Weak Cryptography Testing

1. Introduction

Weak cryptography testing focuses on identifying vulnerabilities related to the use of weak or outdated cryptographic algorithms, protocols, and key management practices. The use of weak cryptography can expose sensitive data to decryption, and can also allow an attacker to impersonate legitimate users or servers. This testing category covers the use of weak SSL/TLS ciphers, padding oracle vulnerabilities, and the transmission of sensitive information over unencrypted channels.

2. CVSS Score Summary

Test Case	Vulnerability	CVSS v3.1 Score	CVSS Vector	Severity
OTG-CRYPST-001	Weak SSL/TLS Ciphers	7.5	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	High
OTG-CRYPST-002	Testing for Padding Oracle	0.0	N/A	Informational
OTG-CRYPST-003	Sensitive Information Sent via Unencrypted Channels	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	Critical

3. Summary of Findings

The most significant finding in this category is the transmission of sensitive information over unencrypted channels. The application uses HTTP for all communication, which means that all data, including login credentials, is sent in cleartext. This could allow an attacker with a privileged network position to intercept and steal sensitive information. Additionally, the server supports weak TLS ciphers, which could allow an attacker to decrypt encrypted traffic.

The test for padding oracle vulnerabilities did not reveal any weaknesses. However, the use of unencrypted channels for all communication is a critical vulnerability that should be addressed immediately. The application should be configured to use HTTPS for all communication, and the server should be configured to use strong TLS ciphers.