Quiz 3 Answers - Information Security

BSCSF21 Morning Quiz

A. Differentiate between Command injection and Code injection by giving an example of each. [2]

Command Injection:

- The attacker executes arbitrary OS commands on the server OS via a vulnerable application
- Leads to OS-level control, allowing attackers to execute arbitrary commands, access system files, or compromise the server
- Example: Injecting the command `rm -rf /` into a form that allows input to be passed to the system shell, or `68.65.120.238 ; cat /etc/passwd`

Code Injection:

- Malicious code is injected into an application, which the application then executes as part of its normal flow
- The injected code runs within the application's context
- Example: Injecting PHP code like `<?php system('whoami'); ?>` into a web application that processes user input

B. Give three commands; download a docker image abc from DockerHub, display created/running containers on your machine, and a command to delete a docker image abc. [2]

1. **Download docker image:** `docker pull abc`
2. **Display containers:** `docker ps` (running) or `docker ps -a` (all containers including stopped)
3. **Delete docker image:** `docker rmi abc`

C. Write down a single SQL statement to display all the names of users and their corresponding passwords, who exist inside dvwa database. [2]

```sql
SELECT user, password FROM dvwa.users;
```

D. What do you mean by session management? [2]

Session management refers to the process of securely handling user sessions in web applications. It involves creating, maintaining, and destroying user sessions to keep track of authenticated users as they navigate through the application. Proper session management includes generating secure session IDs, storing session data securely, implementing session timeouts, and protecting against session hijacking attacks.

E. Give the steps that developer should take to mitigate the SQLi vulnerability. [2]

1. **Use Prepared Statements (Parameterized Queries) -** Separate SQL logic from user input using placeholders
2. **Input Validation and Sanitization -** Validate inputs to ensure they meet expected formats and sanitize special characters
3. **Use Least Privilege Principle -** Database accounts should have minimal necessary permissions
4. **Avoid exposing detailed error messages** to users
5. **Use Web Application Firewalls (WAFs)** to filter malicious SQL injection attempts

---

BSCSF23 Morning Quiz

A. Differentiate between Session ID and cookies. [2]

Session ID:

- A unique identifier assigned to a user session
- Used to track and maintain user state across multiple requests
- Can be stored in cookies, URL parameters, or hidden form fields

Cookies:

- Small pieces of data stored by the web browser on the client side
- Can contain various information including session IDs, user preferences, or tracking data
- Sent automatically with HTTP requests to the same domain
- Can be persistent (stored on disk) or session-based (deleted when browser closes)

B. Name the four components of an HTTP request object. [2]

1. **Request Line** (Method, URL, HTTP Version)
2. **Request Headers**
3. **Request Body/Content**
4. **Query Parameters**

C. Give a comparison between BurpSuite and BeEF. [2]

BurpSuite:

- Comprehensive web application security testing platform
- Used for both server-side and client-side vulnerability assessment
- Includes proxy, scanner, intruder, repeater, and other tools
- Focuses on HTTP/HTTPS traffic analysis and manipulation

BeEF (Browser Exploitation Framework):

- Specialized tool for browser exploitation and client-side attacks
- Hooks web browsers through malicious JavaScript
- Focuses specifically on browser-based attacks and social engineering
- Provides command and control interface for hooked browsers

D. Give a command to generate a wordlist having passwords consisting of only lowercase alphabets. The length of passwords can range from 3 to 5 characters. How many total passwords will be generated? [2]

Command:

```bash
crunch 3 5 abcdefghijklmnopqrstuvwxyz -o wordlist.txt
```

Total passwords: $26^3 + 26^4 + 26^5 = 17{,}576 + 456{,}976 + 11{,}881{,}376 = 12{,}355{,}928$

E. Give the steps that developer should take to mitigate the command injection vulnerability. [2]

1. **Strict Input Validation/Sanitization** - Use whitelist of accepted values and reject any data containing shell metacharacters
2. **Use Safe APIs** - Avoid passing untrusted data directly to system commands; use APIs that don't support shell metacharacters
3. **Escape Shell Commands** - Use functions like `escapeshellcmd()` in PHP to remove shell metacharacters
4. **Apply Principle of Least Privilege** - Run applications with minimal necessary permissions
5. **Input Filtering** - Filter out dangerous characters like `;`, `&`, `&&`, `|`, `||`, `\n`, backticks

