Executive Summary

PURPOSE

This executive summary presents the main findings and recommendations from the Web Application Penetration Test conducted on the target application. The objective was to evaluate the application's security posture, identify vulnerabilities, and determine overall risk exposure.

SCOPE

- Target Application: **Sample Web Application**
- Testing Period: **[Start Date] – [End Date]**
- Assessment Type: **Black-box / Grey-box**
- Main Components: **Web interface, APIs**

KEY FINDINGS

Risk Level	Number of Findings	Examples
Critical	1	SQL Injection vulnerability in login module
High	2	Insecure Direct Object Reference, Cross-Site Scripting (XSS)
Medium	3	Exposed server version, weak session management
Low	4	Information disclosure, verbose error messages

RECOMMENDATIONS

- Address critical and high risk issues as a priority.
- Implement secure coding practices and input validation.
- Perform regular security testing after updates.
- Educate developers and administrators on current threats.

CONCLUSION

The penetration test revealed several security gaps that may impact the confidentiality, integrity, and availability of the application and its data. Management is strongly advised to remediate findings according to their respective risks and continually monitor the security of the web application environment.