VAPT Assessment Overview

For ABC Global

Executive Summary

The Vulnerability Assessment and Penetration Testing (VAPT) conducted by Zelarsoft for ABC Global aimed to evaluate the security posture of the target application hosted in the UAT environment. The primary objectives of this assessment were to identify and assess vulnerabilities within the application, validate the potential for exploitation, and provide actionable recommendations for remediation.

The assessment methodology employed a combination of automated tools and manual testing techniques. Automated tools, such as Burp Suite and OWASP ZAP, were utilized to conduct thorough scans for common vulnerabilities, while manual testing focused on more complex issues such as SQL injection, cross-site scripting (XSS), and logic flaws. The assessment also included a review of configurations, such as SSL/TLS settings and HTTP headers, to ensure compliance with industry standards.

Key findings from the assessment revealed a mix of high, medium, and informational-level vulnerabilities. Notably, issues included the absence of the X-Frame-Options and Strict-Transport-Security (HSTS) headers, which posed significant risks of clickjacking and downgrade attacks, respectively. Other notable vulnerabilities included outdated JavaScript libraries that could potentially be exploited for XSS attacks and missing security headers that could expose the application to various threats.

The risk distribution analysis indicated that critical vulnerabilities could lead to unauthorized access, data leakage, and potential reputational damage for ABC Global. The exploitation of these vulnerabilities could have severe business impacts, emphasizing the need for immediate remediation efforts. Overall, while the assessment identified several weaknesses, it also highlighted areas where the security posture was strong, demonstrating the potential for improvement through targeted actions and adherence to security best practices.

Methodology and Scope

The Vulnerability Assessment and Penetration Testing (VAPT) engagement for ABC Global followed a structured methodology that combined both automated and manual testing techniques. This dual approach ensured comprehensive coverage of potential vulnerabilities across the application and its supporting infrastructure.

For automated testing, industry-standard tools such as OWASP ZAP and Burp Suite were employed. These tools efficiently scanned the target application for common vulnerabilities, including SQL injection, cross-site scripting (XSS), and security misconfigurations. The automated scans provided a baseline of vulnerabilities that required further investigation. In

addition to automated tools, manual testing techniques were implemented to identify complex vulnerabilities that automated tools might overlook. This included testing for logic flaws, custom application vulnerabilities, and thoroughly reviewing the business logic of critical workflows.

The scope of the assessment encompassed a detailed examination of the target application hosted at https://*****.*****.com/ within the User Acceptance Testing (UAT) environment. The assessment included various components essential to the application's security posture, such as the web application server, underlying network infrastructure, and supporting services like DNS and SMTP. The evaluation focused on key application entry points, including user login interfaces, administrative portals, and exposed APIs.

In addition to the application itself, the assessment also covered configuration reviews of critical components, including SSL/TLS settings and HTTP headers. This ensured that the application adhered to best practices for security and compliance with industry standards. By defining a clear scope and employing a robust methodology, the assessment aimed to deliver actionable insights for improving the overall security posture of ABC Global.

Summary of Findings

The Vulnerability Assessment and Penetration Testing (VAPT) for the Application Under Test hosted in the ABC Global UAT environment revealed a total of 174 identified vulnerabilities categorized by severity levels. The breakdown of these vulnerabilities is as follows:

High Severity

- **Count:** 4
- **Vulnerabilities:**
  - Missing Strict-Transport-Security (HSTS) Header
  - Missing X-Frame-Options Header
- **Overview:** These vulnerabilities pose significant risks, including exposure to clickjacking and downgrade attacks, which could lead to unauthorized access and data breaches.

Medium Severity

- **Count:** 39
- **Vulnerabilities:**
  - Cookie without Secure Flag
  - Missing X-Content-Type-Options Header
  - BREACH Attack Potential
  - Multiple instances related to HTTP security headers
- **Overview:** This category includes various issues that could facilitate session hijacking and cross-site scripting (XSS) attacks. The prevalence of missing security headers indicates a common pattern across the assessed application.

Low Severity

- **Count:** 91
- **Vulnerabilities:**
  - Application Error Disclosure
  - Timestamp Disclosure
  - Cookie without SameSite Attribute
  - Uncommon Headers
- **Overview:** While this category comprises vulnerabilities that are less critical, they still present potential information leakage and misuse risks. The high number of findings suggests areas for security enhancements that could improve overall security hygiene.

Informational

- **Count:** 42
- **Vulnerabilities:**
  - Authentication Request Identified
  - Information Disclosure - Suspicious Comments
  - Modern Web Application Best Practices
- **Overview:** These findings provide valuable insights into potential security improvements and best practices, although they do not directly indicate vulnerabilities.