---

BSDSF22 Afternoon Quiz

A. Differentiate between CSRF and SSRF attacks. [2]

CSRF (Cross-Site Request Forgery):

- Tricks a user's browser into executing unwanted actions on a trusted site where the user is authenticated
- Exploits the trust a website has in the user's browser
- Example: Changing passwords, transferring funds without user's knowledge

SSRF (Server-Side Request Forgery):

- Tricks an application into making requests to other servers
- Allows attackers to access sensitive information or interact with systems that should be off-limits
- Exploits server-side misconfigurations
- Example: Accessing internal services, cloud metadata, or restricted endpoints

B. Name the four attack types that an attacker can use while launching a Brute force attack using Intruder tab of BurpSuite. [2]

1. **Sniper** - Single payload set, single position
2. **Battering Ram** - Single payload set, multiple positions (same payload)
3. **Pitchfork** - Multiple payload sets, parallel iteration
4. **Cluster Bomb** - Multiple payload sets, all combinations

C. What is BeEF, and what it is used for? [2]

BeEF (Browser Exploitation Framework) is a penetration testing tool that allows security researchers to assess the security posture of target environments by hooking web browsers and controlling them through a command-and-control interface. It's used for:

- Browser fingerprinting and information gathering
- Client-side attacks and exploits
- Social engineering attacks (fake login dialogs, phishing)
- Testing browser vulnerabilities
- Demonstrating the impact of XSS attacks

D. Using SQLi tool, write down a single command that will display all the rows of users table inside the dvwa database. [2]

```bash
sqlmap -r abc.txt -D dvwa -T users --dump
```

E. Describe pictorially the process of working of SQLi behind the curtain. [2]

SQLi Behind the Curtain Process:

1. **Input Phase:** Untrusted user data (malicious SQL) + Trusted SQL code
2. **Parser Phase:** SQL parser receives combined input but cannot differentiate between data and code
3. **Execution Phase:** Some untrusted user data gets interpreted as SQL code
4. **Result:** Malicious SQL commands executed alongside legitimate queries

---

BSDSF22 Morning Quiz

A. Name the three most common and freely available deliberately insecure web applications, and give a brief description of the front-end back-end technologies used in any one of them. [2]

Three common deliberately insecure web applications:

1. **DVWA (Damn Vulnerable Web Application)**
2. **WebGoat**
3. **Mutillidae**

DVWA Technologies:

- **Front-end:** HTML, CSS, JavaScript
- **Back-end:** PHP
- **Database:** MySQL
- **Web Server:** Apache

B. Precisely describe the role of Target and Repeater tab in BurpSuite. [2]

Target Tab:

- Displays the site map of all discovered content

- Shows the structure of the target application
- Allows scope definition for testing
- Provides an organized view of the application's attack surface

Repeater Tab:

- Allows manual modification and resending of HTTP requests
- Enables testing of individual requests with different parameters
- Useful for analyzing application responses to modified inputs
- Facilitates fine-tuned testing of specific vulnerabilities

C. What is the role of information_schema and mysql database inside MySQL RDBMS. [2]

information_schema:

- Virtual database containing metadata about the server and its databases
- Accessible to all users for querying server metadata
- Contains tables like `schemata` (database names), `tables` (table information), `columns` (column details)

mysql database:

- System database storing database users and their privilege information
- Critical for MySQL server operation
- Controls user accounts, permissions, and configurations
- Contains the `user` table with user accounts and global privileges

D. Give a command to launch a dictionary attack on a Web form having username and password field that uses POST method. [2]

```bash
hydra -L usernames.txt -P passwords.txt target.com http-post-form "/login.php:username=^USER^&password=
```

E. Give a single line description of docker image, docker container, DockerHub and Dockerfile. [2]

- **Docker Image:** A blueprint/template containing everything needed to build a docker container including code, tools, and runtime

- **Docker Container:** A runnable instance of a docker image; a lightweight, portable mini-computer running the image
- **DockerHub:** Default public registry for storing and distributing docker images (like GitHub for code)
- **Dockerfile:** Text file with instructions telling Docker how to build an image (base image, dependencies, configurations)