Ethical Hacking Report: Website Penetration Test (sanitized version)

1. Executive Summary

This report analyses an ethical hacking test done on a site that is about travel industry. The analysis provided a number of results of different levels of criticality, such as XSS and Information type of findings about server settings. No critical weaknesses were found but the issues that were found can become a security threat to the website and its content. This report presents the results of the testing procedure to be conducted on the particular website as well as the detailed description of the typical results along with suggestions on their elimination

2. Scope and Objectives

Scope:

This ethical hacking assessment focuses on the whole website that belongs to [Web Owner's name], found at [Target URL]. The scope includes all the parts of the website that can be accessed and found. This assessment was conducted with the approval and cooperation of the web-owner.

Objectives:

- Conduct vulnerability assessment of the whole site
- Evaluate all the visible and potentially available web pages and features in terms of security
- identify and document all the vulnerabilities throughout the website
- Assess the current state of security of the web application
- Provide a detailed report of all findings, including descriptions, potential impacts, and remediation recommendations
- Ensure that all testing is done ethically avoiding any activity that might harm or interfere with the normal functioning of the website.

3. Methodology

When performing this penetration test, we adopted a step-by-step procedure as a way of making sure that we postulated a competent analysis of the security of the target website. Our methodology consisted of the following phases:

1. **Reconnaissance**: Some of the information collected on the target website include: domain, the website registration information, and IP address all obtained by using Nmap, Whois and nslookup..
2. **Scanning and Enumeration**: It is essential to know the open ports and the services running on them of the target website for which we used Nmap to scan it through a port scan and a service scan.

3. **Vulnerability Analysis**: In this case the scans involved the use of Nessus and OWASP ZAP in order to determine the extent of possible security vulnerabilities in the system and their criticality..
4. **Exploitation Attempts**: We tried to take advantage of the previously recognized flaws with the help of sqlmap and our scripts. It was done systematically so that there would be no compromise to the system in place.
5. **Specific Testing of the Login Page**: specific tests were done on the login function with specific tests made such as SQL Injection and Cross Site Scripting tests..
6. **Reporting**: We documented all findings, including vulnerabilities, their potential impact, and recommendations for remediation.

4. Findings and Vulnerabilities

In this Penetration test, we have noticed that there are some Security risks at Different levels of high, Medium and Low. Here are our key findings:

4.1 Cross-Site Scripting (XSS) in Registration Form

- **Severity**: High
- **Description**: The website's registration form was found to be vulnerable to stored XSS.
- **Potential Impact**: Attackers could potentially steal user sessions, deface the website, or redirect users to malicious sites.

4.2 Missing Security Headers

- **Severity**: Medium
- **Description**: Several important security headers were found to be missing, including Content Security Policy (CSP), X-Frame-Options, Strict-Transport-Security, and X-Content-Type-Options.
- **Potential Impact**: This could make the website more vulnerable to various attacks, including clickjacking and man-in-the-middle attacks.

4.3 Open Ports

- **Severity**: Low
- **Description**: The scan detected several open ports, including common web service ports.
- **Potential Impact**: While not inherently vulnerable, open ports increase the attack surface and should be reviewed for necessity.

4.4 Cloud Metadata Potentially Exposed

- **Severity**: High
- **Description**: OWASP ZAP identified a high-priority issue related to potentially exposed cloud metadata.
- **Potential Impact**: This could lead to unauthorized access to sensitive cloud configuration information.

4.5 Web Server Detection

- **Severity**: Informational
- **Description**: The scan detected a web server running on the host, but the version could not be determined.
- **Potential Impact**: Knowing the web server software can help attackers target specific vulnerabilities, though the impact is minimal without version information.

5. Step-by-Step Ethical Hacking Process

5.1 Reconnaissance and Initial Scanning

- Used Whois to gather domain registration information
- Used nslookup to retrieve DNS information and IP address for the target domain
- Performed basic Nmap scan to identify open ports and services

5.2 Scanning and Enumeration

- Conducted comprehensive Nmap scan to identify all open ports and services
- Performed Nmap vulnerability scanning using built-in scripts

5.3 Detailed Vulnerability Analysis

- Used OWASP ZAP to identify web application vulnerabilities
- Conducted a Nessus scan for comprehensive vulnerability assessment

5.4 Specific Vulnerability Testing

- Performed SQL injection testing using sqlmap
- Conducted manual XSS testing on input fields

6. Recommendations

1. **Implement Input Validation and Output Encoding**:
    - Properly sanitize all user inputs, especially in the registration form.
    - Implement robust server-side input validation.
    - Use appropriate output encoding when rendering user-supplied data.
2. **Implement Security Headers**:
    - Add Content Security Policy (CSP) headers to prevent XSS and other injection attacks.
    - Implement X-Frame-Options header to prevent clickjacking attacks.
    - Add a Strict-Transport-Security header to enforce HTTPS connections.
3. **Review Open Ports**:
    - Audit all open ports and close any that are not necessary for the website's operation.
    - Implement proper firewall rules to restrict access to required ports only.
4. **Enhance Authentication Mechanism**:
    - Implement multi-factor authentication for added security.

    - Enforce strong password policies.
5. **Update Web Server Software**:
    - Ensure the web server is updated to the latest stable version.
    - Implement a regular patching schedule to keep all software up-to-date.

7. Conclusion

The assessment was conducted under ethical hacking principles and different vulnerabilities were identified that need attention. Although no exploitable, critical vulnerabilities were found, the Cross-site scripting (XSS) vulnerability and several misconfigurations may pose threats to the website's users and the website generally.

The most critical issue is the Security vulnerability of Cross-Site Scripting (XSS) for the registration form which has the potential to perform various actions. Furthermore, the site security is not as strong as it should be because these important security headers are missing:

Through the method explained above, the given recommendation can enhance the security of this website regarding input validation, security headers, and the up-to-date software used. Security assessments should be conducted in the course of safeguarding against new threats so as to serve as check-ups.