Task 1: Understanding OWASP Top Ten

Objective: To understand the most critical security risks outlined by OWASP.

Steps:

1. Visit the OWASP website and read about the OWASP Top Ten vulnerabilities.
2. Identify the top 3 risks and write a brief explanation of each.
3. Research examples of each risk in real-world applications.

Question: What are the top 3 most critical web security risks according to OWASP?

Task 2: SSL/TLS Basics

Objective: To understand SSL and its successor TLS, and how they secure web communications.

Steps:

1. Research the differences between SSL and TLS.
2. Learn how SSL/TLS works during a secure handshake.
3. Examine a website's SSL certificate by clicking on the padlock icon in the browser.

Question: What is the main difference between SSL and TLS, and why is TLS preferred today?

Task 3: Authentication vs Authorization

Objective: To distinguish between authentication and authorization.

Steps:

1. Define authentication and authorization in your own words.
2. Create an example scenario where authentication and authorization are required.
3. Research how both processes work in a typical web application.

Question: In a web application, if a user can log in but cannot access certain resources, which part of security (authentication or authorization) is responsible?

Task 4: Cookie-Based Authentication

Objective: To understand how cookie-based authentication works.

Steps:

1. Read about how cookies are used for user sessions in web applications.
2. Use developer tools in a browser to view cookies when logged into a website.
3. Examine the properties of the session cookie (e.g., domain, expiration).

Question: How do session cookies help maintain user authentication across multiple pages of a website?

Task 5: Token-Based Authentication

Objective: To learn how token-based authentication (JWT) works.

Steps:

1. Research how JSON Web Tokens (JWT) are used in authentication.
2. Generate a simple JWT token using an online tool.
3. Explore how tokens are transmitted in API requests.

Question: What are the benefits of using token-based authentication over cookie-based authentication?

Task 6: Network Security Groups (NSGs)

Objective: To learn how Network Security Groups (NSGs) work in cloud environments.

Steps:

1. Learn about NSGs and how they filter traffic in cloud services like Azure or AWS.
2. Create a simple NSG rule in a cloud platform.
3. Test connectivity to a cloud resource by modifying NSG rules.

Question: How do Network Security Groups help secure cloud resources?

Task 7: Web Application Firewall (WAF)

Objective: To understand the function of a Web Application Firewall (WAF).

Steps:

1. Research what a WAF is and how it protects web applications.
2. Check if your web hosting service includes a WAF.
3. Test the protection provided by a WAF against common attacks like SQL injection.

Question: How does a WAF differ from a traditional network firewall in terms of its security focus?

Task 8: Encryption of Data

Objective: To understand how encryption works to protect data.

Steps:

1. Learn the difference between symmetric and asymmetric encryption.
2. Research how encryption is used in data protection, both in transit and at rest.
3. Test encryption using a tool like OpenSSL or similar.

Question: Why is it important to encrypt both data at rest and data in transit?

Task 9: Identity and Access Management (IAM)

Objective: To understand the role of IAM in securing cloud resources.

Steps:

1. Research IAM concepts like roles, permissions, and access policies.
2. Create a sample IAM policy that allows access to a cloud resource for a specific role.
3. Test how IAM controls user access and permissions within a cloud platform.

Question: What is the principle of least privilege, and why is it important in IAM?

Task 10: Vulnerability Testing with OWASP ZAP

Objective: To perform vulnerability testing on a website using OWASP ZAP.

Steps:

1. Install OWASP ZAP and set it up for scanning.

2. Run a scan on a publicly available test site (e.g., OWASP Juice Shop).
3. Review the scan results and identify any critical vulnerabilities.

Question: What types of vulnerabilities can OWASP ZAP detect, and how can it help improve website security?