Patterns and Common Vulnerabilities

The results highlight recurrent issues, particularly the absence of critical HTTP security headers, which are vital for protecting against various attack vectors. The presence of outdated JavaScript libraries was also noted, suggesting a need for regular updates to third-party components. Addressing these vulnerabilities systematically will be crucial in enhancing the security posture of ABC Global and mitigating the associated risks.

Detailed Vulnerability Analysis

1. Missing Strict-Transport-Security (HSTS) Header

- **Risk Level:** High
- **Evidence:** The absence of the Strict-Transport-Security header in HTTP responses was verified by automated scanning tools.
- **Potential Business Impact:** Without HSTS, browsers may default to HTTP, exposing sensitive data to downgrade attacks and man-in-the-middle (MITM) scenarios.
- **Area Affected:** All endpoints of the application.
- **Exploitation:** Attackers can intercept unencrypted traffic, manipulate data, and potentially gain unauthorized access to user sessions. This could lead to significant data breaches, damaging ABC Global's reputation and trustworthiness.

2. Missing X-Frame-Options Header

- **Risk Level:** High
- **Evidence:** Automated scanning revealed that the X-Frame-Options header was absent in responses, as confirmed by the HTTP response headers.
- **Potential Business Impact:** The application is vulnerable to clickjacking attacks, where malicious actors can embed the application in a frame to trick users into performing unintended actions.
- **Area Affected:** User interface components accessible via the browser.
- **Exploitation:** By exploiting this vulnerability, an attacker could create a deceptive interface leading users to perform actions like approving transactions or revealing sensitive information without their consent.

3. Cookie Without Secure Flag

- **Risk Level:** Medium
- **Evidence:** Analysis of HTTP traffic showed cookies transmitted over unencrypted channels, lacking the Secure attribute.
- **Potential Business Impact:** This vulnerability increases the risk of session hijacking, allowing attackers to steal session cookies and impersonate legitimate users.
- **Area Affected:** All session-related cookies.
- **Exploitation:** If cookies are transmitted over HTTP, an attacker can intercept them and gain unauthorized access to user accounts, potentially leading to data theft or unauthorized transactions.

4. Missing X-Content-Type-Options Header

- **Risk Level:** Medium
- **Evidence:** The server response headers lacked the X-Content-Type-Options header.
- **Potential Business Impact:** Browsers may misinterpret MIME types, leading to cross-site scripting (XSS) attacks.
- **Area Affected:** All application endpoints serving content.
- **Exploitation:** If an attacker can manipulate content types, they may inject malicious scripts that execute in the user's browser, compromising user data and application integrity.

5. BREACH Attack Potential

- **Risk Level:** Medium
- **Evidence:** The application was found to allow HTTP compression, which can be exploited under specific conditions.
- **Potential Business Impact:** Sensitive data, such as session tokens, may be recovered, exposing users to account takeover risks.
- **Area Affected:** Sensitive data transmitted over HTTP.

- **Exploitation:** By carefully crafting requests and analyzing the responses, attackers can exploit compression to infer sensitive data, leading to potential breaches.

6. Outdated JavaScript Libraries

- **Risk Level:** High
- **Evidence:** Scanning revealed vulnerabilities in libraries like jQuery (CVE-2015-9251) and Bootstrap (CVE-2019-8331).
- **Potential Business Impact:** Exploitable vulnerabilities in these libraries could allow attackers to execute scripts within the context of the application, leading to data theft or account compromise.
- **Area Affected:** Client-side scripts.
- **Exploitation:** Attackers can exploit these vulnerabilities to inject malicious scripts, leading to unauthorized access to user sessions and sensitive information.

Each of these vulnerabilities presents significant risks to the application's security posture and, by extension, to ABC Global's operational integrity and reputation. Immediate remediation efforts are imperative to mitigate these risks effectively.

Recommendations for Remediation

To address the identified vulnerabilities within the application hosted for ABC Global, the following actionable remediation steps are recommended. These include both short-term fixes for immediate risk reduction and longer-term strategies to ensure ongoing security.

Short-Term Fixes

- **Implement Strict-Transport-Security (HSTS) Header**
  - **Action:** Configure the webserver to include the following header in all HTTP responses:
  - Strict-Transport-Security: max-age=31536000 includeSubDomains; preload
  - **Impact:** This will enforce HTTPS connections and protect against downgrade attacks.
- **Add X-Frame-Options Header**
  - **Action:** Update the server configuration to include:
  - X-Frame-Options: DENY
  - **Impact:** This will prevent clickjacking attacks by disallowing the application from being framed.
- **Secure Cookie Configuration**
  - **Action:** Modify the cookie settings in the application to include the Secure attribute:

  - Set-Cookie: sessionId=abc123; Secure; HttpOnly
  - **Impact:** This ensures cookies are transmitted only over HTTPS, reducing the risk of session hijacking.
- **Implement X-Content-Type-Options Header**
  - **Action:** Configure the server to send the following header:
  - X-Content-Type-Options: nosniff
  - **Impact:** This prevents browsers from MIME type sniffing, reducing the risk of XSS vulnerabilities.
- **Disable HTTP Compression for Sensitive Data**
  - **Action:** Review server settings to disable compression for endpoints that serve sensitive information.
  - **Impact:** This mitigates the BREACH attack potential by preventing attackers from inferring sensitive data.

