad?

Answer:Integrity

1. Which two mitigation methods can be used to thwart injection attacks?

Answer:input sanitization, restricted character sequence and patterns

#### **Web Server Infrastructure**

Web application infrastructure includes sub-components and external applications that provide efficiency, scalability, reliability, robustness, and most critically, security.

1. What stage is the most inner part of the web architecture where data such as, customer names, addresses, account numbers, and credit card info, is stored?

Answer1:Database

1. Which stage includes online forms, word processors, shopping carts, video and photo editing, spreadsheets, file scanning, file conversion, and email programs such as Gmail, Yahoo and AOL.

Answer2: Web application

1. What stage is the component that stores files (e.g. HTML documents, images, CSS stylesheets, and JavaScript files) that's connected to the Internet and provides support for physical data interactions between other devices connected to the web?

Answer3:web application

1. What stage is where the end user interacts with the World Wide Web through the use of a web browser?

Answer4:client

1. Which stage is designed to prevent unauthorized access to and from protected web server resources?

Answer:Firewall

#### **Server Side Attacks**

In today’s globally connected cyber community, network and OS level attacks are well defended through the proper deployment of technical security controls such as, firewalls, IDS, Data Loss Prevention, EndPoint and security. However, web servers are accessible from anywhere on the web, making them vulnerable to attack.

1. What is the process called that cleans and scrubs user input in order to prevent it from exploiting security holes by proactively modifying user input.

Answer: Input Sanitization

1. Name the process that tests user and application-supplied input. The process is designed to prevent malformed data from entering a data information system by verifying user input meets a specific set of criteria (i.e. a string that does not contain standalone single quotation marks).

Answer:Input Validation

1. **Secure SDLC** is the process of ensuring security is built into web applications throughout the entire software development life cycle. Name three reasons why organization might fail at producing secure web applications.

Answer: High implementation costs, insufficient support from management, no quality management, Total reliance on web application firewalls

1. How might an attacker exploit the robots.txt file on a web server?

Answer:Looking where told not to

1. What steps can an organization take to obscure or obfuscate their contact information on domain registry web sites?

Answer: by excluding directories and pages that contain critical information

1. True or False: As a network defender, Client-Side validation is preferred over Server-Side validation because it's easier to defend against attacks.  
   * Explain why you chose the answer that you did.

Answer:It is better to validate user input on Server Side because you can protect against the malicious users, who can easily bypass your Client Side scripting language and submit dangerous input to the server.

#### **Web Application Firewalls**

WAFs are designed to defend against different types of HTTP attacks and various query types such as SQLi and XSS.

WAFs are typically present on web sites that use strict transport security mechanisms such as online banking or e-commerce websites.

1. Which layer of the OSI model do WAFs operate at?

Answer: Layer 7

1. A WAF helps protect web applications by filtering and monitoring what?

Answer: A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app.

1. True or False: A WAF based on the negative security model (Blacklisting) protects against known attacks, and a WAF based on the positive security model (Whitelisting) allows pre-approved traffic to pass.

Answer:

1. True

#### **Authentication and Access Controls**

* + Factor 1: Standard Login Inputs (passwords, PIN, Cognitive questions)
  + Factor 2: Physical keys (Smartcards, Hard tokens)
  + Factor 3: Biometrics( iris/retina scans, hand geometry)
  + Factor 4:Location(GPS detection, callback to a home phone number)

1. True or False: A password and pin is an example of 2-factor authentication.

Answer: False

1. True or False: A password and google authenticator app is an example of 2-factor authentication.

Answer:True

1. What is a constrained user interface?

Answer:Restricts user access to certain areas or the ability to request.