## Unit 15 Submission File: Web Vulnerabilities and Hardening

### Part 1: Q&A

#### The URL Cruise Missile

The URL is the gateway to the web, providing the user with unrestricted access to all available online resources. In the wrong hands can be used as a weapon to launch attacks.

Use the graphic below to answer the following questions:

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocol** | **Host Name** | **Path** | **Parameters** |
| http:// | www.buyitnow.tv | /add.asp | ?item=price#1999 |

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

**Answer: Parameters**

2. 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**

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

**Answer: Hackers, Government, Internal Employees**

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

**Answer: Server directory, form, website, login page, application session**

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

**Answer: Confidentiality**

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

**Answer: Input Sanitization & Validation**

\_\_\_\_

#### Web Server Infrastructure

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

- The same advancements made in web applications that provide users these conveniences are the same components that criminal hackers use to exploit them. Prudent security administrators need to be aware of how to harden such systems.

Use the graphic below to answer the following questions:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stage 1 | Stage 2 | Stage 3 | Stage 4 | Stage 5 |
| Client | Firewall | Webserver | Web Application | Database |

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?

**Answer: Stage 5 SQL Database**

2. 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.

**Answer: Stage 4 Web Application**

3. 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?

**Answer: Stage 3 Web Server**

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

**Answer: Stage 1 Web Client**

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

**Answer: Stage 2 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**

2. 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**

3. \*\*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 & standardization**

**No Quality management**

**Total reliance on web application firewalls**

**Reactive Security postures**

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

**Answer: Reveal the existence information that a WebCrawler is hiding.**

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

**Answer: Ensure they have a service that protect privacy. Typically, a Registrar provides a service that perform the act of protecting an organizations privacy.**

6. 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: False. Its harder to validate on the client side because the system/applications maintained at the client’s discretion. Applications may have available exploits and provide malicious methods for attackers to utilize for impersonation.**

\_\_\_\_

#### 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 Application**

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

**Answer: HTTP/S Traffic**

3. 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:True**

\_\_\_\_

#### Authentication and Access Controls

Security enhancements designed to require users to present two or more pieces of evidence or credentials when logging into an account is called multi-factor authentication.

- Legislation and regulations such as The Payment Card Industry (PCI) Data Security Standard requires the use of MFAs for all network access to a Card Data Environment (CDE).

- Security administrators should have a comprehensive understanding of the basic underlying principles of how MFA works.

1. Define all four factors of multifactor authentication and give examples of each:

**- Factor 1: Standard login inputs (password, PIN, cognitive questions)**

**- Factor 2: Physical keys (smartcard, hard token)**

**- Factor 3: Biometrics (iris/retina scan, hand geometry)**

**- Factor 4: Location (GPS detection, callback to a home phone number)**

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

**Answer: True**

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

**Answer: True**

4. What is a constrained user interface?

**Answer: Restricts what users can see and do based on their privileges**

----

\_\_\_\_

Part 2: The Challenge

The Challenge Instructions

**Challenge #1**

Graphical user interface, text, application

Description automatically generated

**Challenge #2**

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application, chat or text message

Description automatically generated

**Challenge #3**

Graphical user interface, text, application

Description automatically generated