Long-Term Strategies

- **Regularly Update Libraries and Frameworks**
  - **Action:** Establish a schedule for reviewing and updating third-party libraries to their latest secure versions, especially for jQuery and Bootstrap.
  - **Impact:** Keeping libraries up to date reduces the risk of exploitation through known vulnerabilities.
- **Implement Content Security Policy (CSP)**
  - **Action:** Develop and enforce a comprehensive CSP to control which resources can be loaded by the application:
  - Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; object-src 'none';
  - **Impact:** A robust CSP helps prevent XSS and data injection attacks by restricting resource loading.
- **Conduct Regular Security Assessments**
  - **Action:** Schedule periodic VAPT assessments and code reviews to identify and address new vulnerabilities proactively.
  - **Impact:** Ongoing assessments ensure vulnerabilities are discovered and mitigated before they can be exploited.
- **Implement Secure Coding Practices**
  - **Action:** Train development teams on secure coding practices, including input validation, output encoding, and proper error handling.
  - **Impact:** Building security into the development lifecycle minimizes vulnerabilities from the outset.
- **Monitor and Log Security Events**

  - **Action:** Implement logging and monitoring for security-related events to detect and respond to potential threats.
  - **Impact:** Active monitoring can help identify suspicious activities and facilitate timely responses to incidents.

By addressing these vulnerabilities through immediate actions and strategic improvements, ABC Global can significantly enhance its security posture and mitigate risks associated with potential exploitation.

Approval and Action Plan

To effectively implement the recommended remediation steps from the Vulnerability Assessment and Penetration Testing (VAPT) conducted for ABC Global, a structured approval process is essential. This process will ensure that all stakeholders are informed and aligned with the proposed actions. Below is a detailed outline of the levels of approval required, along with timelines for remediation actions and retesting phases.

Levels of Approval

- **Initial Review by Development Team**
  - **Responsibility:** The development team will review the findings and recommendations, assessing the feasibility of the proposed changes.
  - **Timeline:** 1 week from the date of distribution of the report.
- **Security Team Assessment**
  - **Responsibility:** The security team will analyze the proposed remediation steps to ensure they align with security protocols and best practices.
  - **Timeline:** 1 week following the development team's review.
- **Approval from IT Management**
  - **Responsibility:** IT management must approve the remediation plan, including resource allocation and timelines.
  - **Timeline:** 1 week after the security team's assessment.
- **Stakeholder Communication**
  - **Responsibility:** Communicate the approved remediation plan to all relevant stakeholders, including project managers and executives.
  - **Timeline:** 3 days after IT management approval.
- **Implementation by Development Team**
  - **Responsibility:** The development team will execute the remediation steps as per the approved plan.
  - **Timeline:** 4 weeks for implementation, depending on the complexity of the fixes.
- **Retesting by Security Team**

  - **Responsibility:** After implementation, the security team will conduct a retesting phase to validate the effectiveness of the remediation actions.
  - **Timeline:** 2 weeks following completion of implementation.
- **Final Review and Reporting**
  - **Responsibility:** A final report will be generated to document the outcomes of the remediation efforts and any remaining vulnerabilities.
  - **Timeline:** 1 week after retesting completion.

Timelines Overview

Action	Timeline
Initial Review by Development Team	1 week
Security Team Assessment	1 week after initial review
Approval from IT Management	1 week after security assessment
Stakeholder Communication	3 days after IT approval
Implementation by Development Team	4 weeks
Retesting by Security Team	2 weeks after implementation
Final Review and Reporting	1 week after retesting

Best Practices Alignment

This action plan aligns with best practices for cybersecurity governance by ensuring a clear approval hierarchy, timely execution of remediation actions, and thorough validation through retesting. By adhering to this structured approach, ABC Global can effectively mitigate risks associated with the identified vulnerabilities and enhance its overall security posture.

Compliance Considerations

In the context of the identified vulnerabilities from the Vulnerability Assessment and Penetration Testing (VAPT) conducted for ABC Global, it is crucial to examine how these issues relate to established industry standards and regulatory requirements, such as the OWASP Top Ten, ISO 27001, and PCI DSS. Each of these frameworks provides guidelines that align closely with the vulnerabilities identified, emphasizing the importance of secure coding practices, data protection, and risk management.

OWASP Top Ten

The OWASP Top Ten is a widely recognized framework that outlines the most critical security risks facing web applications. Many of the vulnerabilities discovered during the VAPT, such as the absence of the X-Frame-Options header and the lack of a Strict-Transport-Security (HSTS) header, directly correlate with OWASP's recommendations. Specifically, the risks of clickjacking and session hijacking underscore the need for compliance with these guidelines.

ABC Global should prioritize implementing security headers to mitigate these vulnerabilities and align with OWASP's best practices to enhance application security.

ISO 27001

ISO 27001 is an international standard that provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The identified vulnerabilities, particularly those concerning data transmission (e.g., cookies without the Secure flag), pose risks to data integrity and confidentiality. To comply with ISO 27001, ABC Global must undertake risk assessments to identify and address these vulnerabilities. Implementing robust encryption for data in transit, coupled with continuous monitoring and improvement of security policies, will be essential steps toward achieving compliance with this standard.

PCI DSS

For organizations handling payment card information, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is mandatory. The vulnerabilities related to session management, such as cookies lacking the Secure and SameSite attributes, could jeopardize cardholder data security. To align with PCI DSS requirements, ABC Global must ensure that all sensitive data is encrypted during transmission and that appropriate access controls are in place to prevent unauthorized access. Regular vulnerability assessments and timely remediation of identified issues will further support compliance with PCI DSS.

Compliance Actions

To strengthen its risk management strategy and ensure compliance with relevant standards, ABC Global should consider the following actions:

- **Implement Security Headers**: Establish and enforce critical HTTP security headers, including X-Frame-Options, Strict-Transport-Security, and X-Content-Type-Options, to mitigate common vulnerabilities associated with web applications.
- **Conduct Regular Security Training**: Provide ongoing training for developers and staff on secure coding practices and the importance of adhering to compliance standards, such as OWASP and PCI DSS.
- **Perform Routine Vulnerability Assessments**: Schedule regular vulnerability assessments and penetration testing to identify new vulnerabilities and ensure the effectiveness of implemented security measures.
- **Maintain Documentation**: Document all security policies, procedures, and compliance measures to demonstrate adherence to industry standards during audits and assessments.
- **Engage Stakeholders**: Collaborate with relevant stakeholders, including IT management and compliance officers, to ensure that security measures align with organizational goals and regulatory requirements.

By taking these proactive compliance actions, ABC Global can effectively mitigate identified vulnerabilities, align with industry standards, and enhance its overall risk management strategy.

Next Steps and Follow-up Actions

Following the completion of the Vulnerability Assessment and Penetration Testing (VAPT) for ABC Global, it is essential to establish a clear roadmap for remediation and ongoing security enhancement. The following steps outline the recommended actions, timelines, and additional security practices aimed at fortifying the organization's security posture.

Immediate Remediation Actions

- **Address Critical Vulnerabilities**: Prioritize fixing high-severity vulnerabilities such as the missing Strict-Transport-Security (HSTS) and X-Frame-Options headers. This should be completed within the first two weeks following the assessment.

- **Patch Outdated Libraries**: Immediate updates should be made to outdated JavaScript libraries identified during the assessment, ensuring the latest secure versions are implemented within three weeks.

- **Implement Security Headers**: Configure the server to include necessary security headers such as X-Content-Type-Options, and ensure cookies are set with the Secure and SameSite attributes. This should be done within four weeks.

Retesting and Validation

- **Follow-Up Assessment**: Schedule a retest of the application to validate remediation efforts two weeks after the completion of the initial remediation actions. This ensures that vulnerabilities have been effectively mitigated.

Long-Term Security Initiatives

- **Regular Security Audits**: Establish a routine schedule for vulnerability assessments and penetration testing, ideally on a quarterly basis, to identify and address new vulnerabilities proactively.

- **Employee Security Training**: Implement ongoing security awareness programs for all employees, focusing on best practices, phishing prevention, and secure coding practices. Initial training should commence within one month and continue bi-quarterly

- **Monitoring and Incident Response Plan**: Develop and maintain a comprehensive security monitoring program to detect and respond to potential threats in real-time. This should be established within three months, with regular updates as new threats emerge.

- **Security Policy Review**: Conduct a quarterly review of the security policies and procedures to ensure they align with the current best practices and compliance requirements.

By following these steps and implementing additional security initiatives, ABC Global can enhance its long-term security resilience, effectively mitigate risks, and safeguard critical assets against emerging threats.